Anne-Maria Ernvall-Hytönen | Matti Jutila
Juhani Karhumäki | Arto Lepistö (Eds.)

Proceedings of Conference on Algorithmic Number Theory 2007

Turku Centre *for* Computer Science

TUCS General Publication
No 46, December 2007

Proceedings of Conference on Algorithmic Number Theory 2007

Editors:

Anne-Maria Ernvall-Hytönen

Matti Jutila

Juhani Karhumäki

Arto Lepistö

TUCS General Publication
No 46, December 2007

Proceedings of Conference on Algorithmic Number Theory 2007

Preface

During the academic year 2006/2007, an international visitor program was organized by the Department of Mathematics and its research center FUNDIM (Fundamentals of Computing and Discrete Mathematics) at the University of Turku. The scientific program of the year consisted of several visits by various researchers, most of whom are leaders in their own fields, as well as several conferences and workshops. One of the conferences was the Conference on Algorithmic Number Theory, held in Turku, May 8-11, 2007.

The program of the conference was in two parts: The first part was a short course with lectures by Professors Henry Cohen, Alf van der Poorten and Nitin Saxena. The second part was the actual conference itself, with ten invited speakers and ten contributed talks. Among the invited speakers were several internationally acknowledged researchers, including Yuri Matiyasevich, in addition to the already mentioned three speakers. Final versions of the submissions corresponding to the presentations are collected in this book.

The speakers were invited, papers reviewed and the final program decided by the local program committee led by Professor Matti Jutila and PhD Tapani Matalaaho, with help from Professor H.W. Lenstra among others.

The organizing committee was led by Professor Juhani Karhumäki, and consisted of the following members of the staff at the University of Turku: Professor Matti Jutila, Anne-Maria Ernvall-Hytönen, Tuomas Hakkarainen, Petri Salmela, Eeva Suvitie and Roope Vehkalahti. The assistance of the project secretary Elisa Mikkola is gratefully acknowledged.

There are several organizations which provided financial support. The organizers would like to thank the Academy of Finland, the Finnish Cultural Foundation, the Mathematics Foundation at the Finnish Academy of Sciences and the Väisälä Foundation for making the conference possible, and TUCS (Turku Center for Computer Science) for covering the cost of printing the proceedings.

Turku, December 21, 2007

Anne-Maria Ernvall-Hytönen, Matti Jutila,
Juhani Karhumäki and Arto Lepistö

Contents

Sums over Primes

Eric Bach

Computer Sciences Department
University of Wisconsin
Madison, WI 53706

Abstract

This is an expository paper about the problem of finding concrete numerical information for sums of the form $\sum_{p \le x} f(p)$, in which the index is prime. This is in contrast to traditional analytic number theory, which traffics in asymptotics and growth rate estimates. Roughly speaking, we discuss three types of results: theorems giving bounds on the sum valid in an interval, easy to compute analytic estimates for the sum at a given x (which typically assume the Riemann hypothesis), and combinatorial algorithms that can attain very high precision unconditionally, but at exponential cost. We also discuss some related algorithmic problems, such as finding the point at which a prime sum attains a given value, and generating random primes with specified distributions.

An invited talk based on this material was given at the Conference on Algorithmic Number Theory (ANT 2007), Turku, May 10, 2007.

1 Introduction.

We often confront questions about the average, or typical, behavior of the prime numbers. One way to answer them is to study sums in which the index is restricted to be prime. More precisely, we can choose a function f and let

$$S(x) = \sum_{p \le x} f(p). \tag{1}$$

The best known example of this has $f = 1$, which gives

$$\pi(x) = \sum_{p \le x} 1, \tag{2}$$

the prime counting function. It is often preferable, however, to consider a weighted sum such as

$$\theta(x) = \sum_{p \le x} \log p. \tag{3}$$

One justification for the logarithms is that the density of primes near p is $1/(\log p)$, so that this will make the sum grow like x. Another one, closer to historical occurrence, is that the weights in (3) simplify the Laplace transforms by which the sum is studied.

In any case, there is need to understand the behavior of sums involving fairly general f. Of course, without restricting f somehow, the problem is hopeless, as the

sum of any sequence whatsoever has the form (1) with $f(p) = g(\pi(p))$. We will not attempt to codify such restrictions, beyond saying that any analytic manipulations we do will need f to be sufficiently smooth, and for some algorithms, the values of f must be related, for example by a multiplicative property.

On this basic theme, there are many variations. In the sum, one can include prime powers or other "nearly prime" numbers, with the hope of getting results that are simpler to derive but still informative. One can also twist the sums by complex numbers from the unit circle. For example, in problems involving arithmetic progressions, one can twist by roots of unity, and study sums like

$$\sum_{p \le x} \chi(p) f(p), \tag{4}$$

where χ is a Dirichlet character. Finally, one can take the "primes" from number rings, polynomial rings, or even geometric objects like curves and surfaces. All of these generalizations are embraced by the theory of schemes, as explained by Serre [48].

In this paper, we treat (1) as a computational problem. Viewed this way, its evaluation involves two parameters: the prime bound x, and the delivered precision ν. (That is, we require a result with relative error at most $2^{-\nu}$.) If we fix x, then, up to constant factors, the cost of evaluating (1) is the same as the cost of evaluating f, since there are only a fixed number of terms. On the other hand, if we fix ν, then for smooth enough f, an explicit form of the prime number theorem will eventually give us what we want. If we vary x and ν together, though, we have entered *terra incognita*. Although this paper presents methods that are useful for certain ranges of the parameters, we are far from understanding the complexity of (1) in full generality.

The main points can be summarized as follows. Due to the efforts of many researchers, there are fairly good concrete bounds available for the standard prime number sums like (2), and we explain some of the ideas which were used to get these bounds. Assuming the Riemann hypothesis, one can quickly get about half of the digits of a sum, provided that the corresponding integral is not to hard to evaluate. Unconditionally, the best methods for computing exact values of functions like (2) have time bounds given by powers of x, but with exponents much better than a brute force approach would suggest. We close the paper by showing how the estimation of prime number sums plays a role in the design and analysis of algorithms.

2 A Brief Look at Classic Prime Number Theory.

The early history of analytic number theory is admirably summarized by Landau [33, pp. 1-55], and more expansively by Edwards [19] so this section will just cover the highlights.

The first person to speculate openly in a quantitative way about prime densities was most likely Legendre. Around 1800, he said that $\pi(x)$ "probably" had a formula of the form $x/(A \log x + B)$. Gauss had come to similar conclusions somewhat earlier, but only wrote about them later. In particular, in 1849 he wrote a letter to Encke comparing prime counts to the logarithm integral (Cauchy principal value)

$$\mathrm{li}(x) = \int_0^x \frac{dt}{\log t}.$$

This is consistent with Legendre's assertion, in the sense that $x/(\log x - 1)$ matches the first two terms of the asymptotic series of $\mathrm{li}(x)$. Why did Gauss go public with his claim? Around this time, Chebyshev had rigorously proved that for large enough x,

$$0.921 \leq \frac{\pi(x)}{x/(\log x)} \leq 1.106, \tag{5}$$

so we can only guess that Gauss wanted to claim a piece of the action.

Ten years later, Riemann tied the growth rate of $\pi(x)$ to the complex roots of the zeta function

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s},$$

and suggested that

$$\pi(x) \approx \mathrm{li}(x) + \sum_{n \geq 2} \frac{\mu(n)}{n} \mathrm{li}(x^{1/n}). \tag{6}$$

His paper was followed by a half-century of attempts to prove the prime number theorem, which was finally done, independently by Hadamard and de la Vallée Poussin, around 1900.

Although (6) is strikingly accurate early on [39, p. 52; 12, p. 244], it ultimately must fail. This follows from work of Littlewood [35], who proved that $\pi(x) - \mathrm{li}(x)$ must change sign infinitely often. No one yet knows where the first sign change is, but from the work of Bays and Hudson [7] we know it must happen at the latest by 1.4×10^{316}.

All of Riemann's followers used (and still use) methods of complex analysis. It remained a problem to employ the "elementary" real-variable methods pioneered by Chebyshev to prove the prime number theorem, and this was finally done by Erdős and Selberg, around 1950. This was purely a triumph of technique, since any proof using complex analysis can be replaced, at least in principle, by one that avoids it.

Nevertheless, it is interesting to ask which approach, complex or real, is more useful in getting concrete information about prime sums. If moderate precision is needed, the evidence favors of complex methods, because one can exploit formulas that link prime sums to the roots of $\zeta(s)$. However, combinatorial methods based on sieves have proved effective in computing functions such as $\pi(x)$ for very large x.

3 Computations in Prime Number Theory.

Using formulas that were not revealed until the 1930's, Riemann had already computed the first few complex zeros of the zeta function. In particular, he found the first one to be at

$$1/2 + 14.1386... \, i \ .$$

Riemann kept this knowledge to himself, and so the first published numerical information about the roots appeared about 100 years ago. It derives from work of the Scandinavian mathematicians Gram, Lindelöf, and Backlund[1].

[1]Lindelöf is not usually mentioned as a zero hunter, but he did refine the Euler-Maclaurin formula for this purpose. He had bracketed the first ten zeroes when Gram's paper arrived in the mail. Backlund was Lindelöf's student; after a few early papers on number theory, he made his career as an actuary. See Efving [20].

Since then, longer and longer computations, by a number of researchers, have examined the complex roots of the zeta function. A history of this work, with references, appears on the web site of Gourdon and Sebah [22]. It is interesting that the zero counts over time, written in decimal, follow almost a straight line, from 15 in 1903 to $10,000,000,000,000$ in 2007. By analogy with Moore's famous prediction, we might expect future zero counts to double every 2.5 years, reflecting improvements both in algorithms and technology.

Remarkably, all of the known roots have real part $1/2$, as predicted by the Riemann hypothesis (RH). To date, the longest systematic check on this hypothesis is by Gourdon and Demichel [21], who showed that RH holds for the first 10^{13} zeroes, that is, up to height about 2×10^{12}. They also checked blocks of much higher zeroes, to validate random matrix models for the zero distribution.

Many authors, most famously Sylvester [50], also occupied themselves with improving the constants in Chebyshev's theorem. (For modern work along these lines, and a few more references, see [23].) Until the early 1940's, however, no one seems to have asked how large x must be for an approximation like (5) to be valid [42, p. 211]. By then, Titchmarsh had computed more than a thousand zeroes of $\zeta(s)$, and Rosser realized that this knowledge could be used to prove better Chebyshev-style theorems.

The natural approach to this problem would be to use an explicit formula like

$$\psi(x) := \sum_{p^k \le x} \log p = x - \sum_\rho \frac{x^\rho}{\rho} + \cdots , \tag{7}$$

in which ρ stands for a complex zero of the zeta function. However, the sum over these roots is not absolutely convergent, which makes its numerical employment dicey at best[2]. One does much better by averaging (7), as this causes the contributions from higher zeroes, about which we have the least knowledge, to decay more rapidly. By systematically exploiting this idea, Rosser proved many explicit estimates for functions of prime numbers. One elegant one, which became a paper title, is the following: If p_n denotes the n-th prime number, we have

$$p_n > n \log n.$$

Dusart has recently sharpened this, albeit with an increase in titular complexity [17].

The work of Rosser and his collaborators on this topic appears in many papers, spread over nearly four decades [3, 41, 42, 43, 44, 45, 47]. Each paper builds on and refers in detail to the previous ones, in a style that few would say invites casual reading. Therefore, it does not seem inappropriate to summarize the main ideas here. For this purpose it will suffice to discuss upper bounds for ψ.

Rosser did not use probabilistic language but we will find it convenient to do so. Choose a positive integer m, and let $y = \sum_{i=1}^m y_i$, with the y_i i.i.d. uniform on $[0, h]$. Then,

$$\psi(x) \le E[\psi(x+y)] = x + \frac{mh}{2} - E\left[\sum_\rho \frac{(x+y)^\rho}{\rho}\right] + \cdots . \tag{8}$$

If $\rho = \beta + i\gamma$, we have a trivial bound

$$E\left|\frac{(x+y)^\rho}{\rho}\right| \le \frac{x^\beta}{\gamma}(1 + \frac{E[y]}{x}) = \frac{x^\beta}{\gamma}(1 + \frac{mh}{2x}) = \frac{x^\beta}{\gamma}(1 + \frac{m\delta}{2}) \tag{9}$$

[2]One might say, echoing von Neumann's sentiment about random numbers, that anyone who uses numerical analysis to compute such a discontinuous function has gone over to the Dark Side.

Here we have put $h = \delta x$. On the other hand, we can integrate out the y_i's one by one and obtain

$$E\left[\frac{(x+y)^\rho}{\rho}\right] = \frac{1}{h^m}\int_{[0,h]^m} \frac{(x+y_1+\cdots+y_m)^\rho}{\rho}$$
$$= \frac{1}{h^m}\sum_{j=0}^{m}(-)^{m-j}\frac{(x+jh)^{\rho+m}}{\rho(\rho+1)\cdots(\rho+m)}\binom{m}{j}.$$

This leads to the more sophisticated bound [42, p. 222]

$$\left|E\left[\frac{(x+y)^\rho}{\rho}\right]\right| \le \frac{x^{\beta+m}}{\gamma^{m+1}}\frac{\left((1+h/x)^{m+1}+1\right)^m}{h^m} = \frac{x^\beta}{\gamma^{m+1}}\frac{((1+\delta)^{m+1}+1)^m}{\delta^m}. \quad (10)$$

We now have a collection of estimates that we can vary as needed, to get good bounds on ψ. To illustrate this idea, we will now follow Schoenfeld [47] and assume RH. His idea is to take $m = 1$, select a height T, and then use the trivial bound below T and the sophisticated bound above T.

Recall that $N(T)$, the number of complex zeroes with $0 < \gamma < T$, satisfies

$$N(T) = \frac{T}{2\pi}\log\left(\frac{T}{2\pi}\right) - \frac{T}{2\pi} + O(\log T)$$

[26, p. 69]. Integrating by parts, we can then prove

$$\sum_{|\gamma|<T}\frac{1}{|\gamma|} = 2\int_1^T \frac{dN(\gamma)}{\gamma} \sim \frac{1}{2\pi}\log^2\left(\frac{T}{2\pi}\right), \quad (11)$$

and

$$\sum_{|\gamma|\ge T}\frac{1}{\gamma^2} = 2\int_T^\infty \frac{dN(\gamma)}{\gamma^2} \sim \frac{1}{\pi}\left(\frac{\log(T/2\pi)+1}{T}\right). \quad (12)$$

We now split the sum in (8) at height T, and use (9)–(12) to estimate it. Displaying only the main terms that arise, the result is

$$\psi(x) \le x + \sqrt{x}\left[\frac{\delta\sqrt{x}}{2} + \frac{\log^2 T}{2\pi} + \frac{2}{\pi}\frac{\log T}{\delta T}\right] + \cdots. \quad (13)$$

Let B denote the expression in brackets. We note that the second and third terms in B come from low and high zeroes, respectively.

It remains to choose the parameters δ and T. Schoenfeld did not justify his choices, but we can derive them via an optimization process. Setting $\partial B/\partial\delta$ to 0, we get the relation

$$\delta^2 = \frac{4\log T}{\pi T\sqrt{x}}. \quad (14)$$

Also, for large T,

$$\frac{\partial B}{\partial T} \sim \frac{\log T}{\pi T} - \frac{2}{\pi\delta}\frac{\log T}{T^2}.$$

The right side of this vanishes when

$$\delta T = 2. \quad (15)$$

This relation is a kind of "uncertainty principle:" it it tells us we can either average ψ over a short interval or use a low break point T, but we should not do

both. Multiplying (14) by T^2 and using (15), we find $T \log T = \pi\sqrt{x}$, so we get Schoenfeld's parameters

$$\delta = \frac{\log x}{\pi\sqrt{x}}, \qquad T = \frac{2\pi\sqrt{x}}{\log x}.$$

Using these in (13), we get his estimate, in the form

$$\psi(x) \le x + \frac{\log^2 x}{8\pi}\sqrt{x} + \cdots .$$

By carefully bounding the error terms we have ignored here, Schoenfeld was able to prove results (on RH) like[3]

$$|\psi(x) - x| < \frac{1}{8\pi}\sqrt{x}\log^2 x, \qquad \text{for } x \ge 59. \tag{16}$$

This put an estimate of von Koch [30] into explicit form. It is not known if the constant $1/(8\pi)$, or even the form of the error term, is best possible.

All of Rosser's unconditional results relied on the determination of larger and larger zero-free regions for the zeta function. For bounds on $\psi(x)$, his first paper [41] based a universal result on one level of averaging ($m = 1$), going to the next level ($m = 2$) to get sharper results for limited ranges of x. By the next paper [42], he had computed a bound in which m appeared as a parameter, which could then be optimized depending on the range of x for which a theorem was desired. All the remaining papers refined and exploited this strategy, as did Rosser's successors.

Since there is a tradeoff between asymptotic quality and the point at which any bound takes effect, there is no best concrete estimate for any given prime sum. A good result, however, should leave the remaining cases within easy computational reach, and this is certainly true nowadays of Rosser and Schoenfeld's bound [45]

$$|\psi(x) - x| < 0.0242269\frac{x}{\log x}, \qquad \text{for } x \ge 10^8.$$

For some recent bounds of this type on the sums (2), (3), (7), and on the n-th prime number, see Dusart [16]. This also gives references to work on explicit bounds for other functions in prime number theory.

We close this section by briefly mentioning some corresponding work on sums over primes in arithmetic progressions. For a systematic investigation of the complex roots of Dirichlet L-functions, see Rumely [46]. Some explicit bounds on the analog of $\theta(x)$ for arithmetic progressions were computed by Dusart [18]. There has also been work on explicit bounds for sums twisted by additive characters [10].

4 Euler-Maclaurin Formulas and Prime Sums.

In discrete mathematics, we often want to estimate a sum, and this can be done by evaluating the corresponding integral. In numerical analysis, we have the opposite problem, namely, an integral that cannot be done conveniently or at all, which is approximated by a finite sum. In both cases, the bridge is the Euler-Maclaurin formula

$$\sum_{n=1}^{x} f(n) = \int_1^x f(t)dt + \frac{f(1) + f(x)}{2} + \cdots . \tag{17}$$

[3]He asserts $x \ge 73.2$, but some computations show that this is too conservative. His break points for $\theta(x)$ and $\mathrm{li}(x)$ seem to be correct.

(As a mnemonic for this, one can remember that the terms displayed above are equivalent to the trapezoid rule for integration.) The elided terms involve derivatives of f, and can be derived using integration by parts.

The classic number-theoretic application for this is in computing $\zeta(s)$ for complex values of s, by summing n^{-s} for $n \leq x$, and then using Euler-Maclaurin for the remainder. (See Edwards [19], Chapter 6.) Until Riemann's formulas became known, this was, in fact, the method by which all investigators evaluated the zeta function to find its roots.

One can now ask if there is any analog of the Euler-Maclaurin formula for sums over primes. Such a formula, or at least the first parts of it, appears in Landau [33, pp. 197-203]. Let us retrace his argument here.

Since the density of primes near n is about $1/(\log n)$, we should have

$$\sum_{p \leq x} f(p) \approx \sum_{n \leq x} \frac{f(n)}{\log n} \approx \int_2^x \frac{f(t)}{\log t} dt := F(x). \tag{18}$$

How might this be justified? The last approximation, of course, comes from (17), so we need to worry principally about the first one. Define the error ϵ by

$$\pi(t) = \mathrm{li}(t) + \epsilon(t).$$

Then, using integration by parts, we find

$$\sum_{p \leq x} f(p) = \int_2^x f(t) d\pi = \int_2^x f(t)\, d\,\mathrm{li} + \int_2^x f(t) d\epsilon = F(x) + [f\epsilon]_2^x - \int_2^x \epsilon\, df. \tag{19}$$

This shows that any bound on ϵ translates directly into a bound on the error in (18). (Incidentally, this gives another reason to prefer $\mathrm{li}(x)$ over the simpler-looking $x/(\log x)$: it already is an integral, so its derivative will be simpler.)

Traditionally, this is applied to produce equivalent asympotic forms of the prime number theorem. For example, we can use it to see that $\pi(x) \sim \mathrm{li}(x)$ holds iff $\theta(x) \sim x$ does.

Let us now leave asymptotics and ask a practical question. Suppose we use the approximation (18) for numerical work. How accurate will it be? A well-worn rule of thumb states that if RH holds, about 50 percent of the digits will be correct. (To be sure, this rule assumes that the prime bound x and the delivered precision ν are compatible, in the sense that $x2^{-\nu} \approx 1$.) For an example, picked more or less at random, consider

$$\sum_{p \leq 10^6} \sqrt{p} = 5.07766... \times 10^7 \qquad \text{vs.} \qquad \int_2^{10^6} \frac{t^{1/2}}{\log t} dt = 5.08492... \times 10^7.$$

Here we have nearly three figure accuracy, out of six displayed digits.

How can one justify the 50% rule? Asymptotically, we would expect oscillations in ϵ, so that, of the two error terms in (19), the first one should be dominant. If this is true, the relative error is given by

$$\frac{f(x)\epsilon(x)}{F(x)}. \tag{20}$$

Suppose that $f > 0$ and acts like a power of x, in the sense that $f'(x)/f(x) \sim a/x$. If $a > -1$, we have $F(x) \sim xf(x)/((a+1)\log x)$ so (20) can be replaced asymptotically by

$$\frac{(a+1)\log x}{x}\epsilon(x) = O(x^{-1/2}\log^2 x).$$

Here we have used [14, p. 81] (some stronger assumptions are needed for $a = 0$), and (16).

Let us now return to the question of whether the Euler-Maclaurin formula (17) extends to prime sums. As we will see, it does, but it also manifests the obstruction to estimating them accurately. For this reason, it is not as useful computationally as is the formula for sums over general n.

To see this, it will be convenient to allow prime powers, and consider

$$S' = \sum_{p^k \le x} \frac{f(p^k)}{k} = \int_2^x \frac{f(t)}{\log t} d\psi(t).$$

Let $g(t) = f(t)/(\log t)$, and define η by $\psi(t) = t + \eta$. If we substitute these into the integral, we can repeatedly integrate by parts to obtain a sequence of formulas, the k-th of which is

$$S' = F + gE_0|_2^x - g'E_1|_2^x + g''E_2|_2^x - \cdots + (-)^{k-1} E_{k-1} g^{(k-1)}|_2^x + (-)^k \int_2^x E_{k-1} g^{(k)} dt.$$

Here, $E_0 = \eta$, and $E_k = \int_0^x E_{k-1}(t)dt$ for $k \ge 1$. We have

$$E_k = -\sum_\rho \frac{t^{\rho+k}}{\rho(\rho+1)\cdots(\rho+k)} + \cdots,$$

and as remarked by Ingham [26, p. 75], if $k \ge 1$, the indicated sum is absolutely convergent. Thus, if g and its derivatives are not too wild (*ceteris parabis*, as the economists say), the bulk of the error will come from the E_0 term.

Granting this, we can see why simple analytic formulas like [18] cannot do better than the 50% rule indicates. Indeed, Littlewood proved that for any $\epsilon > 0$,

$$\eta = \psi(x) - x \ge (1/2 - \epsilon) x^{1/2} \log\log\log x$$

infinitely often. (See [26, p. 100].)

Another application of the Euler-Maclaurin approach is the idea that the errors in simple approximations like (18) will rise and fall together. For an interesting numerical investigation of this, see Rosser [44].

To put this all in perspective, let us now return to Legendre and Gauss's original problem of formulas for counting the primes. Assuming RH, we have

$$\pi(x) = \int_2^x \frac{dt}{\log t} + O(x^{1/2} \log x).$$

As we noted above, this is consistent with observed data. (When $x = 10^{10}$, we have $\pi(x) = 455052511$ whereas the integral is 455056613.54... .) The logarithm integral, however, cannot be computed in closed form, so we should ask how hard it is to estimate it accurately, say to the nearest integer. Unfortunately, the standard integration methods, such as Simpson's rule, do not run in polynomial time[4]. Rather than look for a better integration method, it is simpler in this case to use a series for the logarithm integral [1]:

$$\int_0^x \frac{dt}{\log t} = \gamma + \log\log x + \sum_{n \ge 1} \frac{(\log x)^n}{n n!}.$$

[4] A composite Simpson rule with step size h will have error proportional to h^4 [9, p. 321]. To get ν bits of our integral, as $\nu \to \infty$, we will need $x/h = \Theta(2^{\nu/4})$ sample points.

In this formula, $\gamma = 0.57721...$ is Euler's constant, which can be computed efficiently [28]. Furthermore, we can approximate logarithms in polynomial time, by a combination of Taylor series and argument reduction [8]. By Stirling's formula, the series terms decrease rapidly once $n/2 > e \log x$, so the effort to get $\mathrm{li}(x)$ to the nearest integer will be polynomial in $\log x$.

Unconditionally, it seems that there is no known polynomial-time algorithm that will compute a nonzero fraction of the digits of $\pi(x)$ correctly. Indeed, the sharpest known form of the prime number theorem has (for some $c > 0$),

$$\pi(x) - \mathrm{li}(x) = O(xe^{-c\lambda(x)}),$$

with $\lambda(x) = (\log x)^{3/5}(\log\log x)^{-1/5}$ [27]. There seems to be no explicit version of this bound, although there are such with a slightly smaller exponent of $\log x$, as follows from [47, Theorem 11]. It would also be an advance to compute more than half the digits correctly in polynomial time, assuming RH or some similar conjecture.

In this direction, Lagarias and Odlyzko [32] have designed a family of analytic algorithms, based on explicit formulas involving roots of the zeta function, for computing $\pi(x)$. They also can be extended to sums of the form (1), in which the Dirichlet series of f is well behaved. The fastest of these runs in time $x^{1/2+o(1)}$. No one has yet implemented any of these algorithms.

5 Exact Computations.

As we have explained above, the accuracy of simple analytic approximations for prime sums is limited by the complex zeroes of the zeta function. To get more precise results, we can turn to methods of a combinatorial flavor.

If we want to compute (1) for all $x \le y$, there is a straightforward method, based on using the sieve of Eratosthenes to list all the primes in $\{2, \ldots y\}$. (This can be readily modified should we want prime powers.) The average cost per prime is very low, as Lehmer [34] has pointed out. If we start with an array indexed from 2 to y, the p-th sieving step will touch about y/p locations. Hence, the total work is about

$$\sum_{p \le y} \frac{y}{p} \sim y \log\log y,$$

by the prime number theorem. The amortized work per prime is thus $O(\log y \log\log y)$ arithmetic operations, and once we have identified the primes, it takes one new evaluation of f to produce each new sum. One application of this is in finding break points for results like (16).

We now examine the problem of computing one particular value of (1). Here, if f is smooth enough, and its values are related, we can do that without examining all the primes. The basic ideas for this go back to the 19th century astronomer Meissel. All versions of this algorithm are exponential in the bit length of x, but the work of Lagarias, Miller, and Odlyzko [31] revealed that a carefully designed one would have much smaller running time than was previously suspected.

They used it to compute $\pi(x)$, but remarked that their algorithm extended to

any instance of (1) in which f is fully multiplicative:[5]

$$f(rs) = f(r)f(s), \text{ for } r, s \geq 1 \ .$$

Below, we sketch an algorithm to compute (1) for such f, using time $x^{2/3+o(1)}$ and space $x^{1/3+o(1)}$.

Let $p_1 < p_2 < p_3 < \cdots$ be the primes. The algorithm is based on combining partially sieved sums of f, and we will need a name for the numbers that survive this process. Accordingly, we say that a number is r-rough if all of its prime factors are $> r$. A typical sieved sum is

$$\phi(x, a) = \sum_{\substack{n \leq x \\ n \ p_a-rough}} f(n). \tag{21}$$

We will choose a to make $p_a \doteq x^{1/3}$. From this we derive the basic dissection of (1):

$$\sum_{p \leq x} f(p) = \phi(x, a) + \sum_{p \leq p_a} f(p) - \phi^{(2)}(x, a) - f(1). \tag{22}$$

Here, $\phi^{(2)}$ is like $\phi(x, a)$ but only involves numbers with two prime factors.

The reasoning behind (22) goes as follows. If a is large, the partially sieved sum $\phi(x, a)$ is almost what we want. To correct it, we must restore the contribution from primes $p \leq p_a$ (which were sieved out), and remove the contribution from numbers of the form pq (which were not). We also subtract $f(1)$ because 1 vacuously satisfies the roughness condition. (Since f is multiplicative, we have $f(1) = 1$ unless f is identically 0.)

Of the two corrections on the right of (22), the first is a sum over relatively small primes, so we can handle it by brute force. For the second one, we use the multiplicativity of f:

$$\phi^{(2)}(x, a) = \sum_{\substack{pq \leq x \\ p_a < p \leq q}} f(pq) = \sum_{p_a < p \leq \sqrt{x}} f(p) \left[\sum_{q \leq x/p} f(q) - \sum_{q \leq p} f(q) + f(p) \right]. \tag{23}$$

We can accumulate this sum by letting the prime p increase, and updating the inner sum for each new p. The primes we need can be found using the segmented sieve of Eratosthenes, but we must keep two segments in memory: one for p (increasing) and one for q (decreasing).

Computing the partially sieved sum is a more intricate process. For this, again relying on multiplicativity, we have the recurrence relation

$$\phi(x, a) = \ \phi(x, a-1) - f(p_a)\phi(x/p_a, a-1). \tag{24}$$

However, a full use of this relation, down to the bottom, is very inefficient. One of the main ideas of [31] is to stop the recursion early. Here we imagine doing that for any $\phi(x/m, b)$ in which the pair (m, b) satisfies either

a) $b = 1$ and $m \leq x^{1/3}$ (an ordinary pair), or

[5]Several people independently had the idea to use this on particular functions. A project to determine when the sum for $f = 1/p$ first crosses 4 is reported on in [6]. Klyve [29] summed this function over arithmetic progressions to compute new approximations to Brun's constant. Déleglise et al. [11] summed $f(p) = p$, and designed a program to handle any multiplicative f.

b) $m > x^{1/3}$ (a special pair).

Since (24) is linear, it is not necessary to pass values up the tree. Rather, the coefficient for a node can be determined from m and b, and it therefore suffices to enumerate the ordinary and special pairs by other means, and add up their contributions. Conceptually, we use the requirements a) and b) to draw a line across the tree, and then identify all the nodes that are crossed by the line.

Ordinary nodes can be evaluated as they are found, if we have an accurate Euler-Maclaurin formula for

$$\phi(x,1) = \sum_{\substack{n \le x \\ n \ odd}} f(n).$$

Of course, this imposes a condition on f, that it be smooth enough for such a formula to exist. (There may also be a direct method for the evaluation, say if $f(n)$ is an integral power n^k.)

To find special nodes, we find their parents. Let's look at a piece of the recursion tree:

$$\begin{array}{ccc} & \phi(x/m', b-1) & \\ \swarrow & & \searrow \\ \phi(x/m', b) & & \phi(x/m, b) \end{array}$$

Here, $m = qm'$. Since the denominator only increases on right branches, we should blame the prime that triggers the increase. Accordingly, we call the right child q-special if $m > x^{1/3}$.

At stage k of the algorithm, we will process the k-th segment $B_k := [kx^{1/3}, (k+1)x^{1/3})$. We note that the three conditions: i) m' is odd, squarefree, and $\le x^{1/3}$; ii) the largest prime factor of m' is $> q$; iii) $\frac{x^{2/3}}{(k+1)q} < m' \le \frac{x^{2/3}}{kq}$, characterize q-special nodes with $x/m \in B_k$.

In our sieving process, we will maintain the values

$$C_q := \text{sum for all previous blocks, sieved to } q-1$$

for $q \le x^{1/3}$. Then, the pseudocode for the sieving process goes as follows:

Set A_i to $f(i)$ for i odd, 0 for i even.
For odd primes $q \le x^{1/3}$:
    Find q-special nodes and compute their ϕ's
    Update C_q to include this block
Set A_i to 0 for all $i \equiv 0 \bmod q$.

Once we have identified a q-special node, we can compute

$$\phi(\frac{x}{qm'}, b) = C_q + \sum_{kx^{1/3} \le i < x/m} A_i.$$

To do this efficiently, we need a special data structure for the array A: it must support random access, as well as sums over ranges. The standard way to do this is to use a binary tree, with sums over subtrees stored at internal nodes.

The analysis of [31] shows that for this algorithm, there will be $O(x^{1/3})$ ordinary pairs and $O(x^{2/3}/(\log x)^2)$ special pairs. The running time is dominated by the cost of finding the special pairs, which has the time and space costs indicated above. Deléglise and Rivat [12] show that the time complexity can be reduced

by logarithmic factors if, in the definition of a special node, $x^{1/3}$ is replaced by something slightly larger.

It is interesting to ask for which f an algorithm of this type can be effective. The following extension appears to be new[6]. Let us call the function f an ATM function (this stands for additive times multiplicative) if there are two other functions g and h such that $f = gh$, and for all $r, s \geq 1$:

$$g(rs) = g(r) + g(s),$$

and

$$h(rs) = h(r) \cdot h(s).$$

We now indicate how the ideas of [31] can be extended to compute (1) for any ATM function f.

First, the dissection (22) can be used as is, since no assumptions were made about f. (We must have $f(1) = 0$, however.)

Second, if we use additivity and then multiplicativity, we see that the ATM property implies that

$$f(rs) = f(r)h(s) + h(r)f(s). \tag{25}$$

This leads to the expression

$$\phi_f^{(2)}(x,a) = \sum_{p_a < p \leq \sqrt{x}} f(p) \sum_{p \leq q \leq x/p} h(q) + \sum_{p_a < p \leq \sqrt{x}} h(p) \sum_{p \leq q \leq x/p} f(q).$$

(The subscript f indicates we are summing over values of f.) Both terms of this can be computed as we did (23). However, the "inner" and "outer" functions are different, so we must accumulate sums for both f and h.

Third, we use a recurrence similar to (24), but with three terms. To derive it, observe that to sieve up to p_a, we can first sieve up to p_{a-1}, and then remove any remaining numbers divisible by p_a. Since the cofactors of these numbers survived the initial sieve, we must have

$$\phi_f(x,a) = \phi_f(x,a-1) - \sum_{\substack{n \leq x/p_a \\ n \ p_{a-1}-rough}} f(p_a n).$$

With (25) this implies

$$\phi_f(x,a) = \phi_f(x,a-1) - h(p_a)\phi_f(x/p_a, a-1) - f(p_a)\phi_h(x/p_a, a-1). \tag{26}$$

We also use (24), but for ϕ_h.

In these recurrences, a ϕ_f node produces two ϕ_f nodes and one ϕ_h node, whereas a ϕ_h node produces only ϕ_h nodes. Therefore, once a path from the root "switches" from f to h, it does not switch back. This means that we can name nodes by triples (m, b, s), in which

$$m = p_{(1)}p_{(2)} \cdots p_{(r)} \tag{27}$$

is a squarefree number, b indicates the level of the node, and r, with $1 \leq s \leq r+1$, indicates where the path from the root switched from f to h. (That is, we divided by $p_{(s)}$ to make the last term in (26).) If $s = r+1$, there was no switch. We choose indices so that $p_{(i)}$ decreases.

[6] A few years ago, V. Miller [37] designed an algorithm to compute $\theta(x)$, which is the sum of an ATM function with $g = \log$ and $h = 1$.

As with the algorithm for multiplicative functions, we obtain the partially sieved sum as a linear combination of contributions from ordinary and special nodes. These are defined and found as before, but now we need to carefully indicate how they are combined.

Let m be given by (27), and $1 \le s \le r+1$. Isolating the prime at which the switch occurs, we have the splitting

$$p_{(1)} \cdots p_{(s-1)} \times p_{(s)} \times p_{(s+1)} \cdots p_{(r)},$$

which defines the coefficient

$$c_s = h(p_{(1)} \cdots p_{(s-1)}) \times f(p_{(s)}) \times h(p_{(s+1)} \cdots p_{(r)}) = g(p_{(s)})h(m).$$

Note that we have used the multiplicativity of h. Also, if $s = r+1$ we deem the contribution from $p_{(s)}$ to be 1. The contribution for a triple (m, b, s) to the value of $\phi_f(x, a)$ in (22) is then

$$(-)^r c_s \phi_h(x/m, b),$$

if $s \le r$, and

$$(-)^r c_s \phi_f(x/m, b),$$

if $s = r+1$.

The other ideas of the algorithm for multiplicative functions can be easily adapted, but there are two important modifications. First, in identifying special nodes, the squarefree $m \le x^{1/3}$ are not just identified, but factored. (To identify all $p_{(s)}$, we cannot just split m; we must factor it.) This can be done by suitably modifying the sieve of Eratosthenes. Second, in the sieve-based procedure for finding ordinary nodes, we need to accumulate partial sums for both ϕ_h and for ϕ_f.

In this way, it is possible to accurately compute all of the functions in Rosser and Schoenfeld's "canon." Along with $\pi(x)$ and $\theta(x)$, their list included $\psi(x)$, which we can evaluate using

$$\psi(x) = \theta(x) + \theta(x^{1/2}) + \theta(x^{1/3}) + \cdots ,$$

the prime harmonic sum

$$\sum_{p \le x} \frac{1}{p},$$

and the sum with no name

$$\sum_{p \le x} \frac{\log p}{p}.$$

They also treated the Mertens-like product $\prod_{c<p\le x}(1 - c/p)$. This can be computed by first evaluating its logarithm, as a combination of multiplicative sums. For example, when $c = 1$ we have

$$\log \prod_{p \le x} \left(1 - \frac{1}{p}\right) = -\sum_{p \le x} \frac{1}{p} - \frac{1}{2} \sum_{p \le x} \frac{1}{p^2} - \cdots .$$

Exact computation of prime sums can also be based on an identity of Vaughan. Deléglise and Rivat [13] used this approach to compute $\psi(x)$, and obtained a running time similar to [31]. It would be an interesting project to extend this algorithm to other types of sums.

We have mainly been concerned with methods for approximating or evaluating (1). We will now digress and treat a related question. For a given value of y, how quickly can we "solve" the equation

$$\sum_{p \le x} f(p) = y?$$

To make this a well defined question, we will assume that the sum is monotonic (that is, f is positive), and seek the least x for which the sum is y or greater. (Note that x must be prime.)

At first glance, it seems that one should use binary search, but there is an interesting "shoot and march" method [6] that uses only one high-precision evaluation of the sum. Here is the idea. We solve the nonlinear equation $F(\hat{x}) = y$, and then compute

$$\sum_{p \le \hat{x}} f(p).$$

If this value is less than y, we search forward, and if it is greater, we search backward.

If we assume RH, we can bound the running time. (This makes it similar to a Las Vegas algorithm, in the sense that the output, when we get it, is guaranteed correct.) Indeed, use RH to determine smooth increasing functions U and L such that

$$L(x) \le \sum_{p \le x} f(p) \le U(x).$$

Define x^+ and x^- by $U(x^-) = L(x^+) = y$. Then, we will have $x^- \le \hat{x} \le x^+$, and our procedure uses *one* evaluation of the sum, plus at most

$$x^+ - x^- \approx \frac{F(x^+) - F(x^-)}{F'(\hat{x})} = \frac{F(x^+) - F(x^-)}{f(\hat{x})} \log \hat{x}.$$

prime tests and evaluations of f.

6 Applications.

We will now briefly discuss how estimates for prime counts and prime sums have been useful in the design and analysis of algorithms.

A glance at the literature (more precisely, a citation database maintained by the Institute for Scientific Information), reveals that Rosser and Schoenfeld's 1962 paper [43] has been cited almost 400 times. Indeed, this is a standard reference for explicit estimates of prime number sums, and it has been put to a wide variety of tasks. As one would expect, it is heavily used in analytic and combinatorial number theory, but there are references to papers on computer algebra, automata theory and complexity, pattern matching, parallel processing, databases, and cryptography. Space does not allow all of these applications to be discussed, but a few personal favorites will be mentioned below.

For certain problems, it is enough to know that the primes are not dense, that is, $\pi(x) = o(x)$. Consider, for example, the unary language

$$11, 111, 11111, 1111111, 11111111111, \ldots$$

that represents the primes. Can this be recognized by a device that uses a fixed amount of memory, irrespective of the input length? Over a single letter alphabet,

the behavior of such a device is completely characterized by a graph of the "next state" mapping, and in this case the graph would have a "rho" shape, with some accepting states in the cycle. (They must be in the cycle since $\pi(x)$ is unbounded.) This implies $\pi(x) = \Omega(x)$, contrary to the prime number theorem, so we conclude that a finite state recognizer cannot exist.

For other applications, we need to know that there are enough primes, that is, that the primes are not too sparse. Undoubtedly the most famous examples come from public key cryptography, which uses primes [15] or pairs of primes [40]. The prime number theorem states that the number of k-bit primes is $\Omega(1/k)$, so a sample of $O(k)$ random numbers is likely to contain one. This is useful, because primality is testable in random polynomial time [49].

Here is a more recent example, coming from machine learning theory [25]. One kind of learning algorithm infers Boolean functions from samples, by processes that repeatedly identify relevant variables. (An input variable is relevant if its change alone, holding other variables constant, can cause the output to change.) This is done by a statistical test, which involves a randomly chosen parameter ρ. The test computes a "relevance" index, whose expected value, averaged over all ρ, is of the form

$$\int_0^1 \phi(\rho)\, d\rho,$$

where $\phi \in \mathbf{Z}[X]$ is positive on $(0, 1)$. We can prove that the index is likely to be large as follows. Since ϕ has integral coefficients, its integral must be at least $1/L$, where $L = \operatorname{lcm}\{1, 2, \ldots, \deg(\phi) + 1\}$. However, the logarithm of L is nothing more than $\psi(\deg \phi + 1)$, so an analytic lower bound on this function provides us with what we want. This argument is related to one of the elementary arguments for the lower bound in Chebyshev's theorem; see Montgomery [38].

Estimation of $\psi(x)$ also plays a role in a common design problem: how do we get long periods by combining small components? More precisely, suppose that $n = n_1 n_2 \ldots n_k$, where the n_i are relatively prime. Further suppose that all $n_i \le x$. How large can we make n?

In the pre-computer era, a standard application for this was in the design of cryptographic rotor machines [24]. For many of these devices, n_i was the period of a rotating switch, and the available technology placed a limit on its size. On the other hand, having n large is an obvious security requirement. Another application, but from the digital age, is residue arithmetic [51]. Here, an integer computation involving only ring operations (addition, subtraction, multiplication) can be sped up by using k registers, the i-th of which does arithmetic mod n_i. Hardware technology, or the state of the marketing art, limits n_i. On the other hand, we want n to be big, so as to handle large problems.

For both problems, the optimal choice is the maximal prime powers $\le x$. Then, we have

$$n = \prod_{p \le x} p^{\lfloor \log x / \log p \rfloor} = e^{\psi(x)} = e^{\theta(x) + O(\sqrt{x})} = e^{x(1+o(1))}.$$

One consequence of this is that a collection of k-bit registers can provide about $1.44 \cdot 2^k$ bits of precision.

For some applications, we need to know not just bounds for prime number sums, but for their "twists." Indeed, many number-theoretic algorithms rely on numbers lying outside proper subgroups of the multiplicative group of integers mod n. On heuristic grounds, it seems plausible to search through the small primes $2, 3, 5, 7, \ldots$

until we get outside the subgroup. Analytic bounds on prime number sums give us information about the likely cost of such a search.

As an example, let us consider prime tests based on Fermat's little theorem and its enhancements. One very elegant test was published by Solovay and Strassen [49]. For an integer x with $0 < x < n$, consider the condition

$$(x|n) \equiv x^{(n-1)/2} \pmod{n}, \tag{28}$$

where the left-hand side indicates the Jacobi symbol. The numbers relatively prime to n satisfying this form a subgroup G, which is nontrivial (for odd n), if and only if n is composite. (When n is prime, it must be the entire group, by Euler's criterion.) Both the Jacobi symbol and the power can be computed efficiently.

Solovay and Strassen conceived their test as a randomized algorithm, but we can also imagine a deterministic version. Its behavior is controlled by the prime sums twisted by a Dirichlet character χ whose kernel contains G. (In other words, we may as well take G to be maximal.) The least witness is then upper bounded by the least $x \geq 1$ with $\chi(x) \neq 1$. (Note that if $\chi(x) = 0$ with $0 < x < n$, we can easily find a factor of n.)

To analyze this, we compare the standard prime sum (1) to its twisted counterpart (4). Up to and including the least witness, the sums must be the same. However, the asymptotic behavior of the sums is different, since since $\zeta(s)$ has a pole at 1, but the twisted zeta function $L(x, \chi)$ does not. Comparing these two bounds, and including information about how the twisted sum grows as a function of n, we get bounds on the least witness.

It seems that this type of argument was first used by Ankeny [2] to estimate the least quadratic nonresidue. By carefully choosing f (with Laplace transforms in mind), one can show, assuming a generalization of the Riemann hypothesis, that any nontrivial subgroup of the multiplicative group of integers mod n must omit a number that is bounded by $2(\log n)^2$ [4]. This is then a bound on the least witness for the Solovay-Strassen [49] and Miller [36] prime tests. For Miller's test, the constant 2 has recently been improved to $3/2$ [52].

We will close by addressing the question of selecting "random" primes. More precisely, for a specific function f, we would like to draw $p \leq x$ with probability proportional to $f(p)$. One application for this is in selecting random integers in factored form, to make cryptographic keys [5]. For this application, we would like to have

$$f(p) \approx \frac{\log p}{p \log x}.$$

Another application is to draw numbers that are guaranteed not to be divisible by small primes, before subjecting them to prime tests.

A naive approach to the problem goes as follows. We first compute all the prime sums up to and including $S = \sum_{p \leq x} f(p)$. Then, divide $(2, S)$ into $\pi(x)$ intervals. We can then choose a random real number $r \in (2, S)$ and output the p corresponding to the interval r is in. Since this requires the normalizing constant S and knowledge of all previous sums, it is only suitable for small x.

If we are willing to sample, however, there is a better "dartboard" method that needs neither a normalizing constant nor a list of primes. For simplicity let x be an integer. To make the dartboard, we define marks

$$0 < t_1 < t_2 < \cdots < t_{x+1} = X,$$

so that $t_i + f(i) \leq t_{i+1}$. Now, there is a mark for every positive integer up to x, not just for the primes, but we do not compute them all. As before, we sample r

from $(0, X)$, but then use binary search or any other efficient method to find the rightmost mark t_p below it. We output p if

$$p \text{ is prime} \qquad \text{and} \qquad r \in [t_p, t_p + f(p)),$$

and try again if not.

By construction, the intervals for each i don't overlap, so the output is correctly distributed. So the only issue is the running time, which is now a random variable. If the gaps are packed tightly together, in the sense that $t_i + f(i)$ is close to t_{i+1}, then the expected number of trials is proportional to

$$\frac{\sum_{n \le x} f(n)}{\sum_{p \le x} f(p)}. \tag{29}$$

To estimate this quantity, we need to evaluate both a sum over integers and the corresponding sum over primes.

In general, this method is efficient when f grows like a power of p. As a general rule, we expect the ratio (29) to be about $\log x$, by the prime number theorem. This rule can fail, however, if f is too small (try $f = 1/p^2$) or too large (try $f = 2^p$).

References

[1] M. Abramowitz and I. A. Stegun. *Handbook of Mathematical Functions*. Dover Publications, 1972.

[2] N. C. Ankeny. The least quadratic non residue. *Ann. of Math. (2)*, 55:65–72, 1952.

[3] K. I. Appel and J. B. Rosser. *Table for estimating functions of primes*, volume 4 of *IDA-CRD Technical Report*. 1961. (Cited in [44].).

[4] E. Bach. *Analytic methods in the analysis and design of number-theoretic algorithms*. ACM Distinguished Dissertations. MIT Press, Cambridge, MA, 1985.

[5] E. Bach. How to generate factored random numbers. *SIAM J. Comput.*, 17(2):179–193, 1988. Special issue on cryptography.

[6] E. Bach and J. Sorenson. Computing prime harmonic sums. Manuscript, 2006. Poster from ANTS-VI Conference available at the web site `http://www.math.tu-berlin.de/~kant/ants/poster.html`.

[7] C. Bays and R. H. Hudson. A new bound for the smallest x with $\pi(x) > \mathrm{li}(x)$. *Math. Comp.*, 69(231):1285–1296 (electronic), 2000.

[8] R. P. Brent. Fast multiple-precision evaluation of elementary functions. *J. Assoc. Comput. Mach.*, 23(2):242–251, 1976.

[9] S. D. Conte and C. de Boor. *Elementary Numerical Analysis: An Algorithmic Approach, 3rd edition*. McGraw-Hill, 1980.

[10] H. Daboussi and J. Rivat. Explicit upper bounds for exponential sums over primes. *Math. Comp.*, 70(233):431–447 (electronic), 2001.

[11] M. Deléglise, J.-L. Nicolas, and P. Zimmermann. E-mail letter to Eric Bach, June 30, 2007.

[12] M. Deléglise and J. Rivat. Computing $\pi(x)$: the Meissel, Lehmer, Lagarias, Miller, Odlyzko method. *Math. Comp.*, 65(213):235–245, 1996.

[13] M. Deléglise and J. Rivat. Computing $\psi(x)$. *Math. Comp.*, 67(224):1691–1696, 1998.

[14] J. Dieudonné. *Infinitesimal calculus*. Hermann, Paris, 1971. Translated from the French.

[15] W. Diffie and M. E. Hellman. New directions in cryptography. *IEEE Trans. Information Theory*, IT-22(6):644–654, 1976.

[16] P. Dusart. Sharper bounds for ψ, θ, π, p_k. Report 1998-06, Laboratoire d'Arithmétique, de Calcul formel et d'Optimisation (LACO), Université de Limoges, 1998.

[17] P. Dusart. The kth prime is greater than $k(\ln k + \ln\ln k - 1)$ for $k \geq 2$. *Math. Comp.*, 68(225):411–415, 1999.

[18] P. Dusart. Estimates of $\theta(x; k, l)$ for large values of x. *Math. Comp.*, 71(239):1137–1168 (electronic), 2002.

[19] H. M. Edwards. *Riemann's zeta function*. Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], New York-London, 1974. Pure and Applied Mathematics, Vol. 58.

[20] G. Elfving. *The history of mathematics in Finland, 1828–1918*, volume 4 of *History of Learning and Science in Finland*. Societas Scientiarum Fennica, Helsinki, 1981.

[21] X. Gourdon. The 10^13 first zeros of the riemann zeta function, and zeroes computation at very large height. Manuscript, October 24th, 2004.

[22] X. Gourdon and P. Sebah. Numbers, constants, and computation. Web site: `http://numbers.computation.free.fr/Constants/`//`constants.html`.

[23] W. E. L. Grimson and D. Hanson. Estimates for the product of the primes not exceeding x. In *Proceedings of the Seventh Manitoba Conference on Numerical Mathematics and Computing (Univ. Manitoba, Winnipeg, Man., 1977)*, Congress. Numer., XX, pages 407–416, Winnipeg, Man., 1978. Utilitas Math.

[24] K. Halton. The tunny machine. In *Codebreakers: The Inside Story of Bletchley Park*, pages 141–148. Oxford University Press, 1993.

[25] L. Hellerstein, B. Rosell, E. Bach, S. Ray, and D. Page. Learning correlation immune functions by skewing: a theoretical analysis. In preparation.

[26] A. E. Ingham. *The distribution of prime numbers*. Cambridge Mathematical Library. Cambridge University Press, Cambridge, 1990. Reprint of the 1932 original, With a foreword by R. C. Vaughan.

[27] A. Ivić. *The Riemann zeta-function*. Dover Publications Inc., Mineola, NY, 2003. Theory and applications, Reprint of the 1985 original [Wiley, New York; MR0792089 (87d:11062)].

[28] E. A. Karatsuba. Fast evaluation of transcendental functions. *Probl. Inf. Transm.*, 27(4):339–360, 1991. Original in: Быстрое вычисление трансцендентных. *Проблемы Передачи Информации*, 27(4):87–110, 1991.

[29] D. Klyve. *Explicit Bounds on Twin Primes and Brun's Constant*. Dissertation. Dartmouth College, 2007.

[30] H. von Koch. Sur la distribution des nombres premiers. *Acta Math.*, 24(1):159–182, 1901.

[31] J. C. Lagarias, V. S. Miller, and A. M. Odlyzko. Computing $\pi(x)$: the Meissel-Lehmer method. *Math. Comp.*, 44(170):537–560, 1985.

[32] J. C. Lagarias and A. M. Odlyzko. Computing $\pi(x)$: an analytic method. *J. Algorithms*, 8(2):173–191, 1987.

[33] E. Landau. *Handbuch der Lehre von der Verteilung der Primzahlen, 3rd edition.* Chelsea, New York, April 1974.

[34] D. H. Lehmer. Computer technology applied to the theory of numbers. In *Studies in Number Theory*, pages 117–151. Math. Assoc. Amer. (distributed by Prentice-Hall, Englewood Cliffs, N.J.), 1969.

[35] J. Littlewood. Distribution des nombres premiers. *C.R. Acad. Sci. Paris*, 158:1869–1872, 1914.

[36] G. L. Miller. Riemann's hypothesis and tests for primality. *J. of Comp. Sys. Sci.*, 13(3):300–317, December 1976. invited publication.

[37] V. Miller. E-mail letter to Eric Bach, October 25, 2007.

[38] H. L. Montgomery. *Ten lectures on the interface between analytic number theory and harmonic analysis*, volume 84 of *CBMS Regional Conference Series in Mathematics*. Published for the Conference Board of the Mathematical Sciences, Washington, DC, 1994.

[39] H. Riesel. *Prime numbers and computer methods for factorization*, volume 126 of *Progress in Mathematics*. Birkhäuser Boston Inc., Boston, MA, second edition, 1994.

[40] R. L. Rivest, A. Shamir, and L. Adleman. A method for obtaining digital signatures and public-key cryptosystems. *Comm. ACM*, 21(2):120–126, 1978.

[41] B. Rosser. The n-th prime is greater than $n \log n$. *Proc. London Math. Soc.*, s2-45(1):21–44, 1939.

[42] B. Rosser. Explicit bounds for some functions of prime numbers. *Amer. J. Math.*, 63:211–232, 1941.

[43] J. B. Rosser and L. Schoenfeld. Approximate formulas for some functions of prime numbers. *Illinois J. Math.*, 6:64–94, 1962.

[44] J. B. Rosser. Unexpected dividends in the theory of prime numbers. In *Proc. Sympos. Appl. Math., Vol. XV*, pages 259–268. Amer. Math. Soc., Providence, R.I., 1963.

[45] J. B. Rosser and L. Schoenfeld. Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$. *Math. Comp.*, 29:243–269, 1975. Collection of articles dedicated to Derrick Henry Lehmer on the occasion of his seventieth birthday.

[46] R. Rumely. Numerical computations concerning the ERH. *Math. Comp.*, 61(203):415–440, S17–S23, 1993.

[47] L. Schoenfeld. Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$. II. *Math. Comp.*, 30(134):337–360, 1976.

[48] J.-P. Serre. Zeta and L functions. In *Arithmetical Algebraic Geometry (Proc. Conf. Purdue Univ., 1963)*, pages 82–92. Harper & Row, New York, 1965.

[49] R. Solovay and V. Strassen. A fast Monte-Carlo test for primality. *SIAM J. Comput.*, 6(1):84–85, 1977. Erratum in 7, 1978, p.118.

[50] J. J. Sylvester. On Tchebycheff's Theory of the Totality of the Prime Numbers Comprised within Given Limits. *Amer. J. Math.*, 4(1-4):230–247, 1881.

[51] N. S. Szabó and R. I. Tanaka. *Residue Arithmetic and its Applications to Computer Technology.* McGraw-Hill, New York, 1967.

[52] S. Wedeniwski. *Primzahltests auf Kommutatorkurven.* Dissertation. University of Tübingen, 2001.

On the index of the Heegner subgroup of elliptic curves

Carlos Castaño-Bernard

Mathematics Section, ICTP,
Strada Costiera 11,
I-34014 Trieste (Italy)
URL: `http://ictp.it/~ccastano/`
Email: `ccastano@ictp.it`

Abstract

Let E be an elliptic curve of conductor N and rank one over $\mathbb{Q}$. So there is a non-constant morphism $X_0^+(N) \longrightarrow E$ defined over $\mathbb{Q}$, where $X_0^+(N) = X_0(N)/w_N$ and w_N is the Fricke involution. Under this morphism the traces of the Heegner points of $X_0^+(N)$ map to rational points on E. In this paper we study the index I of the subgroup generated by all these traces on $E(\mathbb{Q})$. We propose a conjecture that says that if N is prime and $I > 1$, then either the number of connected components ν_N of the real locus $X_0^+(N)(\mathbb{R})$ is $\nu_N > 1$ or (less likely) the order S of the Tate-Šafarevič group $Ш(E)$ of E is $S > 1$. This conjecture is backed by computations performed on each E that satisfies the above hypothesis in the range $N \leq 129,999$.

This paper was prepared for the proceedings of the Conference on Algorithmic Number Theory, Turku, May 8–11, 2007. We tried to make the paper as self contained as possible.

1 Introduction

1.1 Motivation

Let E be an elliptic curve over $\mathbb{Q}$, i.e. a complete curve of genus one with a specified rational point O_E, hence E has a natural structure of a commutative algebraic group with zero element O_E. The Mordell-Weil theorem asserts that the group $E(\mathbb{Q})$ of rational points on E is finitely generated. So the classical Diophantine problem of determining $E(\mathbb{Q})$ is thus the problem of obtaining a finite set of generators for the group $E(\mathbb{Q})$. The finite subgroup $E(\mathbb{Q})^{tors}$ of torsion points of $E(\mathbb{Q})$ is easy to compute. However, finding generators $g_1, \ldots, g_{r_E}$ for the free abelian group $E(\mathbb{Q})/E(\mathbb{Q})^{tors}$ is in general a hard problem. The Birch and Swinnerton-Dyer conjecture predicts (among other things) that the rank r_E of the Mordell-Weil group $E(\mathbb{Q})$ is the order of vanishing at $s = 1$ of the Hasse-Weil L-function $L(E, s)$ attached to E. By the work of Kolyvagin on Euler systems of Heegner points on (certain twists of) modular elliptic curves, and the well-known fact due to Wiles [16], and Breuil, Conrad, Diamond, and Taylor [2] that every elliptic curve E over $\mathbb{Q}$ admits a (non-constant) morphism $\varphi : X_0(N) \longrightarrow E$ over $\mathbb{Q}$, we know that this prediction is true for $r_E = 0$ and 1. We are interested in the latter case, and henceforth we assume that $L(E, s)$ has a simple zero at $s = 1$. Then φ factors through the quotient $X_0^+(N) = X_0(N)/w_N$ associated to the Fricke

involution w_N and the so-called Heegner point construction[1] yields a non-trivial subgroup H of $E(\mathbb{Q})/E(\mathbb{Q})^{tors}$. Gross-Kohnen-Zagier [9, p. 561] proved that the (full) Birch and Swinnerton-Dyer for $r_E = 1$ is equivalent to

$$I_E^2 = c_E \cdot n_E \cdot m_E \cdot |Ш(E)|, \tag{1.1}$$

where I_E is the index of H, $Ш(E)$ is the Tate-Šafarevič group of E, c_E is Manin's constant, m_E is the product of the Tamagawa numbers, and n_E is the index of a certain subgroup of the -1-eigenspace $H_1(E(\mathbb{C});\mathbb{Z})^-$ of complex conjugation acting on $H_1(E(\mathbb{C});\mathbb{Z})$ constructed in terms of classes of Heegner geodesic cycles in $H_1(X_0^+(N)(\mathbb{C});\mathbb{Z})^-$. (The relevant definitions are recalled below.) Let us assume this conjecture. To simplify our discussion let us assume further that the conductor N_E of E is prime so that the index I_E is completely determined by n_E and $|Ш(E)|$. Numerical evidence strongly suggests that there are 109 curves such that $I_E > 1$ out of the 914 curves E of rank one and prime conductor $N \leq 129,999$ in Cremona's Tables [5]. For each of these curves with $I_E > 1$, then either the number ν_N of connected components of the real locus $X_0^+(N)(\mathbb{R})$ of the quotient modular curve $X_0^+(N)$ is $\nu_N > 1$ or, less likely (only 8 cases), $Ш(E)$ is non-trivial. This suggests a non-trivial connection between the topology of $X_0^+(N)(\mathbb{R})$ and the arithmetic of E, which is not expected since ν_N is a certain simple sum of class numbers of real quadratic fields and heuristic considerations suggest that the equality $\nu_N = 1$ is more likely than the inequality $\nu_N > 1$. This paper is about a conjecture (stated in Subsection 3.4) motivated by the above discussion, hoping that it might well furnish an approach to the (full) Birch and Swinnerton-Dyer conjecture for elliptic curves of rank one over $\mathbb{Q}$.

1.2 Acknowledgements

I would like to heartily thank Professor Birch, whose valuable comments encouraged me to investigate further some "loose ends" related to some odd behaviour for the curve **359A** mentioned in my Ph. D. thesis [4, p. 75].

The entries of Table 1 were produced with the help of PARI [12], installed on GNU/Linux computers at the DPMMS of the University of Cambridge (via remote access), and also at the ICTP. The manuscript was prepared for publication using facilities and financial support of the latter.

2 Background

2.1 The Hasse principle and genus one curves

It is a classical Diophantine problem the determination of the set of rational points $C(\mathbb{Q})$ of a given complete non-singular algebraic curve defined over $\mathbb{Q}$. The problem is solved for the case of genus zero. Legendre theorem, as stated by Hasse, says that given any conic C with coefficients in $\mathbb{Q}$ the set $C(\mathbb{Q})$ is non-empty if and only if the set $C(\mathbb{Q}_p)$ is non-empty for every prime p including $p = \infty$, where $\mathbb{Q}_p$ is the field of p-adic numbers, if $p \neq \infty$ and $\mathbb{Q}_p = \mathbb{R}$, if $p = \infty$. Moreover, it is known that it suffices to determine whether $C(\mathbb{Q}_p)$ is non-empty for each prime p that divides the discriminant D of an homogeneous equation $f(X, Y, Z) = 0$ for the conic C. Then by Hensel's lemma we know that $f(X, Y, Z) = 0$ will have a non-trivial zero in $\mathbb{Q}_p$ for $p|D$ if and only if it has an "approximate" zero. Once we have a rational

[1] Heegner points were first studied systematically by Birch [1].

point O on C, it is easy to see that there are an infinite number of them by fixing any line $L \subset \mathbb{P}^2$ defined over $\mathbb{Q}$ (e.g. the X-axis) and parametrise $C(\mathbb{Q})$ with L in the obvious way. This furnishes an algorithm to effectively compute $C(\mathbb{Q})$ in the genus zero case.

Let us consider the genus one case. By the work of Selmer [14] we know that the obvious extension of Legendre's theorem to curves of genus one is not true. For example the curve C in $\mathbb{P}^2$ given by the Selmer cubic

$$3X^3 + 4Y^3 + 5Z^3 = 0$$

is such that $C(\mathbb{Q}_p) \neq 0$ for every prime p, including $p = \infty$. But it turns out that $C(\mathbb{Q}) = \emptyset$. In such cases it is said that C violates the *Hasse principle*. There is a natural way to measure the extent of failure of this principle. The *Jacobian* $E = Jac(C)$ of C is a complete non-singular genus one curve defined over $\mathbb{Q}$ equipped with a commutative algebraic group structure, i.e. E is an elliptic curve, together with an isomorphism $j : C \longrightarrow E$ over $\mathbb{Q}^{alg}$ such that for every element σ in the Galois group $G_{\mathbb{Q}}$ of $\mathbb{Q}^{alg}$ over $\mathbb{Q}$ the map

$$(\sigma \circ j) \circ j^{-1} : Jac\,(T) \longrightarrow Jac\,(T)$$

is of the form $P \mapsto P + a_\sigma$, for some $a_\sigma \in E(\mathbb{Q}^{alg})$. So we may define the *Tate-Šafarevič group* $Ш(E)$ of E as the set of isomorphism classes of pairs (T, ι), where T is a smooth curve defined over $\mathbb{Q}$ of genus 1 such that $T(\mathbb{Q}_p) \neq \emptyset$, for all p prime and $\iota : E \longrightarrow Jac\,(T)$ is an isomorphism defined over $\mathbb{Q}$. (Given T such that $E = Jac(T)$, the map $\sigma \mapsto a_\sigma$ is a 1-co-cycle whose image in the cohomology group $H^1(G_{\mathbb{Q}}, E)$ is uniquely determined by the isomorphism class of (T, ι). So we may identify $Ш(E)$ with a subgroup of $H^1(G_{\mathbb{Q}}, E)$. Cf. Cassels book [3].) Clearly the Hasse principle holds for C if and only if $Ш(E)$ consists of exactly one element, where E is the Jacobian of C. It is conjectured that $Ш(E)$ is finite, i.e. that Hasse principle fails by a "finite amount" in the genus one case.

Cassels' proved that if $Ш(E)$ is indeed finite, then its order is a square.

2.2 Structure of the Mordell-Weil group

The algebraic group structure of an elliptic curve E may be made explicit as follows. Let O_E be the zero element of E. Using the Riemann-Roch theorem we see that the map Albanese map $P \longmapsto P - O_E$ identifies the set $E(K)$ of K-rational points of E with the Picard group $\mathrm{Pic}^0(E/K)$ of E over any field K containing $\mathbb{Q}$. Using again the Riemann-Roch theorem we may see that E has a *Weierstraß model*

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{2.1}$$

where O_E corresponds to $(0 : 1 : 0)$, for a_1, a_2, a_3,a_4, and $a_6 \in \mathbb{Q}$ such that the discriminant Δ of Equation 2.1 is non-zero. It is well-known that the converse holds, so a curve defined by a Weierstraß equation such that $\Delta \neq 0$ is a complete non-singular curve of genus one, and thus an elliptic curve with zero element $O_E = (0 : 1 : 0)$. In particular, the curve obtained by reducing the coefficients of Equation 2.1 modulo a prime number p is an elliptic curve if and only if p does not divide Δ, in which case we say that E has *good reduction* at p. A further consequence of the Riemann-Roch theorem is that the group law is given by the classical chord and tangent construction, which is schematically outlined in Figure 2.1. Using this geometric property we may easily write down explicit rational functions with

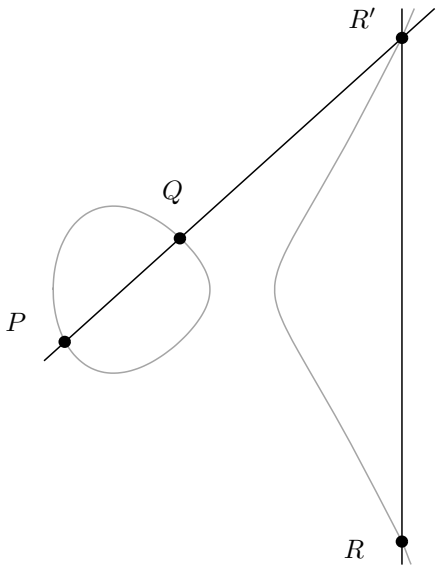


Figure 2.1: Group law $P + Q = R$.

coefficients in $\mathbb{Q}$ on the coordinate functions x and y for the addition law $E \times E \longrightarrow E$ and for the inverse of an element law $E \longrightarrow E$.

The Mordell-Weil theorem asserts that the group $E(\mathbb{Q})$ is a finitely generated abelian group, thus $E(\mathbb{Q}) = E(\mathbb{Q})^{tors} \oplus E(\mathbb{Q})^{free}$, where the torsion subgroup $E(\mathbb{Q})^{tors} \subset E(\mathbb{Q})$ is finite and $E(\mathbb{Q})^{free} \subset E(\mathbb{Q})$ is a free subgroup of (finite) rank r_E. It is well-known that the torsion subgroup $E(\mathbb{Q})^{tors}$ of $E(\mathbb{Q})$ is not difficult to compute. However, a set of generators for $E(\mathbb{Q})^{free}$ is in general hard to obtain. A measure of the arithmetic complexity of a given non-torsion rational point P on E is given by its *Néron-Tate height*

$$\hat{h}(P) = \lim_{n \to \infty} 4^{-n} h(2^n P),$$

where the *naïve height* $h(P)$ of a point $P = (x : y : z)$ in $\mathbb{P}^2(\mathbb{Q})$ is given by $h(P) = \log \max(|x|, |y|, |z|)$, where x, y, and z are integers such that $\gcd(x, y, z) = 1$. It is well-known that $\hat{h}(P)$ does not depend on the choice of Weierstraß model for E and, moreover, it defines a non-degenerate positive definite quadratic form on the r_E-dimensional real vector space $E(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{R}$. The *height paring* is the bilinear form $\langle \cdot, \cdot \rangle$ on $E(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{R}$ such that $\langle P, P \rangle = \hat{h}(P)$, for all $P \in E(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{R}$. The determinant R_E of the r_E by r_E matrix whose entries are given by the height paring $\langle \cdot, \cdot \rangle$ applied to a set of generators of $E(\mathbb{Q})^{free}$ is known as the *regulator* of $E(\mathbb{Q})$.

2.3 The Birch and Swinnerton-Dyer conjecture

As above let E be an elliptic curve defined over $\mathbb{Q}$, and suppose we have used Tate's algorithm [15] to obtain the conductor N_E and a *minimal Weierstraß model* of E, i.e. an integral Weierstraß model of E with $|\Delta|$ minimal. Such discriminant is

known as the *minimal discriminant*[2] of E and denote we it Δ_E. The Hasse-Weil L-function of E over $\mathbb{Q}$ is

$$\begin{aligned} L(E,s) &= \sum_{n=1}^{\infty} a_E(n) n^{-s} \\ &= \prod_{prime\, p \mid N} (1 - a_E(p)p^{-s})^{-1} \prod_{prime\, p \nmid N} (1 - a_E(p)p^{-s} + p^{1-2s})^{-1}, \end{aligned}$$

where

$$a_E(p) = \begin{cases} p + 1 - \#(E(\mathbb{F}_p)), & \textit{good reduction,} \\ 1, & \textit{split reduction,} \\ -1, & \textit{non-split reduction,} \\ 0, & \textit{cuspidal reduction.} \end{cases}$$

Since E is defined over $\mathbb{Q}$ the work of Wiles [16] and Breuil-Conrad-Diamond-Taylor [2] implies that E is modular, and in particular $L(E,s)$ may be analytically continued to the whole complex plane $\mathbb{C}$. (See below.) The Birch and Swinnerton-Dyer conjecture predicts that $L(E,s)$ has a Taylor expansion around $s = 1$ of the form

$$L(E,s) = \kappa_{r_E}(s-1)^{r_E} + \kappa_{r_E+1}(s-1)^{r_E+1} + \ldots,$$

where

$$\kappa_{r_E} = |Ш(E)| m_E \frac{R_E}{|E(\mathbb{Q})^{\mathrm{tors}}|} \Omega_E$$

where m_E is the product of all the local Tamagawa numbers c_p, and Ω_E is the least positive real period of the Néron differential

$$\omega_E = \frac{dX}{2Y + a_1 X + a_3},$$

where a_1 and a_3 are as in Equation 2.1 (assuming the Weierstraß equation is minimal).

Example 2.1. The Selmer cubic C defined by $3X^3 + 4Y^3 + 5Z^3 = 0$ has Jacobian E with Weierstraß model $Y^2 = 4X^3 - 97200$. (Cf. Perlis [13, p. 58].) Using Tate's algorithm we may see that E has conductor $N_E = 24300$ and minimal Weierstraß model $Y^2 = 4X^3 - 24300$. Using this information we may identify E in entry **24300 Y 2** of Cremona's Tables [5]. According to that entry the rank of E is zero and the order of Tate-Šafarevič group predicted by the Birch and Swinnerton-Dyer conjecture is $|Ш(E)| = 3^2$. This is consistent with the fact that the Hasse principle fails for C, as remarked above.

3 On the index I_φ and the topology of $X_0^+(N)(\mathbb{R})$

3.1 Modular parametrisation

Let $X_0(N)$ be the normalisation of the moduli space that classifies pairs (A, A') of elliptic curves together an isogeny $\phi : A \longrightarrow A'$ with cyclic kernel of order N. The curve $X_0(N)$ may be described as follows. Let Γ be the group $\mathrm{SL}_2(\mathbb{R}) = \{ \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) :$

[2]The minimal discriminant Δ_E and the conductor N_E share the same prime divisors, and under certain circumstances they coincide (up to multiplication by ± 1), e.g. when Δ_E is prime.

$ad - cb = 1\}$ modulo multiplication by ± 1, and let Γ act on the upper half plane $\mathfrak{h} = \{z \in \mathbb{C} : \Im(\tau) > 0\}$ in the usual way by letting

$$\tau \mapsto \frac{a\tau + b}{c\tau + d}.$$

First we may identify the complex points of the moduli space $Y(1)$ that classifies elliptic curves E over $\mathbb{C}$ with the complex points of the affine line $\mathbb{A}^1$ by mapping the isomorphism class of $E \cong \mathbb{C}/(\mathbb{Z}\tau + \mathbb{Z})$ to the image of τ in $\Gamma\backslash\mathfrak{h}$ followed by the classical j-invariant map

$$j(\tau) = \frac{E_4^3}{\Delta}(\tau) = \frac{1}{q} + 744 + 196884q + \ldots,$$

where Δ is the cusp form of weight 12 defined by the infinite product $\Delta(\tau) = q\prod_{n>0}(1-q^n)^{24}$, and E_4 is the modular form of weight 4 defined by the series $E_4(\tau) = 1 + 240\sum_{n>0}\sigma_3(n)q^n$, where as usual $\sigma_k(n) = \sum_{0<d|n} d^k$ and $q = e^{2\pi i\tau}$. The obvious action of Γ on the *cusps* $\mathbb{P}^1(\mathbb{Q}) = \mathbb{Q} \cup \{i\infty\}$ is transitive, so the (one-point) compactification $X(1)(\mathbb{C})$ of the complex line $Y(1)(\mathbb{C})$ is the Riemann sphere $X(1) = \Gamma\backslash\mathfrak{h}^*$, where $\mathfrak{h}^* = \mathfrak{h} \cup \mathbb{P}^1(\mathbb{Q})$. We also have a bijection

$$\Gamma_0(N)\backslash\mathcal{H}^* \longrightarrow X_0(N)(\mathbb{C})$$

$$\tau \mod \Gamma_0(N) \longmapsto [\mathbb{C}/(\mathbb{Z}\tau + \mathbb{Z}) \longrightarrow \mathbb{C}/(\mathbb{Z}\tau + \tfrac{1}{N}\mathbb{Z})]$$

where

$$\Gamma_0(N) = \left\{\mu = \begin{pmatrix} a & b \\ d & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) :\ \gamma \equiv 0 \pmod{N}\right\}.$$

The quotient set $\Gamma_0(N)\backslash\mathcal{H}^*$ has a unique complex-analytic structure such that the natural map $\psi : \Gamma_0(N)\backslash\mathcal{H}^* \longrightarrow X(1)(\mathbb{C})$ is a proper. Moreover, the above bijection is in fact an isomorphism between $\Gamma_0(N)\backslash\mathcal{H}^*$ and $X_0(N)(\mathbb{C})$ as Riemann surfaces in such a way that ψ is induced by the projection map $(A, A') \mapsto A$. The degree of ψ is the degree of minimum polynomial $\Phi_N(j, Y) \in \mathbb{C}(j)[Y]$ of $j(N\tau)$ over $\mathbb{C}(j)$, and it turns out that $\Phi_N(X, Y)$ has integral coefficients. So the field of fractions of $\mathbb{Q}[X, Y]/(\Phi_N(X, Y))$ gives the canonical $\mathbb{Q}$-structure of $X_0(N)$.

The *Fricke involution* w_N may be defined as the morphism of $X_0(N)$ to itself induced by mapping an isogeny $\phi : A \longrightarrow A'$ to its dual $\hat{\phi} : A' \longrightarrow A$. In the complex-analytic setting w_N is induced by the involution $\tau \mapsto -\frac{1}{N\tau}$ of $\mathfrak{h}$. Let $X_0^+(N)$ be the quotient of $X_0(N)$ by the group $\{1, w_N\}$. The classical result $\Phi_N(X, Y) = \Phi_N(Y, X)$ implies that the canonical map $X_0(N) \longrightarrow X_0^+(N)$ is defined over $\mathbb{Q}$.

Again let E be an elliptic curve defined over $\mathbb{Q}$. As mentioned above, by the work of Wiles [16] and Breuil-Conrad-Diamond-Taylor [2] we know that E is modular. This means that the Fourier series $f_E(\tau) = \sum_n a_E(n)q^n$ is a normalised newform, and thus $\omega_f = 2\pi i f_E(\tau)d\tau$ is a holomorphic differential on $X_0(N)$ such that the map $\varphi : X_0(N) \longrightarrow E$ defined by

$$\tau \mod \Gamma_0(N) \mapsto \int_{i\infty}^{\tau} \omega_f$$

followed by the classical map $z \mapsto (\wp_\Lambda(z), \wp'_\Lambda(z))$, is a (well-defined) non-constant morphism over $\mathbb{Q}$, where $\wp_\Lambda$ is the Weierstraß $\wp$-function and $\Lambda \subset \mathbb{C}$ is the lattice

generated by the periods of a Néron differential ω_E associated to a minimal Weierstraß model of E. From now on we assume that E has rank one over $\mathbb{Q}$. By the work of Kolyvagin [10], Gross-Kohnen-Zagier [9] and results due to Waldspurger, Bump, Friedberg and Hoffstein, we know that if $r = 0$ or 1, then the order of vanishing of $L(E, s)$ is as predicted by the Birch and Swinnerton-Dyer conjecture (and also that $Ш(E)$ is finite). In particular $L(E, s)$ has a simple zero at $s = 1$ and thus $w_N\omega_f = \omega_f$. So the modular parametrisation factors through the quotient map $X_0^+(N) \longrightarrow X_0(N)$.

3.2 Heegner points

Now suppose we fix a pair of integers (D, r) that satisfy the so-called *Heegner condition*[3] i.e. D is the discriminant of an imaginary quadratic order $\mathcal{O}_D$ of conductor f such that $\gcd(N, f) = 1$ and $r \in \mathbb{Z}$ is such that

$$D \equiv r^2 \pmod{4N}.$$

So we have a proper $\mathcal{O}_D$-ideal $\mathfrak{n}_r = \mathbb{Z}N + \mathbb{Z}\frac{-r+\sqrt{D}}{2} \subset K = \mathbb{Q}(\sqrt{D})$ and $\mathcal{O}_D/\mathfrak{n}_r \cong \mathbb{Z}/N\mathbb{Z}$. So for each proper $\mathcal{O}_D$-ideal $\mathfrak{a} \subset K$ we have a point $x = (\mathbb{C}/\mathfrak{a}, \mathbb{C}/(\mathfrak{n}_r^{-1}\mathfrak{a}))$ on $X_0(N)$. This point x is known as a *Heegner point*, and following Gross [6] we denote it by $x = (\mathcal{O}_D, \mathfrak{n}_r, [\mathfrak{a}])$, where $[\mathfrak{a}]$ is the class of $\mathfrak{a}$ in $\mathrm{Pic}(\mathcal{O}_D)$. The latter set may be identified with the Γ-orbits $\Gamma\backslash\mathcal{Q}_D^0$ of the set $\mathcal{Q}_D^0$ of primitive binary quadratic forms (A, B, C) of discriminant $D = B^2 - 4AC$ and $A > 0$ by writing each $\mathcal{O}_D$-ideal $\mathfrak{a}$ as $\mathfrak{a} = A\mathbb{Z} + \frac{-B+\sqrt{D}}{2}\mathbb{Z}$, for some $(A, B, C) \in \mathcal{Q}_D^0$. Moreover, the $\Gamma_O(N)$-orbits $\Gamma_O(N)\backslash\mathcal{Q}_{N,D,r}^0$ of the set $\mathcal{Q}_{N,D,r}^0$ of $(A, B, C) \in \mathcal{Q}_D^0$ such that $N|A$ and $B \equiv r \pmod{2N}$ may be identified with the set of Heegner points $(\mathbb{C}/\mathfrak{a}, \mathbb{C}/(\mathfrak{n}_r^{-1}\mathfrak{a}))$, and also with the set of $\Gamma_O(N)$-orbits of points $\tau \in \mathfrak{h}$ of the form $\tau = \frac{-B+\sqrt{D}}{2A}$.

The field of definition H of each Heegner point $x = (A, A')$ may be described as follows. Note that a point $x = (A, A')$ on $X_0(N)(\mathbb{C})$ is a Heegner point associated to D if and only if $End(A) = End(A') = \mathcal{O}_D$. So $H = K(j(\tau))$ where $\tau = \frac{-B+\sqrt{D}}{2A}$ is as above, and by the theory of Complex Multiplication the action of the Galois group $\mathrm{Gal}(K^{alg}/K)$ on x is determined by a homomorphism

$$\delta\colon \mathrm{Gal}(K^{alg}/K) \longrightarrow \mathrm{Pic}(\mathcal{O}_D)$$

such that $\delta(\sigma) * x = x^\sigma$, where $*$ is defined by $\mathfrak{b} * x = (\mathcal{O}_D, \mathfrak{n}_r, [\mathfrak{b}^{-1}\mathfrak{a}])$. In other words H is the fixed field of the Galois group $\ker(\delta)$ and $\mathrm{Gal}(H/K) \cong \mathrm{Pic}(\mathcal{O}_D)$. The field H is known as the *ring class field* attached to $\mathcal{O}_D$, i.e. the maximal abelian extension of K unramified at all primes $\mathfrak{p}$ of K which do not divide f. More precisely, the homomorphism δ is the inverse of the Artin reciprocity map, so in fact $\delta(\mathrm{Frob}_\mathfrak{p}) = [\mathfrak{p}]$ for each prime $\mathfrak{p}$ of K which does not divide f, where $\mathrm{Frob}_\mathfrak{p} \in \mathrm{Gal}(H/K)$ is the Frobenius element at $\mathfrak{p}$, which is characterised by the properties $\mathrm{Frob}_\mathfrak{p}\mathfrak{P} = \mathfrak{P}$ and $\mathrm{Frob}_\mathfrak{p}\alpha \equiv \alpha^q \pmod{\mathfrak{P}}$, for each α in the ring of integers $\mathcal{O}_H$ of H, where $\mathfrak{P}$ is a prime ideal of H above $\mathfrak{p}$ and $q = \#(\mathcal{O}_K/\mathfrak{p})$.

To simplify the exposition we assume from now on that the discriminant D is fundamental, and also that $E(\mathbb{Q}) \cong \mathbb{Z}$. The *weighted trace* $y_{D,r,\varphi}$ on E associated to the pair (D, r) is defined by the equation

$$u_D y_{D,r,\varphi} = \sum_{\mathfrak{a} \in \mathrm{Pic}(\mathcal{O}_D)} \varphi(\mathcal{O}_D, \mathfrak{n}_r, [\mathfrak{a}]), \tag{3.1}$$

[3] This condition was introduced by Birch [1].

where

$$u_D = \begin{cases} \frac{1}{2}\#(O_D^\times), & \text{if } \#(O_D^\times) > 2. \\ 2, & \text{if } \#(O_D^\times) = 2 \text{ and } N|D, \\ 1, & \text{otherwise.} \end{cases}$$

We claim that $y_{D,r,\varphi}$ is a rational point on E. Since K is an imaginary quadratic field, the non-trivial element of $\mathrm{Gal}(K/\mathbb{Q})$ is complex conjugation, which acts on Heegner points as $(\mathcal{O}_D, \mathfrak{n}_r, [\mathfrak{a}]) \mapsto (\mathcal{O}_D, \mathfrak{n}_{-r}, [\mathfrak{a}^{-1}])$. Also, note that the action of the Fricke involution w_N is given by $w_N(\mathcal{O}_D, \mathfrak{n}_r, [\mathfrak{a}]) = (\mathcal{O}_D, \mathfrak{n}_{-r}, [\mathfrak{n}^{-1}\mathfrak{a}])$. Therefore the action of w_N on the right-hand side of Equation 3.1 is the same as that of complex conjugation. But we assumed φ factors through the canonical quotient map $X_0(N) \longrightarrow X_0^+(N)$ associated to w_N. Thus the right-hand side of Equation 3.1 is defined over $\mathbb{Q}$. Finally, each Heegner point $\tau \in \mathfrak{h}$ of discriminant D is the fixed point of an element of order u_D of the group generated by $\Gamma_0(N)$ and the Fricke involution w_N (cf. Zagier [17]), and our claim follows.

Recall we assumed $E(\mathbb{Q}) \cong \mathbb{Z}$. So we may fix a generator g_E of the Mordell-Weil group $E(\mathbb{Q})$ of E over $\mathbb{Q}$. The index $I_{D,r,\varphi}$ of $y_{D,r,\varphi}$ in $E(\mathbb{Q})$ may be expressed as

$$y_{D,r,\varphi} = I_{D,r,\varphi} g_E,$$

We are interested in the index I_φ of the group generated by the Heegner points, i.e. the greatest common divisor of the indexes $I_{D,r,\varphi}$ for all pairs (D, r) that satisfy the Heegner condition.

3.3 Heegner paths

Suppose the pair of integers (Δ, ρ) satisfies the Heegner condition, i.e. $\Delta \equiv \rho^2 \pmod{4N}$, and suppose further that Δ is not the square of an integer. Assume the above notation and let $Q = [A, B, C] \in \mathcal{Q}^0_{N,\Delta,\rho}$ The condition $N|A$ implies that all the automorphs of Q lie in $\Gamma_0(N)$. More explicitly, if $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ is a fundamental solution of Pell's equation $X^2 - DY^2 = 1$ then the fundamental automorph of Q given by

$$M_Q = \begin{pmatrix} x - By & -2Cy \\ 2Ay & x + By \end{pmatrix}$$

lies in $\Gamma_0(N)$. We normalise our choice of M_Q by assuming that the eigenvalue $\lambda_Q = x + y\sqrt{D} \in \mathcal{O}_D^\times$ is positive, so that given a base-point $\tau_0 \in \gamma_Q$ the orientation of $\{\tau_0, M_Q\tau_0\}$ coincides with the orientation of

$$\gamma_Q = \left\{ \frac{-B - \sqrt{D}}{2A}, \frac{-B + \sqrt{D}}{2A} \right\},$$

where $\{\tau_0, \tau_1\}$ denotes the geodesic from a point τ_0 to a point τ_1 in $\mathfrak{h} \cup \mathbb{P}^1(\mathbb{R})$. Now let γ_{Q,τ_0} be the closed path on $X_0(N)(\mathbb{C})$ defined by $\{\tau_0, M_Q\tau_0\}$. It is a smooth path on $X_0(N)(\mathbb{C})$ except when it contains an elliptic point of order 2. In that case $\gamma_{Q,\tau_0} = -\gamma_{Q,\tau_0}$ as 1-cycles. Given (D_0, r_0) and (D_1, r_1) that satisfy the Heegner condition we may define the *(twisted) Heegner cycle* as the 1-cycle

$$\gamma_{D_0,D_1,\rho} = \sum_{[Q] \in \Gamma_0(N) \backslash \mathcal{Q}^0_{N,\Delta,\rho}} \chi_{D_0}(Q) \gamma_Q$$

where χ_{D_0} is the *generalised genus character* of Gross-Kohnen-Zagier [9, p. 508]:

$$\chi_{D_0}(Q) = \begin{cases} \left(\frac{D_0}{n}\right), & \text{if } \gcd(A/N, B, C, D_0) = 1 \\ 0, & \text{otherwise.} \end{cases}$$

where $\Delta = D_0 D_1$ and $\rho = r_0 r_1$. Here in the first case n is an integer represented by $[A/N_2, B, CN_2]$, where $N = N_1 N_2$ with $N_i > 0$ $(i = 1, 2)$ and $Q = [A, B, C]$. Note $\gamma_{D_0,D_1,\rho}$ is invariant with respect the action of the Fricke involution w_N, so it defines a 1-cycle on the quotient Riemann surface $X_0^+(N)(\mathbb{C})$. If we assume further that $D_0 < 0$ and $D_1 < 0$, then the Heegner cycle $\gamma_{D_0,D_1,\rho}$ is anti-invariant under the action of complex conjugation on $X_0^+(N)(\mathbb{C})$. In particular the homology class $[\gamma_{D_0,D_1,\rho}]$ represented by the cycle $\gamma_{D_0,D_1,\rho}$ in fact lies in the -1-eigenspace $H_1(X_0^+(N)(\mathbb{C}), \mathbb{Z})^-$. Following Gross-Kohnen-Zagier [9, p. 559] we may define an element $e \in H_1(E(\mathbb{C}), \mathbb{Z})^-$ such that

$$[\gamma(D_0, D_1, r_0 r_1)]_E = I_{D_0,r_0,E} I_{D_1,r_1,E}\, e_E, \tag{3.2}$$

where $[\gamma(D_0, D_1, r_0 r_1)]_E$ is the canonical image in $H_1(E(\mathbb{C}), \mathbb{Z})^-$ of the homology class $[\gamma(D_0, D_1, r_0 r_1)]$, and as above $I_{D_i,r_i,E}$ denotes the index of the trace $y_{D_i,r_i,E}$ in $E(\mathbb{Q})$, for all pairs (D_i, r_i) with $D < 0$ that satisfy the Heegner condition. It is well-known that the index n_E of the subgroup generated by e_E in $H_1(E(\mathbb{C}), \mathbb{Z})^-$ is uniquely defined by the above condition.

Ogg [11] described the real locus $(S/w_m)(\mathbb{R})$ of quotients S/w_m of Shimura curves S, attached to Eichler orders $\mathcal{O}$ of indefinite quaternion algebras over $\mathbb{Q}$, in terms of embeddings of $\mathbb{Q}(\sqrt{m})$ into $\mathcal{O}$. In particular, from his work it is known that the number ν_N of connected components of $X_0^+(N)(\mathbb{R})$ is given by the formula

$$\nu_N = \begin{cases} \frac{h(4N)+h(N)}{2}, & \text{if } N \equiv 1 \pmod 4 \\ \frac{h(4N)+1}{2}, & \text{otherwise.} \end{cases}$$

Moreover, as shown in [4] it is possible to describe explicitly the connected components of $X_0^+(N)(\mathbb{R})$ as a sum of "weighted" Heegner cycles over discriminants $\Delta > 0$ such that $N|\Delta$ and $\Delta|4N$, in analogy with the fixed points of the Fricke involution (cf. Gross [7]).

3.4 The conjecture

As above, let E be an elliptic curve of rank one over $\mathbb{Q}$, and let I_φ be the index of the group generated by the Heegner points, i.e. the greatest common divisor of the indexes $I_{D,r,\varphi}$ for all pairs (D, r) that satisfy the Heegner condition. From now on assume that N_E is prime. In particular E is alone in its isogeny class, so we may write I_E instead of I_φ.

Conjecture 3.1. *If $I_E > 1$ then either the number ν_{N_E} of connected components of the real locus $X_0^+(N_E)(\mathbb{R})$ is $\nu_{N_E} > 1$ or the Tate-Šafarevič group $Ш(E)$ of E is non-trivial.*

There are many examples of elliptic curves in the range of our computations that have $\nu_{N_E} > 1$ but have index $I_E = 1$. So the number of connected components of $X_0^+(N_E)(\mathbb{R})$ does not contain enough information to enable us to predict when $\nu_{N_E} > 1$.

As shown by Gross-Harris [8, pp. 164–165], given any complete, non-singular, geometrically connected curve defined over $\mathbb{R}$ the number ν of connected components of $X(\mathbb{R})$ may be recovered from the homology $\mathbb{F}_2$-vector space $H_1(X, \mathbb{F}_2)$, regarded as a symplectic vector space with involution τ induced by complex conjugation acting on $X(\mathbb{C})$. In fact they prove that

$$\nu = g + 1 - \operatorname{rank}(H)$$

where g is the genus of X, and H is the symmetric submatrix defined by

$$[\tau]_\beta = \begin{pmatrix} I_g & H \\ 0 & I_g \end{pmatrix},$$

where β is a suitable symplectic basis. So our conjecture may be expressed in homological terms. It is hoped that a more refined version of our conjecture may be meaningfully stated in terms of a finer homological invariant associated to the modular parametrisation $X_0^+(N) \longrightarrow E$ over $\mathbb{Q}_p$, specially for $p = \infty$ and $p = N$. Since the Tate-Šafarevič group $Ш(E)$ is defined in terms of local data coming from certain cohomology classes, one may wonder if the canonical subgroup constructed by Gross, Kohnen, and Zagier may be defined similarly in terms of local data from suitable homology classes; perhaps ν_N is just a very crude approximation to the index n_E of a contribution from the prime $p = \infty$ in refined version of our conjecture.

Table 1 (below) was computed as follows. For each elliptic curve E of rank one over $\mathbb{Q}$ and prime conductor $N_E < 129,999$, we computed the greatest common divisor d of the indexes of the image of the Heegner divisor P_D in $E(\mathbb{Q})$, for each fundamental Heegner pair (D, N) such that $|D|$ is less or equal to 163, and $D < 0$. Such d is likely to be the index I_E of the group generated by the images of all Heegner divisors P_D in $E(\mathbb{Q})$ in the range $N_E < 129,999$. All our elliptic curve data comes from Cremona's Tables [5], and we follow the notation used there.

Table 1: Nontrivial indexes I_E for prime $N_E \leq 84701$.

E	I_E	ν_{N_E}	$Ш(E)$	E	I_E	ν_{N_E}	$Ш(E)$
359A	2	2	1	**39133A**	2	2	1
359B	2	2	1	**39133B**	2	2	1
997A	2	2	1	**39301A**	2	14	1
3797A	2	2	1	**40237A**	2	2	1
4159A	2	2	1	**45979A**	4	2	4
4159B	2	2	1	**47143A**	2	2	1
6373A	2	2	1	**47309A**	2	2	1
8069A	2	3	1	**48731A**	4	1	4
8597A	2	6	1	**50329A**	2	3	1
9829A	2	10	1	**51437A**	2	6	1
13723A	2	2	1	**52237A**	2	2	1
17299A	2	2	1	**55837A**	2	14	1
17573A	2	2	1	**59243A**	2	2	1
18097A	2	3	1	**61909A**	2	6	1
18397A	2	2	1	**62191A**	2	5	1
20323A	2	2	1	**63149A**	2	2	1
21283A	2	2	1	**65789A**	2	2	1
23957A	2	6	1	**66109A**	2	2	1
24251A	2	5	1	**66109B**	2	2	1
26083A	2	2	1	**67427A**	2	5	1
28621A	2	2	1	**68489B**	2	3	1
28927A	2	2	1	**69677A**	2	2	1
29101A	2	2	1	**72053A**	2	2	1
29501A	2	2	1	**73709A**	2	2	1
31039A	2	2	1	**74411A**	2	2	1
31319A	2	2	1	**74713A**	4	3	4
33629A	2	2	1	**74797A**	2	2	1
34613A	2	2	1	**77849A**	2	3	1
34721A	2	3	1	**78277A**	2	2	1
35083B	4	1	4	**78919A**	2	2	1
35401A	2	3	1	**81163B**	2	2	1
35533A	2	2	1	**81349A**	2	2	1
36479A	2	11	1	**82301A**	2	2	1
36781A	2	2	1	**84653A**	2	2	1
36781B	2	2	1	**84701A**	2	3	1

Table 2: Nontrivial indexes I_E for prime $85837 \leq N < 129,999$.

E	I_E	ν_{N_E}	$Ш(E)$	E	I_E	ν_{N_E}	$Ш(E)$
85837A	2	2	1	**108971A**	2	2	1
87013A	2	3	1	**113933A**	2	2	1
90001B	2	87	1	**118673A**	2	3	1
90001C	2	87	1	**119689A**	2	3	1
90001D	2	87	1	**119701A**	2	3	1
91381A	2	2	1	**119773A**	2	2	1
92419A	4	1	4	**123791A**	2	2	1
101771A	2	2	1	**124213A**	2	2	1
101879A	2	2	1	**126683A**	2	2	1
102061B	2	6	1	**127669A**	2	2	1
103811A	2	2	1	**129277A**	2	2	1
104239A	4	14	4	**129853A**	2	2	1
104239B	4	14	4				
105143A	2	2	1				
105401A	2	3	1				
105541A	2	2	1				
106277A	2	14	1				
106949A	2	2	1				
106979A	4	1	4				
107981A	2	2	1				

References

[1] B. J. Birch, *Heegner points of elliptic curves*, Symp. Mat., Ist. di Alta Mat., vol. 15, Academic Press, London, 1975, pp. 411–445.

[2] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over* $\mathbf{Q}$*: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939 (electronic).

[3] J. W. S. Cassels, *Lectures on elliptic curves*, Cambridge University Press, Cambridge, 1991.

[4] C. Castaño-Bernard, *On certain sets of Heegner points Heegner paths*, University of Cambridge, 2005, Ph. D. thesis.

[5] J. E. Cremona, *Elliptic curves of conductor* $\leq 20,000$, `http://www.maths.nott.ac.uk/personal/jec/ftp/data/`.

[6] B. H. Gross, *Heegner points on* $X_0(N)$, Modular forms (Durham, 1983), Horwood, Chichester, 1984, pp. 87–105.

[7] ———, *Heegner points and the modular curve of prime level*, J. Math. Soc. Japan **39** (1987), no. 2, 345–362.

[8] B. H. Gross and J. Harris, *Real algebraic curves*, Ann. Sci. École Norm. Sup. (4) **14** (1981), no. 2, 157–182.

[9] B. H. Gross, W. Kohnen, and D. B. Zagier, *Heegner points and derivatives of L-series. II*, Math. Ann. **278** (1987), no. 1–4, 497–562.

[10] V. A. Kolyvagin, *Euler systems*, The Grothendieck Festschrift, Vol. II, Progr. Math., vol. 87, Birkhäuser Boston, Boston, MA, 1990, pp. 435–483.

[11] A. P. Ogg, *Real points on Shimura curves*, Arithmetic and geometry, Vol. I, Progr. Math., vol. 35, Birkhäuser Boston, Boston, MA, 1983, pp. 277–307.

[12] The PARI Group, Bordeaux, *PARI/GP, Version 2.1.5*, `http://www.parigp-home.de/`.

[13] A. R. Perlis, *On the projective geometry of curves of genus one, and an algorithm for the jacobian of such a curve*, University of Arizona, 2004, Ph. D. thesis.

[14] E. S. Selmer, *The Diophantine equation* $ax^3 + by^3 + cz^3 = 0$, Acta Math. **85** (1951), 203–362 (1 plate).

[15] J. T. Tate, *Algorithm for determining the type of a singular fiber in an elliptic pencil*, Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972), Springer, Berlin, 1975, pp. 33–52. Lecture Notes in Math., Vol. 476.

[16] A. Wiles, *Modular elliptic curves and fermat's last theorem*, Ann. of Math. **141** (1995), no. 3, 443–551.

[17] D. Zagier, *Modular points, modular curves, modular surfaces and modular forms*, Workshop Bonn 1984, Lecture Notes in Math., vol. 1111, Springer, Berlin, 1985, pp. 225–248.

On the generalized Fermat equation $ax^p + by^p + cz^p = 0$

Henri Cohen

Abstract

We give a number of methods for studying the equation $ax^p+by^p+cz^p = 0$ including classical algebraic number theory, reciprocity laws, elliptic and hyperelliptic curves, and modular methods. See [2] for much of the material.

1 Introduction

The aim of this work is to give a number of methods for studying the solubility in integers of the equation $ax^n+by^n+cz^n = 0$, where n is assumed to be rather *small*, for instance $n \le 30$. Thus, the emphasis is rather different from that of Fermat's last theorem (FLT), where n can be arbitrary large.

As for FLT, the case $n = 2$ is not interesting since it amounts to finding rational points on a curve of genus 0. Thus we are reduced to the cases $n = 4$ and $n = p \ge 3$ prime. We may also of course assume that $\gcd(a, b, c) = 1$ and that a, b, and c are nth power-free, in an evident sense. These assumptions imply that it is sufficient to look for solutions where x, y, and z are pairwise coprime integers.

2 The case $n = 4$

2.1 The Equation $ax^4 + by^4 + cz^2 = 0$

As for FLT, in this case it is natural to first study the auxiliary equation $ax^4+by^4+cz^2 = 0$. The local solubility conditions are easy to state and prove. For global solubility, we make use of the 2-descent map α on the Jacobian E of the equation, which is the elliptic curve $y^2 = x^3 + abc^2x$. This map from $E(\mathbb{Q})$ to $\mathbb{Q}^*/\mathbb{Q}^{*2}$ is a group homomorphism defined by to $\mathbb{Q}^*/\mathbb{Q}^{*2}$ by $\alpha(\mathcal{O}) = 1$, $\alpha((0,0)) = abc^2$, and otherwise by $\alpha((x,y)) = x$, modulo multiplication by squares of $\mathbb{Q}^*$. The result is that the equation $ax^4 + by^4 + cz^2 = 0$ has nonzero solutions if and only if $-b/c \in \alpha(E(\mathbb{Q}))$.

As amusing special cases we have the following corollaries. Recall first that a *congruent number* is the area of a right triangle with rational sides, and that an important theorem of Tunnell [5] gives an easy characterization of congruent numbers assuming a weak form of the Birch and Swinnerton-Dyer conjecture.

• Let $c \ge 3$ be squarefree and the odd divisors of c are congruent to 1 modulo 8 (this is the local solubility condition). Then if $x^4+y^4 = cz^2$ has a nonzero solution then $2c$ is a congruent number. The converse is not true ($c = 1513$ is the smallest counterexample) but counterexamples are not frequent.

• If $|c|$ is not a perfect square then $x^4 - y^4 = cz^2$ has a solution with $z \ne 0$ *if and only if* $|c|$ is a congruent number.

• Assume the BSD conjecture and let a be squarefree. Then if $a > 0$ and $a \equiv 3$, 5, 13, or 15 modulo 16, or if $a < 0$ and $a \equiv 1$, 2, 6, 7, 9, 10, 11, or 14 modulo 16, the equation $ax^4 + y^4 = z^2$ has infinitely many coprime solutions with $xy \ne 0$.

2.2 The Equation $ax^4 + by^4 + cz^4 = 0$

As usual, the local conditions are easy although tedious to state. As a corollary and using Fermat's well-known result on the equation $x^4 + y^4 = z^2$, we have:

• For all primes p such that $p \equiv 1 \pmod{1160}$ the equation $x^4 + y^4 = p^2 z^4$ is everywhere locally soluble, but is not globally soluble, so is a counterexample to the Hasse principle. In particular, there are infinitely many such counterexamples of this form.

For global solubility, one can appeal either to algebraic methods (number fields), or to geometric methods via coverings by elliptic curves. For the algebraic method we restrict to the equation $x^4 + y^4 = cz^4$ and work in the natural number field $K = \mathbb{Q}(\zeta_8)$ of eighth roots of unity. Following a paper of Bremner–Morton [1], one can state quite general *necessary* conditions for the global solubility of the equation. These conditions are sufficient most of the time. For instance, of the 447 values of c such that $3 \leq c \leq 50416$ for which the equation is locally soluble, 424 can be treated in this way, leaving 23 (5%) indeterminate cases.

One can also use coverings by elliptic curves, and in particular results obtained for the equation $ax^4 + by^4 + cz^2 = 0$ (note that we have three possible choices for such an equation, corresponding the the fact that the Jacobian of our genus 3 curve is isogenous to a product of 3 elliptic curves). This solves 14 of the remaining 23 cases with $c \leq 50416$, leaving 9 cases which need further study.

3 The Equation $ax^p + by^p + cz^p = 0$

We now assume that p is an odd prime. Once again it is not difficult to determine conditions for everywhere local solubility. An interesting question arises in this context. Let ℓ be a prime different from p and not dividing abc. By the Weil bounds (which here are easy) and elementary number theory, the equation $ax^p + by^p + cz^p = 0$ will have a nontrivial solution in $\mathbb{F}_\ell$ as soon as $\ell \neq 1 \pmod{p}$ or $\ell > ((p-1)(p-2))^2$. It seems however experimentally that this latter bound is much too pessimistic. The optimal bound is $\ell > 11$ (instead of 144) for $p = 5$, $\ell > 71$ (instead of 900) for $p = 7$, and so on. I do not know how to prove that something like $\ell > p^3$ suffices in general.

For global solubility, we can use at least three different methods. As in the case $ax^4 + by^4 + cz^4 = 0$ we have the algebraic method, factoring the equation in a suitable number field, and the method using the Jacobian of the curve $ax^p + by^p + cz^p = 0$. In addition, we can use the modular methods, generalizing the theorem of Ribet–Wiles for Fermat's last theorem.

3.1 The Algebraic Methods

Several results can be proved using the algebraic method. One is based on the notion of *suitable ideal divisor*: we may always reduce to an equation of the type $x^p + by^p = cz^p$, and set $K = \mathbb{Q}(b^{1/p})$. We say that $\mathfrak{c} \mid c\mathbb{Z}_K$ is suitable if $\mathfrak{c}$ is primitive, $m \mid c\mathbb{Z}/\mathfrak{c}$ implies that $m \mid f = [\mathbb{Z}_K : \mathbb{Z}[b^{1/p}]]$, $c/\mathcal{N}(\mathfrak{c})$ is a pth power, and any prime ideal dividing $\mathfrak{c}$ and not $f\mathbb{Z}_K$ is of degree 1. We have two results, depending on the class number of K, more precisely on the exponent e of the class group of K. We always assume $b^{p-1} \not\equiv 1 \pmod{p^2}$.

• Assume that $p \mid e$ and that for every suitable divisor $\mathfrak{c}$ of c the ideal $\mathfrak{c}^{e/p}$ is not principal. Then the equation $x^p + by^p + cz^p = 0$ has no nontrivial solutions in pairwise coprime integers.

• Set $r = e \bmod p$, let $U(K)$ be the unit group of K, and assume that $p^2 \nmid b$. For every suitable divisor $\mathfrak{c}$ of c, let γ be a generator of $\mathfrak{c}^e$. For any $\varepsilon \in U(K)$ modulo pth powers, set $\varepsilon\gamma = \sum_{0\le j<p} c_j\theta^j$ with $c_j \in \mathbb{Q}$ and let $P(X) \in \mathbb{Z}[X]$ be the polynomial $P(X) = \sum_{0\le j\le r} fc_jX^j$. Assume that for every pair $(\mathfrak{c}, \varepsilon)$, either there exists j such that $r < j < p$ with $v_p(c_j) = 0$, or there exists k such that $0 \le k \le r-2$ with $v_p(\mathrm{disc}(P^{(k)}(X))) = 0$. Then the equation $x^p + by^p + cz^p = 0$ has no nontrivial rational solutions.

For $p = 3$, the combined conditions of the two theorems mean that $3 \mid hR_3$, where R_3 is the 3-adic regulator.

Other algebraic methods are based on the use of higher reciprocity laws, see [4].

3.2 Elliptic and Hyperelliptic Curves

For $p = 3$ the curve $ax^3 + by^3 + cz^3 = 0$ has genus 1, so the result is very similar to the equation $ax^4 + by^4 + cz^2 = 0$. Here the Jacobian is the curve E with equation $y^2 = x^3 + (4abc)^2$. We make use of the 3-descent group homomorphism α from $E(\mathbb{Q})$ to $\mathbb{Q}^*/\mathbb{Q}^{*3}$ defined by $\alpha(\mathcal{O}) = 1$, $\alpha((0, 4abc)) = (abc)^2$, and otherwise by $\alpha((x, y)) = y - 4abc$, modulo multiplication by cubes of $\mathbb{Q}^*$. The result is that the equation $ax^3 + by^3 + cz^3 = 0$ has nonzero solutions if and only if $b/c \in \alpha(E(\mathbb{Q}))$.

For general p the genus of $ax^p + by^p + cz^p = 0$ is $(p-1)(p-2)/2$, which is too large when $p \ge 5$ to allow for explicit computations. Instead, we use a *covering* by the hyperelliptic curve $y^2 = x^p + a^2(bc)^{p-1}/4$ which is of small genus $(p-1)/2$. Finding the complete set of rational points on this curve is now a feasible task in many cases using the method of Chabauty–Coleman and generalizations.

For instance, for $p = 5$ the algebraic methods again solve most equations, but a few cannot be solved in this way. Using hyperelliptic curves of genus 2 as above M. Stoll has shown that the everywhere locally soluble equations $x^5+7y^5+18z^5 = 0$ and $x^5 + 19y^5 + 24z^5 = 0$ (which cannot be attacked with the algebraic methods) have no nontrivial solutions in $\mathbb{Q}$.

3.3 The Modular Method

We only mention briefly how the modular method of Ribet–Wiles is used on our specific equation. Given a solution to $ax^p + by^p + cz^p = 0$ we construct the Frey curve $Y^2 = X(X - ax^p)(X + By^p)$ which has complete 2-torsion, and using a theorem of Kraus [3], one shows that this curve "arises from" a newform of level essentially equal to $2abc$, which does not depend on x, y, and z. It is easy to make a table of all such newforms, and we then use a method for "bounding exponents", which often gives the desired result. For details on all of this, I refer to S. Siksek's beautiful exposition in [2].

References

[1] A. Bremner and P. Morton, *A new characterization of the integer* 5906, Manuscripta Math. **44** (1983), 187–229.

[2] H. Cohen, *Number Theory Vol I: Tools and Diophantine Equations, and Vol II: Analytic and Modern Tools*, Graduate Texts in Math. **239** and **240**, Springer-Verlag (2007).

[3] A. Kraus, *Majorations effectives pour l'équation de Fermat généralisée*, Can. J. Math. **49** (1997), 1139–1161.

[4] E. S. Selmer, *The Diophantine equation* $ax^3 + by^3 + cz^3 = 0$, Acta Math. **85** (1951), 203–362.

[5] J. Tunnell, *A classical Diophantine problem and modular forms of weight* $3/2$, Invent. Math. **72** (1983), 323–334.

The role of semismooth numbers in factoring large numbers

W.H. Ekkelkamp

1 Introduction

One of the popular systems for encrypting and decrypting messages is the RSA cryptosystem. Its safety is based on the assumption that factoring large numbers is hard. Asymptotically, the best algorithm known for factoring large numbers is the number field sieve, which has a sub-exponential running time.

The most time consuming step in factoring with the number field sieve or the (related) quadratic sieve is the sieving. After initializing the algorithm with some suitable polynomials, we factor many polynomial values and keep the values that are B-smooth. A B-smooth value is a number with all its prime factors up to B. As soon as we have little more B-smooth values than the number of primes below B, we can factor the number we started with.

If we know more about the density of B-smooth numbers, we can estimate how many polynomial values we need to factor and how long the sieving step will take. A well-known approximation of the number $\Psi(x, x^\alpha)$ - values at most x that are x^α-smooth with $0 < \alpha < 1$ - is given by $x\rho(1/\alpha)$, where ρ is the so-called Dickman ρ function, which is the unique continuous solution of the differential-difference equation

$$\begin{cases} \rho(t) = 1 & 0 \le t \le 1 \\ \rho'(t) = -\rho(t-1)/t & t \ge 1. \end{cases}$$

The results based on this approximation are reasonable, but for more accuracy it is better also to use the second order term, introduced by Ramaswami [8]:

$$\Psi(x, x^\alpha) = x\rho(1/\alpha) + (1-\gamma)\frac{x}{\log x}\rho\left(\frac{1-\alpha}{\alpha}\right) + o\left(\frac{x}{\log x}\right), \; x \to \infty,$$

where γ is Euler's constant.

A more efficient way of factoring uses B-smooth numbers with additionally one or two prime factors between B and a larger bound L, the so-called large prime(s). Such numbers are called *semismooth*. Of course, one would like to know how many such numbers one may expect and whether it is better to include the second order term.

If we take a closer look at semismooth numbers with one large prime, include the second order term in our analysis and take $B = x^\alpha$, $L = x^\beta$, we find for their number

$$\begin{aligned} \Psi_1(x, x^\beta, x^\alpha) = x\int_\alpha^\beta \rho\left(\frac{1-\lambda}{\alpha}\right)\frac{\mathrm{d}\lambda}{\lambda} \quad + \\ (1-\gamma)\frac{x}{\log x}\int_\alpha^\beta \rho\left(\frac{1-\lambda-\alpha}{\alpha}\right)\frac{\mathrm{d}\lambda}{\lambda(1-\lambda)} \quad + \quad o\left(\frac{x}{\log x}\right), \; x \to \infty. \end{aligned}$$

In Section 3 we give a more detailed error term. We have derived a similar expression for semismooth numbers with two large primes, as we will see in Section

4. Note that we have an extra degree of freedom here, as we can take different upper bounds for the two large primes.

Zhang [9] has proved that there exist functions $F_1(\alpha,\beta)$ and $G_1(\alpha,\beta)$ such that $\Psi_1(x,x^\beta,x^\alpha) = xF_1(\alpha,\beta) + \frac{x}{\log x}G_1(\alpha,\beta) + O(\frac{x}{\log^2 x})$, but his functions F_1 and G_1 are presented in a more complicated way. His error analysis is a generalization of the work of Knuth and Trabb Pardo [5], whereas our analysis is a generalization of the work of de Bruijn, Ramaswami, and Bach and Peralta.

2 Smooth numbers

Let $n = n_1 n_2 \ldots$ with n_i prime and $n_1 \geq n_2 \geq \ldots$ (where $n_j = 1$ if n has fewer than j prime factors). Then the number of values at most x that are y-smooth can be written as $\Psi(x,y) = \#\{n \leq x : n_1 \leq y\}$. Based on work of De Bruijn [2], we have

Theorem 1. *For any fixed $\epsilon > 0$ the relation*

$$\Psi(x,x^\alpha) = x\rho(\frac{1}{\alpha})\left(1 + O\left(\frac{\log(1/\alpha+1)}{\alpha\log x}\right)\right), \text{ as } x \to \infty,$$

holds uniformly in the range $x^\alpha \geq 2$, $1 \leq \frac{1}{\alpha} \leq \exp\left((\alpha\log x)^{3/5-\epsilon}\right)$.

This theorem is due to Hildebrand [3, 4]. A more precise result was obtained by Ramaswami [8]. We follow the formulation of Norton ([7], p. 12).

Theorem 2. *For $x > 1$, $0 < \alpha < 1$, and $x^\alpha > 2$ we have*

$$\Psi(x,x^\alpha) = x\rho(\frac{1}{\alpha}) + (1-\gamma)\frac{x}{\log x}\rho(\frac{1-\alpha}{\alpha}) + O(\Delta(x,x^\alpha)), \text{ as } x \to \infty,$$

where

$$\Delta(x,x^\alpha) = \begin{cases} \frac{x}{(\log x)^{3/2}} & \text{for } 0 < \alpha < 1/2, \\ \frac{x^\alpha}{\log x} + \frac{x}{\log^2 x} & \text{for } 1/2 \leq \alpha < 1. \end{cases}$$

In this theorem γ is Euler's constant. Our results on semismooth numbers are based on these two theorems.

3 1-Semismooth numbers

A 1-semismooth number is a smooth number with all its prime factors below a certain bound y_2, except for one prime factor $> y_2$, but smaller than a larger bound y_1. The analogue of the Ψ-function for smooth numbers is defined for 1-semismooth numbers as

$$\Psi_1(x,y_1,y_2) = \#\{n \leq x : y_2 < n_1 \leq y_1, n_2 \leq y_2\}.$$

An approximating function is given by the following theorem, which follows directly from Theorem 3.1 in an article of Bach and Peralta [1].

Theorem 3. *If $0 < \alpha < \beta < 1$ and $x^\alpha \geq 2$, then*

$$\Psi_1(x,x^\beta,x^\alpha) = x\int_\alpha^\beta \rho\left(\frac{1-\lambda}{\alpha}\right)\frac{\mathrm{d}\,\lambda}{\lambda} + O\left(\frac{\log(1/\alpha)}{\alpha(1-\beta)}\frac{x}{\log x}\right).$$

Compared with Theorem 3.1 in [1], where only the condition $0 < \alpha < \beta < 1$ is stated, we have an additional condition. This condition originates from the application of a result of de Bruijn [2]. The proof of Theorem 3 can be found in [1]. Here we present the following refinement.

Theorem 4. *If $0 < \alpha < \beta < 1$, $\alpha + \beta < 1$, and $x^\alpha \geq 2$, then we have for $x \to \infty$*

$$\Psi_1(x, x^\beta, x^\alpha) = x \int_\alpha^\beta \rho\left(\frac{1-\lambda}{\alpha}\right) \frac{\mathrm{d}\lambda}{\lambda} + \frac{(1-\gamma)x}{\log x} \int_\alpha^\beta \rho\left(\frac{1-\lambda-\alpha}{\alpha}\right) \frac{\mathrm{d}\lambda}{\lambda(1-\lambda)} + O\left(\left(\frac{\log(\beta/\alpha)}{\alpha^{3/2}} \frac{x}{\log^{3/2} x}\right) + \left(\frac{x^{\alpha+\beta}}{\alpha \log x}\right)\right).$$

The main ingredients of the proof are the definition of 1-semismooth numbers, Theorem 2, partial integration, the prime number theorem $\pi(x) = \mathrm{li}(x) + O(x/\log^c x)$ for any $c > 1$, and careful estimations of the error terms.

We compared both approximating functions with experimental results for the multiple polynomial quadratic sieve (MPQS). We computed the expected number of 1-semismooth numbers after sieving 10096 polynomials and compared this with the real sieving experiment. The second term adds about 10 % to the main term.

x	x^α	x^β	1 term	2 terms	experiment
9.26 E44	2.5 E5	2.5 E7	13 205	14 657	14 884
1.94 E50	3.0 E5	3.0 E7	935	1040	929
2.16 E55	2.5 E5	5.0 E7	25	28	29
3.81 E60	7.5 E5	3.0 E8	63	70	72

4 2-Semismooth numbers

In this section we extend the definition of a 1-semismooth number to two large primes. We recall that a 2-semismooth number is a number with all but two of its prime factors below a certain bound y_2, whereas the other two prime factors are $> y_2$, but $\leq y_1$. The definition of the corresponding Ψ-function is

$$\Psi_2(x, y_1, y_2) = \#\{n \leq x : y_2 < n_2 \leq n_1 \leq y_1, n_3 \leq y_2\}.$$

Lambert has given an approximating function for $\Psi_2(x, y_1, y_2)$ in his thesis [6], consisting of a main term and an error term. However, it may be useful to choose a smaller upper bound for the second largest prime. The corresponding Ψ-function becomes

$$\Psi_2(x, y_1, y_2, y_3) = \#\{n \leq x : n_2 < n_1 \leq y_1, y_3 < n_2 \leq y_2, n_3 \leq y_3\},$$

with $y_3 < y_2 \leq y_1$. If $y_2 = y_1$, we have the same upper bound for both large primes, so it suffices to give the results for the last Ψ-function. Based on Theorem 1, we have the following theorem.

Theorem 5. *Let $\epsilon > 0$ be fixed. If $0 < \alpha < \beta_2 < \beta_1$, $\alpha + \beta_2 + \beta_1 \leq 1$, $x^\alpha \geq 2$, and $\frac{1-2\alpha}{\alpha} \leq \exp((\frac{\alpha}{1-2\alpha} \log x)^{3/5-\epsilon})$, then we have for $x \to \infty$,*

$$\Psi_2(x, x^{\beta_1}, x^{\beta_2}, x^\alpha) = x \left(\int_\alpha^{\beta_2} \int_{\lambda 2}^{\beta_1} \rho\left(\frac{1-\lambda_1-\lambda_2}{\alpha}\right) \frac{\mathrm{d}\lambda_1}{\lambda_1} \frac{\mathrm{d}\lambda_2}{\lambda_2}\right) \left(1 + O\left(\frac{\log(\frac{1}{\alpha})}{\alpha \log x}\right)\right).$$

We will compute the second order term in the next theorem, based on Theorem 2.

Theorem 6. *If* $0 < \alpha < \beta_2 < \beta_1$, $\alpha + \beta_2 + \beta_1 < 1$, *and* $x^\alpha \geq 2$, *then we have for* $x \to \infty$

$$\Psi_2(x, x^{\beta_1}, x^{\beta_2}, x^\alpha) = x \int_\alpha^{\beta_2} \int_{\lambda_2}^{\beta_1} \rho\left(\frac{1-\lambda_1-\lambda_2}{\alpha}\right) \frac{\mathrm{d}\lambda_1}{\lambda_1} \frac{\mathrm{d}\lambda_2}{\lambda_2} +$$

$$(1-\gamma)\frac{x}{\log x} \int_\alpha^{\beta_2} \int_{\lambda_2}^{\beta_1} \rho\left(\frac{1-\lambda_1-\lambda_2-\alpha}{\alpha}\right) \frac{1}{1-\lambda_1-\lambda_2} \frac{\mathrm{d}\lambda_1}{\lambda_1} \frac{\mathrm{d}\lambda_2}{\lambda_2} +$$

$$O\left(\left(\frac{\log(\beta_1/\alpha)\log(\beta_2/\alpha)}{\alpha^{3/2}} \frac{x}{\log^{3/2} x}\right) + \left(\frac{x^{\alpha+\beta_1+\beta_2}}{\alpha \log x}\right)\right).$$

The proof consists of the same ingredients as the proof of Theorem 4. We start with the largest prime and establish an expression for it. Then we repeat the arguments for the second largest prime and get the approximating function as stated in Theorem 6.

We expect similar improvements as for 1-semismooth numbers, when using the second order term.

Zhang [9] has proved that there exist functions $F_2(\alpha, \beta)$ and $G_2(\alpha, \beta)$ such that $\Psi_2(x, x^\beta, x^\alpha) = xF_2(\alpha, \beta) + \frac{x}{\log x} G_2(\alpha, \beta) + O(\frac{x}{\log^2 x})$. The functions F_2 and G_2 are not given explicitly, but defined recursively. Zhang has not considered the case that the large primes have different upper bounds.

5 Conclusions

We have estimated numbers of smooth and semismooth numbers. We have extended these results even further to k large primes with $k \in \mathbb{N}$, but will publish this elsewhere.

Experiments with MPQS indicate that the use of the second order terms contributes about 10 % for x of the size 10^{50}. Most likely the same is true for the number field sieve, but we have not yet verified this.

References

[1] E. Bach and R. Peralta. Asymptotic semismoothness probabilities. *Math. Comp.*, 65(216):1701–1715, 1996.

[2] N. G. de Bruijn. On the number of positive integers $\leq x$ and free of prime factors $> y$. *Indag. Math.* 13 = *Nederl. Acad. Wetensch. Proc. Ser. A.*, 54:50–60, 1951.

[3] A. Hildebrand. On the number of positive integers $\leq x$ and free of prime factors $> y$. *J. Number Theory*, 22(3):289–307, 1986.

[4] A. Hildebrand and G. Tenenbaum. Integers without large prime factors. *J. Théor. Nombres Bordeaux*, 5(2):411–484, 1993.

[5] D. E. Knuth and L. Trabb Pardo. Analysis of a simple factorization algorithm. *Theoret. Comput. Sci.*, 3(3):321–348, 1976/77.

[6] R. Lambert. *Computational aspects of discrete logarithms.* Ph.D. thesis. University of Waterloo, 1996.

[7] K. K. Norton. *Numbers with small prime factors, and the least kth power non-residue.* Memoirs of the American Mathematical Society, No. 106. American Mathematical Society, Providence, R.I., 1971.

[8] V. Ramaswami. The number of positive integers $\leq x$ and free of prime divisors $> x^c$, and a problem of S. S. Pillai. *Duke Math. J.*, 16:99–109, 1949.

[9] C. Zhang. *An extension of the Dickman function and its application.* Ph.D. thesis. Purdue University, 2002.

Some topics concerning the RSA system with key splitting

Anne-Maria Ernvall-Hytönen *

Department of mathematics
University of Turku
FI-20014 University of Turku
FINLAND

1 Introduction

The RSA cryptosystem can be characterized by the equation

$$ed - k\varphi(n) = 1, \tag{1.1}$$

where $e, d, k, n \in \mathbb{Z}$, e is the public exponent, d is the private exponent, n is the public modulus (a product of two different primes which are not told to the public audience) and φ is the Euler φ function. Typically the pair (n, e) is called the public key, but when there is no risk of confusion, e alone is also referred as the public key. In a similar fashion, d is referred as the private key. Now (1.1) is a Diophantine equation of three unknowns and one known number, and the knowledge of the origin of $\varphi(n)$. The only interesting information about d is its residue class modulo $\varphi(n)$, so one may assume that $0 < d < \varphi(n)$. Actually, the parameter k doesn't play any role in the actual encrypting or decrypting but just balances the equation (1.1).

RSA is widely known and after years of attacks against (ie. trials to break) it, still secure. This is not such a wonder because a successful attack against the general RSA scheme would imply a method of factoring numbers which are products of two primes in polynomial time [6].

However, some special cases are not secure. This was shown by Wiener [7] when he broke the system when the private key was at most $\frac{1}{3}n^{1/4}$. At the time he conjectured that the system is breakable as long as $d < n^{1/2}$. However, this is still a conjecture; the best results are by Boneh and Durfee [2] who broke the system when $d < n^{0.292}$ using the approach of Coppersmith [3], and the famous LLL-algorithm due to Lenstra, Lenstra and Lovász [5], and by Blömer and May [1] who excluded several (n, e) pairs.

Small private exponents are extremely attractive because of the shorter computing time. One way to try to save time (or give others the possibility of using one's own RSA private key without telling the actual key), is to split the key, and to direct calculations through one's own device while the server with greater computing capacity would do the most tedious part of the work.

An example of this scenario is the following: Alice realizes that her device doesn't have enough capacity to perform the calculations. She gets an offer of

*This article was written during the author's visit at the Macquarie University, Sydney, and the Australian National University.

computing capacity from Bob. Obviously, she can't trust Bob, and she decides to give his server only part of her private exponent while keeping to herself the rest, so that the alien server doesn't know the actual key. Now the question to consider is, whether the possibly malicious server can figure out the part of the exponent which Alice kept to herself and hereby, crack the system.

Splitting the private exponent d is typically done in the following way:

$$d = f_1 g_1 + f_2 g_2 + \cdots + f_\ell g_\ell, \tag{1.2}$$

where the f's go to one party and the g's to another. It is worth noting that unlike in the "normal" case, it needs to be taken into account that the expression in (1.2) can have a value greater than $\varphi(n)$.

In order to really speed up the computations, one would be tempted to do the splitting extremely unevenly in some circumstances. Assume, for instance, that one device performing computations were a processor in a mobile phone and the other were a computer with a good processor and lots of memory, or that one device were an overly crowded bank's central computer, and the other one were a rarely used but efficient computer somewhere else. It would be extremely handy to divide d into pieces where one device would get large parts (for instance about the same bit size as the original private key) and the other party would get only small parts (for instance, up to one fourth of the original number of bits).

However, it was shown by Ernvall and Nyberg in [4] that one should not split the private exponent into a sum ($d = f_1 + g_2$) or a product ($d = f_1 g_1$) very unevenly.

In the following we consider RSA in the case of the splitted private exponent. We show that the splitting $d = d_1 d_2 + d_3$, which was conjectured to be secure in a talk by Ernvall and Nyberg in Nordsec 2003, is actually not if the public exponent e is fairly small and the splitting is done unevenly. We also discuss the splitting $d = d_1 d_2 + d_3 d_4$.

2 Preliminaries

Write $n = pq$, where p and q are different primes. For security it is typically assumed that if $p < q$, then $q < 2p$. This leads to the following simple estimate

Lemma 1. *For the prime factors p and q of the RSA modulus n there holds*

$$2\sqrt{n} < p + q < 3\sqrt{n}.$$

Proof. The left side of the equation is an easy application of the arithmetic-geometric inequality:

$$\frac{p+q}{2} \geq \sqrt{pq} = \sqrt{n},$$

where the equality would hold if and only if $p = q$ which is not the case. Now it remains to consider the right side of the equation. Assume $p < q$. Then $p < \sqrt{n}$, and therefore, $q < 2\sqrt{n}$, which gives the result. □

This lemma gives an easy but efficient result concerning the size of $\varphi(n)$ as stated in the following corollary

Corollary 2. *For the RSA modulus n there holds*

$$n - \varphi(n) \leq 3\sqrt{n}.$$

In the following, the idea of the classical Wiener attack will be widely used and applied. The Wiener attack is based on the fact that if $a, b, x, y \in \mathbb{Z}$, $\gcd(x, y) = 1$, and

$$\left|\frac{a}{b} - \frac{x}{y}\right| \leq \frac{1}{2y^2},$$

then $\frac{x}{y}$ has to be a convergent of $\frac{a}{b}$ in the simple continued fraction representation. Obviously, if $\gcd(x, y) \neq 1$, then $\frac{x}{y}$ is a convergent with both denominator and the nominator multiplied by some factor. For completeness, we state Wiener's theorem [7].

Theorem 3. *Let $d \leq \frac{1}{3}n^{1/4}$, and $e \leq \varphi(n)$. Then RSA can be broken in polynomial time in the length of n.*

Proof. The equation (1.1) states

$$ed - k\varphi(n) = 1,$$

and from Corollary 2 it follows that the size of $\varphi(n)$ is extremely close to the size of n. Observe that the condition $e \leq \varphi(n)$ implies $k \leq d$. Now we have

$$\begin{aligned}\left|\frac{e}{n} - \frac{k}{d}\right| &= \left|\frac{ed - kn}{nd}\right| = \left|\frac{ed - k\varphi(n) + k\varphi(n) - kn}{nd}\right| \\ &= \left|\frac{1 - k\left(n - \varphi(n)\right)}{nd}\right| \leq \frac{k\left(n - \varphi(n)\right)}{nd} \leq \frac{3k\sqrt{n}}{nd} = \frac{3k}{d\sqrt{n}} \leq \frac{1}{2d^2},\end{aligned}$$

which implies together with $\gcd(k, d) = 1$, that $\frac{k}{d}$ is a convergent of $\frac{e}{n}$. It is well-known that the convergents can be computed in polynomial time in the length of n, and for any convergent candidate, one can solve $\varphi(n)$ from the equation and check whether it is the correct value. □

3 Results

In this section the assumptions look a bit technical, however, they are quite sensible in reality. The conditions for k can be read as assumptions for the product de with respect to n.

Theorem 4. *Let $d = d_1d_2 + d_3$ with $12kd_2 \leq \sqrt{n}$ and $4ed_3d_2 \leq n$, and assume that d_1 is known, $\gcd(k, d_2) = O\left(\log^c n\right)$ and $d_3 = O\left(k \log^c n\right)$ for some constant c. Then one can break the RSA in polynomial time in the length of n.*

Proof.

$$\begin{aligned}\left|\frac{ed_1}{n} - \frac{k}{d_2}\right| &= \left|\frac{ed_1d_2 - kn}{nd_2}\right| = \left|\frac{ed_1d_2 + ed_3 - k\varphi(n) - kn + k\varphi(n) - ed_3}{nd_2}\right| \\ &= \left|\frac{1 - k\left(n - \varphi(n)\right) - ed_3}{nd_2}\right| \leq \frac{3k\sqrt{n}}{nd_2} + \frac{ed_3}{nd_2} = \frac{3k}{d_2\sqrt{n}} + \frac{ed_3}{nd_2} \\ &\leq \frac{3e}{d_2\sqrt{n}} + \frac{ed_3}{nd_2} \leq \frac{1}{2d_2^2}.\end{aligned}$$

Now we know that $\frac{k}{d_2}$ is a convergent of $\frac{ed_1}{N}$. If d_3 is known, then this finishes the proof of the theorem. Otherwise solve the Diophantine equation

$$ed_1d_2 + ed_3 - k\varphi(n) = 1.$$

for possible values of k and d_2. The trick is that d_3 is not essentially larger than k, and $d_3 \equiv e^{-1} - d_1 d_2 \pmod{k}$, so the solution is easy to find. □

Theorem 5. *With the notation of Theorem 4, assume that $ed_1d_2 \leq n$ and $k \leq \sqrt{n}$. If d_1 and d_3 are known, then the system can be broken in polynomial time in the length of n.*

Proof. This case is actually not an application of the Wiener attack but some basic arithmetics with simple estimates. First write the equation (1.1) in the form

$$ed_1d_2 + ed_3 - k(n + 1 - p - q) = 1. \tag{3.3}$$

Then manipulate the equation (3.3) to obtain

$$k = \frac{ed_3}{n} + \frac{-1 - k + (p+q)k + ed_1d_2}{n}.$$

Now estimating is easy. One gets the upper bound

$$k \leq \frac{ed_3}{n} \frac{-1 - k + 3\sqrt{n}k + ed_1d_2}{n} < \frac{ed_3}{n} - \frac{k+1}{n} + 3\frac{k}{\sqrt{n}} + 1 < \frac{ed_3}{n} + 4.$$

and the lower bound

$$k \geq \frac{ed_3}{n} - \frac{k+1}{n} + \frac{2k}{\sqrt{n}} > \frac{ed_3}{n}.$$

Thus, all the possible values for k are integers and lie on the interval $\left(\frac{ed_3}{n}, \frac{ed_3}{n} + 4\right)$. Because there are not many values, one can check all of them individually. For any candidate we consider the equation (3.3) and solve d_2. □

All of these attacks require e to be moderately small. The assumption is somewhat inconvenient but still relevant considering that the temptation to make the public exponent small is fairly large with regards to the computing time and the fact that in the case of non-splitted private exponent, there are no very efficient attacks for small public exponents.

One might now wonder, if some other simple compositions for the private exponent would be useful. In the tradition of splitting in the form (1.2), one could next consider the splitting

$$d = d_1d_2 + d_3d_4,$$

where d_1 and d_3 go to one party and d_2 and d_4 to the other. One needs to be somewhat careful with this scenario, too, as the next theorem shows:

Theorem 6. *Let $e\,|(d_1 - d_3)(d_2 - d_4)| \leq n^{3/4}$, $k \leq \frac{1}{6}n^{1/4}$, $d_2 + d_4 \leq \frac{1}{4}n^{1/4}$ and assume that $\gcd(d_2 + d_4, k) = O(\log^c n)$ and $|d_2 - d_4| = O(k \log^c n)$ for some constant c. Assume that d_1 and d_3 are known. The system can be broken in polynomial time in the length of n.*

Proof. Notice first that

$$d_1d_2 + d_3d_4 = \frac{1}{2}\left((d_1 + d_3)(d_2 + d_4) + (d_1 - d_3)(d_2 - d_4)\right)$$

We will substitute this to equation (1.1) to obtain

$$e\left((d_1 + d_3)(d_2 + d_4) + (d_1 - d_3)(d_2 - d_4)\right) - 2k\varphi(n) = 2.$$

Use of the Wiener approach gives

$$\begin{aligned}\left|\frac{(d_1+d_3)\,e}{n}-\frac{2k}{d_2+d_4}\right| &= \left|\frac{(d_1+d_3)\,(d_2+d_4)\,e-2kn}{n\,(d_2+d_4)}\right| \\ &= \left|\frac{(d_1+d_3)\,(d_2+d_4)\,e+(d_1-d_3)\,(d_2-d_4)\,e-2k\varphi(n)+2k\varphi(n)}{n\,(d_2+d_4)}\right. \\ &\qquad \left.\left|\frac{-2kn-(d_1-d_3)\,(d_2-d_4)\,e}{n\,(d_2+d_4)}\right|\right. \\ &= \left|\frac{2-(d_1-d_3)\,(d_2-d_4)\,e+2k\,(\varphi(n)-n)}{n\,(d_2+d_4)}\right| \leq \frac{1}{2\,(d_2+d_4)^2}.\end{aligned}$$

From this one gets the possibilities for k and d_2+d_4. One may substitute these values and solve the corresponding Diophantine equation. The size restriction for d_2-d_4 guarantees that there are not very many possibilities for the correct value. □

References

[1] J. Blömer and A. May. A generalized Wiener attack on RSA. In *Public key cryptography—PKC 2004*, volume 2947 of *Lecture Notes in Comput. Sci.*, pages 1–13. Springer, Berlin, 2004.

[2] D. Boneh and G. Durfee. Cryptanalysis of RSA with private key d less than $n^{0.292}$. *IEEE Trans. Inform. Theory*, 46(4), 2000.

[3] D. Coppersmith. Small solutions to polynomial equations, and low exponent RSA vulnerabilities. *J. of Cryptology*, 10:233–260, 1997.

[4] A.-M. Ernvall and K. Nyberg. On server-aided computation for RSA protocols with private key splitting. In *Proceedings of NordSec 2003, The Eighth Nordic Workshop on Secure IT Systems, Gjøvik, Norway*, pages 195–206. 2003.

[5] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261(4):515–534, 1982.

[6] A. May. Computing the RSA secret key is deterministic polynomial time equivalent to factoring. In *Advances in cryptology—CRYPTO 2004*, volume 3152 of *Lecture Notes in Comput. Sci.*, pages 213–219. Springer, Berlin, 2004.

[7] M. Wiener. Cryptanalysis of short RSA secret exponents. *IEEE Trans. Inform. Theory*, 36, 1990.

Fast arithmetic: tiger in your tank

Joachim von zur Gathen

b-it
Universität Bonn
Dahlmannstr. 2
D - 53113 Bonn
Email: gathen@bit.uni-bonn.de
URL: http://cosec.bit.uni-bonn.de/

1 Introduction

Following the kind invitation to speak at a meeting of the Academia Europeae in 2006 and the 2007 ANT meeting in Turku, I present a rather idiosyncratic view of some achievements of high-performance algebraic computing, including a speculative area.

The evolution of fast algorithms in this area started in the 1970s. This was also the time of the first energy crisis, and the title is meant to suggest that intelligent usage of resources will gain us a lot of scientific mileage.

I have selected four topics for this presentation:

- Fast multiplication: Cryptographic hardware and polynomial factorization,
- Fast multiplication: Riemann's zeta function,
- Short vectors in integral lattices: Minkowski's geometry of numbers and knapsack cryptography,
- Short vectors in integral lattices: Mertens' conjecture.

Thus we consider two fundamental methods in modern computer algebra: fast multiplication and short vector computations, and for each of them an application to a "modern" and a "classical" task.

2 Fast multiplication

An important setting for algebraic computation is inside rings, with addition and multiplication. Typically, addition is easy to do, and multiplication is the core problem of efficient arithmetic. There are several algorithms for multiplication of n-bit integers or univariate polynomials of degree at most n. The major steps were:

- classical: $O(n^2)$,
- Karatsuba: $O(n^{1.59})$,
- FFT: $O(n \log n \log\log n)$,
- [6] : $n \log n \; 2^{O(\log^* n)}$.

Their cost is illustrated in Figures 2.1 and 2.2, with the total work of the classical method represented by the all-black square at top left. The reader may recognize the fractal "Sierpinski carpet" of Hausdorff dimension $\log_2 3 \approx 1.59$ as the limit of the Karatsuba images. The FFT algorithm, beaten only recently by [6], is due to [21].

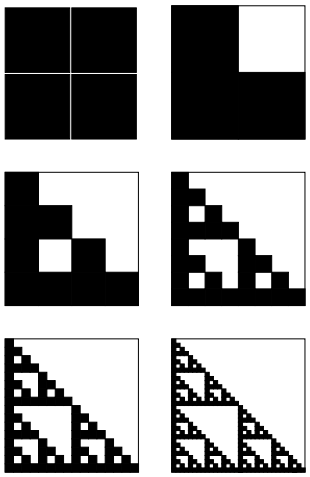


Figure 2.1: Karatsuba.

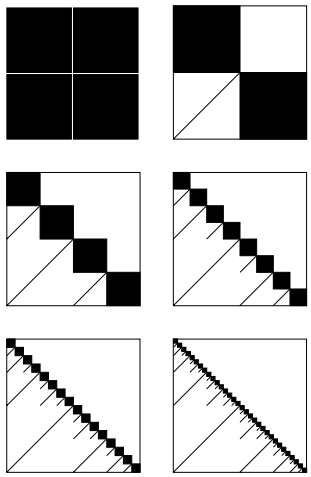


Figure 2.2: FFT.

Other problems can be "reduced" to this, sometimes with an extra factor $O(\log n)$. This includes division with remainder, gcd, Berlekamp-Massey, implicit linear algebra, and evaluation/interpolation.

For an efficient software implementation of fast arithmetic, one has to implement a large variety of algorithms and determine the breakpoints: hybrid methods. Schönhage's adage rules: The development of fast algorithms is slow! Successful implementations are in NTL and Magma. BiPolAr is specifically targetted at *Bi*nary *Pol*ynomial *Ar*ithmetic over the field $\mathbb{F}_2$.

Two measurements illustrate such efforts. Figure 2.3 records an old implementation, on a 167MHz Sparc Ultra 1 (1998). "Cantor" refers to an algorithm similar to the FFT ([4]). The jumps in its running time are highly visible, and in fact it took a lot of effort to reduce them to this size. They present a typical phenomenon in such recursive algorithms.

Table 2.1 shows the time for multiplication of large (and small) integers in the computer algebra system Magma on an Opteron 150 (2.4 GHz, L2 1MB, 1 July 2005). The last column was determined experimentally, normalized so that the last entry equal 1, and suggests a running time of about $n \log^3 n$. The reader should realize that the last row deals with a humungous task: multiplication of two half-a-billion digit integers, with 128 MByte for the product!

Traditional lore held hardware implementations of fast arithmetic infeasible, because

- recursive algorithms generate long data paths, fast multiplication and short vector computations, and for each for each of them an application to a "modern" and a "classical" task.
- only small problem sizes can be dealt with.

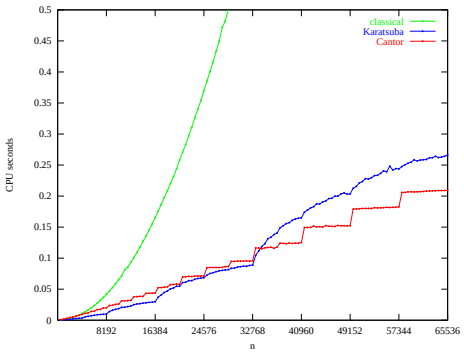


Figure 2.3: Multiplication of polynomials of degree $n-1$ on a 167 MHz Sparc Ultra 1 (1998)

m	sec	time/$n \log^3 n$
18	0.002	0.969
19	0.005	1.030
20	0.011	0.972
21	0.027	1.030
22	0.059	0.979
23	0.132	0.958
24	0.300	0.959
25	0.640	0.905
26	1.560	0.980
27	3.300	0.926
28	8.540	1.074
29	17.670	1.000

Table 2.1: Magma (1 July 2005), Opteron 150 (2.4 GHz, L2 1MB), Multiplication of two n-bit integers with $n = 2^m$.

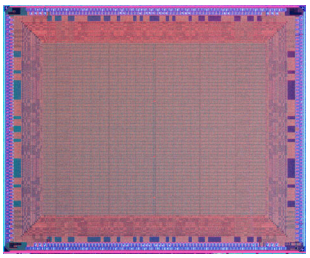


Figure 2.4: The die of a spartan-3 chip.

By now, hardware has grown powerful enough that we can venture into the land of subquadratic algorithms. Karatsuba's multiplication algorithm (from [12]) replaces the "classical" four coefficient multiplications for the product of two linear polynomials by only three:

$$(f_1x + f_0)(g_1x + g_0) = f_1g_1x^2 + ((f_1 + f_0)(g_1 + g_0) - f_1g_1 - f_0g_0)x + f_0g_0.$$

Multiplier type	Number of clock cycles	area	Multiplication time	AT area × time
classical	56	1582	$0.523\mu s$	827
	54	1660	$0.655\mu s$	1087
	30	1480	$0.378\mu s$	559

Table 2.2: Fast multiplication in hardware.

We can substitute x by some other value, say x^4:

$$(f_1x^4 + f_0)(g_1x^4 + g_0) = f_1g_1x^8 + ((f_1 + f_0)(g_1 + g_0) - f_1g_1 - f_0g_0)x^4 + f_0g_0$$

By taking the "coefficients" $f_1, \ldots, g_0$ to be 4-coefficient polynomials, of degree at most 3, we obtain a recipe for 8-coefficient multiplication. Clearly this has a recursive generalization; see e.g., [23], Section 8.1. The Karatsuba circuit is drawn in Figure 2.5 top; the bottom shows the additions inherent in the formula.

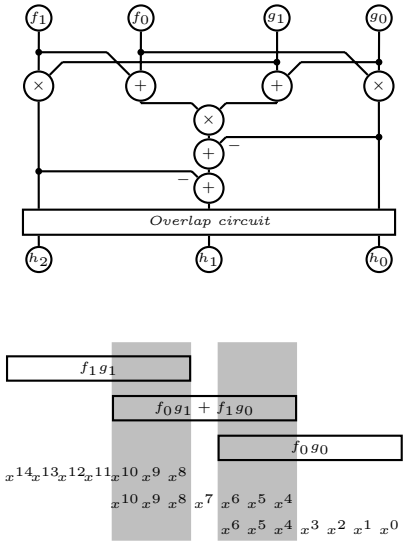


Figure 2.5: Karatsuba and its overlap circuit.

Our work described in [1] and [2] was—as far as I know—the first where the Karatsuba method was successfully put into hardware. In [7] we implemented these ideas and circuits for the multiplication of 240-bit polynomials over $\mathbb{F}_2$ on an FPGA, namely a Xilinx Virtec II Pro with processing elements. Its recursive structure is shown in Figure 2.6. A major component in achieving the timings reported in Table 2.2 was massive pipelining which increases throughput substantially.

Our efforts in this area were driven by the goal of developing an FPGA-based crypto coprocessor. The overall design is shown in Figure 2.7, and Table 2.3 provides some timings. The FPGA timings are on an XCV 2000 E FPGA driven at 12.5 MHz (when did you last use a machine that slow?), and the PC is a Pentium 4 at 2.8 GHz. The curve is taken from the NIST standard.

As a further application of efficient arithmetic we mention a major success story in computer algebra, namely the factorization of polynomials. Using the technology of fast algorithms described above, one can factor univariate polynomials over $\mathbb{F}_2$ with degree over one million ([3]).

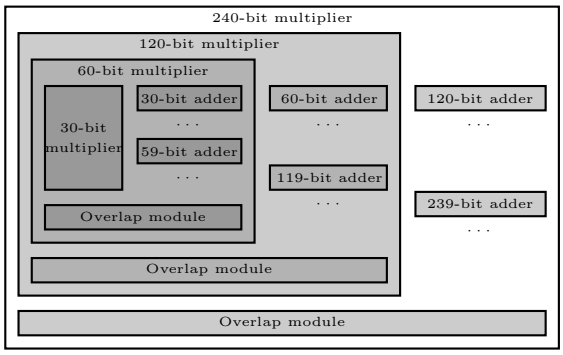


Figure 2.6: 240-bit multiplication, pipelining 30 bits

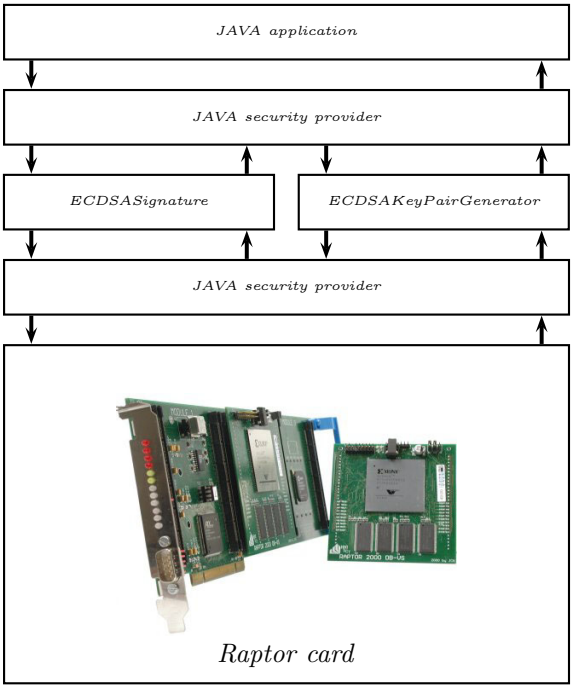


Figure 2.7: Architecture for supporting a Java security provider by an FPGA crypto coprocessor.

Figure 2.9 gives some sample factorizations of randomly chosen polynomials, computed in 1998. The software proceeds along two major threads: distinct-degree factorization by intervals, and Rabin's irreducibility test of the remaining polynomial. When the latter finishes first, the "abort" column shows the current "distinct degree" under consideration. The algorithmic approach has been called the von zur Gathen - Kaltofen - Shoup method ; see [25, 10, 11].

In the spirit of this paper's title, we may look at the environmental cost of this computation. The power consumption of a processor at full speed is about 150 W. Assuming this, the CO_2 footprint of the factorization at degree one million comes to 60 kWh, or about 30 kg CO_2. The same computation with classical arithmetic would cost roughly 75 t CO_2, more by a factor of 2500.

Finite field	$\mathbb{F}_{2^{191}}$
Elliptic curve	$y^2 + xy = x^3 + ax + b$ $a = 1$ $b = 7BC86E2102902EC4D5890E8B6B4981FF27E0482750FEFC03$
Number of points	$1569275433846670190958947355834614995815261150867795429199 \cdot 4$
Key generation time	FPGA: 3.6 ms, PC: 9 ms
Signing time	FPGA: 3 ms, PC: 8 ms
Verification time	FPGA: 4 ms, PC: 16 ms

Table 2.3: Timings for elliptic curve cryptography

Figure 2.8: Shoup - von zur Gathen - Kaltofen.

3 The Riemann Hypothesis

In his landmark paper "Über die Anzahl der Primzahlen unter einer gegebenen Größe" of 1859, [20] initiated the study of the zeta function as a function of a complex variable.

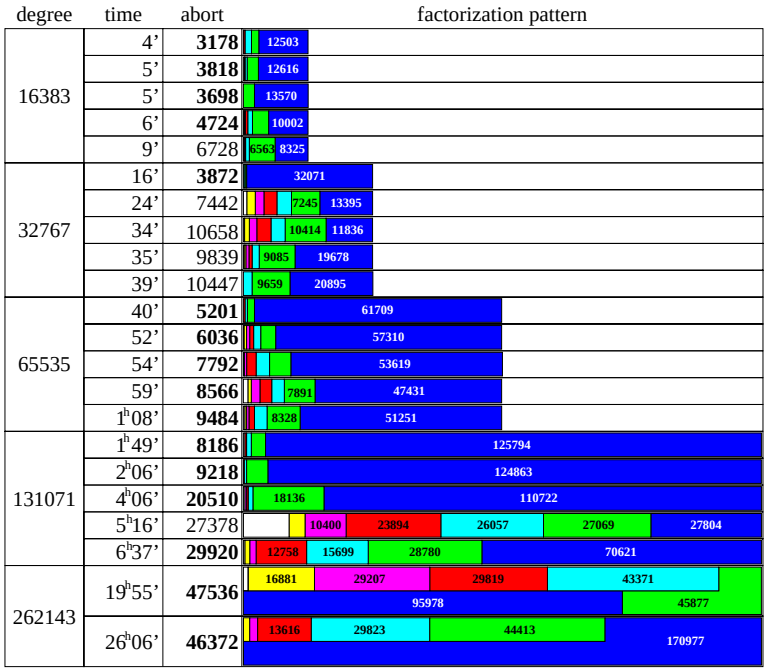


Figure 2.9: Polynomials over $\mathbb{F}_2$.

Leonhard Euler (1707 - 1783) had already stated the equation

$$\zeta(s) = \sum_{n \geq 1} n^{-s} = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}$$

for real $s > 1$, which can be viewed as a concise way of expressing the Fundamental Theorem of Arithmetic, that is, the unique factorization of integers. The sum is convergent for complex s with $\Re(s) > 1$, and ζ can be defined in the complex plane by analytic continuation.

Some values of ζ are shown in Figure 3.1. ζ has "trivial" roots at $-2n$ for $n \in \mathbb{N}$, and Riemann postulated what is today known as the *Riemann Hypothesis*: all nontrivial roots of the zeta function lie on the *critical line* "real part $= 1/2$". Very relaxed, Riemann writes: "Hiervon wäre allerdings ein strenger Beweis zu wünschen; ich habe indes die Aufsuchung desselben nach einigen flüchtigen vergeblichen Versuchen vorläufig bei Seite gelassen, da es für den nächsten Zweck meiner Untersuchung entbehrlich schien."[1]

Riemann's challenge has defied mathematicians ever since. It figured as the eighth in Hilbert's famous list of problems in 1900, and a century later still as one of seven Clay Millenium Problems in 2000. Its implications are numerous. A prime example is the Prime Number Theorem, proven in 1896 by Jacques Hadamard and Charles Jean de La Vallée-Poussin. It gives an approximation to $\pi(x)$, the number of prime numbers up to x:

$$\pi(x) = \frac{x}{\ln\, x} + O(\frac{x}{\ln^2 x}),$$

[1] A rigorous proof of this would nonetheless be desirable; I have, however, left aside the quest for one after several brief and unsuccessful attempts, since it seemed dispensable for the immediate goal of my investigation.

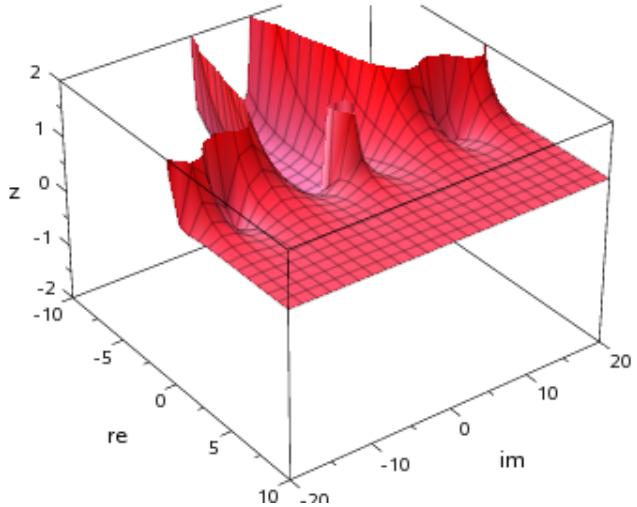


Figure 3.1: Riemann's zeta function $\zeta(s)$ *for* $|\Re(s)| \leq 10$ and $|\Im(s)| \leq 20$, truncated for large values.

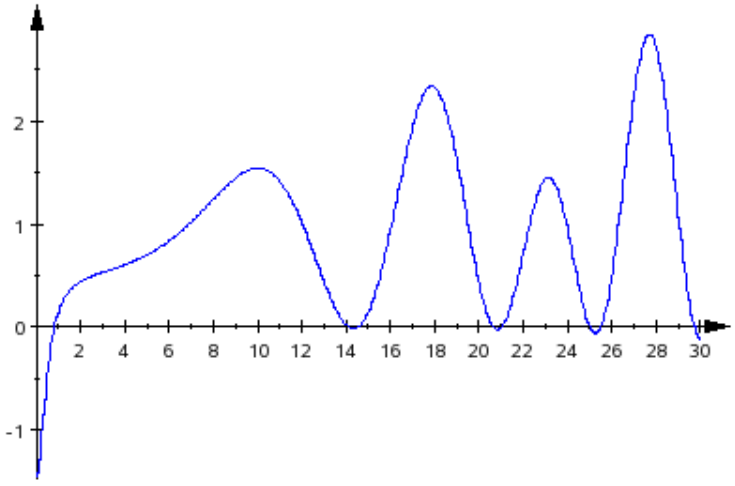


Figure 3.2: The zeta function along the critical line, $0 \leq \Re(s) \leq 30$.

where ln is the natural logarithm. The Riemann Hypothesis implies a huge improvement in the error term: $\pi(x) = \mathrm{li}(x) + O(\sqrt{x \ln x})$, where $\mathrm{li}(x)$ is the logarithmic integral. It approximates π better than $x/\ln x$ does. In some areas of number theory, it is socially acceptable to prove results "under the Riemann Hypothesis" and its generalizations. A proof of the Hypothesis would turn all such statements into proven theorems.

How can there be a connection between the Riemann Hypothesis and fast arithmetic? [18] calculated large numbers of roots of ζ. This is only possible with good algorithms for ζ and for integer multiplication. Pólya and Hilbert conjectured that the roots $\frac{1}{2} + it$ of ζ might correspond to the eigenvalues t of some operator, and to a Hermitian one if all t's are real. They did not put forth any specific operator.

Later a whole probability space of such operators emerged, namely the *Gaussian Unitary Ensemble*. The average distances between its eigenvalues match those for the roots of ζ pretty closely.

The most convincing evidence for this conjecture, so far, is provided by the experiments. As an example, Odlyzko calculated roots number $10^{22}+1$ to $10^{22}+19$ at $t = 1370919909931300000 + x$, as in Figure 3.3. In words, these are the first 19 roots of ζ after root number quazillion.

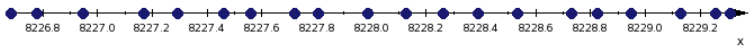


Figure 3.3: Spacing of 19 roots of ζ after root number 10^{22}.

The roots have the "repellent" property of usually keeping a certain distance from their neighbors. The dots in Figure 3.4 present Odlyzko's actual measurements, while the curve gives the corresponding theoretical average for the Gaussian Unitary Ensemble. The astonishingly close match between the two is the strongest piece of evidence yet that some version of the Pólya-Hilbert conjecture might be true.

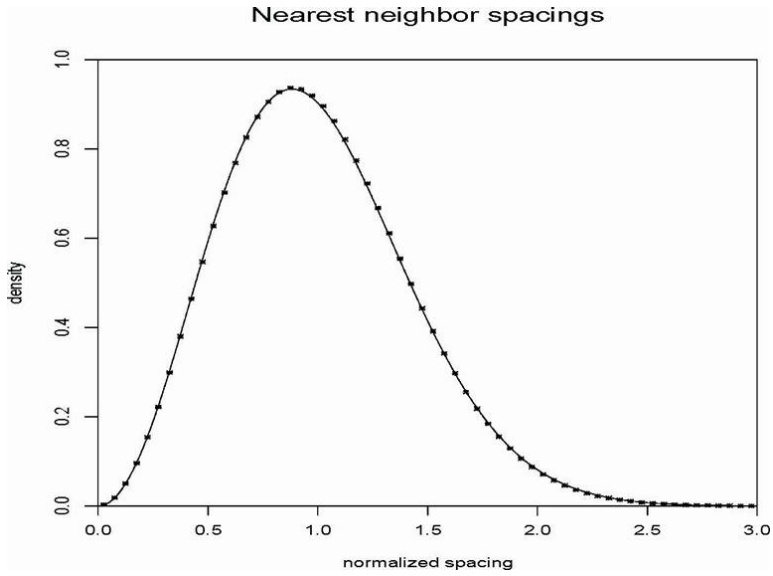


Figure 3.4: Nearest neighbour spacings: dots for ζ, line for Gaussian Unitary Ensemble.

4 Integral lattices

Figure 4.1: Hermann Minkowski (1864-1909)

Hermann Minkowski (1864-1909) was the pioneering inventor of the *geometry of numbers*. He used it mainly to prove number-theoretic results. Today, lattices and their short vectors are central algorithmic tools in computer algebra, cryptography, computational number theory, and other areas.

For the definition, we have linearly independent vectors $a_1, \ldots, a_n \in \mathbb{R}^n$. Then

$$\begin{aligned} L &= \sum_{1 \le i \le n} a_i \mathbb{Z} \\ &= \text{set of integer linear combinations of } a_1, \ldots, a_n \end{aligned}$$

is the *lattice* generated by $a_1 \ldots, a_n$. Furthermore,

$$\begin{aligned} \lambda(L) &= \text{length of a shortest nonzero vector in } L \\ &= \min\{\|x\|_2 \colon x \in L \setminus \{0\}\} \end{aligned}$$

is the first Minkowski minimum of L, in the Euclidean norm $||x||_2 = (\sum_i x_i^2)^{1/2}$.

The famous basis reduction algorithm of []lenlen82 computes efficiently a short nonzero vector $x \in L$ with

$$\|x\|_2 \le 2^{(n-1)/2} \lambda(L).$$

It is natural to ask for smaller approximation factors, and many variations of this method have been found, and the complexity of variants of the problem ranges from NP-complete via "not NP-complete under standard assumptions" to polynomial time as above. The 1982 paper solved the long-standing open problem of factoring univariate polynomials over the rational numbers in polynomial time. Surveys of this active research area are in [17] and [16].

In the *subset sum problem*, we are given positive integers $a_1, \ldots, a_n, s$ and ask whether s is the sum of a subset of the a's, that is, if there are $x_1, \ldots, x_n \in \{0, 1\}$ with

$$\sum_{1 \le i \le n} a_i x_i = s.$$

This problem is NP-complete.

A connection between the subset sum problem and short vectors comes from turning a solution of the subset sum problem into a short vector in the lattice $L \subseteq \mathbb{Z}^{n+1}$ generated by the rows $r_1, \ldots, r_{n+1} \in \mathbb{Z}^{n+1}$ of the matrix

$$\begin{matrix} 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_n \\ 0 & 0 & \cdots & 0 & s \end{matrix}$$

Namely, let $(x_1, \ldots, x_n) \in \{0, 1\}^n$ be a solution of the subset sum problem. Then

$$v = \sum_{1 \le i \le n} x_i r_i + r_{n+1} = (x_1, \ldots, x_n, 0) \in L$$

is a nonzero vector with $\|v\|_2 \le \sqrt{n}$, which is small since the a_i are typically large numbers.

Some special cases of the subset sum problem are easy, for example when $a_i = 2^{i-1}$, where x is just the binary representation of s. After the revolutionary introduction of public-key cryptography by [5], the first concrete such method was the *subset sum cryptosystem* of [8]. In the standard subset sum problem, they choose "easy" $b_1, \ldots, b_n$, random c and m and let $a_i = cb_i \mod m$. In this modular problem, the a_i do not "look" kind of special even if the b_i are the powers of 2, as above. For a while, this was the public-key cryptosystem of choice, even after the invention of RSA. However, looks are deceiving.

[22] showed that this Emperor's clothes are transparent, by constructing a lattice where the short vector, as discussed above, shines through the disguise attempted by c and m. Needless to say, this does not affect the status of NP-completeness, but only works for "easy" b_i. Today lattices are a basic tool in cryptography, both for making and for breaking codes.

5 Mertens' Conjecture

Our final example is a conjecture that Franz Carl Joseph Mertens (1840-1927) stated in 1897 and which was disproved in 1985. The well-known Möbius function μ in number theory is defined for a positive integer n by $\mu(1) = 1$ and

$$\mu(n) = \begin{cases} (-1)^r & n \text{ squarefree with } r \text{ prime factors,} \\ 0 & n \text{ not squarefree.} \end{cases}$$

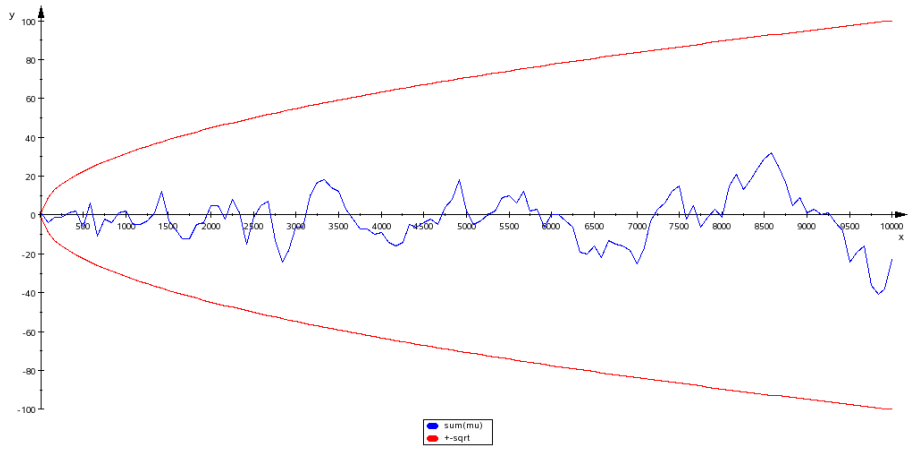


Figure 5.1: Mertens' function up to 10000.

The Mertens function M is its summation: $M(x) = \sum_{n \le x} \mu(n)$.

n	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\mu(n)$	1	−1	−1	0	−1	1	−1	0	0	1	−1	0	−1	1	1
$M(n)$	1	0	−1	−1	−2	−1	−2	−2	−2	−1	−2	−2	−3	−2	−1

Table 5.1: The values of $\mu(n)$ and $M(n)$ for $n \le 15$.

Experiments led [15] to conjecture that

$$|M(x)| \le \sqrt{x} \text{ for all } x \in \mathbb{N}.$$

For a random walk along the line with equiprobable steps $+1$ and -1, the expected (absolute) deviation from the mean 0 is $\sqrt{x}$. Thus for a random function in place of μ, the conjecture holds with high probability. Mertens' paper contains a double-page fold-out table of values as in Table 5.1, and his resignating remark: "Leider begegnet der allgemeine Beweis dieser Eigenschaft beinahe unübersteiglichen Schwierigkeiten."[2] A similar conjecture had been made in 1885 by Stieltjes. [15] showed that his conjecture implies that Riemann Hypothesis.

Almost one hundred years later [19] put the conjecture to rest. They used basis reduction in a lattice in $\mathbb{R}^{70}$ to disprove Mertens' conjecture:

$$\exists x \le \exp(10^{65}) \quad |M(x)| > 1.065\sqrt{x},$$

The current state of the art is in [13]:

$$\exists x \le \exp(1.6 \cdot 10^{40}) \quad |M(x)| > \sqrt{x},$$

$$\frac{M(x)}{\sqrt{x}} \begin{cases} > 1.218, \\ < -1.299, \end{cases}$$

for some values of x. They conjecture that the latter quotient is unbounded, and in fact that

$$\exists x\colon \frac{M(x)}{\sqrt{x}} = \Omega_{\pm}(\sqrt{\ln \ln \ln x}).$$

[2] Unfortunately the general proof of this property meets with almost unsurmountable difficulties.

References

[1] M. Bednara, M. Daldrup, J. Shokrollahi, J. Teich, and J. von zur Gathen. Reconfigurable implementation of elliptic curve crypto algorithms. In *Proc. of The 9th Reconfigurable Architectures Workshop (RAW-02)*, pages 157–164, Fort Lauderdale FL, USA., April 2002.

[2] M. Bednara, M. Daldrup, J. Shokrollahi, J. Teich, and J. von zur Gathen. Tradeoff analysis of FPGA based elliptic curve cryptography. In *Proc. of the IEEE International Symposium on Circuits and Systems (ISCAS-02)*, volume V, pages 797–800, Scottsdale, Arizona, U.S.A., May 2002.

[3] O. Bonorden, J. von zur Gathen, J. Gerhard, O. Müller, and M. Nöcker. Factoring a binary polynomial of degree over one million. 35(1):16–18, 2001. Url: `http://www-math.upb.de/~aggathen/Publications/bongat01.pdf`.

[4] D. G. Cantor. On arithmetical algorithms over finite fields. *J. Combin. Theory Ser. A*, 50(2):285–300, 1989.

[5] W. Diffie and M. E. Hellman. New directions in cryptography. IT-22(6):644–654, November 1976.

[6] M. Fürer. Fast integer multiplication. In *Proceedings of the thirty-ninth annual ACM symposium on Theory of computing*.

[7] C. Grabbe, M. Bednara, J. Shokrollahi, J. Teich, and J. von zur Gathen. Fpga designs of parallel high performance $gf(2^233)$ multipliers. In *Proc. of the IEEE International Symposium on Circuits and Systems (ISCAS 2003), vol. II*, pages 268–271. Bangkok, Thailand, 2003.
Url: `http://www-math.uni-paderborn.de/~aggathen/Publications/grabed03.pdf`.

[8] M. E. Hellman and R. C. Merkle. Hiding information and signatures in trap door knapsacks. *IEEE Trans. on Information Theory*, IT-24(5):525–530, 1978.

[9] F. Hess, S. Pauli, and M. Pohst, editors. *Algorithmic Number Theory*, number 4076, Berlin / Heidelberg, 2006.

[10] E. Kaltofen and V. Shoup. Subquadratic-time factoring of polynomials over finite fields. pages 398–406, 1995.

[11] E. Kaltofen and V. Shoup. Fast polynomial factorization over high algebraic extensions of finite fields. pages 184–188, 1997.

[12] A. Karatsuba and Yu. Ofman. Умножение миогозиачиых чисел на автоматах. *Доклады Ацадемий Наук СССР*, 145(2):293–294, 1962. Translation: A. Karatsuba and Yu. Ofman. Multiplication of multidigit numbers on automata. *Soviet Physics Doclady*, 7:595–596, 1963.

[13] T. Kotnik and H. te Riele. The mertens conjecture revisited. In Hess et al. [9], pages 156–167.

[14] A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász. Factoring polynomials with rational coefficients. *Math. Ann.*, 261(4):515–534, 1982.

[15] F. Mertens. Über eine zahlentheoretische Function. *Sitzungsberichte der Akademie der Wissenschaften, Wien, Mathematisch-Naturwissenschaftliche Classe* 106, 761–830, 1897.

[16] D. Micciancio and S. Goldwasser. *Complexity of Lattice Problems: A Cryptographic Perspective*, volume 671. Kluwer Academic Publishers, March 2002.

[17] P. Q. Nguyen and J. Stern. The two faces of lattices in cryptology. In J. H. Silverman, editor, *Cryptography and Lattices, International Conference (CaLC 2001),* Providence RI, number 2146, pages 146–180, 2001.

[18] A. M. Odlyzko and A. Schönhage. Fast algorithms for multiple evaluations of the Riemann zeta function. *Trans. Amer. Math. Soc.*, 309(2):797–809, 1988.

[19] A. M. Odlyzko and H. J. J. te Riele. Disproof of the Mertens conjecture. *J. Reine Angew. Math.*, 357:138–160, 1985.

[20] B. Riemann. Ueber die anzahl der primzahlen unter einer gegebenen grösse. *Monatsberichte der Berliner Akademie*, pages 671–680, November 1859.

[21] A. Schönhage and V. Strassen. Schnelle Multiplikation grosser Zahlen. *Computing (Arch. Elektron. Rechnen)*, 7:281–292, 1971.

[22] A. Shamir. A polynomial-time algorithm for breaking the basic Merkle-Hellman cryptosystem. *IEEE Trans. Inform. Theory*, 30(5):699–704, 1984.

[23] J. von zur Gathen and J. Gerhard. *Modern computer algebra*. Cambridge University Press, New York, 1999.

[24] J. von zur Gathen and J. Shokrollahi. Efficient FPGA-based Karatsuba multipliers for polynomials over $\mathbb{F}_2$. In B. Preneel and S. Tavares, editors, *Selected Areas in Cryptography (SAC 2005)*, number 3897, pages 359–369, Kingston, ON, Canada, August 2005.

[25] J. von zur Gathen and V. Shoup. Computing Frobenius maps and factoring polynomials. *Comput. Complexity*, 2(3):187–224, 1992.

On the computation of the class numbers of real abelian fields

Tuomas Hakkarainen

TUCS & dpt. of Mathematics
University of Turku, Finland

Abstract

We give a procedure to search for odd prime divisors of class numbers of real abelian fields, excluding primes dividing the degree of the field. We show an extract of our table of odd primes < 10000 that divide the class numbers of fields of conductor < 2000. Cohen–Lenstra heuristics allow us to conjecture that no larger prime divisors should exist. Previous computational results have been mainly limited to prime power conductors.

Introduction

- Van der Linden [5] showed that the class number $h_K = 1$ for real fields K of prime conductor < 163 and $h_K = 4$ for $K = \mathbf{Q}(\zeta_{163} + \zeta_{163}^{-1})$. For composite conductors he presented results for some fields up to conductor 200. These results are the best known and it is difficult to go beyond these limits.
- Recently Schoof [6] computed class number divisors < 80000 for fields of prime conductor < 10000 and provided heuristics that predict these divisors to be class numbers.
- We apply Leopoldt's results on the rational decomposition of the class group and propose a method to compute class number divisors for fields of arbitrary conductor.

Notation

G: the Galois group of K
g: the order of G
f: the conductor of K
χ: a character of K
$\widetilde{\chi}$: a rational conjugacy class of characters ($\widetilde{\chi} = \{\chi^k \mid (k, g_\chi) = 1\}$)
g_χ: the order of χ
f_χ: the conductor of χ
K_χ: the subfield of K with character group $\langle\chi\rangle$
G_χ: the Galois group of K_χ
$\Phi_n(x)$: the nth cyclotomic polynomial

1 Leopoldt's result

Leopoldt in his thesis [4] presented an arithmetic characterization of the real abelian fields, continuing work of Hasse. A main idea was to apply the Wedderburn decomposition of the rational (and p-adic) Galois group ring to the group of units of an abelian field. Leopoldt was able to reduce the study of the class groups of the abelian fields with noncyclic Galois group essentially to the cyclic subfields corresponding to the classes of conjugate characters of the field.

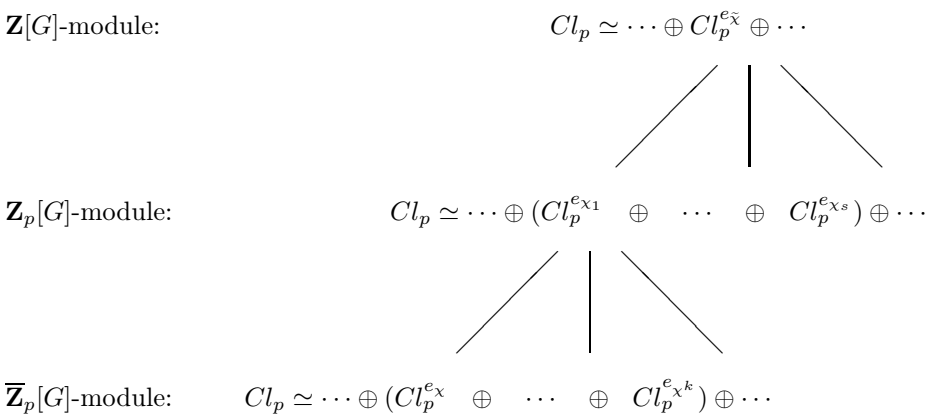


Figure 1.1: Different levels of decomposition of the p-class group $Cl_p, p \nmid g$

- Let E_χ be a subgroup of units of K_χ of norm ± 1 to any proper subfield and F_χ an explicitly given subgroup (the χ-cyclotomic units; see [4]) of E_χ. Both groups (modulo torsion ± 1) are cyclic $\mathbf{Z}[G_\chi]$-modules that only depend on $\widetilde{\chi}$.
- The class number admits the decomposition

$$h_K = \frac{Q_K}{Q_G} \prod_{\widetilde{\chi}} h_\chi$$

  with the product running through the nontrivial rational conjugacy classes of characters and $h_\chi = [E_\chi : F_\chi]$. The rational integers Q_K and Q_G only contain primes dividing g.

2 The method

The outline of the method is as follows. We first put an upper bound for the primes p to be tested. We assume that p is odd and not a divisor of the degree of K. We give a necessary but not sufficient condition for the divisibility of the class number and check the condition for all such primes and all the h_χ. We are left with a small set of primes to be checked further.

Then we present an additional technique to sieve out the primes not dividing the class number. Finally, the remaining primes are proved to be actual class number divisors. This three-part verification procedure is necessary in order to preserve efficiency.

- This procedure is not capable of testing the divisibility by a higher power of p. By using similar methods and some elementary group theory, we have given a generalization of the method to verify this also. We used an idea of G. and M.-N. Gras [2].

2.1 Schwarz's method

Schwarz [7] provided the following condition to effectively test the p-divisibility. Let $\zeta_n = e^{2\pi i/n}$.

Proposition 7 (Schwarz)**.** *Let*

$$\lambda : (\mathbf{Z}/f_\chi\mathbf{Z})^\times \to \{0, \ldots, g_\chi - 1\}$$

be defined by $\chi(i) = \zeta_{g_\chi}^{\lambda(i)}$. *If the prime* $p \nmid 2f_\chi g_\chi$ *divides the* h_χ*-part of the class number of* K_χ*, then*

$$\mathrm{GCD}_{\mathbf{F}_p[x]}\Bigg(\sum_{\substack{i=1 \\ (i,f_\chi)=1}}^{f_\chi - 1} a_i x^{\lambda(i)}, \Phi_{g_\chi}(x) \Bigg) \neq \overline{1},$$

where a_i *are certain rational integers.*

- This condition is efficient to check. In the computations we performed, for any h_χ, the condition was satisfied on average for only 0 to 2 primes from all the odd primes < 10000 not dividing g_χ.

2.2 Second condition for the p-divisibility

To check the remaining primes and the odd primes $p \mid f_\chi$, we continue as follows. We generalize an idea of van der Linden [5].

The group $(E_\chi/F_\chi)_p$ of elements of order p is an $\mathbf{F}_p[G_\chi]$-module isomorphic to $(E_\chi^p \cap F_\chi)/F_\chi^p$. If nontrivial, it must contain a minimal submodule of F_χ/F_χ^p. Since the intersection of two minimal submodules is zero, the p-exponent of h_χ is at least the number of minimal submodules F_i/F_χ^p satisfying $F_i \subseteq E_\chi^p$. Denote by η the generator of $F_\chi/\{\pm 1\}$.

Proposition 8. *Assume that* $p \equiv 1 \pmod{g_\chi}$. *The minimal* $\mathbf{F}_p[G_\chi]$*-submodules of* F_χ/F_χ^p *are* $\langle \eta^{\Phi_{g_\chi}(\sigma)/(\sigma - i)} \rangle$, *where* i *runs through all the zeros of* $\Phi_{g_\chi}(x) \pmod p$ *and* σ *is a generator of* G_χ.

- The proposition generalizes easily to any odd prime p not dividing g_χ.
- To check the condition, we choose a prime $q \equiv 1 \pmod{p\, f_\chi}$ and some $b \in \mathbf{Z}$ satisfying the conditions $b^{f_\chi} \equiv 1 \pmod q$, $b \not\equiv 1 \pmod q$. Then $\zeta_{f_\chi} \equiv b \pmod{\mathcal{Q}}$ for some prime ideal $\mathcal{Q}$ above q in $\mathbf{Q}(\zeta_{f_\chi})$. By writing $\eta^{\Phi_{g_\chi}(\sigma)/f_i(\sigma)}$ as a rational function $r(\zeta_{f_\chi})$, we examine whether

$$r(b)^{\frac{q-1}{p}} \equiv 1 \pmod q. \tag{2.1}$$

If this congruence holds, we choose another pair (q, b) and repeat the test. Passing the test for many pairs is a strong evidence for the p-divisibility; failing the test means that $p \nmid h_\chi$.

2.3 Final verification

We show how to verify that $p \mid h_\chi$, following Gras [2]. For some $\alpha = \eta^{\Phi_{g_\chi}(\sigma)/f_i(\sigma)}$ satisfying (2.1) for many pairs (q, b), we want to prove that α is a pth power. This is equivalent to showing that $\sqrt[p]{\alpha}$ is an element of K_χ. As a unit of K_χ, the element α has g_χ conjugates in K_χ which we all compute. We are able to calculate a real approximation of α and its conjugates α^σ.

If the polynomial $m_p(x) = \prod_\sigma (x - \sqrt[p]{\alpha^\sigma})$ has integral coefficients, then α is a pth power; by rounding off the coefficients we obtain the minimum polynomial of $\sqrt[p]{\alpha}$ if the precision is adequate. By checking whether $m_p(x) \mid m(x^p)$, where $m(x)$ is the minimum polynomial of α, we arrive at the final conclusion.

The verification step is practical only for fields of relatively small degree, but it was sufficient in all the cases we confronted. In a recent class number computation method by Aoki and Fukuda [1], a more efficient verification method is presented.

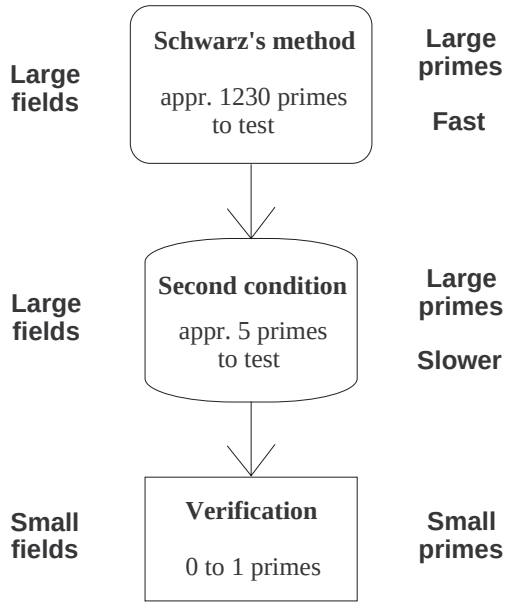


Figure 2.2: Scheme of computation for primes $p < 10000$ for any h_χ

3 Cohen-Lenstra heuristics

Cohen and Lenstra gave conjectural heuristic assumptions on the properties of finite modules over direct products of Dedekind domains. Schoof [6] predicted, based on a speculative extension of the Cohen–Lenstra heuristics, that the class numbers of real abelian fields of prime conductor most likely are relatively small. This generalizes to the fields of arbitrary conductor without difficulty. We list some "probabilities" concerning our computations that arise from this heuristic approach.

- There are a total of 11018 different h_χ for the fields of conductors < 2000. The predicted number of nontrivial h_χ-parts (excluding the primes dividing $2g_\chi$) would be 443. We found 231 nontrivial h_χ in the computations (49 of those were with f_χ prime; they can also be found in the tables in [6]).

- The "probability" that there are no prime divisors > 10000 of any h_χ is at least 91%. Since the largest prime divisor we found is 379 and since the prime divisors found were usually of the form $p = kg_\chi + 1$ with k small, we find it reasonable to believe that our table is a table of class number parts h_χ (omitting the prime divisors $p \mid 2g_\chi$ from study).

4 Results of the computation

We computed the prime divisors $2 < p < 10000$, $p \nmid g_\chi$ of any h_χ for fields up to conductor 2000. The complete table is in [3]; we provide here the class number divisors for the fields of composite conductor < 1000. The conjugacy classes of characters are represented by characters of $(\mathbf{Z}/\mathbf{f}_\chi\mathbf{Z})^\times$.

f_χ	χ	g_χ	p
212	$\omega_4^1\chi_{53}^{13}$	4	5
316	$\omega_4^1\chi_{79}^{39}$	2	3
321	$\chi_3^1\chi_{107}^{53}$	2	3
427	$\chi_7^3\chi_{61}^{15}$	4	5
469	$\chi_7^3\chi_{67}^{33}$	2	3
473	$\chi_{11}^5\chi_{43}^{21}$	2	3
481	$\chi_{13}^2\chi_{37}^4$	18	19
551	$\chi_{19}^9\chi_{29}^7$	4	5
556	$\omega_4^1\chi_{139}^{23}$	6	7
568	$\chi_8^1\chi_{71}^{14}$	10	11
	$\omega_4^1\chi_8^1\chi_{71}^{35}$	2	3
629	$\chi_{17}^8\chi_{37}^2$	18	19
	$\chi_{17}^4\chi_{37}^{18}$	4	5
651	$\chi_3^1\chi_7^3\chi_{31}^6$	10	11
652	$\omega_4^1\chi_{163}^9$	18	19
676	$\omega_4^1\chi_{169}^3$	52	53
692	$\omega_4^1\chi_{173}^{43}$	4	5
697	$\chi_{17}^8\chi_{41}^{20}$	2	3
703	$\chi_{19}^9\chi_{37}^1$	36	37
	$\chi_{19}^3\chi_{37}^9$	12	13
728	$\chi_8^1\chi_7^3\chi_{13}^3$	4	5
753	$\chi_3^1\chi_{251}^{25}$	10	11
756	$\omega_4^1\chi_{27}^2\chi_7^1$	18	19

f_χ	χ	g_χ	p
763	$\chi_7^3\chi_{109}^9$	12	13
779	$\chi_{19}^9\chi_{41}^1$	40	41
785	$\chi_5^2\chi_{157}^{78}$	2	3
793	$\chi_{13}^1\chi_{61}^{55}$	12	37
808	$\omega_4^1\chi_8^1\chi_{101}^{25}$	4	5
817	$\chi_{19}^9\chi_{43}^{21}$	2	5
819	$\chi_9^1\chi_7^1\chi_{13}^2$	6	7
832	$\omega_4^1\chi_{64}^1\chi_{13}^3$	16	7^2
869	$\chi_{11}^5\chi_{79}^1$	78	79
889	$\chi_7^3\chi_{127}^{21}$	6	7
892	$\omega_4^1\chi_{223}^{111}$	2	3
916	$\omega_4^1\chi_{229}^{57}$	4	5
923	$\chi_{13}^3\chi_{71}^7$	20	61
928	$\omega_4^1\chi_{32}^1\chi_{29}^7$	8	17
935	$\chi_5^1\chi_{11}^5\chi_{17}^4$	4	5
940	$\omega_4^1\chi_5^2\chi_{47}^{23}$	2	3
944	$\omega_4^1\chi_{16}^1\chi_{59}^{29}$	4	5
976	$\omega_4^1\chi_{16}^1\chi_{61}^{15}$	4	5
980	$\omega_4^1\chi_5^1\chi_{49}^6$	28	29
985	$\chi_5^2\chi_{197}^{98}$	2	3
988	$\omega_4^1\chi_{13}^2\chi_{19}^3$	6	7
993	$\chi_3^1\chi_{331}^{165}$	2	3
999	$\chi_{27}^2\chi_{37}^{16}$	9	37

Conclusion

The class numbers of the real abelian fields of composite conductor seem to show statistical behaviour similar to the class numbers of the fields of prime conductor.

References

[1] M. Aoki, T. Fukuda, *An algorithm for computing p-class groups of abelian number fields*, Algorithmic Number Theory, Lecture Notes in Comput. Sci., **4076**, Springer, Berlin (2006), pp. 56–71

[2] G. and M.-N. Gras, *Calcul du nombre de classes et des unités des extensions abéliennes réelles de* **Q**, Bull. Sci. Math. (2) **101** (1977), no. 2, pp. 97–129.

[3] T. Hakkarainen, *On the computation of class numbers of real abelian fields*, submitted.

[4] H. W. Leopoldt, *Über Einheitengruppe und Klassenzahl reeller abelscher Zahlkörper*, Abh. Deutsch. Akad. Wiss. Berlin. Kl. Math. Nat. 1953, no. 2 (1954), 48 pp.

[5] F. van der Linden, *Class number computations of real abelian number fields*, Math. Comp. **39** (1982), pp. 693–707.

[6] R. Schoof, *Class numbers of real cyclotomic fields of prime conductor*, Math. Comp. **72** (2003), pp. 913–937.

[7] W. Schwarz, *Über die Klassenzahl abelscher Zahlkörper*, PhD Thesis, University of Saarbrücken (1995), 125 pp.

How to Compute the First Digit of Fibonacci Numbers in Polynomial Time (Extended Abstract)

Mika Hirvensalo[1*] *Juhani Karhumäki*[1]
Alexander Rabinovic[2]

[1]Department of Mathematics
University of Turku
FIN-20014 Turku, Finland
and TUCS–Turku Centre For Computer Science
{mikhirve,karhumak}@utu.fi

[2]Tel Aviv University
School of Computer Science
Ramat Aviv, Tel Aviv 69978, Israel
rabinoa@post.tau.ac.il

1 Introduction

Recursion $F_0 = 0$, $F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$ generates the famous *Fibonacci numbers*. This is one of the oldest and maybe the most well-known recursion. Various aspects of the Fibonacci numbers have been studied for many centuries, and their number-theoretic properties have been explored deeply. The basic knowledge on Fibonacci numbers includes the fact that the ratio F_{n+1}/F_n of two consecutive Fibonacci numbers tends to the *golden ratio* $\varphi = \frac{1+\sqrt{5}}{2}$, and that a closed form for F_n can be expressed as

$$F_n = \frac{1}{\sqrt{5}}(\varphi^n - (1-\varphi)^n). \tag{1.1}$$

Although the value of F_n can be computed by the recursion using $n-1$ additions, equation (1.1) reveals clearly that the magnitude of F_n is exponential in n. It follows that the value of F_n it is out of the capacity of modern computers in practice. Numbers such as $n_1 = 5 \cdot 10^{87}$ are enormously large, but thinking about the decimal expansion, number n_1 can be regarded as a string beginning with 5 and followed by 87 zeros. Thus such a number is rather small *as an algorithmic object*. On the other hand, F_{n_1} is enormous both as a number and as an algorithmic object: It is not even possible to write down the decimal expansion of F_{n_1}, since number of digits required would exceed 10^{87}, the estimated number of the particles in the universe.

Having this situation a natural question is: Can we compute some partial information about F_n in polynomial time, for example its length or the first digit at a given base (at least 3)?

*Supported by the Academy of Finland under grant 208797

It is easy to see that the last, or even the last k, for a fixed k, digits of F_n can be computed in polynomial time. Indeed, such values form an ultimately periodic sequence of numbers, so that the threshold and the period can be computed in a constant time. Hence the problem reduces to the computation $n \mapsto n \pmod p$, where p is the precomputed period. Therefore it can be done in linear time.

On the other hand, to compute even the length of F_n in polynomial time is not obvious. We shall show, that this can be done in polynomial time. It is an easy exercise to modify the algoritm for computing the length to get a polynomial time algorithm for computing the first digit of F_n (see [2]), hence we will omit it from this extended abstract, and only treat the algorithm for computing the length, thus slightly violating the title. The algorithm itself is not complicated, nor difficult to analyze. However, to prove its correctness seems to require deep results on transcendental numbers. This is an extension of a previous work [2], where a simpler function $n \mapsto 2^n$ instead of $n \mapsto F_n$ was considered.

To compute a fixed number of first digits of F_n does no seem to be essentially more difficult question. The situation, however, changes if we ask to compute the "middle" digit of F_n. We do not know how to do it in polynomial time.

For any real number x, notation $\lfloor x \rfloor$ stands for the largest integer M for which inequality $M \leq x$ holds, and $\log_d x$ stands for the d-ary logarithm of x. We also use the standard notation $\ln x$ for the natural logarithm of x.

The *d-ary representation of M* is denoted by $M_{\mathbf{d}}$, and the *length* of d-ary representation of M is defined to be the length of string $M_{\mathbf{d}}$ and denoted by $|M_{\mathbf{d}}|$. Equation $|M_{\mathbf{d}}| = \lfloor \log_d M \rfloor + 1$ is obvious. In the case $d = 3$ we say that $M_{\mathbf{3}}$ is the *ternary* representation of M.

2 The Idea of the Algorithm

In this section we represent the idea of the algorithm for computing $|(F_n)_{\mathbf{3}}|$. The algorithm for computing the first symbol of $(F_n)_{\mathbf{3}}$ is similar.

Without loss of generality we can assume that the input n is given in binary representation, so the *size* of input is $|n_{\mathbf{2}}| = \Theta(\ln n)$. We can therefore state the problem of computing F_n as follows: given an input $n_{\mathbf{2}} \in \{0,1\}^*$, compute $(F_n)_{\mathbf{3}} \in \{0,1,2\}^*$. Hence the size of the input is $\Theta(\ln n)$, whereas the output size is $\Theta(n)$, which is exponential in the input size, and it follows that the problem is intractable.

On the other hand, computing $n_{\mathbf{2}} \mapsto |(F_n)_{\mathbf{3}}|$ is a very different problem. Now the output should be the ternary length of F_n, or, from the algorithmic point of view, a *string* which represents the length. Again, without loss of generality, we can require the output in binary, which means that the output size would be $O(\ln n)$, of the same order than the size of the input.

Equation

$$|(F_n)_{\mathbf{3}}| = \lfloor \log_3 F_n \rfloor + 1 = \lfloor \log_3 \frac{1}{\sqrt{5}} + n \log_3 \varphi + \log_3 (1 - (\frac{1-\varphi}{\varphi})^n) \rfloor + 1 \quad (2.2)$$

gives the idea for computing the length, but the straightforward utilization of (2.2) contains at least three problematic features.

First, knowing $\log_3 \frac{1}{\sqrt{5}}$ and $\log_3 \varphi$ precisely enough allows us to compute an approximation of $\log_3 \frac{1}{\sqrt{5}} + n \log_3 \varphi$, but it must be noted that we should be able to compute $\log_3 \varphi$ at least up to precision $\frac{1}{n}$, since for a larger imprecision the

outcome could clearly be incorrect. It turns out that this problem is very easy to handle, and we omit the details here.

The second problem is the term $r(n) = \log_3(1 - (\frac{1-\varphi}{\varphi})^n)$. It is clear that this term tends to zero exponentially fast as n grows, but we should be able to take its effect into account when computing the floor function.

The third, and a more severe problem is, that even if we could omit $r(n)$ and just to compute $\lfloor \log_3 \frac{1}{\sqrt{5}} + n \log_3 \varphi \rfloor + 1$, approximations for $\log_3 \frac{1}{\sqrt{5}}$ and $\log_3 \varphi$ do not directly offer any tools to compute $\lfloor n \log_3 \frac{1}{\sqrt{5}} + \log_3 \varphi \rfloor$, no matter how precise the approximation are! To see this, let β_n, $n = 1, 2, 3, \ldots$ be a sequence of irrational numbers, and b_n, $n = 1, 2, 3, \ldots$, be a sequence of their very precise rational approximations, $|b_n - \beta_n| \ll 1$ for each n. Let us take some n, and assume, for instance, that $b_n < \beta_n$. If the interval (b_n, β_n) happens to contain an integer M, then $\lfloor b_n \rfloor = M - 1$, whereas the correct value $\lfloor \beta_n \rfloor = M$. In other words, if we do not have apriori knowledge on the distance between β_n and the nearest integer M, we cannot certainly find the value $\lfloor \beta_n \rfloor$ by using only an approximation b_n of β_n. In the next section, we explain how to use deep results of Alan Baker to solve the two latter problems.

3 Baker's Result

The extra information we use for computing $|(F_n)_{\mathbf{3}}|$ is provided in the following theorem, the proof can be found in [1].

Theorem 1 (A. Baker, 1966)**.** *Let $\alpha_1, \ldots, \alpha_k$ be non-zero algebraic numbers with degrees at most d and heights at most A. Further, let $\beta_0, \ldots, \beta_k$ be algebraic numbers with degrees at most d and heights at most $B \geq 2$. Then for*

$$\Lambda = \beta_0 + \beta_1 \log \alpha_1 + \ldots + \beta_k \log \alpha_k$$

we have either $\Lambda = 0$ or $|\Lambda| > B^{-C}$, where C is an effectively computable number depending only on k, d, A, and the branch of the logarithm chosen.

Now we choose $k = 3$, $\beta_0 = 0$, $\beta_1 = N \in \mathbb{N}$, $\beta_2 = -1$, $\beta_3 = -n \in \mathbb{N}$, $\alpha_1 = 3$, $\alpha_2 = \frac{1}{\sqrt{5}}$, and $\alpha_3 = \varphi$ to get $\Lambda = M \ln 3 - \ln \frac{1}{\sqrt{5}} - n \ln \varphi$. It is easy to see that $\Lambda \neq 0$ always, and by using Baker's theorem, we can efficiently find constants C_1 and C_2 such that

$$\left| M - \log_3 \frac{1}{\sqrt{5}} - n \log_3 \varphi \right| \geq \frac{1}{C_1 n^{C_2}} \tag{3.3}$$

for all $M, n \in \mathbb{N}$ (technical details are omitted here).

Inequality (3.3) shows that $\log_3 \frac{1}{\sqrt{5}} + n \log_3 \varphi$ is bounded away from any positive integer M by 1/polynomial(n). This information is enough to compute

$$|(F_n)_{\mathbf{3}}| = \lfloor \log_3 \frac{1}{\sqrt{5}} + n \log_3 \varphi + \log_3(1 - (\frac{1-\varphi}{\varphi})^n) \rfloor + 1$$

in polynomial time, since we know that the last term in floor function tends to zero exponentially (technical details omitted).

References

[1] A. Baker. *Transcendental number theory.* Cambridge University Press, London, 1975.

[2] M. Hirvensalo and J. Karhumäki. Computing partial information out of intractable one—the first digit of 2^n at base 3 as an example. In *Mathematical foundations of computer science 2002*, volume 2420 of *Lecture Notes in Comput. Sci.*, pages 319–327. Springer, Berlin, 2002.

Lower bounds on the period of some pseudorandom number generators

Pär Kurlberg[1] *Carl Pomerance*[2]

[1]Department of Mathematics
KTH
SE-100 44 Stockholm
Sweden
kurlberg@math.kth.se

[2]Mathematics Department
Dartmouth College
Hanover, NH 03755-3551
U.S.A.
carl.pomerance@dartmouth.edu

1 Introduction

We are interested in obtaining lower bounds on the periods of two standard pseudorandom number generators from number theory—the linear congruential generator, first introduced by D. H. Lehmer, and the so called power generator. For the former, given integers e, b, n (with $e, n > 1$) and a seed $u = u_0$, we compute the sequence

$$u_{i+1} \;=\; eu_i + b \pmod{n}.$$

For the power generator, given integers $e, n > 1$ and a seed $u = u_0 > 1$, we compute the sequence

$$u_{i+1} \;=\; u_i^e \pmod{n}$$

so that $u_i = u^{e^i} \pmod{n}$. The particular case $e = 2$ is known as the Blum–Blum–Shub (BBS) generator [1]. This generator is not only simple to compute, but it has certain attractive aspects from a cryptographic perspective, especially when n is the product of two large primes that are both congruent to 3 modulo 4.

These two generators give rise to (ultimately) periodic sequences, and it is of interest to compute the periods—a useful pseudorandom number generator should have a long period. Further, to show that the sequence satisfies various equidistribution properties, exponential sum techniques are often applicable provided that the period is sufficiently large. Moreover, if the period is very short when n is a product of two primes, certain cycling attacks on the RSA public key system apply.

In this note[1] we consider the problem of the period statistically as n varies, either over all integers, or over certain subsets of the integers that are used in practice, namely the set of primes and the set of "RSA moduli," that is, numbers which are the product of two primes of the same magnitude.

If $(e, n) = 1$, then the sequence $e^i \pmod{n}$ is purely periodic and its period is the least positive integer k with $e^k \equiv 1 \pmod{n}$. We denote this order as $\ell_e(n)$. If

[1]The results presented here summarise results obtained by the authors in [11].

$(e, n) > 1$, the sequence $e^i \pmod n$ is still (ultimately) periodic, with the period given by $\ell_e(n_{(e)})$ where $n_{(e)}$ is the largest divisor of n that is coprime to e. In what follows we shall denote $\ell_e(n_{(e)})$ by $\ell_e^*(n)$. The periods of both the linear congruential and power generators may be described in terms of this function. For the linear congruential generator we have $u_i = e^i(u + b(e-1)^{-1}) - b(e-1)^{-1} \pmod n$ when $e-1$ is coprime to n, so that if we additionally have $u+b(e-1)^{-1}$ coprime to n, the period is exactly $\ell_e^*(n)$. In general, the period is always a divisor of $\ell_e^*(n)(e-1, n)$.

For the power generator, the period is exactly $\ell_e^*(\ell_u^*(n))$. For most of this note we shall assume that u is chosen so that $\ell_u^*(n)$ is as large as possible for a given modulus n. This maximum, following Carmichael, is denoted $\lambda(n)$ and equals the order of the largest cyclic subgroup of $(\mathbf{Z}/n\mathbf{Z})^\times$. For the power generator, we thus will study $\ell_e^*(\lambda(n))$. Note that it is especially important to use the function ℓ_e^* rather than ℓ_e when considering the modulus $\lambda(n)$, since for $n > 2$, $\lambda(n)$ is always even, and in general, $\lambda(n)$ is divisible by the fixed number e for a set of numbers n of asymptotic density 1.

1.1 Previous work

For $n = p$ and p a prime number, the order of e modulo p has been studied extensively. In [15] Pappalardi showed that there exist $\alpha, \delta > 0$ such that $\ell_e(p) \geq p^{1/2}\exp((\log p)^\delta)$ for all but $O(x/\log^{1+\alpha} x)$ primes $p \leq x$. He also asserted, assuming the Generalized Riemann Hypothesis[2] (GRH), that if $\psi(x)$ is any increasing function tending to infinity as x tends to infinity (but not too quickly), then $\ell_e(p) > p/\psi(p)$ for all but $O(\pi(x)\log(\psi(x))/\psi(\sqrt{x}))$ primes $p \leq x$, where as usual, $\pi(x)$ is the total number of all primes $p \leq x$. A similar result is given by Erdős and Murty in [2]. Also in [2], it is shown that if $\varepsilon(x)$ is any decreasing function tending to zero as x tends to infinity, then $\ell_e(p) \geq p^{1/2+\varepsilon(p)}$ for all but $o(\pi(x))$ primes $p \leq x$, and in [8] Indlekofer and Timofeev give a similar lower bound with an explicit estimate on the number of exceptional primes. A further strengthening of this result has recently been shown by Ford [5]. Note that it follows immediately from work of Goldfeld, Motohashi, Fouvry, and Baker–Harman that there is a positive constant γ such that $\ell_e(p) > p^{1/2+\gamma}$ for a positive proportion of the primes p, with the current record being $\gamma = 0.677$.

A somewhat related new result is found in [9] where the authors show that the geometric mean for $\ell_e(p)$ for primes $p \leq x$ is at least $x^{0.58}$ for x sufficiently large. This gives a small improvement on the essentially trivial result with exponent 0.5.

The period of the power generator $u^{e^i} \pmod{pl}$ was studied in Friedlander, Pomerance and Shparlinski [6], where p, l are primes of the same magnitude. One of the results there is that this period is $> (pl)^{1-\varepsilon}$ for most choices of u, e, p, l. However, once the exponent e is fixed, say at 2, their results are weaker.

As for $\ell_e(n)$ for n a positive integer, in [12] Kurlberg and Rudnick proved that there exists $\delta > 0$ such that $\ell_e(n) \gg n^{1/2}\exp((\log n)^\delta))$ for all but $o(x)$ integers $n \leq x$ that are coprime to e. Further, in [10], Kurlberg showed that the GRH implies that for each $\varepsilon > 0$, we have $\ell_e(n) \gg n^{1-\varepsilon}$ for all but $o(x)$ integers $n \leq x$ that are coprime to n, and in [13] Li and Pomerance improved the lower bound to $\ell_e(n) \geq n(\log n)^{-(1+o(1))\log\log\log n}$, a result that is best possible.

Acknowledgement. P.K. supported in part by the Göran Gustafsson Foundation, the Royal Swedish Academy of Sciences, and the Swedish Research Council. C.P.

[2]When we refer to the Generalized Riemann Hypothesis in this note we shall mean the Riemann Hypothesis for zeta functions ζ_K, where K runs over the Kummer extensions $K = \mathbf{Q}(\sqrt[q]{e}, \exp(2\pi i/q))$, $e \geq 2$, q prime.

supported in part by the National Science Foundation (DMS-0401422). P.K. would also like to thank the organizers of ANT for their kind invitation to speak.

2 The results

2.1 The linear congruential generator

By the previous remarks, the period of the linear congruential generator, for e, b fixed and n taking values among the integers, is essentially the same as $\ell_e^*(n)$, and thus the next Theorem shows that the period is larger than $n^{1/2+\varepsilon(n)}$, respectively $n^{1/2+\gamma_1}$, for all n in a full, respectively positive, density subset of the integers.

Theorem 1. *Results on $\ell_e^*(n)$:*

1. *Suppose $\varepsilon(x)$ tends to zero arbitrarily slowly as $x \to \infty$. Then $\ell_e^*(n) \geq n^{1/2+\varepsilon(n)}$ for all but $o_\varepsilon(x)$ integers $n \leq x$.*
2. *There is a positive constant γ_1 such that $\ell_e(n) \geq n^{1/2+\gamma_1}$ for a positive proportion of the integers n.*

2.2 The power generator

As we have seen, the length of the period for the sequence (u_i) equals $\ell_e^*(\lambda(n))$ if u is chosen apropriately. We thus begin by considering $\ell_e^*(\lambda(n))$ for 3 natural classes of moduli, namely primes, the products of two primes of the same magnitude, and general integer moduli. (Note that $\lambda(p) = p - 1$.)

Theorem 2. *Results on $\ell_e^*(p-1)$:*

1. *Suppose $\varepsilon(x)$ tends to zero arbitrarily slowly as $x \to \infty$. Then $\ell_e^*(p-1) \geq p^{1/2+\varepsilon(p)}$ for all but $o_\varepsilon(\pi(x))$ primes $p \leq x$.*
2. *There is a positive constant γ_2 such that $\ell_e^*(p-1) \geq p^{1/2+\gamma_2}$ for a positive proportion of the primes p.*
3. *(GRH) For each fixed $\varepsilon > 0$ we have $\ell_e^*(p-1) > p^{1-\varepsilon}$ for all but $o_\varepsilon(\pi(x))$ primes $p \leq x$.*

Now consider RSA moduli, namely integers of the form pl where p, l are primes with $p, l \leq Q$ (where Q is an arbitrary bound). Using our results on $\ell_e^*(p-1)$, we can prove the following theorem.

Theorem 3. *Results on $\ell_e^*(\lambda(pl))$:*

1. *Suppose $\varepsilon(x)$ tends to zero arbitrarily slowly as $x \to \infty$. Then $\ell_e^*(\lambda(pl)) \geq (pl)^{1/2+\varepsilon(pl)}$ for all but $o_\varepsilon(\pi(Q)^2)$ pairs of primes $p, l \leq Q$.*
2. *There is a positive constant γ_3 such that for a positive proportion of the pairs of primes $p, l \leq Q$, we have $\ell_e^*(\lambda(pl)) \geq (pl)^{1/2+\gamma_3}$.*
3. *(GRH) For each fixed $\varepsilon > 0$ we have $\ell_e^*(\lambda(pl)) > (pl)^{1-\varepsilon}$ for all but $o_\varepsilon(\pi(Q)^2)$ pairs of primes $p, l \leq Q$.*

Instead of considering specifically RSA moduli $n = pl$, one may consider the general case where no restriction is made on the modulus n. In our next theorem we establish similar results as above for this order.

Theorem 4. *Results on* $\ell_e^*(\lambda(n))$*:*

1. *Suppose* $\varepsilon(x)$ *tends to zero arbitrarily slowly as* $x \to \infty$*. Then* $\ell_e^*(\lambda(n)) \geq n^{1/2+\varepsilon(n)}$ *for all but* $o_\varepsilon(x)$ *integers* $n \leq x$*.*
2. *There is a positive constant* γ_4 *such that* $\ell_e^*(\lambda(n)) \geq n^{1/2+\gamma_4}$ *for a positive proportion of the integers* n*.*
3. *(GRH) For each fixed* $\varepsilon > 0$ *we have* $\ell_e^*(\lambda(n)) > n^{1-\varepsilon}$ *for all but* $o_\varepsilon(x)$ *integers* $n \leq x$*.*

In fact, we can actually achieve a best possible result in part 3 of Theorem 4, namely:

Theorem 5. *If the GRH is true, then for each fixed integer* $e \geq 2$*,*

$$\ell_e^*(\lambda(n)) \;=\; n \cdot \exp(-(1+o(1))(\log\log n)^2 \log\log\log n)$$

as $n \to \infty$ *through a set of asymptotic density* 1*.*

We may also handle the situation for a general modulus n and u fixed, i.e., we do not need to make the assumption that u is chosen in an optimal way.

Theorem 6. *Assuming the GRH, for any fixed integers* $e, u \geq 2$*, the period of the sequence* $u^{e^i} \pmod n$ *is equal to*

$$n \cdot \exp(-(1+o(1))(\log\log n)^2 \log\log\log n)$$

as $n \to \infty$ *through a certain set of integers of asymptotic density* 1*.*

3 A brief outline of the arguments

We give a brief outline of the ideas used to prove the first cases of Theorems 1 and 4, namely unconditional proofs of the periods of the two generators both being slightly larger than $\sqrt{n}$ for full density subsets of the integers. For full details and proofs of the other statements we refer the reader to [11].

3.1 On the order of e modulo n

We begin by outlining the argument that $\ell_e^*(n) > n^{1/2+\varepsilon(n)}$ on a set of asymptotic density 1; that is, we prove the first item in Theorem 1.

We begin with a Lemma that allows us to replace $\ell_e^*(n)$ by $\prod_{p|n} \ell_e^*(p)$, at the price of losing a factor of at most $\lambda(n)/n$.

Lemma 7. *For any natural number* n *we have*

$$\ell_e^*(n) \;\geq\; \frac{\lambda(n)}{n} \prod_{p|n} \ell_e^*(p) \;=\; \frac{\lambda(n)}{n} \prod_{p|n,\ p\nmid e} \ell_e(p).$$

Now, although $\lambda(n)$ can be as small as $(\log n)^{c_1 \log\log\log n}$ for some $c_1 > 0$, as shown by Erdős, Pomerance, and Schmutz in [4], it readily follows from Theorem 5 of [6] that $\lambda(n)$ is quite large for most integers[3].

[3]In fact, in [4] it was also shown that $\lambda(n) = n/(\log n)^{\log\log\log n + A + o(1)}$, where $A \simeq 0.227$, for most integers.

Lemma 8. *For x sufficiently large, the number of integers $n \le x$ with $\lambda(n) \le n\exp(-(\log\log n)^3)$ is at most $x/(\log x)^{10}$.*

As mentioned in the introduction, if $\varepsilon(x) \to 0$ as $x \to \infty$, then $\ell_e^*(p) > p^{1/2+\varepsilon(p)}$ for almost all prime p. In other words, $\ell_e^*(p)$ is fairly large for "typical" primes p. Thus, if the product of the "typical" prime divisors of a generic integer n is of size comparable with n, we find that $\ell_e^*(n) > n^{1/2+\varepsilon(n)}$ for most n. We can make this more precise as follows.

Suppose $\mathcal{P}$ is a subset of the prime numbers. We let $\pi_{\mathcal{P}}(x)$ denote the number of primes $p \le x$ with $p \in \mathcal{P}$. For a positive integer n we let $n_{\mathcal{P}}$ denote the largest divisor of n that is free of prime factors outside of $\mathcal{P}$.

Assume $\varepsilon(x)$ is an arbitrary monotonic function with

$$\varepsilon(x) = o(1), \quad \varepsilon(x) > 1/\log\log x, \quad \varepsilon(x^{1/\log\log x}) < 2\varepsilon(x), \tag{3.1}$$

where the last two conditions hold for x sufficiently large. We now partition the primes into 3 sets:

$$\begin{aligned} \mathcal{L} &= \{p \text{ prime} : \ell_e^*(p) \le p^{1/2}/\log p\} \\ \mathcal{M} &= \{p \text{ prime} : p^{1/2}/\log p < \ell_e(p) \le p^{1/2+2\varepsilon(p)}\} \\ \mathcal{H} &= \{p \text{ prime} : \ell_e(p) > p^{1/2+2\varepsilon(p)}\}, \end{aligned}$$

where we use the mnemonic low, medium, and high (order) for $\mathcal{L}, \mathcal{M}, \mathcal{H}$. Note that $\mathcal{L}$ contains the prime factors of e. Further, let $\omega(n)$ denote the number of prime number divisors of n.

By an argument due to Hooley [7], we can show that the "low order" primes are rare enough that the sum of their reciprocals converge.

Lemma 9. *We have $\pi_{\mathcal{L}}(x) = O(x/\log^3 x)$ so that $\sum_{p\in\mathcal{L}} 1/p = O(1)$. In addition, we have*

$$\sum_{n_{\mathcal{L}}=n} \frac{1}{n} \;=\; \prod_{p\in\mathcal{L}} (1-1/p)^{-1} \;=\; O(1). \tag{3.2}$$

For a positive integer n, let $\gamma(n)$ denote the largest squarefree divisor of n, sometimes called the "core" or "radical" of n. Using Lemma 9, together with the Erdős-Kac theorem (or the Hardy-Ramanujan theorem on the normal number of prime divisors of integers), we can show that a generic integer n has the following properties: the low order part $n_{\mathcal{L}}$ of n is quite small, the core of n is quite large, and n does not have too many prime divisors. More precisely, we have:

Lemma 10. *But for a set of natural numbers n of asymptotic density 0 we have: $n_{\mathcal{L}} < \log n$, $n/\gamma(n) < \log n$, and $\omega(n) < 2\log\log n$.*

Our next question of interest is how large can we expect $n_{\mathcal{M}}$ to be for most numbers n. Since most numbers do not have a divisor very near their square root, there is hope that this ingredient can be used. In fact, Erdős and Murty used this idea to show that $\pi_{\mathcal{M}}(x) = o(\pi(x))$, and Pappalardi and Indlekofer–Timofeev got more quantitative versions of this result. We state a consequence from the latter paper.

Lemma 11 ([8], Cor. 6)**.** *With $\varepsilon(x)$ as specified in* (3.1)*, we have $\pi_{\mathcal{M}}(x) = O(\varepsilon(x)^{1/12}\pi(x))$.*

We now show that as a consequence of Lemma 11, not many integers n have a large divisor composed of primes from $\mathcal{M}$. Let Λ denote the von Mangoldt function.

Lemma 12. *With $\varepsilon(x)$ as specified in* (3.1)*, the number of integers $n \le x$ with $n_{\mathcal{M}} > n^{1/3}$ is $O(\varepsilon(x)^{1/12}x)$.*

Proof. We have

$$\sum_{n\le x} \log n_{\mathcal{M}} = \sum_{n\le x} \sum_{\substack{d\mid n \\ d_{\mathcal{M}}=d}} \Lambda(d) \;=\; \sum_{\substack{d_{\mathcal{M}}=d \\ d\le x}} \Lambda(d) \left\lfloor \frac{x}{d} \right\rfloor \;\le\; x \sum_{\substack{p\in\mathcal{M} \\ p\le x}} \frac{\log p}{p} + O(x).$$

Now, using Lemma 11 and (3.1),

$$\begin{aligned}
\sum_{p\in\mathcal{M},\ p\le x} \frac{\log p}{p} &= \frac{\log x}{x}\pi_{\mathcal{M}}(x) + \int_2^x \frac{\log t - 1}{t^2}\pi_{\mathcal{M}}(t)\,dt \\
&\ll \int_2^x \frac{\varepsilon(t)^{1/12}}{t}\,dt + o(1) \\
&= \int_2^{x^{1/\log\log x}} \frac{\varepsilon(t)^{1/12}}{t}\,dt + \int_{x^{1/\log\log x}}^x \frac{\varepsilon(t)^{1/12}}{t}\,dt + o(1) \\
&\ll \frac{\log x}{\log\log x} + \varepsilon(x)^{1/12}\log x \;\ll\; \varepsilon(x)^{1/12}\log x.
\end{aligned}$$

Thus,

$$\sum_{n\le x} \log n_{\mathcal{M}} \;\ll\; \varepsilon(x)^{1/12} x \log x,$$

and the result follows readily. □

We are now ready to prove the first part of Theorem 1.

Theorem 13. *Suppose $\varepsilon(n)$ satisfies* (3.1)*. But for a set of integers n of asymptotic density 0 we have*

$$\ell_e^*(n) \;>\; n^{1/2+\varepsilon(n)}.$$

Proof. By Lemma 8 we may assume that $\lambda(n) > n\exp(-(\log\log n)^3)$. Thus, from Lemma 7 and Lemma 10 we have

$$\begin{aligned}
\ell_e^*(n) &> \exp(-(\log\log n)^3) \prod_{p\mid n/n_{\mathcal{L}}} \ell_e(n) \\
&\ge \exp(-(\log\log n)^3) \prod_{p\mid n_{\mathcal{M}}} (p^{1/2}/\log p) \prod_{p\mid n_{\mathcal{H}}} p^{1/2+2\varepsilon(p)} \\
&\ge \exp(-(\log\log n)^3 - \omega(n)\log\log n)\gamma(n_{\mathcal{M}})^{1/2}\gamma(n_{\mathcal{H}})^{1/2+2\varepsilon(n)} \\
&\ge \exp(-2(\log\log n)^3) n^{1/2} n_{\mathcal{H}}^{2\varepsilon(n)}.
\end{aligned}$$

By Lemmas 10 and 12 we may also assume that $n_{\mathcal{H}} > n^{3/5}$. Thus, our result follows from (3.1). □

3.2 On the order of e modulo $\lambda(n)$

The proof in this case is fairly similar. Using Lemma 7 we obtain the bound

$$\ell_e^*(\lambda(n)) \ge \frac{\lambda(\lambda(n))}{\lambda(n)} \prod_{p\lambda(n)} \ell_e(p)$$

Using the following result of Martin and Pomerance [14] on the normal order of $\lambda(\lambda(n))$ we may control the ratio $\lambda(\lambda(n))/\lambda(n)$.

Theorem 14 (Martin–Pomerance [14]). *As $n \to \infty$ through a certain set of integers of asymptotic density 1, we have*

$$\lambda(\lambda(n)) = n \cdot \exp(-(1+o(1))(\log\log n)^2 \log\log\log n).$$

Thus, $\lambda(\lambda(n)) > n/\exp((\log\log n)^3)$ almost always.

Now, by using the fact (see [3]) that the normal order of $\omega(\lambda(n))$ is equal to $(\log\log n)^2/2$, together with the fact (easily deduced from (6) and (7) in [4]) that the estimate

$$\log(\lambda(n)/\gamma(\lambda(n))) \ll \log\log n/\log\log\log n$$

holds for most n, it is possible to obtain the following analog of Lemma 10.

Lemma 15. *We have*

$$\begin{aligned} \lambda(n)_{\mathcal{L}} &< \exp((\log\log n)^2) \\ \lambda(n)/\gamma(\lambda(n)) &< \log n \\ \omega(\lambda(n)) &< (\log\log n)^2 \end{aligned}$$

almost always.

A similar, but more elaborate, argument to the one used to prove Lemma 12, then gives the following result.

Lemma 16. *Let $\varepsilon(x)$ satisfy* (3.1). *Almost all numbers n have the property that $\lambda(n)_{\mathcal{M}} < n^{2/5}$.*

With these results at our disposal, the argument used in Theorem 13 easily gives that

$$\ell_e^*(\lambda(n)) > n^{1/2+\varepsilon(n)}$$

for most n.

References

[1] L. Blum, M. Blum, and M. Shub. A simple unpredictable pseudorandom number generator. *SIAM J. Comput.*, 15(2):364–383, 1986.

[2] P. Erdős and M. R. Murty. On the order of a (mod p). In *Number theory (Ottawa, ON, 1996)*, pages 87–97. Amer. Math. Soc., Providence, RI, 1999.

[3] P. Erdős and C. Pomerance. On the normal number of prime factors of $\phi(n)$. *Rocky Mountain J. Math.*, 15(2):343–352, 1985. Number theory (Winnipeg, Man., 1983).

[4] P. Erdős, C. Pomerance, and E. Schmutz. Carmichael's lambda function. *Acta Arith.*, 58(4):363–385, 1991.

[5] K. Ford. The distribution of integers with a divisor in a given interval. *Annals Math.*, to appear.

[6] J. B. Friedlander, C. Pomerance, and I. E. Shparlinski. Period of the power generator and small values of Carmichael's function. *Math. Comp.*, 70(236):1591–1605, 2001. Corrigendum, *op. cit.*, 71(240):1803–1806, 2002.

[7] C. Hooley. On Artin's conjecture. *J. Reine Angew. Math.*, 225:209–220, 1967.

[8] K.-H. Indlekofer and N. M. Timofeev. Divisors of shifted primes. *Publ. Math. Debrecen*, 60(3-4):307–345, 2002.

[9] S. V. Konyagin, C. Pomerance, and I. E. Shparlinski. On the distribution of pseudopowers. Preprint.

[10] P. Kurlberg. On the order of unimodular matrices modulo integers. *Acta Arith.*, 110(2):141–151, 2003.

[11] P. Kurlberg and C. Pomerance. On the period of the linear congruential and power generators. *Acta Arith.*, 119(2):149–169, 2005.

[12] P. Kurlberg and Z. Rudnick. On quantum ergodicity for linear maps of the torus. *Comm. Math. Phys.*, 222(1):201–227, 2001.

[13] S. Li and C. Pomerance. On generalizing Artin's conjecture on primitive roots to composite moduli. *J. Reine Angew. Math.*, 556:205–224, 2003.

[14] G. Martin and C. Pomerance. The iterated Carmichael λ-function and the number of cycles of the power generator. *Acta Arith.*, 118(4):305–335, 2005.

[15] F. Pappalardi. On the order of finitely generated subgroups of $\mathbf{Q}^*$ (mod p) and divisors of $p-1$. *J. Number Theory*, 57(2):207–222, 1996.

Fast scalar multiplication on elliptic curves

Tanja Lange

We review the use of elliptic curves in cryptography and show how multi-scalar multiplication naturally occurs in the applications. The standard group law in affine or projective coordinates distinguishes between doublings and general additions. Several other coordinate systems and addition formulae were introduced to implement scalar multiplication on elliptic curves more efficiently. Usually the systems try to optimize the speed of doublings since they are much more frequent than additions in scalar multiplications, particularly in windowing methods. If multi-scalar multiplication is the target, however, the speed of additions gets more and more interesting and so other choices should be made.

The situation changes again if the system is implemented on a smart card since then additional care needs to be taken not to leak the secret through side channels such as time or power consumption. The easiest countermeasure is to introduce so-called "dummy" operations and to perform extra curve additions on data that is not further used. This approach implies that as many doublings as additions are used and again the speed of additions becomes interesting. A different solution is to use "unified" group operations, that are formulae that work the same for additions and for doublings. Clearly, there are exceptions but they are very unlikely to appear. Using these formulae has the advantage that no dummy operations are needed and so efficient scalar and multi-scalar multiplication methods can be used; on the downside, this approach prohibits fast doublings and often slightly more field operations are needed per group operation.

In this talk we deal with an alternative representation of elliptic curves. We show how the group laws are computed and give operation counts. The system is interesting if inversions must be avoided and if many additions are needed. The group laws can be turned into unified formulae and lead to the fastest unified formulae known.

Galois Groups with Minimal Ramification

Nadya Markin

School of Mathematical Sciences
University College Dublin
Republic of Ireland

Abstract

Let K be a number field and G a finite group. We study the realization of G as a Galois group over K with restricted ramification. For this purpose, we define $Ram_K(G)$ (resp. $ram_K(G)$) to be the minimum number of ramifying primes (resp. finite primes) of K required to realize G as a Galois group over K. We provide an upper bound for $Ram_K(G)$ in case G is a finite nilpotent group. We use modular forms to come up with an infinite family of non-abelian groups that can be realized with just one finite ramifying prime. Combined with other methods we establish that $ram_{\mathbb{Q}}(GL_2(\mathbb{F}_p)) = 1$ for infinitely many primes p and for all primes $p < 106591$.

1 Introduction

Let K be a number field. Given a finite group G, a fundamental question of Inverse Galois Theory is whether G occurs as a Galois group of some extension L of K. If the answer to this question is positive, we say that G can be *realized* over K. In 1937 Scholz and Reichardt showed independently that every finite group of order l^n, where l is an odd prime can be realized over $\mathbb{Q}$. In 1954 Shafarevich [Sha] showed that every finite solvable group G can be realized over a fixed number field K. Let L be a finite Galois extension of K, $\mathcal{O}_L$ its ring of integers and $\mathfrak{p}$ a finite prime of K. Then $\mathfrak{p}$ is said to be *ramified* in L when the ramification index e in the decomposition $\mathfrak{p}\mathcal{O}_L = \mathfrak{p}_1^e \cdots \mathfrak{p}_r^e$ is greater than one. Only finitely many primes $\mathfrak{p}$ of K are ramified in any given extension L of K, they are the primes that divide $\mathfrak{d}_{L/K}$, the discriminant of L over K. When $\mathfrak{p}$ is an archimedean prime of K, we say that $\mathfrak{p}$ is ramified in L when the extension $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ is non-trivial, where $K_{\mathfrak{p}}$ is the completion of K with respect to the absolute value $|\cdot|_{\mathfrak{p}}$ and $|\cdot|_{\mathfrak{P}}$ is an absolute value of L extending $|\cdot|_{\mathfrak{p}}$. A natural question to ask is how many ramifying primes are necessary in order to realize a given finite group over a fixed number field K. This motivates the following definition.

Definition 9. *Let K be a number field and G a finite group. Then let $Ram_K(G)$ (resp. $ram_K(G)$) be the minimum number of primes (resp. finite primes) ramified in L, as L runs over all extensions of K with Galois group G.*

As a direct consequence of Minkowski's bound on the discriminant, every non-trivial extension of $\mathbb{Q}$ has at least one finite ramifying prime, so we have $ram_{\mathbb{Q}}(G) \geq 1$ for any non-trivial group G. The question of ramification bounds for abelian groups is completely answered. By the Theorem of Kronecker-Weber, every abelian extension of $\mathbb{Q}$ is contained in a cyclotomic extension. This gives us a lower bound, while Dirichlet's Theorem on primes in arithmetic progression gives an upper bound on $Ram_{\mathbb{Q}}(A)$, where A is an abelian group. We obtain

$$Ram_{\mathbb{Q}}(A) = d(A),$$

where $d(A)$ is the minimum number of generators of A. Our central interest is studying bounds on $Ram_K(G)$ for various families of groups.

2 Central Lifts

The Local-Global principle together with ramification conditions can ensure solvability of certain embedding problems. We have the following lemma:

Lemma 10. *Consider the embedding problem below.*

$$\begin{array}{ccccccccc} & & & & & & G_{\mathbb{Q}} & & \\ & & & & & \overset{\phi}{\swarrow} & \downarrow{\scriptstyle \rho} & & \\ 1 & \longrightarrow & C_2 & \longrightarrow & G & \xrightarrow[\alpha]{} & \bar{G} & \longrightarrow & 1 \end{array} \tag{2.1}$$

Let K be the fixed field of $ker(\rho)$ in an algebraic closure $\bar{\mathbb{Q}}$ of $\mathbb{Q}$. If only one prime q of $\mathbb{Q}$ is ramified in K, then the embedding problem above is solvable. Moreover, a solution ϕ can be chosen such that $\bar{\mathbb{Q}}^{ker(\phi)}$ is unramified outside $\{q, \infty\}$.

The lemma above is applied in Section 4 in order to realize $GL_2(F_p)$ for $p = 5, 7$ with one finite ramifying prime.

We use the solvability of certain central lifts to prove the non-existence of imaginary A_4-extensions over $\mathbb{Q}$ with a single finite ramifying prime. This result was originally conjectured by Doud in [Do2]:

Theorem 11. *If $L/\mathbb{Q}$ is an A_4-extension in which only one finite prime is ramified, then L is totally real.*

3 Ramification Bounds for Nilpotent Groups

Realization of a group G of order l^n over $\mathbb{Q}$ by the method of Scholz-Reichardt gives the ramification bound $Ram_{\mathbb{Q}}(G) \leq n$ for a group G of order l^n. In 1998 Geyer and Jarden generalized in [GJ] the method of Scholz-Reichardt to an arbitrary number field K. Their method of realizing l-groups yields a similar ramification bound. Namely, for a finite group G of prime-power order l^n and a number field K not containing a primitive l^{th} root of unity ζ_l,

$$Ram_K(G) \leq n + t(K),$$

where $t(K)$ is a constant depending only on K. We generalize the method of Geyer-Jarden to obtain a similar ramification bound for nilpotent groups. We obtain the following result.

Theorem 12. *Let K be a number field and $\{l_j \mid \ 1 \leq j \leq r\}$ a set of rational primes such that $\zeta_{l_j} \notin K \ \forall j$. Let $G = \prod_{j=1}^{r} G_j$, be a nilpotent group where each G_j is a Sylow l_j-subgroup of G with $|G_j| = l_j^{n_j}$.*

Then there exists a non-negative integer $t = t(K)$ and an extension L/K such that $G \cong Gal(L/K)$ and the number of primes of K ramified in L is at most $\max_{j=1}^{r}\{n_j\} + t$. Thus we obtain the upper bound

$$Ram_K(G) \leq \max_{j=1}^{r}\{n_j\} + t.$$

4 Families of Groups Ramified at a Single Finite Prime

In [Pla] B. Plans uses the results of Yamomoto on class numbers of quadratic extensions of $\mathbb{Q}$ to show that Schinzel's Hypothesis H implies that for every integer $n > 0$ the dihedral and symmetric groups D_n, S_n can be realized with one finite ramifying prime. We want to find other infinite families of non-abelian groups that share this property. We use the result of Serre-Deligne [SD] on cusp forms of weight k to obtain a family of groups $\{G = GL_2(\mathbb{F}_p)\}$ for infinitely many primes p that can be realized with ramification at a single finite prime. A few small primes were treated separately. The cases $p = 5, 7$ were constructed by obtaining lifts of known extensions: Klüners' database [Klu] gives us polynomials which realize S_5 and $PGL_2(\mathbb{F}_7)$ with one ramifying prime. We lift the obtained extensions using Lemma 10 to realize $GL_2(\mathbb{F}_p)$ for $p = 5, 7$ with one finite ramifying prime. Combining these results, we have the following:

Proposition 13. *$ram_{\mathbb{Q}}(GL_2(\mathbb{F}_p)) = 1$ for infinitely many primes p and for all p such that $p < 106591$.*

It is worth noting some nonexistence results that follow when we restrict to ramification at a single small prime. For example, we use Odlyzko bounds ([Od]) to obtain the following result:

Proposition 14. *There is no Galois extension of $\mathbb{Q}$ of degree $8n$ unramified outside $\{2, \infty\}$, where $n > 1$ is odd.*

Some interesting results on extensions unramified outside $\{2, \infty\}$ can be found in [Har, Tat].

Acknowledgements: This work was part of my Ph.D. thesis completed under the supervision of my advisor Nigel Boston and coadvisor Stephen Ullom whom I both thank for their invaluable time and guidance.

References

[Do1] D.Doud, *S_4 and $\tilde{S}_4$ Extensions of $\mathbb{Q}$ Ramified at Only One Prime*, Journal of Number Theory 75, 1999, pp.185-197.

[Do2] D. Doud, *Deformations of Three Dimensional Galois Representations*, Ph.D. Thesis, University of Illinois at Urbana-Champaign, 1999.

[GJ] W.-D. Geyer and M. Jarden, *Bounded Realization of l-Groups over Global Fields*, Nagoya Math. J., Vol. 150, 1998, pp.13-62.

[Har] D. Harbater, *Galois Groups with Prescribed Ramification*, Contemporary Mathematics, Volume 174, 1994, pp. 35-60.

[Klu] J.Klüners, `http://www.math.uni-duesseldorf.de/~klueners/minimum/minimum.html`.

[Mar] N. Markin, *Galois Groups with Restricted Ramification*, Ph.D. Thesis, University of Illinois at Urbana-Champaign, 2006.

[Od] A.M. Odlyzko, *On Conductors and Discriminants*, Algebraic Number Fields (A. Frohlich, eds) Durham Symposium, 1975, Academic Press, London, 1977, pp.377-407.

[Pla] B.Plans, *On the Minimal Number of Ramified Primes in Some Solvable Extensions of* $\mathbb{Q}$, Pacific Journal of Mathematics, Vol 215 no.2, 2004, pp.381-391.

[SD] H.P.F Swinnerton-Dyer, *On l-adic Representations and Congruences for Coefficients of Modular Forms*, LNM 350, Springer-Verlag, 1972, pp.1-56.

[Sha] I.R. Shafarevich, *Extensions with Given Points of Ramification* (Russian), Inst. Hautes Etudes Sci. Publ. Math. Vol 18, 1963, pp.71-95.

[Tat] J. Tate, *The non-existence of certain Galois extensions of* $\mathbb{Q}$ *unramified outside* 2, Arithmetic geometry (Tempe, AZ, 1993), Contemporary Mathematics, 174, pp.153–156, American Mathematical Society, Providence, RI, 1994.

Riemann's Zeta Function: Some Computations and Conjectures

Yu. V. Matiyasevich

Abstract

The Riemann Hypothesis is reformulated as statements about the eigenvalues of certain matrices entries of which are defined via the Taylor series coefficients of the zeta function. These eigenvalues demonstrate interesting visual patterns allowing one to state a number of conjectures.

Preliminary version of this paper was placed in [6, 7].

1 The Hypothesis

One of the most interesting and important objects in number theory is Riemann's zeta function $\zeta(z)$. It can be defined for $\Re(z) > 1$ by the Dirichlet series

$$\zeta(z) = \sum_{n=1}^{\infty} \frac{1}{n^z}. \tag{1.1}$$

The function can be extended to the entire complex z-plane with the exception of the point $z = 1$ which is the only pole of $\zeta(z)$. Points $\mathrm{z}_1 = -2,\ \mathrm{z}_2 = -4,\ \ldots,\ \mathrm{z}_n = -2n, \ldots$ are known as the *trivial zeros* of the function $\zeta(z)$. We have the famous

Riemann Hypothesis (version 1). *All non-trivial zeros of the function* $\zeta(z)$ *lie on the* critical line $\Re(z) = \frac{1}{2}$.

2 Trivial zeroes

There is a tradition (taking its origin in Riemann's seminal paper [8]) to get rid of the trivial zeros by dealing with the function

$$\xi(z) = \pi^{-\frac{z}{2}}(z-1)\zeta(z)\Gamma(1+\tfrac{z}{2}) \tag{2.1}$$

rather than with the function $\zeta(z)$ itself (we use modern notation for this function, Riemann used $\xi(t)$ to denote the function which is today denoted $\Xi(t)$). The poles of the factor $\Gamma(1+\frac{z}{2})$ in (2.1) cancel the trivial zeros of $\zeta(z)$ and similarly the factor $z-1$ cancels the pole of $\zeta(z)$. The factor $\pi^{-\frac{z}{2}}$ influence neither zeros nor poles but it allows one to state the *functional equation* in a pretty form:

$$\xi(z) = \xi(1-z). \tag{2.2}$$

In this paper we won't deprive zeta function of its trivial zeros but try to take advantage of our knowledge of precise positions of these zeros. To this end we will work with the entire function

$$\zeta^*(z) = 2(z-1)\zeta(z). \tag{2.3}$$

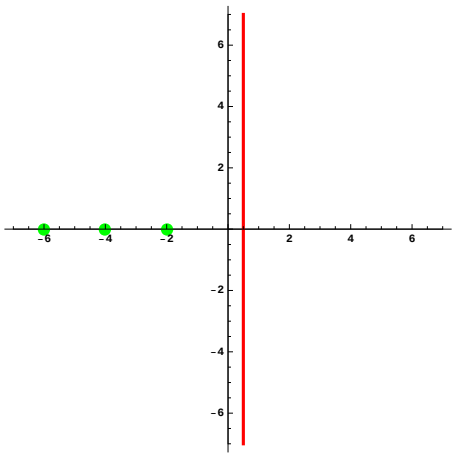


Figure 3.1: z-plane

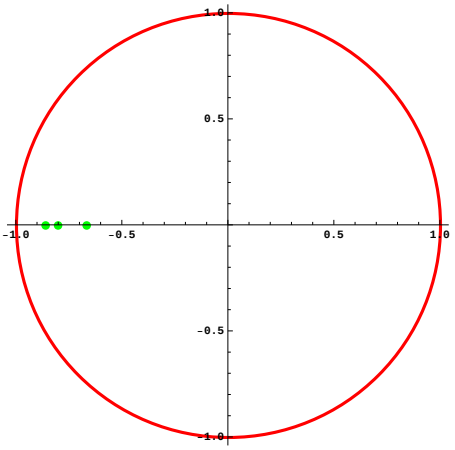


Figure 3.2: w-plane

For our purpose we could also omit the factor $z-1$ and/or use the factor $\pi^{-\frac{z}{2}}$; this would change the picture(s) so probably separate paper(s) will be devoted to these variations. The factor 2 in (2.3) results in the equality

$$\zeta^*(0) = 1 \tag{2.4}$$

which slightly simplifies some forthcoming formulas.

According to (2.2) the non-trivial zeros of $\zeta(z)$ lie symmetrically around the critical line, so we have

Riemann Hypothesis (version 2). *The trivial zeros* $\mathrm{z}_1 = -2$, $\mathrm{z}_2 = -4$, $\ldots$, $\mathrm{z}_n = -2n, \ldots$ *are the only zeros of the function* $\zeta^*(z)$ *lying in the half-plane* $\Re(z) < \frac{1}{2}$.

3 Change of the variable

A half-plane is a natural object when one deals with Dirichlet series. However, we are going to deal with Taylor series, and for them circles are more natural regions. So we make a change of variable:

$$z = \frac{w}{w+1}, \qquad w = \frac{z}{1-z}. \tag{3.1}$$

Under this transformation the critical line becomes the *critical circle* $|w| = 1$, the half-plane $\Re(z) < \frac{1}{2}$ becomes the interior of this circle, and points

$$\mathrm{w}_1 = \frac{\mathrm{z}_1}{1-\mathrm{z}_1} = -\frac{2}{3}, \ \ldots, \ \mathrm{w}_n = \frac{\mathrm{z}_n}{1-\mathrm{z}_n} = -\frac{2n}{2n+1}, \ldots \tag{3.2}$$

become the *trivial zeros of the function*

$$\tilde{\zeta}(w) = \zeta^*(\tfrac{w}{w+1}). \tag{3.3}$$

With this new notation we have

Riemann Hypothesis (version 3). *The trivial zeros* $\mathrm{w}_1 = -\frac{2}{3}$, $\ldots$, $\mathrm{w}_n = -\frac{2n}{2n+1}, \ldots$ *are the only zeros of the function* $\tilde{\zeta}(w)$ *lying in the open circle* $|w| < 1$.

4 Subhypothesises

It isn't very convenient to work near the critical circle (full of zeros) so we split the Riemann Hypothesis into an infinite series of weaker statements:

RH_l, the l-th Riemann subhypothesis (version 1). *The trivial zeros* $\mathrm{w}_1 = -\frac{2}{3},\ \ldots,\ \mathrm{w}_l = -\frac{2l}{2l+1}$ *are the only zeros of the function* $\tilde{\zeta}(w)$ *lying in the closed disk* $|w| \le \frac{2l+1}{2l+2}$.

While each of the subhypotheses is weaker than the Riemann Hypothesis, taken together, they are equivalent to it:

Riemann Hypothesis (version 4). *For every* m *the subhypothesis* RH_m *is true.*

5 First question

Let us ask a "naïve" question: *Why is* RH_1 *true?* More precisely, *how can we see that* RH_1 *is true?* To answer this question we can expand the function $1/\tilde{\zeta}(w)$ into the Taylor series:

$$1/\tilde{\zeta}(w) = 1 + \tau_1 w + \cdots + \tau_n w^n + \ldots \tag{5.1}$$

Now according to RH_1 the point $\mathrm{w}_1 = -\frac{2}{3}$ should be the only pole of the function (5.1) lying inside the circle $|w| \le \frac{3}{4}$. Respectively, we have

RH_1 (version 2). *For* $m \to \infty$

$$\tau_m \;=\; \big(-\tfrac{3}{2}\big)^m (\mathrm{R}_1 + o(1)) \tag{5.2}$$

for some non-zero constant R_1.

It is easy to see that

$$\begin{aligned} \mathrm{R}_1 &= \frac{3}{2\tilde{\zeta}'(-2/3)} && (5.3)\\ &= -\frac{1}{36\zeta'(-2)} && (5.4)\\ &= 0.91228851841347\ldots && (5.5)\\ &> 0 && (5.6) \end{aligned}$$

so we have

RH_1 (version 3).

$$\lim_{m\to\infty} ((-1)^m \tau_m)^{\frac{1}{m}} \;=\; \tfrac{3}{2}. \tag{5.7}$$

6 Determinant representation

It is easy to see that coefficients $\tau_1,\ \tau_2, \dots$ from (5.1) can be expressed in terms of the coefficients in the Taylor expansion

$$\tilde{\zeta}(w) = 1 + \theta_1 w + \dots + \theta_m w^m + \dots . \tag{6.1}$$

More precisely,

$$\tau_m = (-1)^m \det(L_{1,m}) \tag{6.2}$$

where $L_{1,m}$ is the following Toeplitz matrix:[1]

$$L_{1,m} = \begin{pmatrix} \theta_1 & 1 & 0 & \dots & 0 & 0 \\ \theta_2 & \theta_1 & 1 & \dots & 0 & 0 \\ \theta_3 & \theta_2 & \theta_1 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \theta_{m-1} & \theta_{m-2} & \theta_{m-3} & \dots & \theta_1 & 1 \\ \theta_m & \theta_{m-1} & \theta_{m-2} & \dots & \theta_2 & \theta_1 \end{pmatrix}. \tag{6.3}$$

Then, we have

RH$_1$ (version 4). *For* $m \to \infty$

$$\det(L_{1,m}) \ = \ \big(-\tfrac{3}{2}\big)^m (\mathrm{R}_1 + o(1)) \tag{6.4}$$

with the constant R_1 *defined by* (5.3)–(5.4)

and

RH$_1$ (version 5).

$$\lim_{m\to\infty} \big(\det(L_{1,m})\big)^{\frac{1}{m}} \ = \ \tfrac{3}{2}. \tag{6.5}$$

7 Eigenvalues on average

Naturally,

$$\det(L_{1,m}) = \lambda_{1,m,1}\lambda_{1,m,2}\dots\lambda_{1,m,m} \tag{7.1}$$

where $\lambda_{1,m,1},\ \lambda_{1,m,2},\ \dots,\ \lambda_{1,m,m}$ are the eigenvalues of the matrix $L_{1,m}$. Thus, we have

RH$_1$ (version 6).

$$\lim_{m\to\infty} \left(\prod_{n=1}^{m} \lambda_{1,m,n}\right)^{\frac{1}{m}} = \frac{3}{2}. \tag{7.2}$$

The (multi)set $\{\lambda_{1,m,1},\ \lambda_{1,m,2},\dots\lambda_{1,m,m}\}$ will be called the λ-*spectrum* and will be denoted $\mathrm{Spec}^{\lambda}_{1,m}$.

[1] Clearly, we can change the order of the columns in this matrix and obtain a Hankel matrix whose determinant has the same absolute value; the resulting picture(s) are rather different and will be considered in Sections 18–21.

8 Positions of individual eigenvalues

According to RH_1 the (geometric) mean of $\lambda_{1,m,1}$, $\lambda_{1,m,2}$, ..., $\lambda_{1,m,m}$ approaches $\frac{3}{2}$ when m goes to infinity, but neither RH_1 nor RH itself tells us anything directly about the distribution of these eigenvalues. Are they as random as, say, the imaginary parts of the non-trivial zeros of $\zeta(z)$? Do the eigenvalues cluster or are they spread around the whole w-plane? Is there any similarity between eigenvalues corresponding to different values of m?

The author was curious to calculate[2] the values of the spectra $\mathrm{Spec}^{\lambda}_{1,m}$ for initial values of m and have a look at them. Some pictures are included in this paper, an updated collection of pictures can be downloaded from [5].

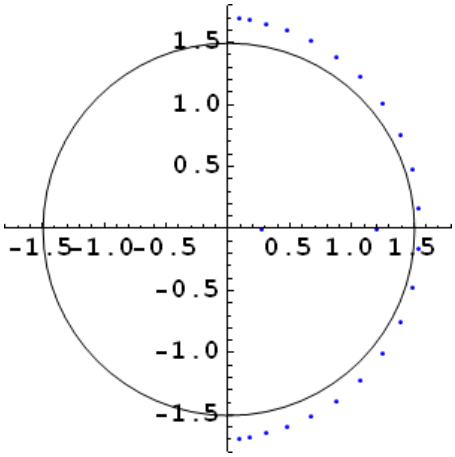


Figure 8.1: $\mathrm{Spec}^{\lambda}_{1,24}$

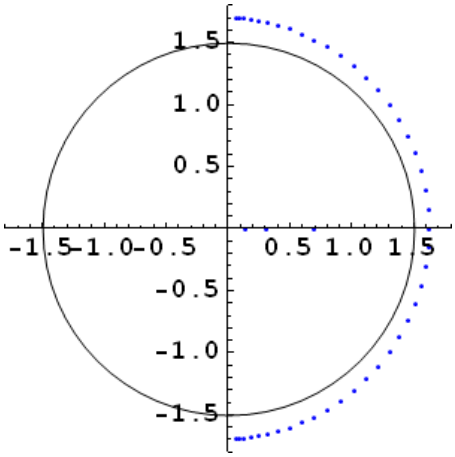


Figure 8.2: $\mathrm{Spec}^{\lambda}_{1,48}$

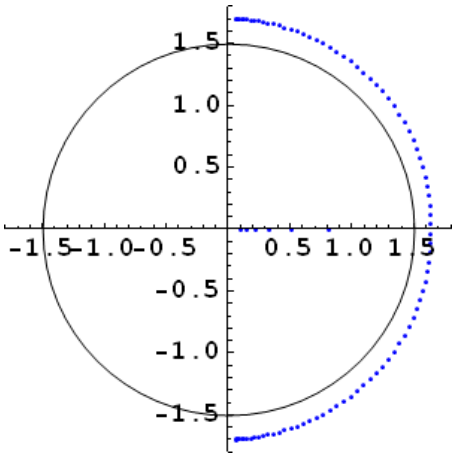


Figure 8.3: $\mathrm{Spec}^{\lambda}_{1,96}$

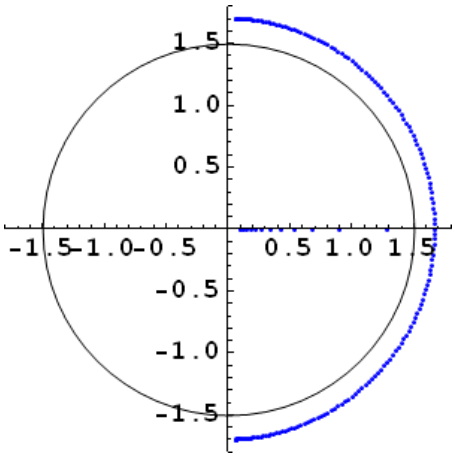


Figure 8.4: $\mathrm{Spec}^{\lambda}_{1,192}$

Figures 8.1–8.4 show spectra $\mathrm{Spec}^{\lambda}_{1,m}$ for $m = 24, 48, 96, 192$ respectively together with the circle $|w| = \frac{3}{2}$, the "ideal" place for the eigenvalues according to

[2]Calculations were done mainly with MATHEMATICA and partly with PARI on a personal computer; larger scale computations are very desirable for getting more insight.

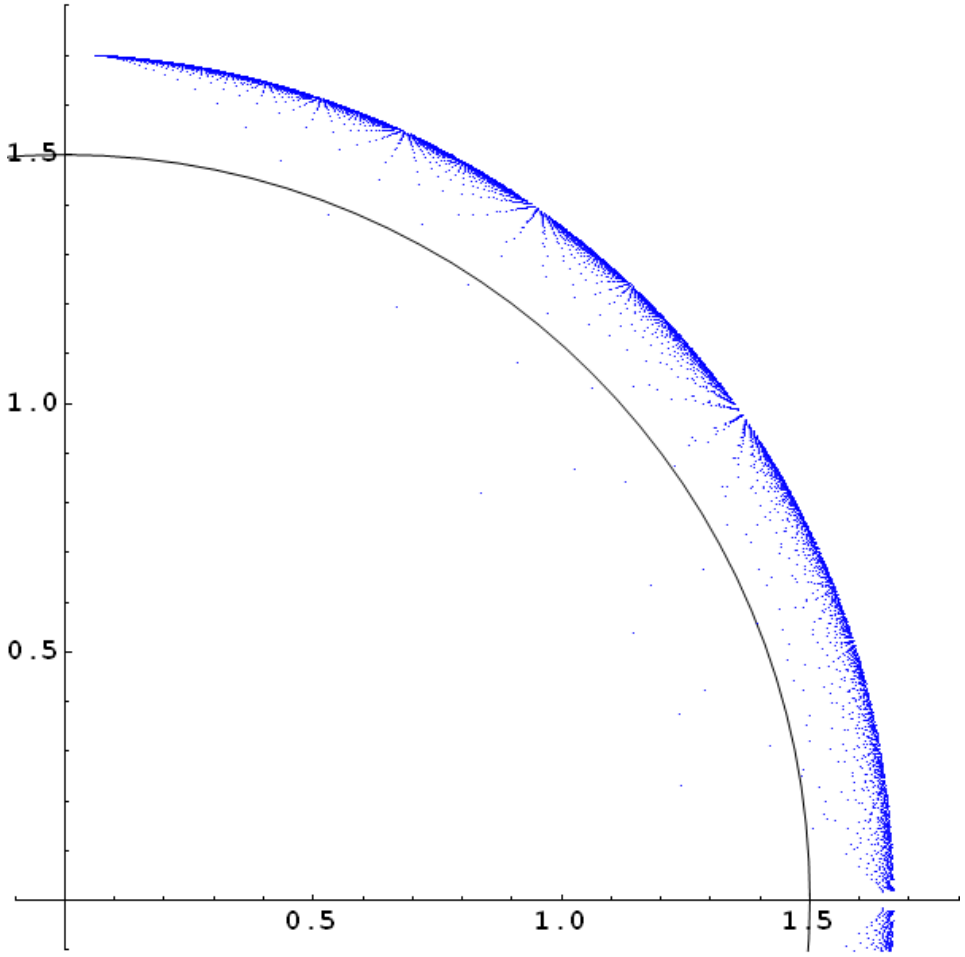


Figure 8.5: $\cup_{m=1}^{192} \mathrm{Spec}_{1,m}^{\lambda}$

(7.2). Figure 8.5 shows the union $\cup_{m=1}^{192}\mathrm{Spec}_{1,m}^{\lambda}$ (in the first quadrant). The "hidden life of Riemann's zeta function" is best seen from an animation showing the $\mathrm{Spec}_{1,1}^{\lambda}$, $\mathrm{Spec}_{1,2}^{\lambda}$, ... in succession; such an animation can be downloaded from [5]; there you can also find higher resolution versions of the above pictures and many others.

Looking at the pictures we can say that the λ-spectrum $\mathrm{Spec}_{1,m}^{\lambda}$ is the union of the *arrow* $\mathrm{Arr}_{1,m}$ consisting entirely of real eigenvalues and the *bow* $\mathrm{Bow}_{1,m}$; for counting purpose it is reasonable to consider sometimes the largest real eigenvalue as belonging to the bow rather than to the arrow. Formally, if the number of real eigenvalues in the spectrum $\mathrm{Spec}_{1,m+1}^{\lambda}$ is less than the number of real eigenvalues in the spectrum $\mathrm{Spec}_{1,m}^{\lambda}$, then we consider the largest real eigenvalue in the spectrum $\mathrm{Spec}_{1,m}^{\lambda}$ as belonging to $\mathrm{Bow}_{1,m}$ and not belonging to arrow $\mathrm{Arr}_{1,m}$.

9 First Conjectures

The above pictures suggest the following conjectures.

Conjecture 1A$_1$. *There are no multiple eigenvalues.*

Conjecture 1B$_1$. $\sup_m(\max(\mathrm{Arr}_{1,m}))$ *is a positive number.*

Conjecture 1C$_1$. $\inf_m(\min(\mathrm{Arr}_{1,m}))$ *is a positive number.*

Conjecture 1D$_1$. *The numbers* $\mathrm{arr}_{1,m} = ||\mathrm{Arr}_{1,m}||$ *and* $\mathrm{bow}_{1,m} = ||\mathrm{Bow}_{1,m}||$ *of eigenvalues belonging to the arrow* $\mathrm{Arr}_{1,m}$ *and to the bow* $\mathrm{Bow}_{1,m}$ *respectively don't decrease when* m *increases.*

Conjecture 1E$_1$. *If*

$$\mathrm{Arr}_{1,m} = \{\lambda_{1,m,1}, \lambda_{1,m,2}, \ldots, \lambda_{1,m,\mathrm{arr}_{1,m}}\}, \tag{9.1}$$

$$\mathrm{Arr}_{1,m+1} = \{\lambda_{1,m+1,1}, \lambda_{1,m+1,2}, \ldots, \lambda_{1,m+1,\mathrm{arr}_{1,m+1}}\} \tag{9.2}$$

and

$$\lambda_{1,m,1} < \lambda_{1,m,2} < \cdots < \lambda_{1,m,\mathrm{arr}_{1,m}}, \tag{9.3}$$

$$\lambda_{1,m+1,1} < \lambda_{1,m+1,2} < \cdots < \lambda_{1,m+1,\mathrm{arr}_{1,m+1}} \tag{9.4}$$

then

$$\lambda_{1,m+1,1} < \lambda_{1,m,1}, \quad \lambda_{1,m+1,2} < \lambda_{1,m,2}, \ldots \lambda_{1,m+1,\mathrm{arr}_{1,m}} < \lambda_{1,m,\mathrm{arr}_{1,m}}. \tag{9.5}$$

Conjecture 1F$_1$. *Assign the weight* $\frac{1}{m}$ *to each of the points* $\lambda_{1,m,1}, \lambda_{1,m,2}, \ldots, \lambda_{1,m,m}$ *and denote by* $\lambda_{1,m}$ *corresponding discrete measure. Then*

1F$'_1$. *there exists a limiting continuous measure* $\lambda_1(w)$ *concentrated on a "limiting bow" and a "limiting arrow";*

1F$''_1$. $\int \log(w)\mathrm{d}\lambda_1(w) = \log\left(\frac{3}{2}\right)$.

Clearly, Conjecture 1F$_1$ implies Subhypothesis RH$_1$.

10 Purely Trivial Zeros

It is natural to try to understand to what extent the distribution of $\lambda_{1,m,1}$, $\lambda_{1,m,2}$, ..., $\lambda_{1,m,m}$ is due to the trivial zeros, and what is the contribution of the non-trivial zeros. To this end we can consider the function

$$\zeta_{\mathrm{T}}(z) = \frac{\zeta^*(z)}{2\xi(z)} \tag{10.1}$$

$$= \frac{\pi^{\frac{z}{2}}}{\Gamma(1+\frac{z}{2})}. \tag{10.2}$$

The points $\mathrm{z}_1 = -2,\ \mathrm{z}_2 = -4,\ \ldots,\ \mathrm{z}_n = -2n, \ldots$ are the only zeros of the function $\zeta_{\mathrm{T}}(z)$. The factor 2 in the denominator of (10.1) implies the equality

$$\zeta_{\mathrm{T}}(0) = 1 \tag{10.3}$$

analogous to the equality (2.4).

By analogy with (3.3) and (6.1), for every analytic function $f(z)$ such that

$$f(0) = 1 \tag{10.4}$$

we can consider the transformed function

$$\tilde{f}(w) = f\left(\tfrac{w}{1+w}\right) \tag{10.5}$$

with the expansion

$$\tilde{f}(w) = 1 + \theta_1(f)w + \cdots + \theta_m(f)w^m + \ldots, \tag{10.6}$$

form the matrices $L_{1,m}(f)$, counterparts of (6.3), with eigenvalues $\lambda_{1,m,1}(f)$, $\lambda_{1,m,2}(f)$ ..., $\lambda_{1,m,m}(f)$, and state various versions of subhypothesis $\mathrm{RH}_1(f)$.

Figures 10.1–10.4 show spectra $\mathrm{Spec}^{\lambda}_{1,m}(\zeta_{\mathrm{T}})$ in black color together with $\mathrm{Spec}^{\lambda}_{1,m}(\zeta^*)$ in blue color for $m = 24,\ 48,\ 96,\ 192$ respectively. These figures suggest that the distribution of the λ's is to a great extent determined by the trivial zeros.

The gamma function is supposed to be "simple", "completely understood", a function about which we know everything; it would be natural, as a first step towards the Riemann Hypothesis, to understand the character of the numbers $\lambda_{1,m,n}(\zeta_{\mathrm{T}})$.

11 Further Questions

Now, how could we see that RH_2, RH_3, ... are true? The Taylor expansion (5.1) doesn't tell us anything directly about the other poles of the function $1/\tilde{\zeta}(w)$. One way to overcome this obstacle could be to consider the function

$$\hat{\zeta}_l(z) = \frac{\zeta^*(z)}{\prod_{k=1}^{l-1}(1-\frac{z}{\mathrm{z}_k})}; \tag{11.1}$$

a separate paper may be devoted to the corresponding eigenvalues $\lambda_{1,m,1}(\hat{\zeta}_l)$, $\lambda_{1,m,2}(\hat{\zeta}_l)$ ..., $\lambda_{1,m,m}(\hat{\zeta}_l)$.

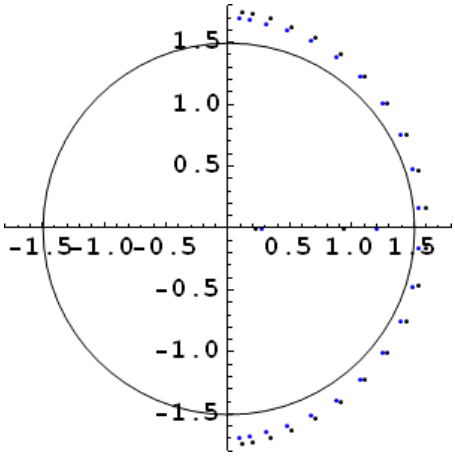


Figure 10.1: $\mathrm{Spec}^{\lambda}_{1,24}(\zeta^*)$ and $\mathrm{Spec}^{\lambda}_{1,24}(\zeta_{\mathrm{T}})$

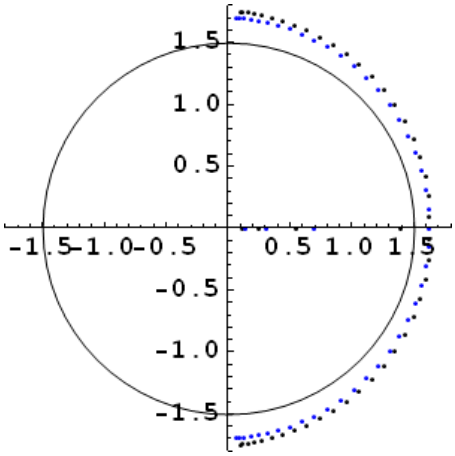


Figure 10.2: $\mathrm{Spec}^{\lambda}_{1,48}(\zeta^*)$ and $\mathrm{Spec}^{\lambda}_{1,48}(\zeta_{\mathrm{T}})$

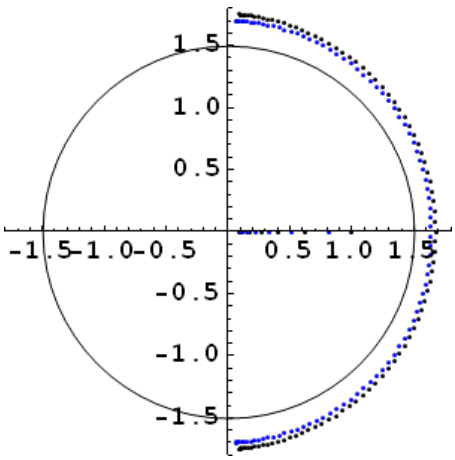


Figure 10.3: $\mathrm{Spec}^{\lambda}_{1,96}(\zeta^*)$ and $\mathrm{Spec}^{\lambda}_{1,96}(\zeta_{\mathrm{T}})$

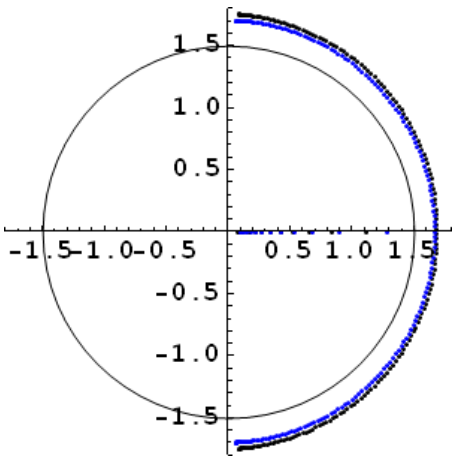


Figure 10.4: $\mathrm{Spec}^{\lambda}_{1,192}(\zeta^*)$ and $\mathrm{Spec}^{\lambda}_{1,192}(\zeta_{\mathrm{T}})$

12 Padé approximations

However, another approach to RH_m for arbitrary m looks more promising. This approach treats the first m trivial zeros "on equal" and is based on Padé approximations.

To begin with, let $P_{1,m}(w)$ and $Q_{1,m}(w)$ be polynomials such that

$$\tilde{\zeta}(w) \approx \frac{P_{1,m}(w)}{Q_{1,m}(w)} = \frac{1 + p_{1,m,1}w}{1 + q_{1,m,1}w + \cdots + q_{1,m,m}w^m} \tag{12.1}$$

$$= \tilde{\zeta}(w) + O(w^{m+2}) \tag{12.2}$$

It can be checked that

$$p_{1,m,1} = -\frac{\tau_{m+1}}{\tau_m} \tag{12.3}$$

and hence, according to (5.2), for $m \to \infty$

$$p_{1,m,1} \to \frac{3}{2} \tag{12.4}$$

and, respectively,

$$P_{1,m}(w) \to 1 + \tfrac{3}{2}w = 1 - \frac{w}{\mathrm{w}_1}. \tag{12.5}$$

Now let us consider the general case. Let let $P_{l,m}(w)$ and $Q_{l,m}(w)$ be such polynomials that

$$\tilde{\zeta}(w) \approx \frac{P_{l,m}(w)}{Q_{l,m}(w)} = \frac{1 + p_{l,m,1}w + \cdots + p_{l,m,l}w^l}{1 + q_{l,m,1}w + \cdots + q_{l,m,m}w^m} \tag{12.6}$$

$$= \tilde{\zeta}(w) + O(w^{l+m+1}) \tag{12.7}$$

According to a theorem of de Montessue [2, 3] (see also [1]) for every l, subhypothesis RH_l implies the following generalization of (12.5): *For all l for $m \to \infty$*

$$P_{l,m}(w) \to \prod_{k=1}^{l} \left(1 - \frac{w}{\mathrm{w}_l}\right). \tag{12.8}$$

We are going to deal only with the leading coefficient of $P_{l,m}(w)$ for which (12.8) implies the following generalization of (12.4):

Subhypothesis $\mathbf{RH}_l^{\mathbf{w}}$ (version 1). *For $m \to \infty$*

$$p_{l,m,l} \to \mathrm{W}_l \tag{12.9}$$

where

$$\mathrm{W}_l = \prod_{k=1}^{l} \left(-\frac{1}{\mathrm{w}_l}\right) = \prod_{k=1}^{l} \frac{2k+1}{2k}. \tag{12.10}$$

13 Back to the Riemann Hypothesis

Each subhypothesis $\mathrm{RH}_l^{\mathrm{w}}$ is, formally, weaker than the corresponding subhypothesis RH_l, nevertheless, taken together the subhypotheses $\mathrm{RH}_l^{\mathrm{w}}$ are equivalent to the subhypotheses RH_l, and thus we have

Riemann Hypothesis (version 5). *For every m the subhypothesis $\mathrm{RH}_l^{\mathrm{w}}$ is true.*

In order to see why it is so, suppose that the Riemann Hypothesis isn't valid, and let $\check{z}$ be a non-trivial zero of $\zeta(z)$ with $\Re(\check{z}) < \frac{1}{2}$. Then $\check{w} = \frac{\check{z}}{1-\check{z}}$ is a non-trivial zero of $\tilde{\zeta}(w)$ with $|\check{w}| < 1$. In the closed circle $|w| \le |\check{w}|$ there are only finitely many zeros of $\tilde{\zeta}(w)$; let us denote them by $\check{w}_1, \ldots, \check{w}_l$. By the above cited theorem of de Montessue, for $m \to \infty$

$$P_{l,m}(w) \to \prod_{k=1}^{l} \left(1 - \frac{w}{\check{w}_l}\right) \tag{13.1}$$

and hence

$$p_{l,m,l} \to \prod_{k=1}^{l} \left(-\frac{1}{\check{w}_l}\right). \tag{13.2}$$

It is easy to see that

$$\left|\prod_{k=1}^{l} \left(-\frac{1}{\check{w}_l}\right)\right| > \left|\prod_{k=1}^{l} \left(-\frac{1}{\mathrm{w}_l}\right)\right| = |\mathrm{W}_l| \tag{13.3}$$

which gives the required contradiction with (12.9).

14 More Determinants

An explicit expression for $p_{l,m,l}$ can be given (Jacobi [4], see also [1]):

$$p_{l,m,l} = \frac{\det(L_{l,m+1}(\zeta^*))}{\det(L_{l,m}(\zeta^*))} \tag{14.1}$$

where

$$L_{l,m}(f) = \begin{pmatrix} \theta_l(f) & \theta_{l-1}(f) & \ldots & \theta_{l-m+1}(f) \\ \theta_{l+1}(f) & \theta_l(f) & \ldots & \theta_{l-m+2}(f) \\ \vdots & \vdots & \ddots & \vdots \\ \theta_{l+m-1}(f) & \theta_{l+m-2}(f) & \ldots & \theta_l(f) \end{pmatrix} \tag{14.2}$$

with $\theta_0(f) = 1$ and $\theta_j(f) = 0$ for $j < 0$.

In terms of these matrices we have the following counterpart of (6.4):

$\mathrm{RH}_l^{\mathrm{w}}$ (version 2). *For $m \to \infty$*

$$\det(L_{l,m}(\zeta^*)) \;=\; \mathrm{W}_l^m(\mathrm{R}_l(\zeta^*) + o(1)). \tag{14.3}$$

with some constant $\mathrm{R}_l(\zeta^*)$.

In order to pass from (5.2), the second version of RH_1, to (5.7), the third version of RH_1, we needed the inequality (5.6) which we got from the numerical value (5.5). However, it is easy to see that $\mathrm{RH}_1(f)$ implies the inequality $\mathrm{R}_1(f) > 0$ for every function f satisfying condition (10.4). Namely, by analogy with (5.3) $\mathrm{RH}_1(f) = -\frac{1}{\mathrm{z}_1 f'(\mathrm{z}_1)}$ and $f'(\mathrm{z}_1) > 0$ because $\mathrm{z}_1 = -\frac{2}{3}$ is the least (in absolute value) zero of $f(z)$. By a similar argument, for every l the inequality $\mathrm{R}_l(f) > 0$ is implied by $\mathrm{RH}_l(f)$, and we have

$\mathrm{RH}_l^{\mathrm{w}}$ (version 3).

$$\lim_{m\to\infty} (\det(L_{l,m}(\zeta^*)))^{\frac{1}{m}} = \mathrm{W}_l. \tag{14.4}$$

15 More Eigenvalues

By analogy with (7.1), we have the representation

$$\det(L_{l,m}(f)) = \lambda_{l,m,1}(f)\lambda_{l,m,2}(f)\dots\lambda_{l,m,m}(f) \tag{15.1}$$

where $\lambda_{l,m,1}(f),\ \lambda_{l,m,2}(f),\ \dots,\ \lambda_{l,m,m}(f)$ are the eigenvalues of the matrix $L_{l,m}(f)$. Then, we have

$\mathrm{RH}_l^{\mathrm{w}}$ (version 4).

$$\lim_{m\to\infty} \left(\prod_{n=1}^{m} \lambda_{l,m,n}(\zeta^*) \right)^{\frac{1}{m}} = \mathrm{W}_l. \tag{15.2}$$

The (multi)set $\{\lambda_{l,m,1}(f),\ \lambda_{l,m,2}(f), \dots \lambda_{l,m,m}(f)\}$ will be called the λ-*spectrum* of the function f and will be denoted $\mathrm{Spec}^{\lambda}_{l,m}(f)$.

16 More about positions of eigenvalues

Figures 16.1–16.4 show spectra $\mathrm{Spec}^{\lambda}_{2,m}(\zeta^*)$ for $m = 24,\ 48,\ 96,\ 192$ respectively (higher resolution pictures and corresponding animation be downloaded from [5]).

We see that $\mathrm{Spec}^{\lambda}_{2,m}(\zeta^*)$ consists of the arrow, the bow (now looking into the opposite direction), and a new element, looking like a circle, which will be called *orbit*. The animation shows that the orbit has, on its right-hand side, a *rendezvous* with the arrow and, on its left-hand side, another *rendezvous* with the bow.

Figures 16.5–16.8 show spectra $\mathrm{Spec}^{\lambda}_{3,m}(\zeta^*)$ for $m = 24,\ 48,\ 96,\ 192$ respectively (higher resolution pictures and corresponding animation be downloaded from [5]).

We see that $\mathrm{Spec}^{\lambda}_{3,m}(\zeta^*)$ consists of the arrow, the bow (now rather rudimentary and looking into the same direction as in the case of $\mathrm{Spec}^{\lambda}_{1,m}$), and two orbits which constitute *target*. The animation shows that the inner orbit has, on its right-hand side, the rendezvous with the arrow and has, on its left-hand side, the rendezvous with the outer orbit. In its turn, the outer orbit has, on its left-hand side, the rendezvous with the inner orbit and has, on its right-hand side, the rendezvous with the bow.

One might expect that the target of the spectra $\mathrm{Spec}^{\lambda}_{4,m}(\zeta^*)$ would consist of three orbits but this is not the case. Figures 16.9–16.12 show spectra $\mathrm{Spec}^{\lambda}_{4,m}(\zeta^*)$

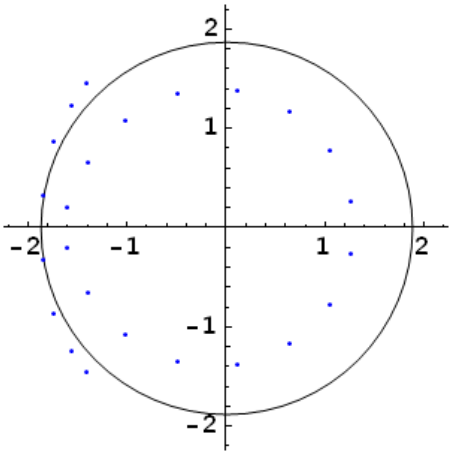


Figure 16.1: $\mathrm{Spec}^{\lambda}_{2,24}(\zeta^*)$

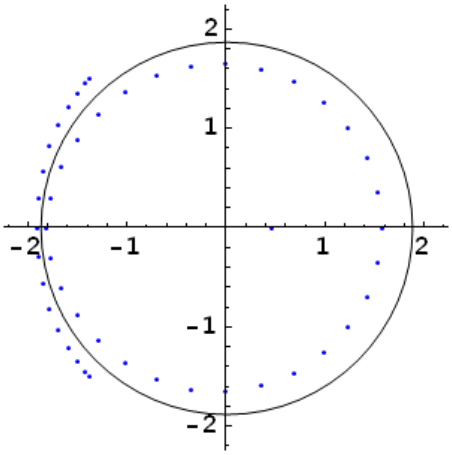


Figure 16.2: $\mathrm{Spec}^{\lambda}_{2,48}(\zeta^*)$

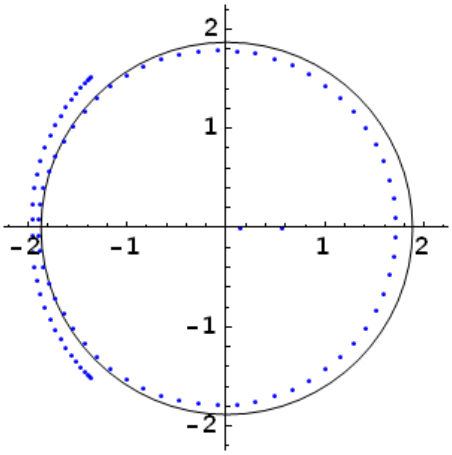


Figure 16.3: $\mathrm{Spec}^{\lambda}_{2,96}(\zeta^*)$

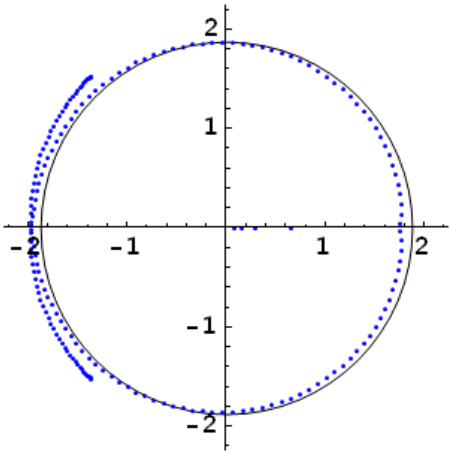


Figure 16.4: $\mathrm{Spec}^{\lambda}_{2,192}(\zeta^*)$

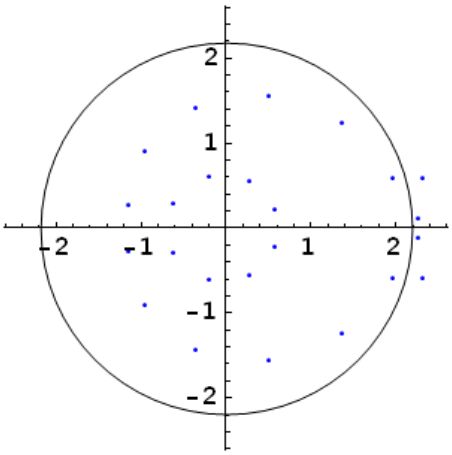


Figure 16.5: $\mathrm{Spec}^{\lambda}_{3,24}(\zeta^*)$

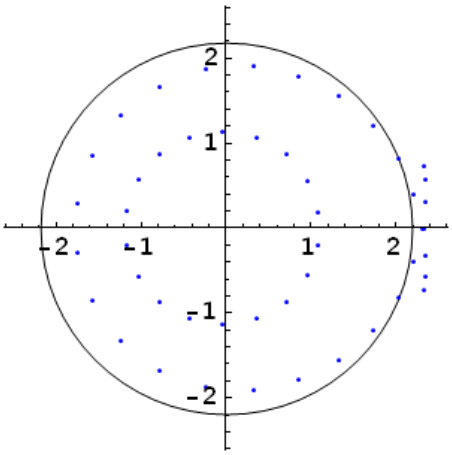


Figure 16.6: $\mathrm{Spec}^{\lambda}_{3,48}(\zeta^*)$

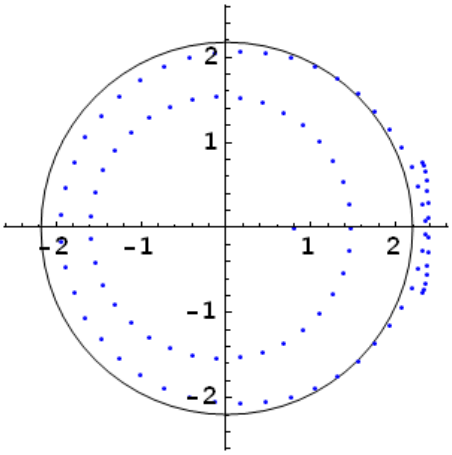


Figure 16.7: $\mathrm{Spec}^{\lambda}_{3,96}(\zeta^*)$

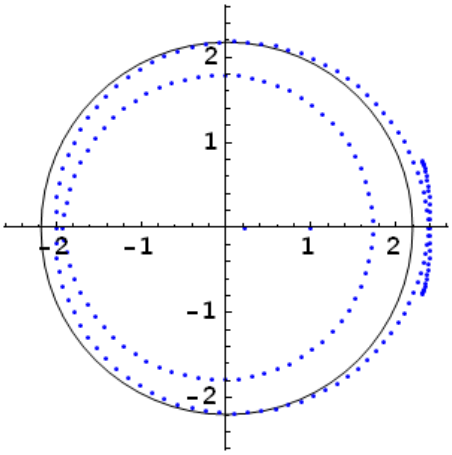


Figure 16.8: $\mathrm{Spec}^{\lambda}_{3,192}(\zeta^*)$

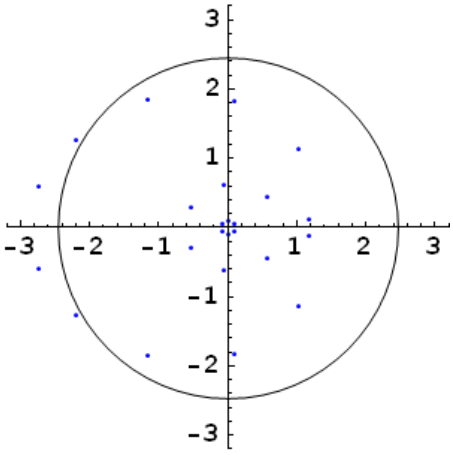


Figure 16.9: $\mathrm{Spec}^{\lambda}_{4,24}(\zeta^*)$

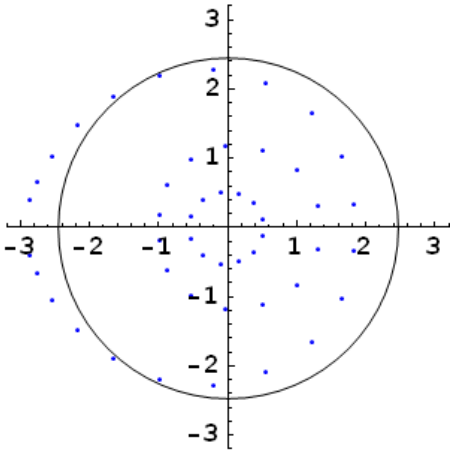


Figure 16.10: $\mathrm{Spec}^{\lambda}_{4,48}(\zeta^*)$

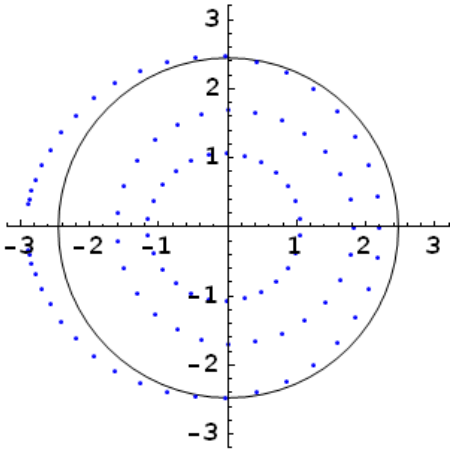


Figure 16.11: $\mathrm{Spec}^{\lambda}_{4,96}(\zeta^*)$

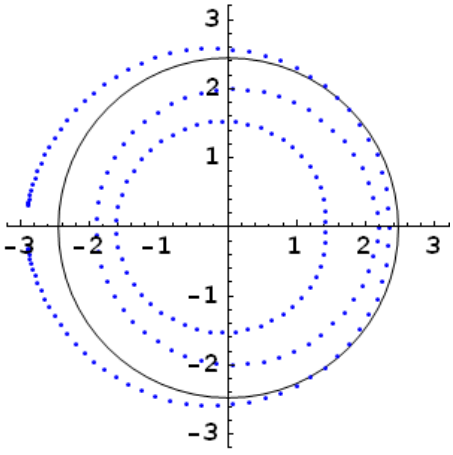


Figure 16.12: $\mathrm{Spec}^{\lambda}_{4,192}(\zeta^*)$

for $m = 24,\ 48,\ 96,\ 192$ respectively. (higher resolution pictures and corresponding animation be downloaded from [5]). We see that the entire structure of the spectra $\mathrm{Spec}^{\lambda}_{4,m}(\zeta^*)$ is the same as in the case of the spectra $\mathrm{Spec}^{\lambda}_{3,m}(\zeta^*)$ but the bow isn't rudimentary any longer, on the contrary, it is almost a circle.

The third orbit in the target appears in the spectra $\mathrm{Spec}^{\lambda}_{5,m}(\zeta^*)$. Figures 16.13–16.16 show spectra $\mathrm{Spec}^{\lambda}_{5,m}(\zeta^*)$ for $m = 24,\ 48,\ 96,\ 192$ respectively. (higher resolution pictures and corresponding animation be downloaded from [5]).

Similar, the fourth orbit in the target appears in the spectra $\mathrm{Spec}^{\lambda}_{6,m}(\zeta^*)$. Figures 16.17–16.20 show spectra $\mathrm{Spec}^{\lambda}_{6,m}(\zeta^*)$ for $m = 24,\ 48,\ 96,\ 192$ respectively. (higher resolution pictures and corresponding animation be downloaded from [5]).

The fifth orbit in the target appears in the spectra $\mathrm{Spec}^{\lambda}_{7,m}(\zeta^*)$. Figures 16.21–16.24 show spectra $\mathrm{Spec}^{\lambda}_{7,m}(\zeta^*)$ for $m = 24,\ 48,\ 96,\ 192$ respectively (higher resolution pictures and corresponding animation be downloaded from [5]).

The above pictures don't show the arrows in any of $\mathrm{Spec}^{\lambda}_{5,m}(\zeta^*)$, $\mathrm{Spec}^{\lambda}_{6,m}(\zeta^*)$, $\mathrm{Spec}^{\lambda}_{7,m}(\zeta^*)$ for $m = 24,\ 48,\ 96,\ 192$ but probably the arrows will appear for sufficiently large m.

17 More Conjectures

The above pictures suggest the following conjectures which, in particular, generalize conjectures $1\mathrm{A}_1$–$1\mathrm{F}_1$.

Conjecture 1A. *There are never multiple eigenvalues in* $\mathrm{Spec}^{\lambda}_{l,m}(\zeta^*)$.

Conjecture 1B. *For all* l, $\sup_m(\max(\mathrm{Arr}_{l,m}(\zeta^*)))$ *is a positive number.*

Conjecture 1C. *For all* l, $\inf_m(\min(\mathrm{Arr}_{l,m}(\zeta^*)))$ *is a positive number.*

Accepting the same agreement about the largest real eigenvalue in $\mathrm{Spec}^{\lambda}_{l,m}(\zeta^*)$ as was done above in the case of $\mathrm{Spec}^{\lambda}_{1,m}(\zeta^*)$, we can state the following two conjectures.

Conjecture 1D. *For all* l *and* k, *the numbers* $\mathrm{arr}_{l,m}(\zeta^*) = ||\mathrm{Arr}_{l,m}(\zeta^*)||$, $\mathrm{orb}_{l,m,k}(\zeta^*) = ||\mathrm{Orb}_{l,m,k}(\zeta^*)||$ $\mathrm{bow}_{l,m}(\zeta^*) = ||\mathrm{Bow}_{l,m}(\zeta^*)||$ *of eigenvalues belonging to the arrow* $\mathrm{Arr}_{l,m}(\zeta^*)$, *the orbit* $\mathrm{Orb}_{l,m,k}(\zeta^*)$, *and the bow* $\mathrm{Bow}_{l,m}(\zeta^*)$ *respectively don't decrease when* m *increases.*

Conjecture 1E. *For all* l, *if*

$$\mathrm{Arr}_{l,m}(\zeta^*) = \{\lambda_{l,m,1}(\zeta^*), \ldots, \lambda_{l,m,\mathrm{arr}_{l,m}(\zeta^*)}(\zeta^*)\}, \tag{17.1}$$

$$\mathrm{Arr}_{l,m+1}(\zeta^*) = \{\lambda_{l,m+1,1}(\zeta^*), \ldots, \lambda_{l,m+1,\mathrm{arr}_{l,m+1}(\zeta^*)}(\zeta^*)\} \tag{17.2}$$

and

$$\lambda_{l,m,1}(\zeta^*) < \lambda_{l,m,2}(\zeta^*) < \cdots < \lambda_{l,m,\mathrm{arr}_{l,m}(\zeta^*)}(\zeta^*), \tag{17.3}$$

$$\lambda_{l,m+1,1}(\zeta^*) < \lambda_{l,m+1,2}(\zeta^*) < \cdots < \lambda_{l,m+1,\mathrm{arr}_{l,m+1}(\zeta^*)}(\zeta^*) \tag{17.4}$$

then

$$\lambda_{l,m+1,1}(\zeta^*) < \lambda_{l,m,1}(\zeta^*), \ldots, \lambda_{l,m+1,\mathrm{arr}_{l,m}(\zeta^*)}(\zeta^*) < \lambda_{l,m,\mathrm{arr}_{l,m}(\zeta^*)}(\zeta^*). \tag{17.5}$$

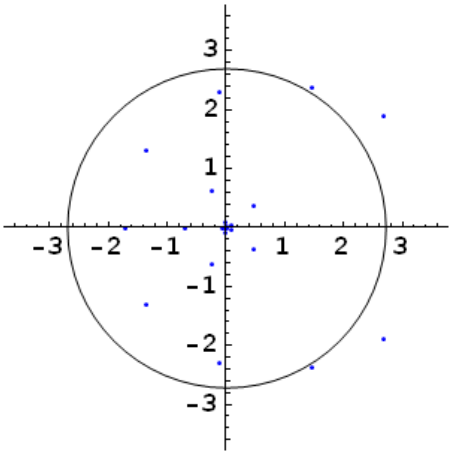


Figure 16.13: $\mathrm{Spec}^{\lambda}_{5,24}(\zeta^*)$

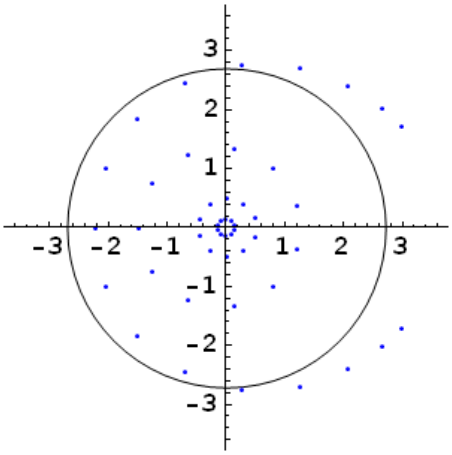


Figure 16.14: $\mathrm{Spec}^{\lambda}_{5,48}(\zeta^*)$

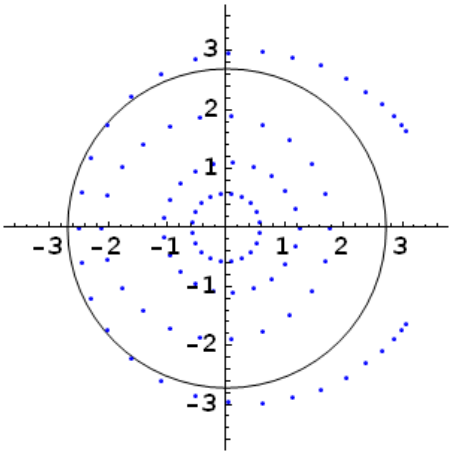


Figure 16.15: $\mathrm{Spec}^{\lambda}_{5,96}(\zeta^*)$

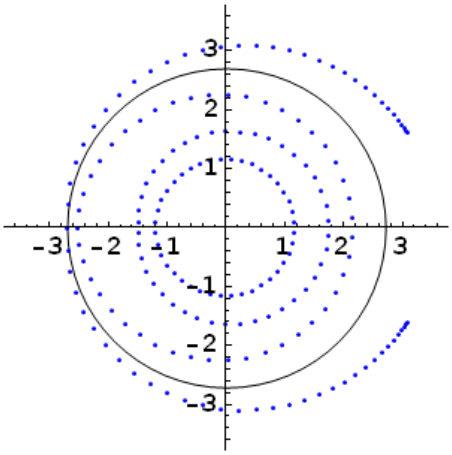


Figure 16.16: $\mathrm{Spec}^{\lambda}_{5,192}(\zeta^*)$

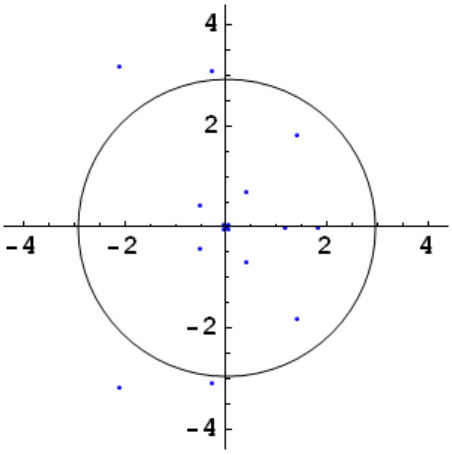


Figure 16.17: $\mathrm{Spec}^{\lambda}_{6,24}(\zeta^*)$

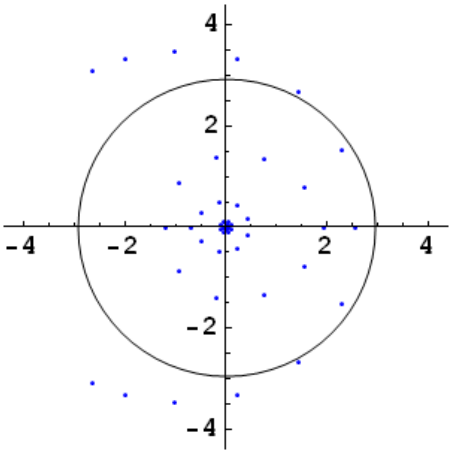


Figure 16.18: $\mathrm{Spec}^{\lambda}_{6,48}(\zeta^*)$

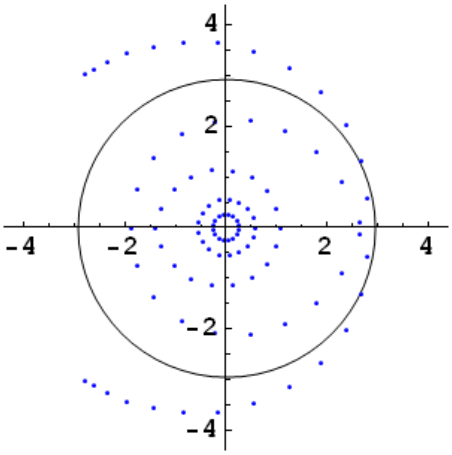


Figure 16.19: $\mathrm{Spec}^{\lambda}_{6,96}(\zeta^*)$

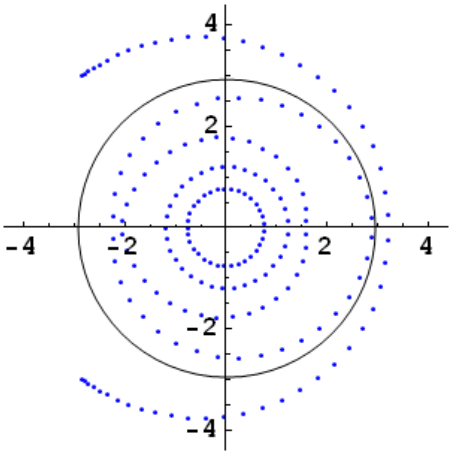


Figure 16.20: $\mathrm{Spec}^{\lambda}_{6,192}(\zeta^*)$

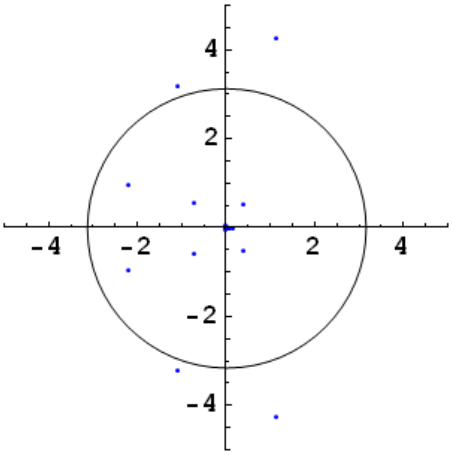


Figure 16.21: $\mathrm{Spec}^{\lambda}_{7,24}(\zeta^*)$

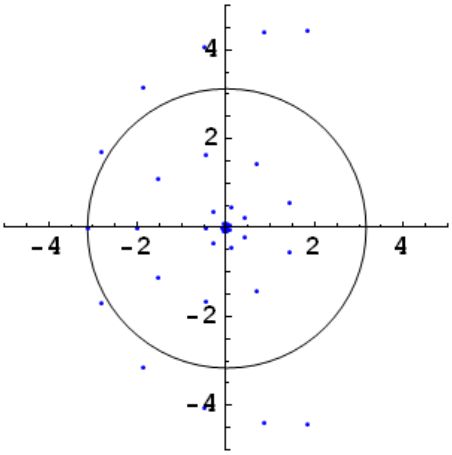


Figure 16.22: $\mathrm{Spec}^{\lambda}_{7,48}(\zeta^*)$

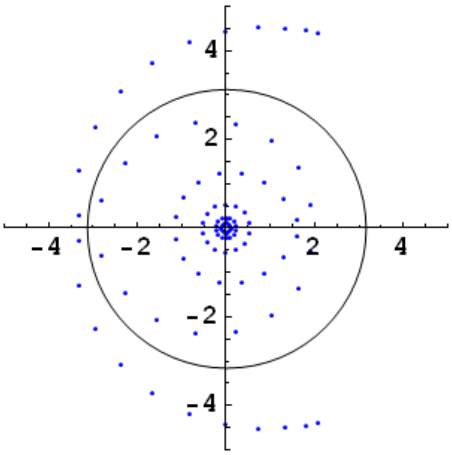


Figure 16.23: $\mathrm{Spec}^{\lambda}_{7,96}(\zeta^*)$

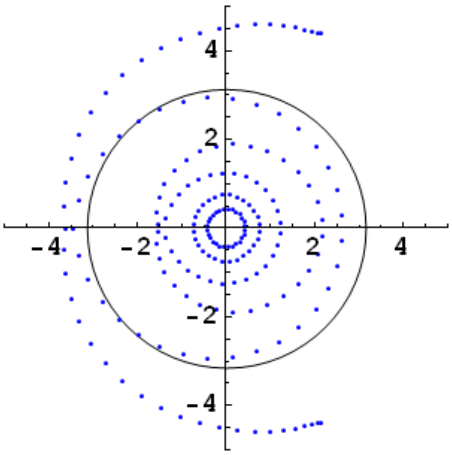


Figure 16.24: $\mathrm{Spec}^{\lambda}_{7,192}(\zeta^*)$

Conjecture 1F. *For given l and m, assign the weight $\frac{1}{m}$ to each point $\lambda_{l,m,1}(\zeta^*), \lambda_{l,m,2}(\zeta^*), \dots, \lambda_{l,m,m}(\zeta^*)$ and denote by $\lambda_{l,m}(\zeta^*)$ the corresponding discrete measure. Then*

1F′. *for $m \to \infty$ there exists a limiting continuous measure $\lambda_l^{\zeta^*}(w)$ concentrated on a "limiting bow", a "limiting arrow", and a "limiting target" consisting of a number of "limiting orbits";*

1F″. $\int \log(w) \mathrm{d}\lambda_l^{\zeta^*}(w) = \log(\mathrm{W}_l)$.

Clearly, Conjecture 1F implies the Riemann Hypothesis.

An precise definition of the bow $\mathrm{Bow}_{l,m}$ and of individual orbits $\mathrm{Orb}_{l,m,k}$ constituting the target $\mathrm{Targ}_{l,m}$ is a subtle matter because of the rendezvous. The following conjectures implicitly presuppose that "*It is possible to split* $\mathrm{Spec}_{l,m}^{\lambda}(\zeta^*)$ *into* $\mathrm{Arr}_{l,m}(\zeta^*)$, $\mathrm{Orb}_{l,m,k}(\zeta^*)$, *and* $\mathrm{Bow}_{l,m}(\zeta^*)$ *in such a manner that...*".

Conjecture 1G. *For every l and k the number of eigenvalues in $\mathrm{Arr}_{l,m}(\zeta^*)$, $\mathrm{Orb}_{l,m,k}(\zeta^*)$, and $\mathrm{Bow}_{l,m}(\zeta^*)$ doesn't decrease with the growth of m.*

Conjecture 1H. *For every $l > 1$, m, and k the eigenvalues from the orbit $\mathrm{Orb}_{l,m,k}(\zeta^*)$ almost lie on a circle and are almost equidistributed on it.*

Conjecture 1I. *For every $l > 1$ the limiting target $\mathrm{Targ}_l(\zeta^*)$ consists of some number $\mathrm{targ}_l(\zeta^*)$ of limiting orbits $\mathrm{Orb}_{l,k}(\zeta^*)$ and*

1I′ *all limiting orbits are circles;*

1I″ *on each limiting orbit the limiting measure $\lambda_l^{\zeta^*}(w)$ is constant;*

1I‴ *the limiting orbits $\mathrm{Orb}_{l,k}(\zeta^*)$ can be numbered in such a way that for $k < \mathrm{targ}_l(\zeta^*)$ the limiting orbit $\mathrm{Orb}_{l,k}(\zeta^*)$ lies inside the limiting orbit $\mathrm{Orb}_{l,k+1}(\zeta^*)$ and touches it at one real point $\mathrm{Rend}_{l,k}(\zeta^*)$ called the* rendezvous-point*; the innermost limiting orbit has rendezvous point $\mathrm{Rend}_{l,0}(\zeta^*)$ with the limiting arrow $\mathrm{Arr}_l(\zeta^*)$, and the outmost limiting orbit has rendezvous point $\mathrm{Rend}_{l,\mathrm{targ}_l(\zeta^*)}(\zeta^*)$ with the limiting bow $\mathrm{Bow}_l(\zeta^*)$; moreover, $\mathrm{Rend}_{l,k+1}(\zeta^*) < \mathrm{Rend}_{l,k}(\zeta^*)$ for even k and $\mathrm{Rend}_{l,k+1}(\zeta^*) > \mathrm{Rend}_{l,k}(\zeta^*)$ for odd k.*

18 Hankel matrix representation

As it was indicated in Section 1.6, we can give an alternative representation for the numbers τ_m (defined by the expansion (15.1)), in the form of determinants, by rearranging the columns of the matrices $L_{1,m}$ introduced by (6.3). More generally, we rearrange the columns of the matrices $L_{l,m}(f)$ defined by (14.2):

$$M_{l,m}(f) = \\ -(-1)^{\frac{(m+1)(m+2)}{2}} \begin{pmatrix} \theta_{l+m-1}(f) & \theta_{l+m-2}(f) & \dots & \theta_l(f) \\ \theta_{l+m-2}(f) & \theta_{l+m-3}(f) & \dots & \theta_{l-1}(f) \\ \vdots & \vdots & \ddots & \vdots \\ \theta_l(f) & \theta_{l-1}(f) & \dots & \theta_{l-m+1}(f) \end{pmatrix}. \quad (18.1)$$

Clearly, for all l and m we have

$$\det(M_{l,m}(f)) = \det(L_{l,m}(f)), \tag{18.2}$$

so we have the following reformulations of versions 2 and 3 of subhypothesis $\mathrm{RH}_l^{\mathrm{w}}$ from Sections 1.14 (with W_l defined by (12.10)):

$\mathbf{RH}_l^{\mathbf{w}}$ (version 2′). *For* $m \to \infty$

$$\det(M_{l,m}(\zeta^*)) \;=\; \mathrm{W}_l^m(\mathrm{R}_l(\zeta^*) + o(1)). \tag{18.3}$$

with some constant $\mathrm{R}_l(\zeta^*)$.

$\mathbf{RH}_l^{\mathbf{w}}$ (version 3′).

$$\lim_{m\to\infty} (\det(M_{l,m}(\zeta^*)))^{\frac{1}{m}} \;=\; \mathrm{W}_l. \tag{18.4}$$

19 Yet More Eigenvalues

By analogy with (15.1), we have the representation

$$\det(M_{l,m}(f)) = \mu_{l,m,1}(f)\mu_{l,m,2}(f)\dots\mu_{l,m,m}(f) \tag{19.1}$$

where $\mu_{l,m,1}(f),\ \mu_{l,m,2}(f),\ \dots,\ \mu_{l,m,m}(f)$ are the eigenvalues of the matrix $M_{l,m}(f)$. Respectively, we have

$\mathbf{RH}_l^{\mathbf{w}}$ (version 5).

$$\lim_{m\to\infty} \left(\prod_{n=1}^{m} \mu_{l,m,n}(\zeta^*) \right)^{\frac{1}{m}} = \mathrm{W}_l. \tag{19.2}$$

The (multi)set $\{\mu_{l,m,1}(f),\ \mu_{l,m,2}(f), \dots \mu_{l,m,m}(f)\}$ will be called *μ-spectrum* of the function f and will be denoted $\mathrm{Spec}_{l,m}^{\mu}(f)$.

20 Positions of the μ eigenvalues

According to (19.2), the (geometric) mean of $\mu_{1,m,1}(\zeta^*),\ \mu_{1,m,2}(\zeta^*),\ \dots,\ \mu_{1,m,m}(\zeta^*)$ approaches W_l when m goes to infinity, which is similar to the behavior of the eigenvalues $\lambda_{1,m,1}(\zeta^*),\ \lambda_{1,m,2}(\zeta^*),\ \dots,\ \lambda_{1,m,m}(\zeta^*)$. However, there are many differences between the distribution of the eigenvalues from spectra $\mathrm{Spec}_{l,m}^{\mu}(\zeta^*)$ and $\mathrm{Spec}_{l,m}^{\lambda}(\zeta^*)$.

The first such difference is evident: the numbers $\mu_{1,m,1}(\zeta^*),\ \mu_{1,m,2}(\zeta^*),\ \dots,\ \mu_{1,m,m}(\zeta^*)$, being the eigenvalues of a Hankel matrix with real entries, are all real themselves.

Computations suggest that in contrast to the case of the λ-spectra, the union $\cup_{m=1}^{\infty}\mathrm{Spec}_{l,m}^{\mu}(\zeta^*)$ is bounded neither from above nor from below. Moreover, the point 0 is a limit point of this set. That is why it is reasonable to consider the sets

$$\mathrm{Spec}_{l,m}^{\ln|\mu|}(f) = \{\ln|\mu| : \mu \in \mathrm{Spec}_{l,m}^{\mu}(f)\} \tag{20.1}$$

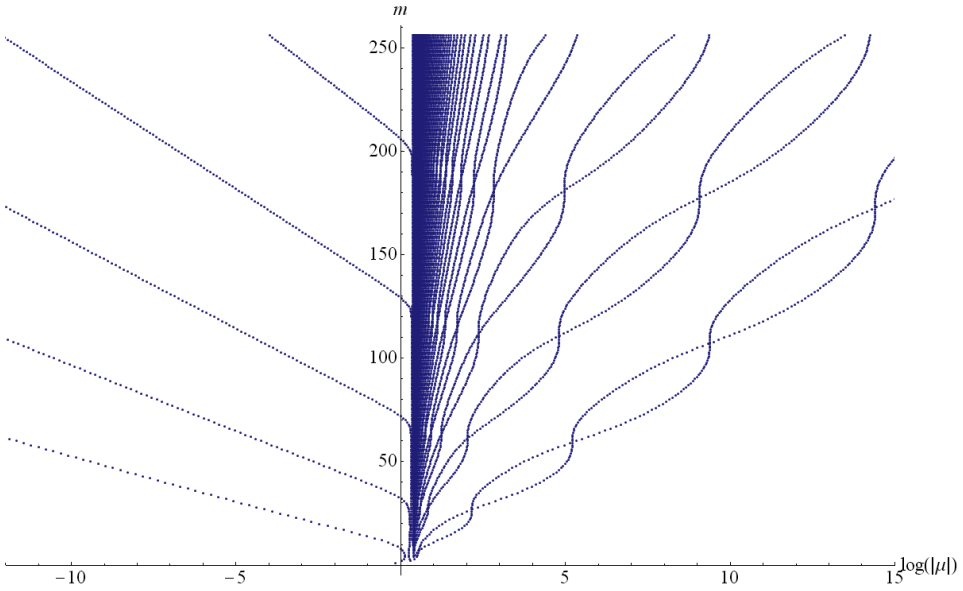


Figure 20.1: $\mathrm{Spec}_{1,m}^{\ln|\mu|}(\zeta^*),\ m = 1, \ldots, 256.$

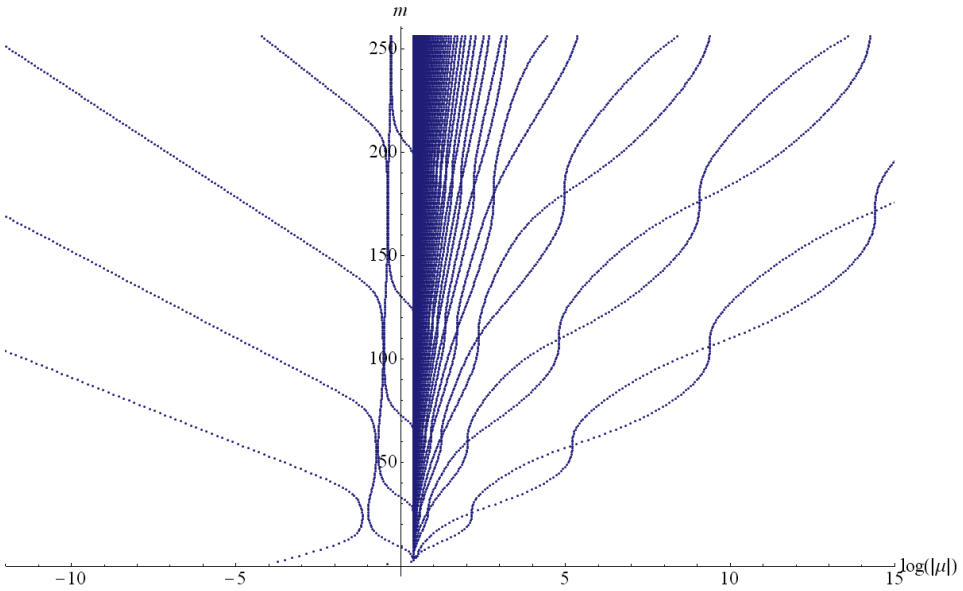


Figure 20.2: $\mathrm{Spec}_{2,m}^{\ln|\mu|}(\zeta^*),\ m = 1, \ldots, 256.$

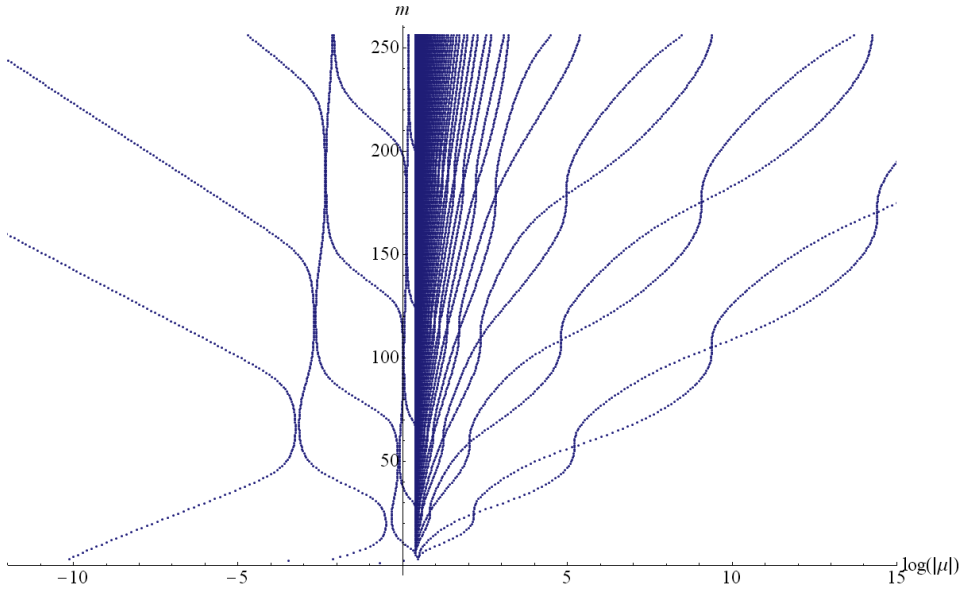


Figure 20.3: $\mathrm{Spec}_{3,m}^{\ln|\mu|}(\zeta^*),\ m = 1, \ldots, 256.$

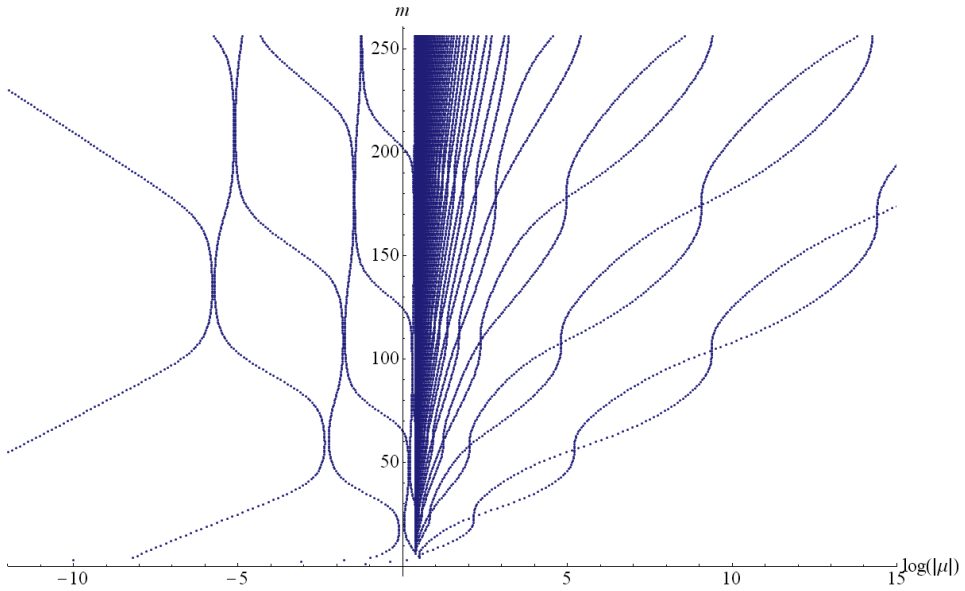


Figure 20.4: $\mathrm{Spec}_{4,m}^{\ln|\mu|}(\zeta^*),\ m = 1, \ldots, 256.$

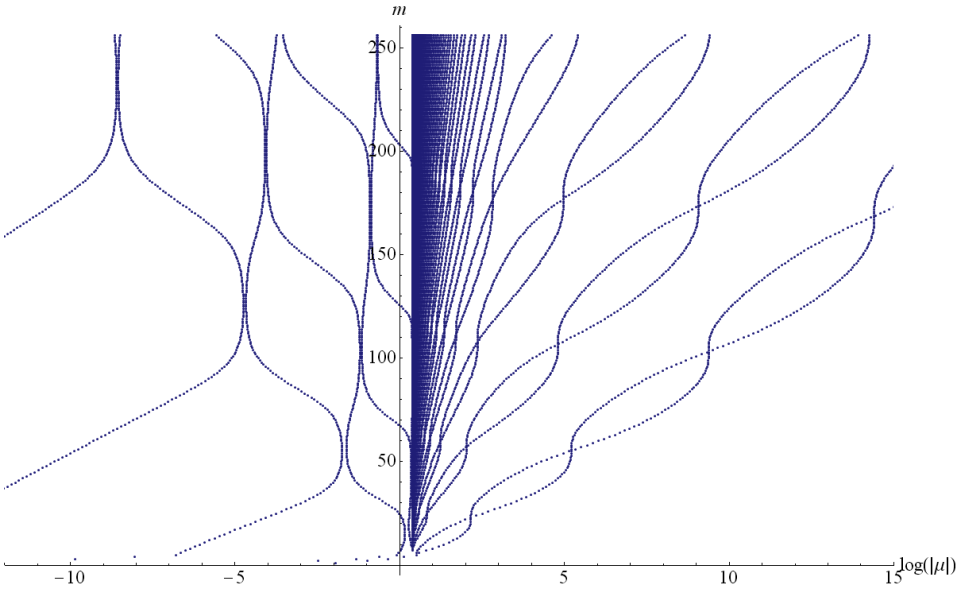


Figure 20.5: $\mathrm{Spec}_{5,m}^{\ln|\mu|}(\zeta^*),\ m = 1, \ldots, 256.$

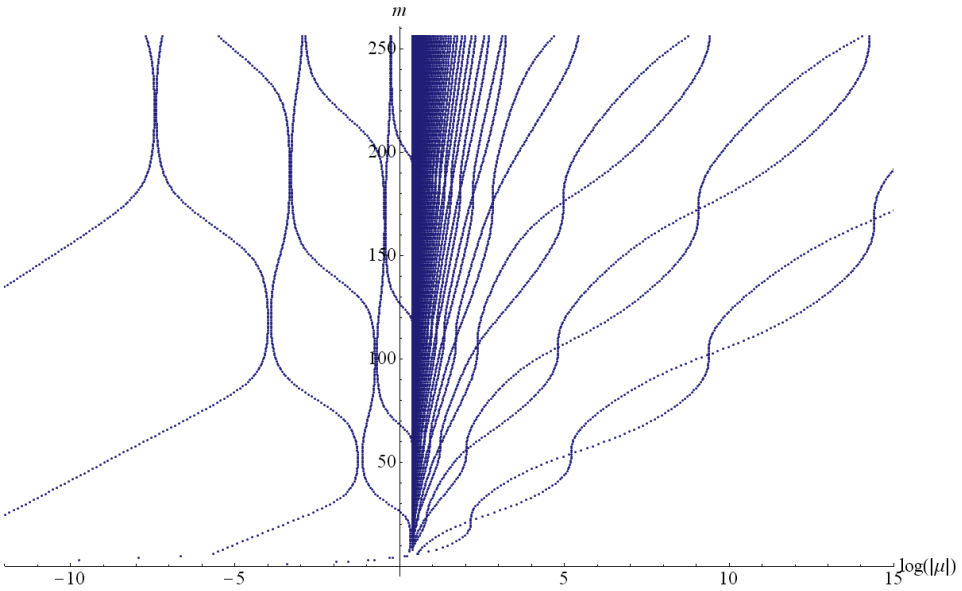


Figure 20.6: $\mathrm{Spec}_{6,m}^{\ln|\mu|}(\zeta^*),\ m = 1, \ldots, 256.$

which will be called *logarithmic μ-spectra*. When exhibiting several logarithmic μ-spectra, we will shift the lines vertically, that is, an eigenvalue $\ln|\mu|$ from $\mathrm{Spec}_{l,m}^{\ln|\mu|}(f)$ will be placed at point $(x,y)=(\ln|\mu|,m)$.

Figures 20.1–20.6 show spectra $\mathrm{Spec}_{1,m}^{\ln|\mu|}(\zeta^*)$, ..., $\mathrm{Spec}_{2,m}^{\ln|\mu|}(\zeta^*)$ for $m=1,\dots,256$ (higher resolution version of these pictures can be downloaded from [5] as well as some animations showing these spectra and thus revealing another kind of "hidden life of Riemann's zeta function").

The pictures and the animations show that with the growth of m some elements of $\mathrm{Spec}_{l,m}^{\ln|\mu|}(\zeta^*)$ go to $-\infty$ while others go to $+\infty$; the former will be called *electrons* and the latter will be called *trains* (we postpone formal definition of splitting $\mathrm{Spec}_{l,m}^{\ln|\mu|}(\zeta^*)$ into *lower part* $\mathrm{Spec}_{l,m}^{\ln|\mu|<}(\zeta^*)$, consisting of the electrons, and *upper part* $\mathrm{Spec}_{l,m}^{\ln|\mu|>}(\zeta^*)$ consisting of the trains).

The names "electrons" and "trains" were suggested by the following visual patterns. The electrons behave like charged particles, namely, they bounce. The trains all go in pairs (a surprising feature!) and every now and then they overtake one another.

21 New Conjectures

The above pictures suggest the following conjectures.

Conjecture 2A. *For all l*

$$\lim_{m\to\infty}\max(\mathrm{Spec}_{l,m}^{\ln|\mu|}(\zeta^*))=+\infty. \tag{21.1}$$

Conjecture 2B. *For all l*

$$\lim_{m\to\infty}\min(\mathrm{Spec}_{l,m}^{\ln|\mu|}(\zeta^*))=-\infty. \tag{21.2}$$

It is impossible to see from the above pictures whether for the μ-spectra there is a counterpart of Conjecture 1F about the λ-spectra. To make this clearer, in analogy with this conjecture, let us assign to each point of $\mathrm{Spec}_{l,m}^{\ln|\mu|}(\zeta^*)$ the weight $\frac{1}{m}$, and denote by $\mu_{l,m}^{\zeta^*}(x)$ the corresponding discrete measure on real numbers. Further, let $F_{l,m}^{\zeta^*}(x)$ denote the corresponding distribution function. In terms of these functions we have

$\mathbf{RH}_l^{\mathbf{w}}$ (version 6).

$$\lim_{m\to\infty}\left(\int_{-\infty}^{+\infty}x\,\mathrm{d}F_{l,m}^{\zeta^*}(x)\right)=\log(\mathrm{W}_l). \tag{21.3}$$

Figures 21.1–21.12 show these functions for $l=1,6$ and $m=8,16,32,64,256$. These pictures suggest

Conjecture 2C. *For every l functions $F_{l,m}^{\zeta^*}(x)$ have, as $m\to\infty$, the pointwise limiting continuous distribution function $F_l^{\zeta^*}(x)$.*

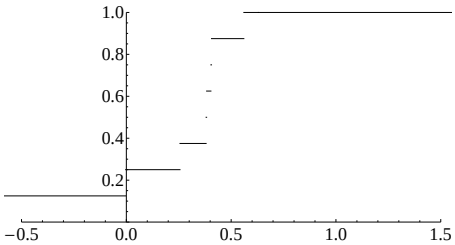


Figure 21.1: $F^{\zeta^*}_{1,8}(x)$.

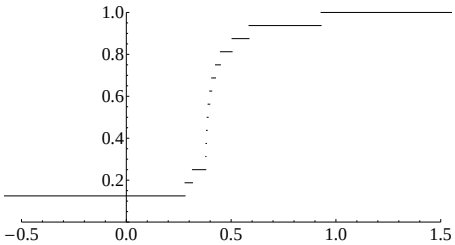


Figure 21.2: $F^{\zeta^*}_{1,16}(x)$.

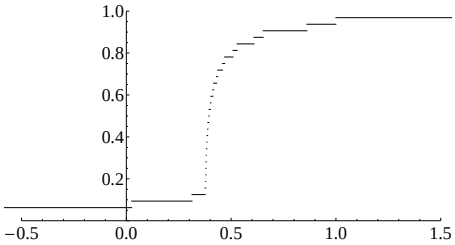


Figure 21.3: $F^{\zeta^*}_{1,32}(x)$.

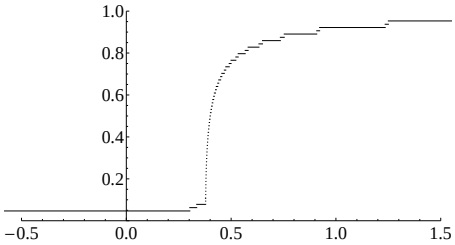


Figure 21.4: $F^{\zeta^*}_{1,64}(x)$.

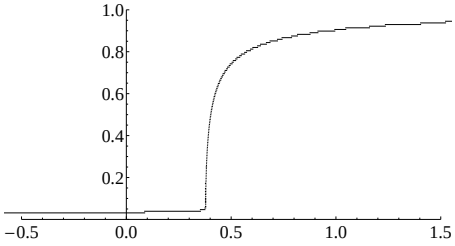


Figure 21.5: $F^{\zeta^*}_{1,128}(x)$.

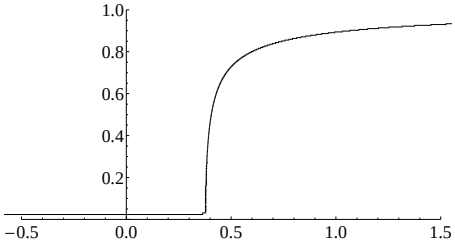


Figure 21.6: $F^{\zeta^*}_{1,256}(x)$.

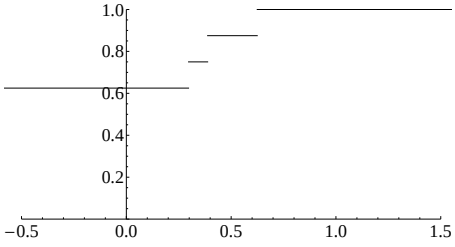


Figure 21.7: $F^{\zeta^*}_{6,8}(x)$.

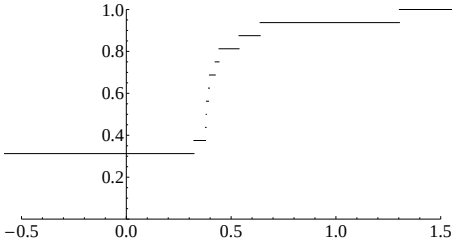


Figure 21.8: $F^{\zeta^*}_{6,16}(x)$.

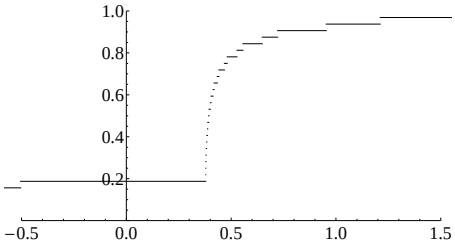


Figure 21.9: $F^{\zeta^*}_{6,32}(x)$.

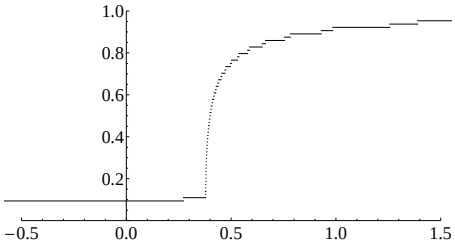


Figure 21.10: $F^{\zeta^*}_{6,64}(x)$.

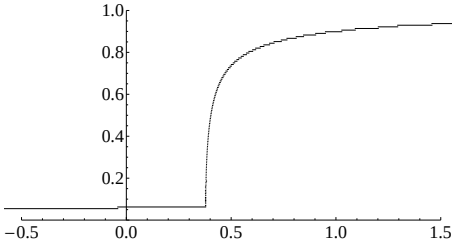


Figure 21.11: $F^{\zeta^*}_{6,128}(x)$.

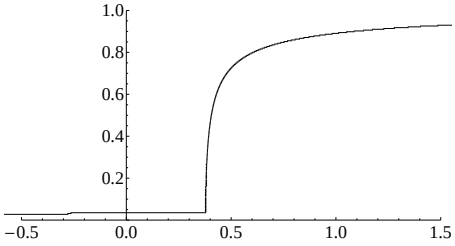


Figure 21.12: $F^{\zeta^*}_{6,256}(x)$.

This is an analog of part 1F′ of Conjecture 1F for λ-spectra. However, it seems that part 1F″ of this conjecture has no analog for μ-spectra. According to (21.3), such an analog would say that for all l

$$\int_{-\infty}^{+\infty} x \, \mathrm{d}F_l^{\zeta^*}(x) = \log(\mathrm{W}_l). \tag{21.4}$$

But theses integrals do not seem to exist:

Conjecture 2D. *For every l*

$$\int_{-\infty}^{0} x \, \mathrm{d}F_l^{\zeta^*}(x) = -\infty, \qquad \int_{0}^{+\infty} x \, \mathrm{d}F_l^{\zeta^*}(x) = +\infty. \tag{21.5}$$

This implies that the validity of (21.3) should be due to some fine correlation between eigenvalues from $\mathrm{Spec}^{\ln|\mu|<}_{l,m}(\zeta^*)$ and $\mathrm{Spec}^{\ln|\mu|>}_{l,m}(\zeta^*)$. The subtleness of this correlation follows from (very surprising)

Conjecture 2E. *All distribution functions $F_l^{\zeta^*}(x)$ coincide; that is, for all l and x*

$$F_l^{\zeta^*}(x) = F^{\zeta^*}(x) \tag{21.6}$$

for some continuous distribution function $F^{\zeta^*}(x)$.

Acknowledgement

The author is very grateful to Martin Davis for some help with the English.

References

[1] Baker G. A., Jr. *Essntials of Padé Approximations*. Academic Press, New York, SanFrancisco, London, 1975.

[2] de Montessue de Ballore. Sur le fraction continues algébriques. *Bull. Soc. Math. France*, 30, 28–36, 1902.

[3] de Montessue de Ballore. Sur le fraction continues algébriques. *Rend. Circ. Math. Palermo*, 19, 1–73, 1905.

[4] Jacobi C. G. J. Uber die Darstellung einer Reihe Gegebner Werthe durch eine Gebrochne Rationale Function. *J. Reine Angew. Math.*, 30, 127–156, 1846.

[5] Matiyasevich, Yu. Hidden Life of Riemann's Zeta Function. `http://logic.pdmi.ras.ru/~yumat/personaljournal/zetahiddenlife`.

[6] Matiyasevich, Yu. Hidden Life of Riemann's Zeta Function 1. Arrow, Bow, and Targets. `http://www.citebase.org/abstract?id=oai:arXiv.org:0707.1983`, 2007.

[7] Matiyasevich, Yu. Hidden Life of Riemann's Zeta Function 2. Electrons and Trains. To be submitted to ArXive.

[8] Riemann, B. Über die Anzhal der Primzahlen unter einer gegebenen Grösse. *Monatsberichter der Berliner Akademie*, November, 1959. Included into: Riemann, B. *Gesammelte Werke*. Teubner, Leipzig, 1892; reprinted by Dover Books, New York, 1953.

Absolute quadratic pseudoprimes

Richard G.E. Pinch

2 Eldon Road, Cheltenham, Glos GL52 6TU, U.K.
rgep@chalcedon.demon.co.uk

Abstract

We describe some primality tests based on quadratic rings and discuss the absolute pseudoprimes for these tests.

1 Introduction

We describe some primality tests based on quadratic rings and discuss the absolute pseudoprimes for these tests.

2 Primality tests

We briefly recall some standard probabilistic primality tests. We assume throughout that N is the integer under test, and that N is already known to be odd and not a perfect power.

The *Fermat criterion* with base b is the condition $b^{N-1} \equiv 1 \bmod N$. We shall usually distinguish between a *criterion* or *condition*, which is a necessary condition for primality, and a *test*, which specifies the details of the application of that criterion. For example, we would expect a Fermat test to include a preliminary trial division (at least as far as 2), possibly a test to eliminate perfect powers, and to specify a method (deterministic or random) for selecting the base b. A *(Fermat) probable prime* base b is a number N which passes this test: a *(Fermat) pseudoprime* is a composite number which passes. An *absolute (Fermat) pseudoprime* is a composite number which satisfies the Fermat criterion for every base b with $(b, n) = 1$. It is well-known that these are just the *Carmichael* numbers: N is a Carmichael number iff N is square-free with at least three prime factors and $p - 1 | N - 1$ for every prime p dividing N.

For background on Carmichael numbers and details of previous computations we refer to our previous paper [24]: in that paper we described the computation of the Carmichael numbers up to 10^{15} and presented some statistics. These computations have since been extended [26] to 10^{16}, using the same techniques.

We can refine this to the *Fermat–Euler criterion* by requiring that $b^{(N-1)/2} \equiv \pm 1 \bmod N$, and again by identifying the sign to form the *Euler–Jacobi criterion* $b^{(N-1)/2} \equiv \left(\frac{b}{N}\right) \bmod N$, where $\left(\frac{b}{N}\right)$ is the Jacobi symbol. This latter is the primality criterion of Solovay–Strassen [31],[32].

Proposition 15. *1. If N is an absolute pseudoprime for the Fermat–Euler criterion we have $b^{(N-1)/2} \equiv +1 \bmod N$ for all b prime to N.*

2. There are no absolute pseudoprimes for the Euler–Jacobi criterion.

Proof. For the first part, suppose that p and q are distinct prime factors of N. Given b prime to N, write $b = b_1 b_2$ where $b_1 \equiv b \bmod p$ and $\equiv 1 \bmod q$; so we have $b_2 \equiv 1 \bmod p$ and $\equiv b \bmod q$. The assumption on N implies that $b_i^{(N-1)/2} \equiv \pm 1 \bmod N$ for $i = 1, 2$, but in each case the sign must be $+1$ considering $b_1^{(N-1)/2} \bmod q$ and $b_2^{(N-1)/2} \bmod p$. So $b^{(N-1)/2} = (b_1 b_2)^{(N-1)/2} \equiv 1 \bmod N$.

The second part follows by observing that N is not a perfect square, so $\left(\frac{b}{N}\right) = -1$ for some b. □

The final extension to the Fermat criterion which we consider is the *strong* or Miller–Rabin criterion [20],[21],[27]. Given an odd N, write $N - 1 = 2^r s$, with s odd, and for $b \bmod N$ form the sequence

$$b^s, b^{2s}, \ldots, b^{2^{r-1}s}, b^{2^r s} = b^{N-1} \mod N$$

in which each term is the square of the preceding. The criterion requires that the sequence end in 1, and further that the first occurence of 1 either be at the first term, or be preceded by -1.

It is clear that the Miller–Rabin criterion includes the Fermat–Euler criterion: in fact it includes the Euler–Jacobi criterion as well. There are thus no absolute pseudoprimes for this criterion: indeed, the proportion of bases b for which a composite number can satsify the criterion is at most $1/4$.

3 Quadratic rings

A variety of primality tests have been proposed which extend the Fermat test to a quadratic ring. Let N and d be integers: we shall assume throughout that N is odd and d is prime to N. Let $R = R(N, d)$ denote the quadratic ring $\mathbb{Z}[X]/\langle N, X^2 - d\rangle$. It is natural to denote the image of X in this ring by $\sqrt{d}$. If M and N are coprime then the Chinese Remainder Theorem gives a natural isomorphism between $R(MN, d)$ and $R(M, d) \oplus R(N, d)$, so we shall be interested in the case when N is an odd prime power p^f.

We define an automorphism $'$ of $R = R(N, d)$ by mapping $\sqrt{d} \mapsto -\sqrt{d}$: this is inudeced by the automorphism $X \mapsto -X$ of $\mathbb{Z}[X]$, which is compatible with the quotient map. The fixed points of $'$ form a subring $F(N, d)$ which is just the copy of $\mathbb{Z}/\langle N\rangle$ inside R. The *norm* of an element β is $\mathcal{N}(\beta) = \beta\beta'$: this map takes values in $\mathbb{Z}/\langle N\rangle$. If $\mathcal{N}(\beta)$ is invertible (prime to N), then so is β, with $\beta^{-1} = \beta'/\mathcal{N}(\beta)$. The unit group R^* contains the *corational* or *twisted multiplicative group* $C(N, d)$, consisting of the elements of norm one. The action of $'$ on C is given by $\beta \mapsto \beta^{-1}$. The *anti-norm* is defined on R^* by $\mathcal{A}(\beta) = \beta/\beta'$.

We denote the set of elements of norm b by $C_b(p, d)$. If non-empty, it is a coset of $C = C_1$.

3.1 Prime modulus

We first consider the case when N is a prime p. If d is a quadratic non-residue of p then R is the field $\mathbb{F}_{p^2}$, whereas if d is a quadratic residue of p, then R is the direct sum $\mathbb{F}_p \oplus \mathbb{F}_p$. Hence the unit group R^* is either a cyclic group of order $p^2 - 1$ or a direct product of two cyclic groups of order $p - 1$. If R is $\mathbb{F}_{p^2}$, the automorphism $'$ is the Frobenius automorphism $\beta \mapsto \beta^p$: otherwise it is the interchange of the two direct summands.

The norm map is $\mathcal{N}(\beta) = \beta^{p+1}$ in $\mathbb{F}_{p^2}$ and $(a,b) \mapsto ab$ in $\mathbb{F}_p \oplus \mathbb{F}_p$; the anti-norm is $\mathcal{A}(\beta) = \beta^{1-p}$ in $\mathbb{F}_{p^2}$ and $(a,b) \mapsto a/b$ in $\mathbb{F}_p \oplus \mathbb{F}_p$.

The corational group C is either the subgroup generated by the anti-norm γ^{p-1} of a generator γ of R^* when $R = \mathbb{F}_{p^2}$, or the set of elements corresponding to the form (x, x^{-1}) when $R = \mathbb{F}_p \oplus \mathbb{F}_p$. It is cyclic of order $p - \left(\frac{d}{p}\right)$, that is, $p+1$ or $p-1$ respectively.

If β is an element of R then β^p is either β' or β in the two cases: we can express this succinctly by saying that the *Frobenius condition*

$$(x + y\sqrt{d})^p \quad = \quad x + \left(\frac{d}{p}\right) y\sqrt{d} \tag{3.1}$$

holds.

The subring F fixed by $'$ is the field $\mathbb{F}_p$ in each case, either as a subfield of $\mathbb{F}_{p^2}$ or as the diagonal in $\mathbb{F}_p \oplus \mathbb{F}_p$. So in each case F^* is cyclic of order $p-1$.

The norm map has kernel C and image F^*. The anti-norm has kernel F^* and image C. The restriction of the anti-norm to C is just $\beta \mapsto \beta^2$, with kernel $C \cap F^* = \{\pm 1\}$ and image a cyclic group of order $\left(p - \left(\frac{d}{p}\right)\right)/2$.

When $R = \mathbb{F}_{p^2}$, the norm map is surjective , so C_b is a non-empty coset of $C = C_1$, of order $p+1$. When $R = \mathbb{F}_p \oplus \mathbb{F}_p$ then $C_b = \{(a, b/a) : a \in \mathbb{F}_p\}$ is a coset of C of order $p-1$.

We briefly consider the special case C_{-1}. When $R = \mathbb{F}_{p^2}$, this is the set of odd powers of $\gamma^{(p-1)/2}$, where γ is a generator of the cyclic group R^*. When $R = \mathbb{F}_p \oplus \mathbb{F}_p$, this is the set of pairs $(b, -1/b)$ for $b \in {\mathbb{F}_p}^*$. We note that the map $\beta \mapsto \beta^2$ maps C_- onto C in the first case and onto the index 2 subgroup of pairs $(b^2, 1/b^2)$ in the second case.

Proposition 16. *Let $\beta \in \mathbb{F}_{p^2}$ with $\mathcal{N}(\beta) = B$. If the order of B in ${\mathbb{F}_p}^*$ is e, then the order of β in ${\mathbb{F}_{p^2}}^*$ is $e(p+1)$.*

Proof. Let $B = g^f$ where $ef = p-1$ and g is a generator of ${\mathbb{F}_p}^*$. Let γ be a generator of ${\mathbb{F}_{p^2}}^*$ with $\mathcal{N}(\gamma) = \gamma^{p+1} = g$, and let $\beta = \gamma^r$. We have $\mathcal{N}(\beta) = \beta^{p+1} = \gamma^{r(p+1)} = B = g^f = \gamma^{(p+1)f}$, so $r(p+1) \equiv (p+1)f \bmod p^2-1$ and $r \equiv f \bmod p-1$, say $r = f + s(p-1)$. Replacing γ by γ^{1+se}, which is again a generator of ${\mathbb{F}_{p^2}}^*$, we may assume that $\beta = \gamma^f$. The order of β is then $(p^2-1)/f = e(p+1)$. □

Lemma 17. *Let G be a cyclic group of order r. The number of solutions to the equation $X^n = b$ in G is zero or (n,f) where the order of b in G is e and $ef = r$. For solutions to exist, it is necessary and sufficient that $n/(n,f)$ be prime to $r/(n,f)$.*

Proof. Choose a generator g of G so that $b = g^f$, and put $X = g^y$. The equation becomes $ny \equiv f \bmod r$, and hence $y.n/(f,n) \equiv f/(f,n) \bmod r/(f,n)$. Since $f/(f,n)$ is coprime to $n/(f,n)$, it is clearly necessary for solutions to exist that $n/(n,f)$ be coprime to $r/(f,n)$.

Suppose now that this condition holds. The equation for y has a unique solution y modulo $r/(f,n)$, and hence (f,n) solutions modulo r. □

3.2 Prime powers

We now consider the structure of $R(p^f, d)$. The map $\rho : R(p^f, d) \to R(p, d)$ given by reduction modulo p is a ring homomorphism, with kernel $pR(p^f, d)$ of order $p^{2(f-1)}$. An element $\beta \in R(p^f, d)$ is invertible iff the norm $\mathcal{N}(\beta)$ is invertible in

$\mathbb{Z}/\langle p^f \rangle$ iff $\mathcal{N}(\beta)$ is prime to p iff $\rho(\mathcal{N}(\beta)) = \mathcal{N}(\rho(\beta))$ is invertible in $\mathbb{Z}/\langle p \rangle$ iff $\rho(\beta)$ is invertible in $R(p,d)$. So the restriction of ρ to R^* is a group homomorphism onto $R(p,d)^*$ and has kernel with order a power of p.

If d is a quadratic non-residue of p then it cannot be congruent to a square modulo p^f for any f. If d is a quadratic residue of p then by Hensel's Lemma (since $p > 2$), d is a square modulo p^f for any $f \geq 1$ and so $R(p^f, d)$ is isomorphic to the direct sum $\mathbb{Z}/\langle p^f \rangle \oplus \mathbb{Z}/\langle p^f \rangle$.

The group $R(p^f, d)^*$ is cyclic of order $p^{2f-2}(p^2-1)$ if d is a quadratic non-residue of p, since we can lift a generator of ${\mathbb{F}_{p^2}}^*$ to a generator of R^* (see, for example, [25]). If d is a quadratic residue of p, then R^* is $\mathbb{Z}/\langle p^f \rangle^* \oplus \mathbb{Z}/\langle p^f \rangle^*$, a direct product of two cyclic groups of order $p^{f-1}(p-1)$.

We consider the cosets C_b. Again if $\left(\frac{d}{p}\right) = +1$ then $C_b = \{(a, b/a) : a \in \mathbb{Z}/\langle p^f \rangle\}$ is a coset of C of order $p^{f-1}(p-1)$. If $\left(\frac{d}{p}\right) = -1$ then a solution to $\mathcal{N}(\beta) \equiv b \bmod p$ can be lifted by Hensel's Lemma to a solution modulo p^f, so C_b is again a non-empty coset of C, of order $p^{f-1}(p+1)$.

Proposition 18. *Let $R = R(p^f, d)$ with $f > 1$. There are elements of multiplicative order divisible by p in every coset C_b.*

Proof. If $\left(\frac{d}{p}\right) = +1$ then $C_b = \{(a, b/a) : a \in \mathbb{Z}/\langle p^f \rangle\}$ and we can choose a to have multiplicative order divisible by p: the order of the pair $(a, b/a)$ will then be a multiple of that of a and hence of p.

If $\left(\frac{d}{p}\right) = -1$, we consider the elements of order not divisible by p: there are $p^2 - 1$ of these. Since the reduction map ρ is one-to-one on such elements, there are $p+1$ elements of order prime to p in C_1 and so every coset C_b has at most $p+1$ such elements. Hence each coset has elements of order divisible by p. □

Proposition 19. *Let $R = R(p, d)$. Let $\alpha \in C$ and $b \in F$. The equations $\mathcal{N}(\beta) = b$, $\mathcal{A}(\beta) = \alpha$ are soluble if α and b are both squares or both non-squares in C and F respectively.*

Proof. If $\left(\frac{d}{p}\right) = +1$ then let $\beta \leftrightarrow (r, s) \in \mathbb{F}_p \oplus \mathbb{F}_p$ and $\alpha \leftrightarrow (a, 1/a)$. The equations on β are equivalent to $rs = b$, $r/s = a$, and these are equivalent to $r^2 = ab$, $s^2 = b/a$. These are soluble iff ab is a square in $\mathbb{F}_p$, which is in turn equivalent to the stated conditions on α and b.

If $\left(\frac{d}{p}\right) = -1$ then let γ be a generator of ${\mathbb{F}_p}^*$, and write $\beta = \gamma^x$, $b = \gamma^{(p+1)y}$ and $\alpha = \gamma^{(p-1)z}$. The equations on β are equivalent to $(p+1)x \equiv (p+1)y$ and $(p-1)x \equiv (p-1)z$ modulo $p^2 - 1$: these are equivalent to $x \equiv y \bmod p-1$ and $x \equiv z \bmod p+1$. By the Chinese Remainder Theorem these are soluble simultaneously iff $y \equiv z \bmod (p-1, p+1)$, that is, modulo 2. Again this is equivalent to the stated conditions on α and b. □

3.3 Lucas sequences

Let $\beta = x + y\sqrt{d}$ satisfy the equation $X^2 - AX + B = 0$ where A is the trace $\beta + \beta'$ and B is the norm $\beta\beta'$. We define the *Lucas sequences* $U_k(A, B)$ and $V_k(A, B)$

associated to β by

$$U_k = \frac{\beta^k - \beta'^k}{\beta - \beta'} \tag{3.2}$$

$$V_k = \beta^k + \beta'^k \tag{3.3}$$

or equivalently

$$\beta^k = \frac{V_k + U_k\sqrt{d}}{2}.$$

There are recurrence relationships

$$\begin{array}{lll} U_0 = 0, & U_1 = 1, & U_{k+1} = AU_k - BU_{k-1} \\ V_0 = 2, & V_1 = A, & V_{k+1} = AV_k - BV_{k-1} \end{array}$$

There are fast formulae for evaluating U and V using the duplication formulae

$$U_{2k} = U_k V_k \tag{3.4}$$

$$V_{2k} = V_k^2 - 2B^k \tag{3.5}$$

and

$$U_{2k+1} = U_{k+1}V_k - B^k \tag{3.6}$$

$$V_{2k+1} = V_{k+1}V_k - AB^k \tag{3.7}$$

which are particularly convenient if $B = \pm 1$: see, for example, Riesel [28] (4.30–47) and Joye and Quisquater [15].

The *Dickson polynomials* $g_k(X, -B)$ are defined by

$$g_k(X, -B) = \sum_{j=0}^{\lfloor k/2 \rfloor} \frac{k}{k-j}\binom{k-j}{j}(-B)^j X^{k-2j}$$

and have the property that

$$V_k = g_k(-A, -B).$$

See Lidl and Niederreiter [19] (7.6).

4 Fermat-type tests and strengthening

We can generalise the notion of the Fermat test to other families of groups. Let $\mathcal{G}$ be a family of abelian groups $G(N)$ defined for all positive integers N composed of integers from some infinite set $\mathcal{P}$ of primes. We suppose that these groups satisfy the *Chinese Remainder property*, that is, $G(MN) \cong G(M) \oplus G(N)$ whenever M and N are coprime. We also assume that the group operations in $G(N)$ are easy to perform. We denote the order of $G(N)$ by $\phi_{\mathcal{G}}(N)$ and the exponent by $\lambda_{\mathcal{G}}(N)$. We suppose that there is a function $F(N)$ which is easily computable and agrees with $\lambda_{\mathcal{G}}(N)$ whenever N is prime. We further suppose that the groups in $\mathcal{G}$ have the *splitting property*: if $x \in G(MN)$ is a *splitting element*, that is, satisfies $x = (1, z) \in G(M) \oplus G(N)$, where 1 is the identity of $G(M)$ and z is not the identity of $G(N)$, then there is a fast algorithm for factoring MN.

The $\mathcal{G}$-Fermat test for primality of N is to take a random element of $b \in G(N)$ and to test whether $b^{F(N)}$ is the identity in $G(N)$. If not, N is certainly composite:

otherwise we call N an $\mathcal{G}$-probable prime, and an $\mathcal{G}$-pseudoprime if it is in fact composite. An *absolute* $\mathcal{G}$-pseudoprime has this property whenever $b \in G(N)$.

The first example of such a system is the multiplicative group $G(N) = (\mathbb{Z}/\langle N \rangle)^*$. We have $\mathcal{P} = \{$ all primes $\}$ and $F(p) = p - 1$. The splitting property is achieved by applying Euclid's algorithm to find $\mathrm{hcf}\{x - 1, N\}$ if x is a splitting element.

We can express a number of the quadratic tests in the same framework, using groups associated to the quadratic ring $R(N, d)$. If we take $G(N)$ to be the unit group C in $R(N, d)^*$, then $F(p) = p - \left(\frac{d}{p}\right)$, and the Fermat condition becomes test A^1.

Now let π be a prime: we shall usually take $\pi = 2$. We assume throughout that N is always prime to π. Define the *π-strengthening* of the $\mathcal{G}$-Fermat test for N by writing $f(N) = \pi^r s$ with s prime to π, and forming the sequence

$$b^s, \quad b^{\pi s}, \ \ldots \ , \ b^{\pi^r s} \in G(N) \ :$$

the test requires that the sequence end in 1, which is the Fermat condition, and further that the first occurence of 1 in the sequence not be preceded by a splitting element.

The Miller–Rabin test is the 2-strengthening of the usual Fermat test: a splitting element will be an $e \not\equiv 1 \bmod N$ with $e^2 \equiv 1$, by considering $\mathrm{hcf}\{e \pm 1, N\}$.

We can express the effect of the π-strengthening by letting $o_\pi(b, G(N))$ be the power of π dividing the order of b in the group $G(N)$. The additional requirement of the π-strengthening is that the value of $o_\pi(b, G(p_i^{a_i}))$ should be the same for every prime power $p_i^{a_i}$ dividing N. If so, we call this common value the *level* of b: it is the position in the sequence of the first occurrence of 1.

For a group $G(p^a)$, we define the *π-dimension* d of $G(p^a)$ as the dimension of the elements of $G(p^a)$ of order dividing π as a vector space over $\mathbb{F}_\pi$, and the *π-height* h of $G(p^a)$ as the maximal power of π dividing the order of any element of $G(p^a)$: so h is the largest value of any $o_\pi(b, G(p^a))$. In particular, each of π^d and π^h divides $\phi_{\mathcal{G}}(p^a)$ and π^h divides $\lambda_{\mathcal{G}}(p^a)$.

4.1 Groups of dimension 1

Suppose for the moment that the dimension $d = 1$, so that the π-part of $G(p^a)$ is cyclic and $\phi_{\mathcal{G}}(p^a) = \pi^h m$ with m prime to π. Let $c(l)$ denote the proportion of $b \in G(p^a)$ for which $o_\pi(b, G(p^a)) = l$. We have $c(0)$ equal to the proportion of elements x of $G(p^a)$ which satisfy $x^m = 1$, so $c(0) = m/\phi_{\mathcal{G}}(p^a) = \pi^{-h}$. Each subsequent $c(l)$ for $0 < l \leq h$ is the proportion of elements of $G(p^a)$ which satisfy $x^{\pi^l m} = 1$ but not $x^{\pi^{l-1} m} = 1$, that is, $c(l) = \pi^{l-h}(1 - \pi^{-1})$.

Put $N = \prod_{i=1}^t p_i^{a_i}$. Let $c_i(l)$ denote the proportion of $b \in G(p_i^{a_i})$ for which $o_\pi(b, G(p_i^{a_i})) = l$. Let $W(N)$ be the number of element of $G(N)$ which satisfy the Fermat part of the criterion, and $S_\pi(N)$ the number which satisfy the π-strengthening. We have

$$S_\pi(N) = W(N) \sum_{l=0}^{r} \prod_{i=1}^{t} c_i(l).$$

Proposition 20. *Suppose that $d = 1$. Let $F(N) = \pi^r s$ with s prime to π. The proportion of elements which satisfy the π-strengthening of the Fermat criterion is at most π^{-H} if r or one of the h_i is zero, and at most π^{1-t} otherwise.*

Proof. Let $S = \sum_{l=0}^{r} \prod_{i=1}^{t} c_i(l)$. Put $H = \sum_i h_i$ and let $\rho = \min\{r, h_i\}$. The term $\prod_{i=1}^{t} c_i(l)$ is π^{-H} for $l = 0$; π^{tl-H-t} for $l \leq \rho$; and zero otherwise.

If $\rho = 0$ then $S = \prod_{i=1}^{t} c_i(0) = \pi^{-H}$. So consider the case $\rho \geq 1$. We have all the $h_i \geq 1$ and $H \geq \rho t \geq t \geq 1$. So

$$S = \pi^{-H}\left(1 + \sum_{l=1}^{\rho} \pi^{t(l-1)}\right) = \pi^{-H}\left(1 + \frac{\pi^{t\rho} - 1}{\pi^t - 1}\right)$$

Suppose that $0 \leq a \leq H - 1$. We have

$$\left(\pi^{H-a} - \pi\right)(\pi^a - 1) \geq 0$$

and, rearranging, $\pi^H + \pi^1 \geq \pi^{H-a} + \pi^{1+a}$ (alternatively, consider them as integers written in base π). So

$$\pi^H + \pi \geq \pi^{H+1-t} + \pi^t,$$

$$\pi^{H+1} + \pi \geq \pi^H + \pi^{H+1-t} + \pi^t,$$

$$\pi^{\rho t} - 1 \leq \pi^H - 1 \leq \pi^{H+1} - \pi^t - \pi^{H+1-t} + 1 = \left(\pi^t - 1\right)\left(\pi^{H+1-t} - 1\right)$$

$$\frac{\pi^{\rho t} - 1}{\pi^t - 1} + 1 \leq \pi^{H+1-t}$$

giving $S \leq \pi^{1-t}$ as required. □

5 Quadratic primality tests

We can use the Frobenius criterion (3.1) as a primality testing criterion. Given N, we select an arbitrary d prime to N and $\beta = x + y\sqrt{d}$. The symbol $\left(\frac{d}{N}\right)$ is interpreted as the Jacobi symbol: its computation can be carried our by a variant of the Euclidean Algorithm and verifies that $(d, n) = 1$ as a by-product. We require that $B = \mathcal{N}(\beta)$ be prime to N and then that the Frobenius condition hold for N to be declared probably prime. See Grantham [12, 11].

There are a number of specialisations of this condition. We let A denote the Frobenius condition (3.1) for the number N: that is, for any $\beta = x + y\sqrt{d}$ we have $V_N \equiv x$ and $U_N \equiv \left(\frac{d}{N}\right) y$ modulo N, where U_k and V_k are the Lucas sequences (3.3) associated to β. We let B denote the condition that $V_N \equiv x \bmod N$, and C the condition that $U_{N-\epsilon} \equiv 0 \bmod N$, where $\epsilon = \left(\frac{d}{N}\right)$.

Let X denote one of these conditions. We introduce some notation for various specialisations of the condition X. We let $X(d)$ denote the requirement that the condition hold for a given discriminant d. We let X_ϵ, where ϵ is $+$ or $-$, denote the requirement that the condition hold whenever $\left(\frac{d}{N}\right) = \epsilon$. We let X^b denote the requirement that the condition hold for all β with norm b. So A^1_-, for example, denotes the condition that $\beta^N = \beta'$ for all $\beta = x + y\sqrt{d}$ of norm 1 with $\left(\frac{d}{N}\right) = -1$.

We refer to these conditions collectively as *quadratic* primality criteria.

Proposition 21. *For given $\epsilon = \pm 1$, the conditions B_ϵ and C_ϵ together are equivalent to A_ϵ.*

Proof. It is clear that A_ϵ implies both of B_ϵ and C_ϵ. In the other direction, suppose that $\beta = x + y\sqrt{d}$ satisfies both of B_ϵ and C_ϵ, where $\left(\frac{d}{N}\right) = \epsilon$.

If $\epsilon = +1$ we have $\beta^N = x + z\sqrt{d}$ for some z and $\beta^{N-1} = v + 0\sqrt{d}$. So $\beta^N = v\beta = vx + vz\sqrt{d}$. Equating coefficients, we have $vx \equiv x \bmod N$, so $v \equiv 1$ and $z \equiv y$: that is, $\beta^N \equiv \beta$.

If $\epsilon = -1$ we have $\beta^N = x + z\sqrt{d}$ for some z and $\beta^{N+1} = v + 0\sqrt{d}$. So $\beta^N = v\beta'/B = (v/B)(x - y\sqrt{d})$. Equating coefficients, we must have $v = B$ and $\beta^N \equiv \beta'$.

So in each case condition A_ϵ is satisfied. □

We note that the result applies to the specialisations A^b_ϵ, B^b_ϵ, C^b_ϵ.

Consider condition A_-, which requires that $\beta^N \equiv \beta' \bmod N$. This implies that $\beta^{N+1} = \beta\beta' = B$, and so implies that $B^{N-1} \equiv 1 \bmod N$. It also implies that $(\beta/\beta')^N = \beta'/\beta$, so $\alpha^{N+1} = 1$ for all α in the corational group C_1. We can thus interpret criterion A_- or A as including the conventional Fermat criterion and its analogue for the corational group.

5.1 Absolute quadratic pseudoprimes

We consider composite numbers satisfying one of these criteria for all permissible choices of β: we call such a number an *absolute pseudoprime* for the relevant criterion.

We put $\beta = x + y\sqrt{d}$ with norm $B = x^2 - dy^2$. We assume throughout that N is not a prime power, that N is prime to $6dB$ and that, if $B \neq 1$ then N is prime to $B - 1$.

Proposition 22. *1. An absolute pseudoprime for criteria A_+, A_- or B must be a Carmichael number.*

2. There are no absolute pseudoprimes for criterion A.

3. An absolute pseudoprime for criterion A^{-1}_ϵ must also be an absolute pseudoprime for criterion A^1_ϵ for each $\epsilon = \pm 1$.

4. The criteria $C_\pm$ are equivalent to $A^1_\pm$ respectively.

5. An absolute pseudoprime for a criterion A^b_+ must be a Carmichael number.

6. An absolute pseudoprime for a criterion $A^b_\pm(d)$ must be square-free.

Proof. 1. Consider $\beta = x + 0\sqrt{d}$. The condition implies $x^n \equiv x \bmod N$, for any value of x, and so N must be a Carmichael number.

2. Consider $\beta = \sqrt{d}$. The condition implies $d^{(N-1)/2} \equiv \left(\frac{d}{N}\right) \bmod N$, for which it is already known there are no absolute pseudoprimes by Proposition 15.

3. Consider the map $\beta \mapsto \beta^2$ for d with $\left(\frac{d}{p}\right) = -1$. As already noted this map on C_{-1} is onto C_1 and the Frobenius condition holds for β^2 if it holds for β. So if condition $A^{-1}_\pm$ holds for all $\beta \in C_{-1}$, then condition $A^1_\pm$ must hold for all $\alpha \in C_1$.

4. We have $U_{N-\epsilon} \equiv 0 \bmod N$ all β iff $\beta^{N-\epsilon} \in F$ all β iff $\beta^{N-\epsilon} = (\beta')^{N-\epsilon}$ all β iff $\alpha^{N-\epsilon} = 1$ all $\alpha \in C$, since the anti-norm is onto C, iff $\alpha^N = \alpha$ resp. α' all $\alpha \in C$.

5. Suppose p^f is a prime power factor of N and $\left(\frac{d}{p}\right) = +1$. We have $(a, b/a)^N \equiv (a, b/a) \bmod p^f$, so in particular $a^N \equiv a \bmod p^f$ for any a, and any $p^f | N$. Hence N must be a Carmichael number.

6. The map $\beta \mapsto \beta^N$ is required to be a permutation of the appropriate set C_b. But if p^f divides N with $f > 1$ then by Proposition 18 the coset C_b in $R(p^f, d)$ contains elements of order divisible by p and the map cannot be one-to-one on such elements.

□

Indeed, we can strengthen (4) by noting that from Lemma 19 the conditions $C_\pm^b$ for two values of b, one a quadratic residue and the other a quadratic non-residue, together imply $A_\pm^1$.

Theorem 23. *1. The requirements for an absolute pseudoprime for each of the quadratic criteria are those given in Table 1.*

2. There are no absolute pseudoprimes for criteria A_-^b ($b \neq 1$), A_-, A^1 or A.

Proof. Suppose that p is a prime factor of N and that N satisfies one of the conditions stated. We let $\beta = x + y\sqrt{d}$ with norm $B = x^2 - dy^2$.

A_+ We have $\beta^N \equiv \beta \bmod p$, so $\beta^{N-1} \equiv 1 \bmod p$. The order of β modulo p can be $p^2 - 1$ or $p - 1$ according as $\left(\frac{d}{p}\right) = -1$ or $+1$: we require either $p^2 - 1 | N - 1$ or $p - 1 | N - 1$ respectively. Since the value of $\left(\frac{d}{p}\right)$ is not constrained by knowing $\left(\frac{d}{N}\right)$, we require $p^2 - 1 | N - 1$.

A_+^b We have $\beta^N \equiv \beta \bmod p$ for $B = b$. The order of such β modulo p can be $e(p+1)$ or $p - 1$ according as $\left(\frac{d}{p}\right) = -1$ or $+1$, where e denotes the multiplicative order of b in ${\mathbb{F}_p}^*$. We require $\operatorname{lcm}\{p - 1, e(p + 1)\}$ to divide $N - 1$.

A_+^1 We have $\beta^N \equiv \beta \bmod p$ for $B = 1$. The order of β modulo p can be $p - \left(\frac{d}{p}\right)$ and we require $p - \left(\frac{d}{p}\right) | N - 1$. Again the value of $\left(\frac{d}{p}\right)$ is unconstrained so we require $\operatorname{lcm}\{p - 1, p + 1\} = \left(p^2 - 1\right)/2$ to divide $N - 1$.

A_- We have $\beta^N \equiv \beta' \bmod p$. If $\left(\frac{d}{p}\right) = -1$ then $\beta^N = \beta' = \beta^p$ and we require the order of β, which can be $p^2 - 1$, to divide $N - p$. If $\left(\frac{d}{p}\right) = +1$ then it can be the case that β' is not equal to any power of β in R^*, which is not cyclic: for example, suppose β corresponds to $(1, -1) \in \mathbb{F}_p \oplus \mathbb{F}_p$ so that $\beta' \leftrightarrow (-1, 1)$. So there is no condition on p and N which will guarantee that N satisfies the condition in this case. We note that if β corresponds to $(a, b) \in \mathbb{F}_p \oplus \mathbb{F}_p$, then we are requiring that $a^N \equiv b$ and $b^N \equiv a$. So the β which satisfy this condition are the $\beta \leftrightarrow (a, a^N)$ with $a^{N^2} \equiv a \bmod p$: the number of such β is maximised when $p - 1 | N^2 - 1$, and there are then $p - 1$ such values of β.

A_-^b We have $\beta^N \equiv \beta' \bmod p$ when $B = b$: we assume $b \neq 1$. If $\left(\frac{d}{p}\right) = -1$ then $\beta^N = \beta' = \beta^p$ and we require the order of β, which can be $e(p+1)$, to divide $N - p$, where e is the order of b in ${\mathbb{F}_p}^*$. If $\left(\frac{d}{p}\right) = +1$ then it can again be the case that β' is not equal to any power of β: consider $\beta \leftrightarrow (1, b)$. Again there is no condition on p and N which will guarantee that N satisfies the condition. If $\beta \leftrightarrow (a, b/a)$, we are requiring that $a^N \equiv b/a$ and $(b/a)^N \equiv a \bmod p$. So we require $a^{N+1} \equiv b$ and $a^{N+1} \equiv b^N \bmod p$, which is impossible unless $b^N \equiv b \bmod p$, which is equivalent to the condition that $e | N - 1$ where

e is the multiplicative order of $b \bmod p$. We now have the condition that $a^{N+1} \equiv b \bmod p$. Put $p-1 = ef$. By Lemma 17 the number of solutions to this equation is maximised when $f|N+1$ and n/f is prime to e: when this occurs, the number of solutions is f.

A_-^1 Again we have $\beta^N \equiv \beta' \bmod p$ when $B = 1$, so $\beta^{N+1} \equiv 1 \bmod p$. The order of β can be the order of C, that is, $p - \left(\frac{d}{p}\right)$, so we require $\operatorname{lcm}\{p-1, p+1\} = \left(p^2-1\right)/2$ to divide $N+1$.

B We have $\beta^N = (x + y\sqrt{d})^N = x + z\sqrt{d}$ for some z. Since N is necessarily a Carmichael number, we have $\beta^N(\beta')^N = (\beta\beta')^N = B^N \equiv B \bmod N$, so that $z^2 \equiv y^2 \bmod N$ if this condition is satisfied. For any p dividing N we therefore have $z \equiv \pm y \bmod p$, so that $\beta^N = \beta$ or β' in $R(p,d)$. The condition $\beta^N = \beta'$ need not hold in the case $\left(\frac{d}{p}\right) = +1$, as discussed in case A_-, and there is no condition on p and N which will ensure that this holds. The condition $\beta^N = \beta$ is equivalent to requiring that the order of β, which can be p^2-1, divide $N-1$.

$B_\pm^b$ We have $\beta^N \equiv (x + y\sqrt{d})^N \equiv x + z\sqrt{d} \bmod N$ for some z whenever $\mathcal{N}(\beta) = x^2 - dy^2 = b$. Suppose that p^f is a prime power factor of N with $\left(\frac{d}{p}\right) = +1$. Consider $\beta \leftrightarrow (1, b) \in \mathbb{Z}/\langle p^f \rangle \oplus \mathbb{Z}/\langle p^f \rangle$, so that $\beta^N \leftrightarrow (1, b^N)$. We have $1 + b \equiv 1 + b^N \bmod p^f$, so that $b^N \equiv b \bmod p^f$. Now consider $\beta \leftrightarrow (a, b/a)$. We have $a + b/a \equiv a^N + b^N/a^N \equiv a^N + b/a^N \bmod p^f$. So $(a^{N-1} - 1)a \equiv b(a^{N-1} - 1)/a^N$, that is, $(a^{N-1} - 1)(a - b/a^N) \equiv 0 \bmod p^f$. If $b \not\equiv 1 \bmod p$ it cannot happen that $a^{N+1} \equiv b \bmod p^f$ for all $a \bmod p^f$, so we require that $a^{N-1} \equiv 1 \bmod p^f$ for all a: that is, that $f = 1$ and $p-1|N-1$. If $b \equiv 1 \bmod p$ then the two factors $a^{N-1} - 1$ and $a^{N+1} - b$ cannot both be divisible by p unless $a \equiv \pm 1 \bmod p$. This cannot be the case since $p > 3$. So the alternative condition $f = 1$ and $p-1|N+1$ will also suffice to ensure that the condition holds. We see that in any case N must be squarefree.

Now consider the case when $\left(\frac{d}{p}\right) = -1$. Suppose $p|N$. We have $\beta^N + (\beta')^N \equiv \beta + \beta' \bmod p$, so $\beta^N + (b/\beta)^N \equiv \beta + b/\beta$. We have $\beta^N - \beta \equiv b(\beta^N - \beta)/\beta^{N+1}$, so $(\beta^N - \beta)(1 - b/\beta^{N+1}) \equiv 0 \bmod p$. The two factors cannot both be divisible by p unless $\beta^{N-1} \equiv 1$ and $\beta^{N+1} \equiv b \bmod p$, which entail $\beta^2 \equiv b$: since $\beta\beta' \equiv b$ this requires $\beta \equiv \beta' \bmod p$. Otherwise, we have the alternative conditions $\beta^{N-1} \equiv 1 \bmod p$ or $\beta^{N+1} \equiv b \bmod p$. Since by Proposition 16 the order of β can be $e(p+1)$, where e is the multiplicative order of $b \bmod p$, we require $e(p+1)|N-1$ for the first condition to hold. For the second condition we have $\beta^{N+1} \equiv b \bmod p$ iff $\beta^{N+1} \equiv \beta\beta'$ iff $\beta^N \equiv \beta'$ iff $\beta^N \equiv \beta^p$, which requires that $e(p+1)|N-p$.

B^{-1} We have $b = -1$, so the multiplicative order of b is 2. We require that N be square-free, that $p-1|N-1$ and that $2(p+1)$ divide either $N-1$ or $N-p$ for each p.

B^1 We have $b = 1$, so the multiplicative order of b is 1. We require that N be square-free, that $p-1|N \pm 1$ and that $p+1$ divide $N-1$ or $N-p$.

□

Criterion	$\left(\frac{d}{p}\right) = +1$	P	$\left(\frac{d}{p}\right) = -1$	In general
A_+	$p-1 \mid N-1$		$p^2-1 \mid N-1$	$p^2-1 \mid N-1$
A_+^b	$p-1 \mid N-1$		$e(p+1) \mid N-1$	$\mathrm{lcm}\{p-1, e(p+1)\} \mid N-1$
A_+^{-1}	$p-1 \mid N-1$		$2(p+1) \mid N-1$	$\mathrm{lcm}\{p-1, 2(p+1)\} \mid N-1$
A_+^1	$p-1 \mid N-1$		$p+1 \mid N-1$	$(p^2-1)/2 \mid N-1$
A_-	$\boxed{p-1 \mid N^2-1}$	$\frac{1}{p-1}$	$p^2-1 \mid N-p$	$\boxed{p^2-1 \mid N-p}$
A_-^b	$\boxed{e \mid N-1}$ and $\boxed{f \mid N+1}$	$\frac{1}{e}$	$e(p+1) \mid N-p$	$e(p+1) \mid N-p$ and $\boxed{f \mid N+1}$
A_-^{-1}	$\boxed{(p-1)/2 \mid N+1}$	$\frac{1}{2}$	$2(p+1) \mid N-p$	—
A_-^1	$p-1 \mid N+1$		$p+1 \mid N+1$	$(p^2-1)/2 \mid N+1$
B	$p-1 \mid N-1$		$p^2-1 \mid N-1$ or $p^2-1 \mid N-p$	$p^2-1 \mid N-1$ or $p^2-1 \mid N-p$
B^b	$p-1 \mid N-1$		$e(p+1) \mid N-1$ or $e(p+1) \mid N-p$	$\mathrm{lcm}\{p-1, e(p+1)\} \mid N-1$ or $\mathrm{lcm}\{p-1, e(p+1)\} \mid N-p$
B^{-1}	$p-1 \mid N-1$		$2(p+1) \mid N-1$ or $2(p+1) \mid N-p$	$\mathrm{lcm}\{p-1, 2(p+1)\} \mid N-1$ or $\mathrm{lcm}\{p-1, 2(p+1)\} \mid N-p$
B^1	$p-1 \mid N-1$ or $p-1 \mid N+1$		$p+1 \mid N-1$ or $p+1 \mid N+1$	$p-1 \mid N \pm 1$ and $p+1 \mid N \pm 1$

Table 1: Requirements for absolute pseudoprimes for criteria of type A and B. Column P gives the proportion of bases for which the criterion can be satisfied when this is not 1: the requirements for such cases are boxed. e denotes the multiplicative order of b modulo p and $f = (p-1)/e$.

Lidl, Müller and Oswald [17], [18], [23] characterize a *strong Fibonacci pseudoprime* as a Carmichael number $N = \prod p_i$ with one of the following properties: either *(Type I)* an even number of the p_i are $\equiv 3 \bmod 4$ with $p^2-1 \mid N-1$ for the $p_i \equiv 3 \bmod 4$ and $p_i+1 \mid N \pm 1$ for the $p_i \equiv 1 \bmod 4$; or *(Type II)* there is an odd number of p_i, all $\equiv 3 \bmod 4$, and $p_i^2-1 \mid N-p_i$ for all p_i. (A strong type II Fibonacci pseudoprime is termed a *strong* (-1)*-Dickson pseudoprime* in [23].) They were not able to exhibit any such numbers. We found just one Type I strong Fibonacci pseudoprime less than 10^{16}, already mentioned in [24], namely

$$443372888629441 = 17 \cdot 31 \cdot 41 \cdot 43 \cdot 89 \cdot 97 \cdot 167 \cdot 331,$$

and none of Type II. This also answered the question of Di Porto and Filipponi [5].

Guillaume and Morain [13] quote Williams [33] as defining a Δ*-Lucas pseudoprime* by the condition $U_{N-\epsilon} \equiv 0 \bmod N$ for all Lucas sequences with defining equation $X^2 - PX + Q$ with $P^2 - 4Q = \Delta$ and $(N, \Delta Q) = 1$. The is just condition $C(\Delta)$, equivalent to $A^1(\Delta)$ by Proposition 22 (4). We recover the result that N is an absolute pseudoprime for this test iff N is square-free and $p - \epsilon_p \mid N - \epsilon_N$.

Guillaume and Morain [13] further define a *strong Dickson-*(c) *pseudoprime* if the Dickson polynomial $g_N(m, c) \equiv m \bmod N$ for all m. This is equivalent to $V_N \equiv m$ for the Lucas sequence attached to the polynomial $X^2 - mX + c$. So this is just condition B^c.

A *strong Fibonacci pseudoprime* is a strong Dickson-(-1) pseudoprime: this is just condition B^{-1}. We find that such a pseudoprime is a Carmichael number satisfying $2(p+1) \mid N-1$ or $N-p$.

A *superstrong Dickson pseudoprime* is a strong Dickson-(c) pseudoprime for all c, hence satisfies condition B. We require such a number to be a Carmichael

number with $p^2-1|N-1$ or $N-p$.

Gordon [8],[7], [9],[10] defines an *D-elliptic pseudoprime* to be an N such that $\left(\frac{D}{p}\right)=-1$ and $p+1|N+1$ for all $p|N$, where $-D$ is a discriminant of class-number 1.

Williams [33] asked whether there are any Carmichael numbers N with an odd number of prime divisors and the additional property that for $p|N$, $p+1|N+1$. There are no such Carmichael numbers up to 10^{16}. We note that type II strong Fibonacci pseudoprimes are a special case of this condition.

Jones[1] has defined various special kinds of Carmichael numbers N. A *Lucas–Carmichael-(−) number* has the property that $p|N$ implies $(p-1)/2$ and $(p+1)/2$ both divide $N-1$: it is *strong* if $p-1$ and $p+1$ both divide $N-1$ and *unusually strong* if p^2-1 divides $N-1$.

The five Lucas–Carmichael-(−) numbers up to 10^{16} are

$$\begin{aligned}
28295303263921 &= 29\cdot 31\cdot 67\cdot 271\cdot 331\cdot 5237,\\
443372888629441 &= 17\cdot 31\cdot 41\cdot 43\cdot 89\cdot 97\cdot 167\cdot 331,\\
582920080863121 &= 41\cdot 53\cdot 79\cdot 103\cdot 239\cdot 271\cdot 509,\\
894221105778001 &= 17\cdot 23\cdot 29\cdot 31\cdot 79\cdot 89\cdot 181\cdot 1999,\\
2013745337604001 &= 17\cdot 37\cdot 41\cdot 131\cdot 251\cdot 571\cdot 4159.
\end{aligned}$$

The number 582920080863121 is a strong Lucas–Carmichael-(−) number, and a pseudoprime for criterion A^1_+ and hence B^1. The number 443372888629441 is unusually strong, and pseudoprime for criteria A_+ and B; hence also for A^{-1}_+, A^1_+, B^{-1} and B^1.

A *Lucas–Carmichael-(+) number* has the property that $p|N$ implies $(p-1)/2$ and $(p+1)/2$ both divide $N+1$: it is *strong* if $p-1$ and $p+1$ both divide $N-1$ and *unusually strong* if $p^2-1|N+1$.

The seven Lucas–Carmichael-(+) numbers up to 10^{13} are

$$\begin{aligned}
6479 &= 11\cdot 19\cdot 31,\\
84419 &= 29\cdot 41\cdot 71,\\
1930499 &= 89\cdot 109\cdot 199,\\
7110179 &= 37\cdot 41\cdot 43\cdot 109,\\
15857855 &= 5\cdot 13\cdot 17\cdot 113\cdot 127,\\
63278892599 &= 13\cdot 47\cdot 137\cdot 239\cdot 3163,\\
79397009999 &= 23\cdot 29\cdot 41\cdot 43\cdot 251\cdot 269.
\end{aligned}$$

Of these, 79397009999 is unusually strong. It is a pseudoprime for criteria A^1_- and B^1.

6 Strong quadratic tests

Arnault [1] defines a *strong Lucas test* for an odd number N as follows: let $\epsilon=\left(\frac{d}{N}\right)$ and put $N-\epsilon=2^r s$ with s odd. The criterion requires that either $U_s\equiv 0 \bmod N$ or $V_{2^j s}\equiv 0$ for some j with $0\le j<r$.

He shows that the proportion of tests which falsely declare N prime is at most $1/2$, and indeed at most $4/15$ if N is not of the special form $N=pq$ with p and $q=p+2$ twin primes and $\left(\frac{D}{p}\right)=-1$, $\left(\frac{D}{q}\right)=+1$.

[1]Private communication.

Since $U_{2k} = U_k V_l$ by equation (3.4), the condition implies that $U_{N-\epsilon} \equiv 0 \bmod N$: this is condition C in the table above, and we have seen that it is equivalent to the Fermat criterion for the corational groups $C(N, d)$. The strong Lucas test is thus the 2-strengthening of test C.

7 A Bayesian result

We noted that for a given composite number, the probability of the strong test incorrectly returning `probable prime` on a random base is at most $\frac{1}{4}$.

More important in practice is the probability that a number which has passed the strong test is in fact composite. We consider, for example, a process which chooses odd numbers N of a given size uniformly at random and outputs N if it passes r rounds of the strong test with random bases. Damgård and Landrock [2] and Kim and Pomerance [16] give results in this direction.

In this section we indicate how similar results may be obtained for the 2-strengthening of criterion A.

It ios necessary to specify a sample space of integers to apply the test to: we consider the space $\mathcal{M}_k$ of all odd k-bit integers taken uniformly at random. Our strategy is to find "small" subsets $\mathcal{E}_m$ of $\mathcal{M}_k$ such that if N is composite and not in $\mathcal{E}_m$ then the probability that N passes the test is also small.

Let $\Psi(N) = N - \left(\frac{d}{N}\right)$. Let $\Phi_{\mathcal{G}} = \Phi$ be the multiplicative function extending $\Phi(p) = \Psi(p) = p - \left(\frac{d}{p}\right)$ for prime p.

Suppose $N \in \mathcal{M}_k$, and put $N = \prod_i^d p_i^{a_i}$. For $p_i \mid N$, let $c_i = \mathrm{hcf}(\Phi(p_i), \Psi(N))$ and let $b_i c_i = \Phi(p_i)$. We have a bound on the probability of composite N passing the criterion

$$\mu(N) \leq 2^{-d+1} \prod_{i=1}^{d} \frac{b_i}{p_i}$$

coming from the 2-strengthening part of the criterion.

Put $X = 2^k$. We have $|\mathcal{M}_k| = \frac{1}{4}X$. Fix m with $2 \leq m \leq \sqrt{k/2}$ and put $A = 2^{m-1}$, $\delta = 1/m$. Put $Y = \frac{1}{2}X^{\delta}$. Put

$$\mathcal{E}_m = \{N \in \mathcal{M}_k \mid N \text{ is composite}, b_i < A \text{ for some } p_i | N \text{ with } p_i > Y\}.$$

Proposition 24. *For $2 \leq m \leq \sqrt{k/2}$ the set $\mathcal{E}_m$ of composite numbers satisfies*

- *(i) for composite $N \in \mathcal{M}_k \setminus \mathcal{E}_m$, we have $\mu(N) \leq 2^{-m}$;*
- *(ii) $|\mathcal{E}_m|/|\mathcal{M}_k| = O\left(\frac{m}{k}\right) 2^{2m-k/m}$.*

Proof. Put

$$W(N) = \frac{1}{\Psi(N)} \prod_i c_i = \frac{1}{N} \prod_i \frac{1}{b_i}$$

We first need to show (i). Suppose that N is composite and not in $\mathcal{E}_m$.

If $d > m$ then $\mu(N) \leq 2^{-m} W(N) \leq 2^{-m}$, as required. So we suppose that $N \notin \mathcal{E}_m$ and that $d \leq m$.

Suppose first that $n \notin \mathcal{E}_m$ because the prime factors p_i of N all satisfy $p_i < Y$. Put $D = \prod_i p_i$. Now N/D is coprime to $\Psi(N)$ but divides $\Phi(N)$: indeed

$$\Phi(N) = N \prod_{p|N} \left(\frac{p-1}{p}\right) = \frac{N}{D} \prod_{p|N} (p-1).$$

Now $D < Y^m$ and $N > \frac{1}{2}X$, so

$$N/D \geq NY^{-m} = N\left(\frac{1}{2}X^{\delta}\right)^{-m} \geq \frac{1}{2}X/2^{-m}X = 2^{m-1}.$$

Now $W(N) \leq D/N$, so $W(N) \leq 2^{1-m}$ and again $\mu(N) \leq 2^{-m}$.

Finally suppose that N has a prime factor $p_i > Y$; since $N \notin \mathcal{E}_m$, we must have $b_i > A$. Then $W(N) < 1/A$ and since $\mu(N) \leq W(N)/2$, we have $\mu(N) < 1/2A = 2^{-m}$.

We now prove part (ii). Fix a prime $p > Y$. Suppose $N \in \mathcal{E}_m$ because $p|N$ with $p > Y$ and $b < A$. Now $N \equiv 0 \mod p$ and $N \equiv \left(\frac{d}{N}\right) \mod c$. Since $c|p \pm 1$, we have p and c coprime, and so N satisfies a congruence condition modulo pc. Since N cannot equal p, the number of such N in $\mathcal{M}_k$ is at most $\frac{1}{2}X/pc$, which is $\frac{1}{2}Xb/p(p-1)$.

Summing over all $p > Y$ and $b < A$, we have

$$|\mathcal{E}_m| \leq \sum_{p>Y}\sum_{b<A}\frac{\frac{1}{2}Xb}{p(p-1)} \leq \sum_{p>Y}\frac{XA^2}{p^2} = \mathrm{O}\left(\frac{XA^2}{Y}\right).$$

□

Theorem 25.

$$\mathbb{P}(N \textit{ composite}|N \textit{ passes } r \textit{ tests}) = O\left(k\,2^{-\sqrt{k}/2}\right).$$

Proof. We have

$$\mathbb{P}(N \text{ composite}|N \text{ passes } r \text{ tests}) = \frac{\mathbb{P}(N \text{ composite and } N \text{ passes } r \text{ tests})}{\mathbb{P}(N \text{ passes } r \text{ tests})}$$

Now

$$\begin{aligned}\mathbb{P}(N \text{ composite and passes } r \text{ tests}) &< \mathbb{P}(N \in \mathcal{E}_m \text{ and passes } r \text{ tests})\\ &\quad + \mathbb{P}(N \text{ composite and } N \notin \mathcal{E}_m \text{ and passes } r \text{ tests})\\ &< 2^{-m} + \mathrm{O}\left(\frac{m}{k}\,2^{2m-k/m}\right)\end{aligned}$$

and

$$\mathbb{P}(N \text{ passes } r \text{ tests}) > \mathbb{P}(N \text{ prime}) > 1/k,$$

using the Prime Number Theorem. Hence

$$\mathbb{P}(N \text{ composite}|N \text{ passes } r \text{ tests}) < k(2^{-m} + \mathrm{O}\left(\frac{m}{k}\,2^{2m-k/m}\right)).$$

Now putting $m = \sqrt{k}/2$ we have

$$\mathbb{P}(N \text{ composite}|N \text{ passes } r \text{ tests}) = \mathrm{O}\left(k2^{-\sqrt{k}/2}\right).$$

□

References

[1] François Arnault, *The Rabin–Monier theorem for Lucas pseudoprimes*, Math. Comp. **66** (1997), no. 218, 869–881.

[2] Ivan Damgård and Peter Landrock, *Improved bounds for the Rabin primality test*, in Ganley [6], Proceedings, 3rd IMA conference on cryptography and coding, Cirencester, December 1991., pp. 117–128.

[3] D.W. Davies (ed.), *Advances in cryptology* — EUROCRYPT *'91*, Lecture notes in Computer Science, vol. 547, Berlin, Springer–Verlag, 1991.

[4] Jean-Marie De Koninck and Claude Levesque (eds.), *Number theory: proceedings of the international number theory conference, Université de Laval, 1987*, Berlin, Walter de Gruyter, 1989.

[5] A. Di Porto and P. Filipponi, *A probabilistic primality test based on the properties of certain generalized Lucas numbers*, in Günther [14], pp. 211–223.

[6] M. Ganley (ed.), *Cryptography and coding III*, IMA conference series (n.s.), vol. 45, Institute of Mathematics and its Applications, Oxford University Press, 1993, Proceedings, 3rd IMA conference on cryptography and coding, Cirencester, December 1991.

[7] Dan M. Gordon, *On the number of elliptic pseudoprimes*, Math. Comp. **52** (1989), no. 185, 231–245.

[8] Daniel M. Gordon, *Pseudoprimes on elliptic curves*, in De Koninck and Levesque [4], pp. 290–305.

[9] Daniel M. Gordon and Carl Pomerance, *The distribution of Lucas and elliptic pseudoprimes*, Math. Comp. **57** (1991), no. 196, 825–838, See also [10].

[10] ———, *The distribution of Lucas and elliptic pseudoprimes: corrigendum*, Math. Comp. **60** (1993), no. 202, 877, Corrigendum to [9].

[11] Jon Grantham, *A probable prime test with high confidence*, J. Number Theory **72** (1998), no. 1, 32–47.

[12] ———, *Frobenius pseudoprimes*, Math. Comp. **70** (2001), no. 234, 873–891.

[13] Dominique Guillaume and François Morain, *Building pseudoprimes with a large number of prime factors*, Appl. Algebra Engrg. Comm. Comput. **7** (1996), no. 4, 263–267.

[14] C.G. Günther (ed.), *Advances in cryptology* — EUROCRYPT *'88*, Lecture notes in Computer Science, vol. 330, Berlin, Springer–Verlag, 1988.

[15] Marc Joye and Jean-Jacques Quisquater, *Efficient computation of full Lucas sequences*, Electronics Letters **32** (1996), no. 6, 537–538.

[16] Su Hee Kim and Carl Pomerance, *The probability that a random probable prime is composite*, Math. Comp. **53** (1989), no. 188, 721–741.

[17] Rudolf Lidl and Winfried B. Müller, *A note on strong Fibonacci pseudoprimes*, in Seberry and Pieprzyk [29], pp. 311–317.

[18] Rudolf Lidl, Winfried B. Müller, and Alan Oswald, *Some remarks on strong Fibonacci pseudoprimes*, Appl. Algebra Engrg. Comm. Comput. **1** (1990), 59–65.

[19] Rudolf Lidl and Harald Niederreiter, *Finite fields*, second ed., Encyclopaedia of Mathematics and its applications, vol. 20, Cambridge University Press, Cambridge, 1997.

[20] G.L. Miller, *Riemann's hypothesis and tests for primality*, Conference Record of Seventh Annual ACM Symposium on Theory of Computation (Albuquerque, New Mexico), ACM, 5–7 May 1975, pp. 234–239.

[21] ———, *Riemann's hypothesis and tests for primality*, J. Comp. System Sci. **13** (1976), 300–317.

[22] R.A. Mollin (ed.), *Number theory and its applications*, Dordrecht, Kluwer Academic, 1989, Proceedings of the NATO Advanced Study Institute on Number Theory and Applications.

[23] W.B. Müller and A. Oswald, *Dickson pseudoprimes and primality testing*, in Davies [3], pp. 512–516.

[24] Richard G.E. Pinch, *The Carmichael numbers up to* 10^{15}, Math. Comp. **61** (1993), 381–391, Lehmer memorial issue.

[25] ———, *Recurrent sequences modulo prime powers*, in Ganley [6], Proceedings, 3rd IMA conference on cryptography and coding, Cirencester, December 1991., pp. 297–310.

[26] ———, *The Carmichael numbers up to* 10^{16}, March 1998, `arXiv:math.NT/9803082`.

[27] Michael O. Rabin, *Probabilistic algorithm for testing primality*, J. Number Theory **12** (1980), no. 1, 128–138.

[28] Hans Riesel, *Prime numbers and computer methods for factorization*, second ed., Progress in mathematics, vol. 126, Birkhauser, Boston, 1994.

[29] Jennifer Seberry and Josef Pieprzyk (eds.), *Advances in cryptology* - AUSCRYPT *'90*, Lecture notes in Computer Science, vol. 453, Berlin, Springer–Verlag, 1990.

[30] Jennifer Seberry and Yuliang Zheng (eds.), *Advances in cryptology* - AUSCRYPT *'92*, Lecture notes in Computer Science, vol. 718, Berlin, Springer–Verlag, 1993.

[31] R. Solovay and V. Strassen, *A fast Monte-Carlo test for primality*, SIAM J. Comput. **6** (1977), no. 1, 84–85.

[32] ———, *Erratum: A fast Monte-Carlo test for primality*, SIAM J. Comput. **7** (1978), no. 1, 118.

[33] Hugh C. Williams, *On numbers analogous to the Carmichael numbers*, Canad. Math. Bull. **20** (1977), 133–143.

The Carmichael numbers up to 10^{21}

Richard G.E. Pinch

2 Eldon Road, Cheltenham, Glos GL52 6TU, U.K.
rgep@chalcedon.demon.co.uk

Abstract

We extend our previous computations to show that there are 20138200 Carmichael numbers up to 10^{21}. As before, the numbers were generated by a back-tracking search for possible prime factorisations together with a "large prime variation". We present further statistics on the distribution of Carmichael numbers.

1 Introduction

A *Carmichael number* N is a composite number N with the property that for every b prime to N we have $b^{N-1} \equiv 1 \mod N$. It follows that a Carmichael number N must be square-free, with at least three prime factors, and that $p-1|N-1$ for every prime p dividing N: conversely, any such N must be a Carmichael number.

For background on Carmichael numbers and details of previous computations we refer to our previous paper [1]: in that paper we described the computation of the Carmichael numbers up to 10^{15} and presented some statistics. These computations have since been extended to 10^{16} [2], 10^{17} [3], 10^{18} [4] and now to 10^{21}, using similar techniques, and we present further statistics.

2 Organisation of the search

We used improved versions of strategies first described in [1].

The principal search was a depth-first back-tracking search over possible sequences of primes factors $p_1, \ldots, p_d$. Put $P_r = \prod_{i=1}^{r} p_i$, $Q_r = \prod_{i=r+1}^{d} p_i$ and $L_r = \operatorname{lcm}\{p_i - 1 : i = 1, \ldots, r\}$. We find that Q_r must satisfy the congruence $N = P_r Q_r \equiv 1 \mod L_r$ and so in particular $Q_d = p_d$ must satisfy a congruence modulo L_{d-1}: further $p_d - 1$ must be a factor of $P_{d-1} - 1$. We modified this to terminate the search early at some level r if the modulus L_r is large enough to limit the possible values of Q_r, which may then be factorised directly.

We also employed the variant based on proposition 2 of [1] which determines the finitely many possible pairs (p_{d-1}, p_d) from P_{d-2}. In practice this was useful only when $d = 3$ allowing us to determine the complete list of Carmichael numbers with three prime factors up to 10^{21}.

2.1 A large prime variation

Finally we employed a different search over large values of p_d, in the range $2.10^6 < p_d < 10^{10.5}$, using the property that $P_{d-1} \equiv 1 \mod (p_d - 1)$.

If q is a prime in this range, we let P run through the arithmetic progression $P \equiv 1 \mod q-1$ in the range $q < P < X/q$ where $X = 10^{21}$. We first check whether

$N = Pq$ satisfies $2^N \equiv 2 \bmod N$: it is sufficient to test whether $2^N \equiv 2 \bmod P$ since the congruence modulo q is necessarily satisfied. If this condition is satisfied we factorise P and test whether $N \equiv 1 \bmod \lambda(N)$.

The approximate time taken for $X^t \leq q < X^{1/2}$ is

$$\sum_{X^t < q < X^{1/2}} \frac{X}{q^2} \approx X^{1-t}.$$

3 Statistics

n	$C(10^n)$
3	1
4	7
5	16
6	43
7	105
8	255
9	646
10	1547
11	3605
12	8241
13	19279
14	44706
15	105212
16	246683
17	585355
18	1401644
19	3381806
20	8220777
21	20138200

Table 1: Distribution of Carmichael numbers up to 10^{19}.

We have shown that there are 20138200 Carmichael numbers up to 10^{21}, all with at most 12 prime factors. We let $C(X)$ denote the number of Carmichael numbers less than X and $C(d, X)$ denote the number with exactly d prime factors. Table 1 gives the values of $C(X)$ and Table 2 the values of $C(d, X)$ for X in powers of 10 up to 10^{21}.

X	3	4	5	6	7	8	9	10	11	12	total
3	1	0	0	0	0	0	0	0	0	0	1
4	7	0	0	0	0	0	0	0	0	0	7
5	12	4	0	0	0	0	0	0	0	0	16
6	23	19	1	0	0	0	0	0	0	0	43
7	47	55	3	0	0	0	0	0	0	0	105
8	84	144	27	0	0	0	0	0	0	0	255
9	172	314	146	14	0	0	0	0	0	0	646
10	335	619	492	99	2	0	0	0	0	0	1547
11	590	1179	1336	459	41	0	0	0	0	0	3605
12	1000	2102	3156	1714	262	7	0	0	0	0	8241
13	1858	3639	7082	5270	1340	89	1	0	0	0	19279
14	3284	6042	14938	14401	5359	655	27	0	0	0	44706
15	6083	9938	29282	36907	19210	3622	170	0	0	0	105212
16	10816	16202	55012	86696	60150	16348	1436	23	0	0	246683
17	19539	25758	100707	194306	172234	63635	8835	340	1	0	585355
18	35586	40685	178063	414660	460553	223997	44993	3058	49	0	1401644
19	65309	63343	306310	849564	1159167	720406	196391	20738	576	2	3381806
20	120625	98253	514381	1681744	2774702	2148017	762963	114232	5804	56	8220777
21	224763	151566	846627	3230120	6363475	6015901	2714473	547528	42764	983	20138200

Table 2: Values of $C(X)$ and $C(d, X)$ for $d \leq 10$ and X in powers of 10 up to 10^{21}.

References

[1] Richard G.E. Pinch, *The Carmichael numbers up to* 10^{15}, Math. Comp. **61** (1993), 381–391, Lehmer memorial issue.

[2] ———, *The Carmichael numbers up to* 10^{16}, March 1998, `arXiv:math.NT/9803082`.

[3] ———, *The Carmichael numbers up to* 10^{17}, April 2005, `arXiv:math.NT/0504119`.

[4] ———, *The Carmichael numbers up to* 10^{18}, April 2006, `arXiv:math.NT/0604376`.

Continued Fractions in Function Fields defined over an Infinite Field . . . with emphasis on the quadratic case

Alf van der Poorten

ceNTRe for Number Theory Research
Killara, NSW 2071, Australia
alf AT maths DOT usyd DOT edu DOT au

1 Continued Fractions of Quadratic Irrationals

I begin by recalling that the symbol $\alpha = [\, a_0 \,,\, a_1 \,,\, a_2 \,,\, \ldots\ldots \,]$ defined by

$$\alpha = [\, a_0 \,,\, a_1 \,,\, a_2 \,,\, \ldots \,] = a_0 + 1/[\, a_1 \,,\, a_2 \,,\, a_3 \,,\, \ldots \,] \quad \text{and } [\, a_0 \,] = a_0$$

denotes a *continued fraction expansion* of α. Set $[\, a_0 \,,\, a_1 \,,\, a_2 \,,\, \ldots \,,\, a_h \,] = x_h/y_h$. One then readily confirms by induction on h that the *convergents* x_h/y_h, more to the point the *continuants* x_h and y_h, are given by the *matrix correspondence*

$$\begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_h & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} x_h & x_{h-1} \\ y_h & y_{h-1} \end{pmatrix}.$$

It follows readily that $x_h/y_h - x_{h-1}/y_{h-1} = (-1)^{h-1}/y_{h-1}y_h$; hence that

$$x_h/y_h = 1/y_0y_1 - 1/y_1y_2 + \cdots + (-1)^{h-1}/y_{h-1}y_h \,;$$

and thus that formally

$$\alpha - x_h/y_h = \sum_{j=1}^{\infty} (-1)^{h+j}/y_{h+j-1}y_{h+j} \,.$$

Further, define the *complete quotients* α_h of α by $\alpha = [\, a_0 \,,\, a_1 \,,\, \ldots \,,\, a_h \,,\, \alpha_{h+1} \,]$. Then by the matrix correspondence we have

$$\begin{pmatrix} x_h & x_{h-1} \\ y_h & y_{h-1} \end{pmatrix} \begin{pmatrix} \alpha_{h+1} & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} x_h\alpha_{h+1} + x_{h-1} & x_h \\ y_h\alpha_{h+1} + y_{h-1} & y_h \end{pmatrix}$$

and, therefore after a matrix inversion, we see that

$$\alpha_{h+1} = -(y_{h-1}\alpha - x_{h-1})/(y_h\alpha - x_h).$$

Hence, plainly, given that the correspondence entails $x_{-1} = 1$, $y_{-1} = 0$, we get

$$\alpha_1\alpha_2 \cdots \alpha_{h+1} = (-1)^{h+1}/(x_h - y_h\alpha) \,; \qquad (*)$$

so $-\log|x_h - y_h\alpha|$ defines a weighted distance the continued fraction expansion has traversed from α to α_{h+1}.

1.1 Units and periodicity

Denote by ω a real quadratic irrational integer, say with trace $\omega + \overline{\omega} = t$ and norm $\omega\overline{\omega} = n$; to distinguish ω from $\overline{\omega}$ suppose that $\omega > \overline{\omega}$. I now note that the existence of a nontrivial unit $x - \omega y$, to wit of an element of norm $(x-\omega y)(x-\overline{\omega}y) = x^2 - txy + ny^2 = \pm 1$ with $y \neq 0$, implies that ω has a periodic continued fraction expansion.

To see that, consider a decomposition of the ideal matrix N:

$$N = \begin{pmatrix} x & -ny \\ y & x - ty \end{pmatrix} = \begin{pmatrix} a_0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} a_1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} a_r & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \qquad (\dagger)$$

obtained, say, by operating on the rows of the given matrix of determinant ± 1. I allege that it follows that

$$[\,\overline{a_0\,,\,a_1\,,\,\ldots\,,\,a_r\,,\,0}\,] = [\,a_0\,,\,\overline{a_1\,,\,a_2\,,\,\ldots\,,\,a_r + a_0}\,] = \omega$$

displays a periodic expansion of ω. Suppose instead that $[\,\overline{a_0\,,\,a_1\,,\,\ldots\,,\,a_r\,,\,0}\,] = \gamma$; that is, $\gamma = [\,a_0\,,\,a_1\,,\,\ldots\,,\,a_r\,,\,0\,,\,\gamma\,]$. Then, by the correspondence,

$$\gamma \longleftrightarrow \begin{pmatrix} x & -ny \\ y & x - ty \end{pmatrix} \begin{pmatrix} \gamma & 1 \\ 1 & 0 \end{pmatrix} \longleftrightarrow (\gamma x + ny)/(\gamma y + x - ty)\,,$$

so $\gamma(\gamma y + x - ty) = \gamma x + ny$. But this is $y(\gamma^2 - t\gamma + n) = 0$ and since $y \neq 0$ we must have $\gamma = \omega$.

Thus the existence of a nontrivial unit $x - \omega y$ yields a periodic expansion for ω.

Conversely, $(*)$ implies that such an expansion

$$\omega = [\,a_0\,,\,\overline{a_1\,,\,a_2\,,\,\ldots\,,\,a_r + a_0}\,]$$

yields a unit $x_{r-1} - \omega y_{r-1}$.

Indeed, the complete quotients of ω are readily seen all to be of the shape $\omega_h = (\omega + P_h)/Q_h$ with

$$(\omega + P_h)(\overline{\omega} + P_h) = -Q_{h-1}Q_h \quad \text{and } P_h + P_{h+1} = a_h Q_h.$$

One then sees readily that taking norms in the distance formula $(*)$ immediately yields

$$x_h^2 - tx_h y_h + ny_h^2 = (-1)^{h+1} Q_{h+1}\,.$$

Of course $Q_0 = 1$, so our presumption of periodicity entails that also $Q_r = 1$ whence, as claimed, $x_{r-1} - \omega y_{r-1}$ is a nontrivial element of norm $(-1)^r = \pm 1$.

1.2 Comment

In my summary above I have deliberately said nothing about the nature of the *partial quotients* a_h constituting the continued fraction expansion. Indeed, I need say nothing because I intend to point out that my remarks make sense although they be entirely formal and compatible with essentially any specification.

To that end, I distinguish between *a* continued fraction expansion and *the* continued fraction expansion or the *admissible* expansion, with the latter referring to the usual simple continued fraction expansion.

1.3 Existence of a unit

Specifically, the box principle entails that the continued fraction expansion of an irrational element of a real quadratic *number* field always is periodic.

By Dirichlet's box principle there are infinitely many pairs of integers (p, q) so that $|q\omega - p| < 1/q$, whence $\left|p^2 - tpq + nq^2\right| < \omega - \overline{\omega} + 1$. So there are infinitely many of those pairs (p, q) so that $p^2 - tpq + nq^2 = k$ for some k with $|k| < \omega - \overline{\omega} + 1$. More, there are of course infinitely many pairs (p, q) and (p', q') so that $p \equiv p'$ and $q \equiv q' \pmod{k}$. Then $(p^2 - tpq + nq^2)(p'^2 - tp'q' + nq'^2) = k^2$ and, with $kx = pp' - tpq' + nqq'$ and $ky = pq' - p'q$, we have $x^2 - txy + ny^2 = 1$, displaying a nontrivial unit $x - \omega y$ of $\mathbb{Z}[\omega]$.

It is no great matter to replace ω by $\alpha = (\omega + P)/Q$ in this argument and to prove the existence of a unit, say $r - s\alpha$. It is an interesting exercise to find conditions α must satisfy so that the ideal matrix corresponding to that unit has a decomposition (†) with all the partial quotients a_i positive integers.

2 Continued Fractions of Formal Laurent Series

The function field analogue of a real number is an element of $\mathbb{K}((X^{-1}))$, a formal Laurent series $F(X) = \sum_{h=-k}^{\infty} f_h X^{-h}$; the *admissible* partial quotient is its polynomial part $\sum_{h=0}^{k} f_{-h} X^h$.

My opening remarks on continued fractions apply essentially unchanged and immediately yield

$$\deg(y_h F - x_h) = -\deg y_h - \deg a_{h+1}\,,$$

showing that the distance from F to its complete quotient F_{h+1} is the sum of the degrees of the partial quotients a_0 to a_{h+1}. Conversely, a rational function x/y is an admissible convergent to F if and only if $\deg(yF - x) < -\deg y$.

If the base field $\mathbb{K}$ is infinite then it is *normal*, see §6.3, for all partial quotients to have degree one.

Just so, it is rare happenstance for an algebraic function field $\mathbb{K}(X, Y)$ to contain a nontrivial unit, one not in $\mathbb{K}$ (box principle arguments fail because there are infinitely many different polynomials of bounded degree).

2.1 Pseudo-elliptic integrals

I should point out that any actual expansion in the algebraic case is almost always very messy; see §6.3. I give the list of partial quotients of two very different examples. First, set $\mathcal{C} : Z^2 - (X^2 - X + 1)Z - X = 0$. Very unusually, Z has a periodic continued fraction expansion, namely

$$Z = [\,\overline{X^2 - X + 1\,,\, X - 1\,,\, X - 1}\,]\,.$$

Those who know such things know[1] that there must be an associated *pseudo-elliptic* integral. Noting that the discriminant of the equation defining Z is $D(X) = X^4 - 2X^3 + 3X^2 + 2X + 1$ one finds that

$$\int^X \frac{4t - 1}{\sqrt{t^4 - 2t^3 + 3t^2 + 2t + 1}}\,dt = \log\bigl(X^4 - 3X^3 + 5X^2 - 2X + (X^2 - 2X + 2)\sqrt{X^4 - 2X^3 + 3X^2 + 2X + 1}\,\bigr).$$

[1] i.e. It is well known ...

This is an example of a class of integrals

$$\int^X \frac{f(t)}{\sqrt{D(t)}}\,dt = \log\bigl(a(X) + b(X)\sqrt{D(X)}\bigr)$$

with $\deg D$ of even degree, say $\deg D = 2g+2$, and with square leading coefficient, say D monic. I leave it as an amusing exercise to confirm that the polynomial f is of degree g because it is the quotient of the derivative a' of the polynomial a by the polynomial b. The point is that $u = a + b\sqrt{D}$ must be a unit; the substitution $t \leftarrow u(t)$ then shows the integral to be truly elementary.

I explain at §6.2 that periodicity of the present continued fraction expansion is equivalent to a point at infinity on the elliptic curve $\mathcal{C}$ being torsion, in the present exmple of order 4, the degree of the unit displayed above.

2.2 The general case over infinite fields

Second, if we replace D by $D+1$ then we obtain a generic expansion nicely illustrating the behaviour of *Néron–Tate height*. Accordingly take $Z^2 - (X^2 - X + 1)Z - (X + 1/4) = 0$; then

$$\begin{aligned}
Z = [&X^2 - X + 1\,,\ X - \tfrac{5}{4}\,,\ \tfrac{16}{21}X - \tfrac{172}{441}\,,\ -\tfrac{9261}{3968}X - \tfrac{2963079}{984064}\,,\\
&-\tfrac{244047872}{2572789149}X + \tfrac{8108465945600}{34035427652121}\,,\ -\tfrac{21440698686186129}{5680165411225 60}X + \tfrac{16653223342999891329867}{21323340953740902400}\,,\\
&-\tfrac{8004782194034334760 96000}{8860777035260048771581 8861}X - \tfrac{16859983834782888001075248542515200}{25635131593910153951220171179626 3641}\,,\\
&\tfrac{800831983560491889993413827955254732939 61}{4879841035416179945492502935817420800 00}X\\
&-\tfrac{25536930067406278242073181647452394463736417754609 9}{6339537114335863047661888439234806417423597568000}\,,\\
&\tfrac{2058967214933789234321452104092213283070090699484765880320000}{503230723831903952989142036290969243284756393383295955214733129}X\\
&-\tfrac{1339214560032185955670845227717641527576031482702974152155592958515609600 00}{2295347473317007513504838832081344217172192053169949881662822066226067080592 1}\,,\ \ldots]
\end{aligned}$$

Even a computer chokes on numbers growing at such a pace.

Of course this expansion is not eventually periodic; but one might well wonder how one actually proves such a thing.

2.3 A proof of non-periodicity

$$\begin{aligned}
Z = [&X^2 - X + 1\,,\ X - \tfrac{5}{2^2}\,,\ \tfrac{2^4}{3\cdot 7}X - \tfrac{2^2\cdot 43}{3^2\cdot 7^2}\,,\ -\tfrac{3^3\cdot 7^3}{2^7\cdot 31}X - \tfrac{3^2\cdot 7^2\cdot 6719}{2^{10}\cdot 31^2}\,,\\
&-\tfrac{2^{13}\cdot 31^3}{3^4\cdot 7^4\cdot 13229}X + \tfrac{2^{10}\cdot 5^2\cdot 31^2\cdot 329591}{3^4\cdot 7^4\cdot 13229^2}\,,\ -\tfrac{3^3\cdot 7^3\cdot 13229^3}{2^{16}\cdot 5\cdot 31^4\cdot 1877}X + \tfrac{3^2\cdot 7^2\cdot 13229^2\cdot 21577726507}{2^{18}\cdot 5^2\cdot 31^4\cdot 1877^2}\,,\\
&-\tfrac{2^{20}\cdot 5^3\cdot 31^4\cdot 1877^3}{3\cdot 7\cdot 11\cdot 13229^4\cdot 12524251}X - \tfrac{2^{18}\cdot 5^2\cdot 31^4\cdot 47\cdot 1877^2\cdot 2693\cdot 1180897}{3^2\cdot 7^2\cdot 11^2\cdot 13229^4\cdot 12524251^2}\,,\\
&+\tfrac{11^3\cdot 13229^4\cdot 12524251^3}{2^{24}\cdot 5^4\cdot 31^5\cdot 1877^4\cdot 130960463}X - \tfrac{11^2\cdot 13229^4\cdot 2109269\cdot 12524251\cdot 208276252871}{2^{28}\cdot 5^3\cdot 31^6\cdot 1877^4\cdot 130960463^2}\,,\\
&\tfrac{2^{32}\cdot 5^4\cdot 31^7\cdot 1877^4\cdot 130960463^3}{3^2\cdot 7\cdot 11^4\cdot 67\cdot 331\cdot 13229^4\cdot 12524251^4\cdot 32646599}X\\
&-\tfrac{2^{28}\cdot 5^4\cdot 31^6\cdot 1877^4\cdot 130960463^2\cdot 672668401\cdot 6280895711017969}{3^4\cdot 7^2\cdot 11^4\cdot 67^2\cdot 331^2\cdot 13229^4\cdot 12524251^4\cdot 32646599^2}\,,\ \ldots\ldots].
\end{aligned}$$

The discriminant of $X^4 - 2X^3 + 3X^2 + 2X + 2$ is $2^4\cdot 3^3\cdot 31$ (and, in any case there is no reduction at 2). We read from the continued fraction expansion that $\mathbb{F}_5(X,Z)$ contains a nontrivial unit of degree 6 while $\mathbb{F}_{11}(X,Z)$ contains one of degree 7. Hence, by a theorem of Serre on the reduction behaviour of torsion subgroups of an abelian variety, $\mathbb{Q}(X,Z)$ cannot contain a nontrivial unit and so the expansion above is indeed *not* periodic.

2.4 Reducing a continued fraction expansion

I have just now used the principle that the first partial quotient that explodes mod p in fact blows up to some partial quotient over $\mathbb{F}_p$ of *higher degree*.

To explain that, it turns out to be better to study the sequence x_h/y_h of convergents than the sequence a_h of partial quotients. Of course the respective *continuants* x_h and y_h are as badly behaved under reduction as are the partial quotients, but their quotients x_h/y_h are quite polite.

After multiplying both the continuants x and y by the lowest common multiple of the denominators of their coefficients, we have $x/y = x'/y'$ where x' and y' have integer coefficients. Denote their respective reductions mod p by $\overline{x}'$ and $\overline{y}'$. I point out that obviously

$$\deg(yF - x) < -\deg y \quad \text{entails} \quad \deg(\overline{y}'\overline{F} - \overline{x}') < -\deg \overline{y}' \,;$$

that is, every convergent of F yields a convergent of $\overline{F} \equiv F \pmod{p}$ by reduction mod p (and a distance argument confirms that every convergent of $\overline{F}$ comes from one or more convergents of F).

3 An Ideal Convention

As before, $\omega^2 - t\omega + n = 0$; P and Q denote integers.

There is a useful correspondence $\alpha = (\omega + P)/Q \longleftrightarrow \langle Q, \omega + P\rangle_{\mathbb{Z}}$ between elements and $\mathbb{Z}$-modules based on the identity

$$\omega(\omega + P) = (t + P)(\omega + P) - (n + tP + P^2)\,.$$

It entails that the $\mathbb{Z}$-module is a $\mathbb{Z}[\omega]$-ideal if and only if Q divides the norm $(\omega + P)(\overline{\omega} + P)$ of its denominator.

> Writing $\beta = (\sqrt{-163} + 17)/21$ is less than ideal; it is bad conduct and is *not admissible*.
>
> In fact, $\beta = (\sqrt{-7987} + 119)/147$
>
> and β corresponds to a $\mathbb{Z}[7\sqrt{-163}]$-ideal.

Multiplication of ideals then corresponds to composition of quadratic forms, where $\langle Q, \omega + P\rangle$, or of course α, corresponds to the form $Q(X - \alpha Y)(X - \overline{\alpha}Y)$. I and all competent writers always tacitly observe the convention noted here.

4 Bounded Period Length

Set $D_x = D(x)$. In the early sixties [8], Andrzej Schinzel asked for polynomials D, say defined over $\mathbb{Z}$, so that the period length of the continued fraction expansion of $\sqrt{|D_x|}$ is bounded for x in $\mathbb{Z}$.

1. D must have square leading coefficient and be of even degree, say $\deg D = 2g + 2$.
2. Set $Y^2 = D$. The domain $\mathbb{Q}[X][Y]$, must be *exceptional* in that it contains a nontrivial unit; in effect, the numerical periods all come from "numberisation" of the function field period.

3. Some such unit must *specialise* to a unit in the number field.

The case $g = 0$, say $D(X) = A^2X^2 + 2BX + C$, is special in that there always is a nontrivial unit; it requires $(B^2 - A^2C)\big|4\gcd(A^2, B)^2$. All these cases boil down to $D(X) = A^2X^2 + 4C$ with $C\big|A$. For detail, see the paper [5].

By folklore (concerning possible torsion on the Jacobian of a hyperelliptic curve of genus g, see §6.2), for positive g the fundamental unit is of degree at most $O(g^2)$. It follows (and is observed experimentally) that the numerical families with bounded period length have short period length, no greater than $O\big((\log|D_x|)^2\big)$. This is in some contrast to the "expected" length, $O\big((D_x)^{1/2}\big)$ or so, see the survey [10].

By the way, all known families of numerical discriminants for which we can explicitly detail a unit belong to the families with bounded period length. It seems a fair bet that even just the failure of Schinzel's condition (iii) yields periods of "typical" length; it is of interest to check that experimentally.

5 Continued Fractions in Real Quadratic Number Fields

It loses little generality to consider only purely periodic expansions; to wit, to expand only reduced elements.

Suppose $\alpha = (\omega + P)/Q$ is *reduced*, namely that $\alpha > 1$ but its conjugate satisfies $-1 < \overline{\alpha} < 0$. Set

$$\alpha = a - \overline{\rho}\,, \text{ with } a = \lfloor\alpha\rfloor\text{; and notice that } \rho = a - \overline{\alpha}.$$

Then obviously $-1 < \overline{\rho} < 0$ and because plainly also $a = \lfloor\rho\rfloor$ we have $\rho > 1$. So also ρ is reduced.

Because ρ reduced entails $-1/\overline{\rho}$ reduced, it follows (by conjugation) that the continued fraction expansion of α must be purely periodic.

More, if α is reduced then both

$$0 < Q < \omega - \overline{\omega} \quad \text{and} \quad 0 < t + 2P < \omega - \overline{\omega}\,.$$

Hence the box principle provides an alternative proof that reduced elements (or if one prefers, the corresponding reduced ideals) each belong to a periodic cycle. Moreover, we see that each belongs to one of only finitely many disjoint such cycles.

6 The Quadratic Function Field Case

Define Z by $\mathcal{C} : Z^2 - AZ - R = 0$, where A and R are polynomials with $\deg A = g+1$ and $\deg R \le g$. Suppose $\deg Z > \deg \overline{Z}$.

Note that if I write $D = A^2 + 4R$ then $Z = \frac{1}{2}(Y + A)$.

An element $\alpha = (Z + P)/Q$ is reduced if $\deg\alpha > 0$ but $\deg\overline{\alpha} < 0$. If so, then $\deg Q \le g$ and $\deg P < g$.

6.1 Normal "cycles"

Over an infinite base field $\mathbb{K}$ almost every reduced α is a complete quotient in one of infinitely many disjoint normal "cycles", generically of infinite length, all of whose partial quotients have degree 1 — equivalently with complete quotients for which always $\deg Q = g$ and, slightly less trivially, for which always $\deg P = g - 1$.

I the sequel I presume that the polynomials P and Q have indeed be so chosen that $\alpha = (Z + P)/Q = (Z + P_0)/Q_0$ initiates a normal cycle.

In studying this case, one may consider a tableau of steps, $h \in \mathbb{Z}$,

$$\alpha_h = (Z + P_h)/Q_h = a_h - (\overline{Z} + P_{h+1})/Q_h$$

with $\deg a_h := 1$, $P_h(X) = d_h X^{g-1} + \cdots$, and determine a relation on $(d_h)_{h\in\mathbb{Z}}$ depending only on the curve $\mathcal{C}$, that is, on Z. If $g = 1$ then, for example,

$$d_{h-1}d_h^2 d_{h+1} = v^2\big(d_h + A(w)\big), \text{ where } R(X) = v(X - w)\,.$$

6.2 What the continued fraction does

Recall that the continued fraction expansion is a tableau of steps

$$\alpha_h = (Z + P_h)/Q_h = a_h - (\overline{Z} + P_{h+1})/Q_h$$

with $\deg a_h := 1$, $h \in \mathbb{Z}$. Suppose $Q_h(\vartheta_h) = 0$. Then $\big(\vartheta_h, -P_h(\vartheta_h)\big)$ is a point on $\mathcal{C} : Z^2 - AZ - R = 0$, albeit defined over some extension field of the base field.

In different words: set $Q_h(X) = u_h X^g + \cdots$. Each step reports the *Mumford representation* $(Q_h/u_h, -P_h)$ of a "point" M_h on the curve $\mathcal{C}$ (correctly speaking, a *divisor* M_h on the Jacobian of $\mathcal{C}$). It is straightforward to confirm that $M_h = M_0 + hS$, where S is the divisor at infinity.

So a continued fraction step is precisely the addition of the divisor S. The existence of a nontrivial unit, say of degree m, in $\mathbb{K}[X][Z]$ is therefore equivalent to the divisor S at infinity being torsion of order m.

6.3 "Messiness" of the expansion

It is quite easy to see, for formal power series over an infinite field, that partial quotients are almost always of degree one. We need only notice that a remainder $\sum_{h\geq 1} f_h X^{-h}$ has a reciprocal with polynomial part of degree greater than one, and thus gives rise to a partial quotients of degree greater than one, if and only if $f_1 = 0$. More, the partial quotient is $f_1^{-1}X - f_2 f_1^{-2}$ if $f_1 \neq 0$, and the next remainder is $(f_2^2 - f_1 f_3)f_1^{-3}X^{-1} +$ terms of lower degree in X.

A little more precisely, 'the sequential remainders have leading coefficient some determinant, and hence some multivariate polynomial, in the coefficients of the formal power series. But such a polynomial is nonzero "almost always", or "with probability one" ' — [6], p.375. The matter of "messiness" is dealt with in detail by Knuth [6] in the context of his discussion of the Euclidean aalgorithm for polynomials over $\mathbb{Z}$, where one is baulked by the "explosive growth" of the coefficients of the intermediate remainders.

Over $\mathbb{F}_p$ one finds experimentally that partial quotients of generic formal power series are of degree at least 2 with probability $1/p$, of degree at least 3 with probability $1/p^2$, ... More to the point, one sees that data for algebraic functions, suggesting strongly that those formal power series behave "typically".

I also note an important paper of Enrico Bombieri and Paula Cohen [2] *proving* that the phenomena touched upon in my present remarks hold also for simultaneous Padé approximation of higher degree algebraic functions.

Here, however, I concentrate on the quadratic case. In that special case, the box principle entails that a continued fraction expansion of a formal power series over a finite field must be periodic. Thus every prime must appear in the denominator of infinitely many partial quotients of the expansion at §2.3. I remark implicitly

that the messiness of the example expansion illustrates, given §6.2, the behaviour of Néron–Tate height and now ask, as exercise or discussion item, whether the observations I hint at here themselves entail the known behaviour of Néron–Tate height on the relevant varieties.

7 . . . over an Infinite Base Field

There are several phenomena that may surprise readers familiar only with the case of quadratic functions over finite base fields.

7.1 Quasi-periodicity

In a function field a non-trivial unit need not of course have norm ± 1; it suffices for it to have nonzero norm in the base field. In consequence it is not quite true that the existence of a non-trivial unit in a domain $\mathbb{K}[X][Z]$ guarantees periodicity of the continued fraction expansion of elements of that domain. However, an instructive exercise, if an element with polynomial trace has a quasi-periodic expansion then it certainly has a periodic expansion.

7.2 Poor conductivity

If an element has a periodic expansion it does not follow that multiples of it by a rational function will have a periodic expansion.

An instructive example, in effect $\sqrt{X^2+uX+v}/X$, which has a normal expansion, is discussed *in extenso* by David Cantor [3].

7.3 Singular hyper-elliptic curves

Readers will notice that this remark expands upon the preceding comment. Given the curve $\mathcal{C} : Z^2 - AZ - R = 0$ the formulaire providing the expansion of $\alpha = (Z+P)/Q$ seems conditioned only by the degree $g+1$ of A notwithstanding that the genus of $\mathcal{C}$ may be lower than g. Only the genus zero case seems to be distinguished by the actual expansion in that the coefficients in its partial quotients may grow at no more than exponential rate. However, I believe it to be open as to whether or not the coefficients are in fact constrained to grow at no greater rate.

8 Division Polynomials and their Analogues

8.1 The Elliptic Case, $g = 1$

Recall my writing $P_h(X) = d_h X^g + \cdots$. It turns out that the relation

$$d_{h-1}d_h^2 d_{h+1} = v^2\big(d_h + A(w)\big), \text{ where } R(X) = v(X-w)$$

is, after the transformation $U = Z$, $V - v = XZ$ of $\mathcal{C}$ to a cubic model in variables (U, V) with the d_h the U co-ordinates of the points $M + hS$ on $\mathcal{C}$, just the identity

$$\big(\wp(a+b)-\wp(b)\big)\big(\wp(a)-\wp(b)\big)^2\big(\wp(a-b)-\wp(b)\big) = -\alpha\big(\wp(a)-\wp(b)\big)+\beta\,,$$

where $\alpha = \wp'(b)^2$, $\beta = \wp'(b)^2(\wp(2b)-\wp(b))$.

More, the definition $C_h = d_{h-1}d_{h+1}/d_h^2$ — giving a *Somos sequence* $(C_h)_{h\in\mathbb{Z}}$ satisfying $C_{h-2}C_{h+2} = v^2C_{h-1}C_{h+1} + v^2A(w)C_h^2$ — picks out the (square root of the) denominator of each d_h and generically yields a sequence of integers.

The C_h may be identified as the h-th *division polynomials* shifted by the initial data M and — after a strategic prior translation by $(-x, -y)$ — indeed are polynomials in the variables (x, y).

One says that the recurrence relation is bi-linear and of *width* 4 (the maximal difference of the indices). My paper [7] with Chris Swart, more particularly its references, provides a useful introduction to these matters.

Given the definitions I provide, it may seem surprising that the reductions mod p of Somos sequences yield interesting data; see for example [9].

8.2 The General Case

David Cantor [4] has a cute strategy for obtaining relations on $(d_h)_{h\in\mathbb{Z}}$ for general g. To hint at his method, I set $\alpha = \alpha_0$ and $N = \alpha\overline{\alpha}$, $T = \alpha + \overline{\alpha}$. I denote the convergents given by the expansion of α by x_h/y_h. Now consider the ideal matrices

$$N_h := \begin{pmatrix} x_h & -Ny_h \\ y_h & x_h - Ty_h \end{pmatrix} = \begin{pmatrix} x_h & x_{h-1} \\ y_h & y_{h-1} \end{pmatrix} \begin{pmatrix} 1 & (P_{h+1} - P)/Q \\ 0 & Q_{h+1}/Q \end{pmatrix} =: M_h \begin{pmatrix} 1 & (P_{h+1} - P)/Q \\ 0 & Q_{h+1}/Q \end{pmatrix}.$$

By the way, as it indeed should, the last matrix corresponds to

$$(\alpha + (P_{h+1} - P)/Q)/(Q_{h+1}/Q) = (Z + P_{h+1})/Q_{h+1}\,.$$

One sees that products $N_{r-i}N_{s+i}$ do not arise from convergents (are not reduced) but that for any $g + 1$ distinct i, say for $i = 0, 1, \ldots, g$, there is a $\mathbb{K}$-linear combination of the products which equals N_{r+s+1}.

Using such an observation, Cantor constructs vanishing determinants of dimension $(g + 2) \times (g + 2)$ which ultimately allow him to obtain recursion formulas for a higher genus *analogue* of the division polynomials.

Specifically, his h-th polynomial vanishes at all "points" whose h-th multiple is not generic — that is, with divisor given by a k-tuple for some k smaller than g.

The relevant recursive identities are $(g+1)$-linear width $2g+2$ analogues of the bi-linear Somos recursions. A simple elimination allows one to transform them to greater width bi-linear recursions. For example, see [1] for an explicit construction, if $g = 2$ then the natural relation is tri-linear with width 6 but may be rewritten as bi-linear of width 8.

References

[1] Harry W. Braden, Victor Z. Enolskii, and Andrew N. W. Hone, 'Bilinear recurrences and addition formulæ for hyperelliptic sigma functions', *J. Nonlinear Math. Phys.* **12** (2005), suppl. 2, 46–62.

[2] E. Bombieri and P. B. Cohen, 'Siegel's Lemma, Padé Approximations and Jacobians' (with an appendix by Umberto Zannier, and dedicated to Enzio De Giorgi), *Ann. Scuola Norm. Sup. Pisa* Cl. Sci. (4) **25** no. 1-2, (1998), 155–178.

[3] David G. Cantor, 'On the continued fractions of quadratic surds', *Acta Arith.* **68**.4 (1994), 295–305.

[4] David G. Cantor, 'On the analogue of the division polynomials for hyperelliptic curves', *J. für Math.* **447** (1994), 91–145.

[5] Kell Cheng and Hugh Williams, 'Some results concerning certain periodic continued fractions', *Acta Arith.* **117**.3 (2005), 247–264.

[6] Donald E. Knuth, *The Art of Computer Programming*, **2** Seminumerical Algorithms (1969; 2nd printing), pp360ff.

[7] Alfred J. van der Poorten and Christine S. Swart, 'Recurrence relations for elliptic sequences: every Somos 4 is a Somos k', *Bull. London Math. Soc.* **38**.4 (2006), 546–554.

[8] A. Schinzel, 'On some problems of the arithmetical theory of continued fractions', *Acta Arith.* **6** (1961), 393–413; and 'II' *ibid.* (1962), 287–298.

[9] Joseph H. Silverman, 'p-adic properties of division polynomials and elliptic divisibility sequences', *Math. Ann.* **332**.2 (2005), 443–471; 'Addendum ...', *ibid.*, 473–474.

[10] H. C. Williams, 'Solving the Pell equation', in *Number theory for the millennium, III* (Urbana, IL, 2000), 397–435, A K Peters, Natick, MA, 2002.

Symmetry phenomenons in linear forms in multiple zeta values

Tanguy Rivoal

Institut Fourier, CNRS UMR 5582
Université Grenoble 1
100 rue des Maths, BP 74
38402 Saint-Martin d'Hères cedex
France.

The following text, based on joint work with J. Cresson and S. Fischler [6, 7], corresponds to the talk I gave at Turun Yliopisto in may 2007 during the ANT conference. I warmly thank the organisers of this conference for the invitation, especially Tapani Matala-Aho.

A generalisation of the Riemann zeta function $\zeta(s)$ is given by the multiple zeta value (abreviated as MZV ; note that in french, the word *polyzêta* is now often used for this series) defined for all integers $p \geq 1$ and all p-tuples $\underline{s} = (s_1, s_2, \ldots, s_p)$ of integers ≥ 1, with $s_1 \geq 2$, by

$$\zeta(s_1, s_2, \ldots, s_p) = \sum_{k_1 > k_2 > \ldots > k_p \geq 1} \frac{1}{k_1^{s_1} k_2^{s_2} \ldots k_p^{s_p}}.$$

The integers p and $s_1 + s_2 + \ldots + s_p$ are the depth and the weight of $\zeta(s_1, s_2, \ldots, s_p)$ respectively. MZVs naturally appear when, for example, one considers products of values of the zeta function, e.g $\zeta(n)\zeta(m) = \zeta(n+m) + \zeta(n,m) + \zeta(m,n)$. In a certain sense, this enables us to "linearise" these products. Except a few identities such as $\zeta(2,1) = \zeta(3)$ (due to Euler), the arithmetical nature of MZVs is no better understood than that of $\zeta(s)$. However, the set of MZVs has a very rich structure which is well understood, at least conjecturally. (See [16]). For example, let us consider the $\mathbb{Q}$-vector spaces $\mathcal{Z}_p$ of $\mathbb{R}$ which are spanned by the 2^{p-2} MZVs of weight $p \geq 2$: $\mathcal{Z}_2 = \mathbb{Q}\zeta(2)$, $\mathcal{Z}_3 = \mathbb{Q}\zeta(3) + \mathbb{Q}\zeta(2,1)$, $\mathcal{Z}_4 = \mathbb{Q}\zeta(4) + \mathbb{Q}\zeta(3,1) + \mathbb{Q}\zeta(2,2) + \mathbb{Q}\zeta(2,1,1)$, etc. Set $v_p = \dim_{\mathbb{Q}}(\mathcal{Z}_p)$. We have the following conjecture, whose (i) is due to Zagier and (ii) to Goncharov.

Conjecture 1. *(i) For any integer $p \geq 2$, we have $v_p = c_p$, where c_p is defined by the linear recursion $c_{p+3} = c_{p+1} + c_p$, where $c_0 = 1$, $c_1 = 0$ and $c_2 = 1$.*

(ii) The $\mathbb{Q}$-vector spaces $\mathbb{Q}$ and $\mathcal{Z}_p$ $(p \geq 2)$ are in direct sum.

Hence, the sequence $(v_p)_{p \geq 2}$ should grow like α^p (where $\alpha \approx 1,3247$ is a root of the polynomial $X^3 - X - 1$), which is much less than 2^{p-2}. Thus, conjecturally, there exist many linear relations between MZVs of the same weight and none between those of different weight: in this direction, the theorem of Goncharov [9] and Terasoma [14] claims that $v_p \leq c_p$ for all integers $p \geq 2$. It remains to prove the opposite inequality to show (i), but no non-trivial lower bound for v_p is yet known: even if classical relations give $v_2 = v_3 = v_4 = 1$, we do not know how to prove that $v_5 = 2$, which is equivalent to the irrationality of $\zeta(5)/(\zeta(3)\zeta(2))$. Conjecture 1 is also interesting because it implies the following one.

Conjecture 2. *The numbers* $\pi, \zeta(3), \zeta(5), \zeta(7), \zeta(9)$, *etc, are algebraically independent over* $\mathbb{Q}$.

This conjecture seems completely out of reach. A number of diophantine results have been proved in weight 1, i.e, in the case of the Riemann zeta function (see [8]):

(*i*) The number $\zeta(3)$ is irrational (Apéry [1]);

(*ii*) The dimension of the vector space spanned over $\mathbb{Q}$ by 1, $\zeta(3)$, $\zeta(5), \ldots$, $\zeta(A)$ (with A odd) grows at least as fast as $\log(A)$ ([2, 12]);

(*iii*) At least one of the four numbers $\zeta(5), \zeta(7), \zeta(9), \zeta(11)$ is irrational (Zudilin [19]).

These results can be proved by the study of certain series of the form

$$\sum_{k=1}^{\infty} \frac{P(k)}{(k)_{n+1}^{A}} \tag{0.1}$$

where $P(X) \in \mathbb{Q}[X]$, $n \geq 0$, $A \geq 1$. Here, we use the Pochhammer symbol, defined by $(k)_\alpha = k(k+1)\ldots(k+\alpha-1)$. The above series can be written as a linear combination over $\mathbb{Q}$ of 1 and the values of zeta at integers. The crucial point is we can find special polynomials P such that in these combinations only certain value of zeta occur: $\zeta(3)$ in case (*i*), values $\zeta(s)$ with s odd in cases (*ii*) and (*iii*). This comes from (in the last two cases, and also in certain proofs of (*i*)) a symmetry property linked to the very-well-poised aspect of the series (0.1) (see [2] ou [12]):

Theorem 1. *Let* $P \in \mathbb{Q}[X]$ *of degree at most* $A(n+1)-2$, *such that*

$$P(-n-X) = (-1)^{A(n+1)+1} P(X).$$

Then, the series (0.1) *is a linear combination, with rational coefficients, of* 1 *and* $\zeta(s)$ *with* s *an odd integer between* 3 *and* A.

Our aim is to present two generalisations, in arbitrary depth, of this symmetry phenomenon, and whose proofs are given in [7]. We hope that such generalisations will make new diophantine results (irrationality or linear independence) for the underlying MZVs possible.

Our first result deals with "uncoupled" series, i.e, series over all p-tuples $(k_1, \ldots, k_p) \in \mathbb{N}^{*p}$:

Theorem 2. *Consider integers* $p \geq 1$, $n \geq 0$ *and* $A \geq 1$. *Let* $P \in \mathbb{Q}[X_1, \ldots, X_p]$ *be a polynomial of degree* $\leq A(n+1)-2$ *with respect to each of the variables, such that*

$$\begin{aligned} &P(X_1, \ldots, X_{j-1}, -X_j - n, X_{j+1}, \ldots, X_p) \\ &\qquad = (-1)^{A(n+1)+1} P(X_1, \ldots, X_{j-1}, X_j, X_{j+1}, \ldots, X_p) \end{aligned}$$

for any $j \in \{1, \ldots, p\}$. *Then, the multiple series*

$$\sum_{k_1, \ldots, k_p \geq 1} \frac{P(k_1, \ldots, k_p)}{(k_1)_{n+1}^{A} \cdots (k_p)_{n+1}^{A}} \tag{0.2}$$

is a polynomial with rational coefficients, of degree at most p, *in the* $\zeta(s)$, *for* s *an odd integer between* 3 *and* A.

For example, when $A = 3$ or $A = 4$, this series is a polynomial in $\zeta(3)$. When $p = 1$, we exactly obtain Theorem 1 (for all A).

From the point of view of diophantine applications, the main drawback of Theorem 2 is that the summation of $k_1, \ldots, k_p$ is uncoupled. We now describe three disadvantages of uncoupled series.

First of all, uncoupled series always give polynomials in values of ζ at integers, even if we omit the symmetry condition in Theorem 2. This remark shows that MZVs cannot really appear in this setup.

Secondly, let us consider Ball's series

$$S_n = n!^2 \sum_{k=1}^{\infty} (k + \frac{n}{2}) \frac{(k-n)_n (k+n+1)_n}{(k)_{n+1}^4}.$$

For all integer n, S_n is a linear form in 1 and $\zeta(3)$; this follows from Theorem 1. (The series S_n exactly coincids with the linear forms used by Apéry to prove the irrationality of $\zeta(3)$; without going into details, let us mention that this coincidence is not all trivial and is the first application of the *denominators conjecture* proved in [11].) For all integers $p \geq 1$, the series S_n^p is obviously an uncoupled series of the the form considered in Theorem 2 with

$$\begin{aligned} &P(X_1, \ldots, X_p) \\ &= n!^{2p} (X_1 + \frac{n}{2}) \ldots (X_p + \frac{n}{2}) (X_1 - n)_n \ldots (X_p - n)_n (X_1 + n + 1)_n \ldots (X_p + n + 1)_n \end{aligned}$$

and $A = 4$. Therefore, S_n^p is a polynomial in $\zeta(3)$ of degree (at most) p, from which we could hope to deduce the transcendence of $\zeta(3)$. However, S_n^p does not contain anymore diophantine information than S_n and it can only gives the irrationality of $\zeta(3)$.

Finally, the multiple series which appear in irrationality proofs are generally of the form

$$\sum_{k_1 \geq \ldots \geq k_p \geq 1} \frac{P(k_1, \ldots, k_p)}{(k_1)_{n+1}^A \ldots (k_p)_{n+1}^A}, \tag{0.3}$$

i.e, the summation is over ordered indices; it is to this kind of series that one can apply the algorithm decribed in [6]. For example, when $p = 2$, $A = 2$ and

$$P(X_1, X_2) = n!(X_1 - X_2 + 1)_n (X_2 - n)_n (X_2)_{n+1},$$

Sorokin [13] shows that the sum (0.3) is exactly the linear form in 1 and $\zeta(3)$ used by Apéry. More generaly, a conjecture of Vasilyev [15] claimed that a certain multiple integral, equals to

$$n!^{p-\varepsilon} \sum_{k_1 \geq \cdots \geq k_p \geq 1} \frac{(k_1 - k_2 + 1)_n \ldots (k_{p-1} - k_p + 1)_n (k_p - n)_n}{(k_1)_{n+1}^2 \ldots (k_{p-1})_{n+1}^2 (k_p)_{n+1}^{2-\varepsilon}}, \tag{0.4}$$

is a rational linear form in zeta values at integers ≥ 2 of the same parity as $\varepsilon \in \{0, 1\}$. The integral formulation of this conjecture was proved in [20] and a refined version was proved in [11]: the method is to prove that the series (0.4) is also equal to a simple series to which Theorem 1 applies. Zlobin [18] recently obtained a completely different proof by a direct study of the series (0.4), in the spirit of the combinatorial methods developped in [6, 7]. It is then possible to prove results

of essentially the same nature as those of [2, 12]: this confirms our feeling that multiple series with ordered indices are the interesting ones.

We showed in [6] that any convergent series of the form (0.3) can be written as a rational linear form in MZVs of weight at most pA and of depth at most p (this result was also obtained independently by Zlobin [17]). Furthermore, we produced an algorithm, implemented [5] in Pari, to explicitly compute such a linear combination. This enabled us to discover the symmetry property that we now describe in the special case of depth 2 for the reader's convenience.

Theorem 3. *Consider integers $n \geq 0$ et $A \geq 1$, with n even. Let $P \in \mathbb{Q}[X_1, X_2]$ be a polynomial in two variables, of degree $\leq A(n+1)-2$ in each one, such that*

$$\begin{cases} P(X_1, X_2) = -P(X_2, X_1) \\ P(-n - X_1, X_2) = (-1)^{A(n+1)+1} P(X_1, X_2) \\ P(X_1, -n - X_2) = (-1)^{A(n+1)+1} P(X_1, X_2) \end{cases} \tag{0.5}$$

Then, the double series (0.3) *is a linear combination, with rational coefficients,*

- *of 1,*
- *of the values $\zeta(s)$ with s an odd integer such that $3 \leq s \leq 2A$,*
- *of the differences $\zeta(s, s') - \zeta(s', s)$ with s, s' odd integers such that $3 \leq s < s' \leq A$.*

(Let us note here that in the series (0.3), the variables $k_1, \ldots, k_p$ are linked by non-strict inequalities, as in [6], but contrary to the definition of MZVs. This does not cause any problems, since it is easy to go from statements with non-strict inequalities to statements with strict inequalities, and vice-versa.)

Of course, in (0.5), the third condition is a consequence of the first two. If $A = 4$, this theorem shows that the double series

$$\sum_{k_1 \geq k_2 \geq 1} \frac{P(k_1, k_2)}{(k_1)^4_{n+1} (k_2)^4_{n+1}}$$

is a linear form in 1, $\zeta(3)$, $\zeta(5)$ and $\zeta(7)$ (which was far from obvious a priori since this a double series). For $A = 3$, we get a linear form in 1, $\zeta(3)$, $\zeta(5)$. Finally, for $A = 2$, we get a linear form in 1 and $\zeta(3)$.

To state our main result in arbitrary depth, we need the following notation. For integers $p \geq 0$ and $s_1, \ldots, s_p \geq 2$, we set

$$\zeta^{\mathrm{as}}(s_1, \ldots, s_p) = \sum_{\sigma \in \mathfrak{S}_p} \varepsilon_\sigma \zeta(s_{\sigma(1)}, \ldots, s_{\sigma(p)}),$$

where ε_σ is the signature of the permutation σ. We call such a linear combination of MZVs an *antisymmetric MZV* (even if, for $p \geq 2$, it is not an MZV in general). These are convergent series since each s_i is supposed ≥ 2. For $p = 1$, we have $\zeta^{\mathrm{as}}(s) = \zeta(s)$. The natural convention is to set $\zeta^{\mathrm{as}}(s_1, \ldots, s_p) = 1$ when $p = 0$ because there exists one unique bijection of the empty set onto itself. For $p = 2$, we have $\zeta^{\mathrm{as}}(s_1, s_2) = \zeta(s_1, s_2) - \zeta(s_2, s_1)$ and, when $p = 3$,

$$\begin{aligned} \zeta^{\mathrm{as}}(s_1, s_2, s_3) & \\ &= \zeta(s_1, s_2, s_3) + \zeta(s_2, s_3, s_1) + \zeta(s_3, s_1, s_2) - \zeta(s_2, s_1, s_3) \\ &\qquad - \zeta(s_1, s_3, s_2) - \zeta(s_3, s_2, s_1). \end{aligned}$$

By definition, for all $\sigma \in \mathfrak{S}_p$, we have

$$\zeta^{\mathrm{as}}(s_{\sigma(1)}, \ldots, s_{\sigma(p)}) = \varepsilon_\sigma \zeta^{\mathrm{as}}(s_1, \ldots, s_p),$$

and $\zeta^{\mathrm{as}}(s_1, \ldots, s_p) = 0$ once two of the s_i's are equal. It seems reasonable to us that in general an antisymmetric MZV is not a polynomial in values of the Riemann zeta function. However, any "symmetric" MZV (defined as $\zeta^{\mathrm{as}}(s_1, \ldots, s_p)$ but omiting the signature ε_σ) is a polynomial in $\zeta(s)$ (by [10], Theorem 2.2).

Let $\mathscr{A}_p$ denotes the set of polynomials $P(X_1, \ldots, X_p) \in \mathbb{Q}[X_1, \ldots, X_p]$ such that:

$$\begin{cases} \text{For all } \sigma \in \mathfrak{S}_p, \text{ we have} \\ \qquad P(X_{\sigma(1)}, X_{\sigma(2)}, \ldots, X_{\sigma(p)}) = \varepsilon_\sigma P(X_1, X_2, \ldots, X_p). \\ \\ \text{For all } j \in \{1, \ldots, p\}, \text{ we have} \\ \qquad P(X_1, \ldots, X_{j-1}, -X_j - n, X_{j+1}, \ldots, X_p) \\ \qquad\qquad = (-1)^{A(n+1)+1} P(X_1, \ldots, X_{j-1}, X_j, X_{j+1}, \ldots, X_p). \end{cases}$$

There are redondances in these conditions. If the first one is satisfied, then it is enough to check the second one for one single value of j. For example, $\mathscr{A}_2$ is exactly the set of polynomials P satisfying the conditions (0.5). Moreover, if $P \in \mathscr{A}_p$ then P has the same degree in each variable $X_1, \ldots, X_p$. Clearly, the definition of $\mathscr{A}_p$ also depends on the parity of $A(n+1)$. We can now state our main result.

Theorem 4. *Consider integers $n \geq 0$ and $A, p \geq 1$, with n even. Let $P \in \mathscr{A}_p$ be of degree $\leq A(n+1) - 2$ in each of the variables. Then, the series*

$$\sum_{k_1 \geq \ldots \geq k_p \geq 1} \frac{P(k_1, \ldots, k_p)}{(k_1)_{n+1}^A \ldots (k_p)_{n+1}^A} \tag{0.6}$$

is a rational linear combination of products of the form

$$\zeta(s_1) \ldots \zeta(s_q) \zeta^{\mathrm{as}}(s'_1, \ldots, s'_{q'}),$$

where

$$\begin{cases} q, q' \geq 0 \text{ integers such that } 2q + q' \leq p, \\ s_1, \ldots, s_q, s'_1, \ldots, s'_{q'} \text{ odd integers } \geq 3, \\ s_i \leq 2A - 1 \text{ for all } i \in \{1, \ldots, q\}, \\ s'_i \leq A \text{ for all } i \in \{1, \ldots, q'\}. \end{cases} \tag{0.7}$$

When $q' = 0$, the antisymmetric MZV $\zeta^{\mathrm{as}}(s'_1, \ldots, s'_{q'})$ is equal to 1 and we obtain a product of values of ζ at odd integers. When $q = q' = 0$, this produit is empty and we obtain 1.

If $p = 1$, Theorem 4 states that (0.6) is a linear combination of 1 and the $\zeta(s)$ with odd s such that $3 \leq s \leq A$: this is just Theorem 1.

If $p = 2$, we obtain exactly Theorem 3.

If $p = 3$, the theorem states that the series is a linear combination of

- products of at most two values of ζ at odd integers ≥ 3,
- antisymmetric MZVs $\zeta^{\mathrm{as}}(s_1, s_2)$ with $s_1, s_2 \geq 3$ odd,
- antisymmetric MZVs $\zeta^{\mathrm{as}}(s_1, s_2, s_3)$ with $s_1, s_2, s_3 \geq 3$ odd.

In depth $p \geq 4$, terms such as $q \geq 1$ and $q' \geq 2$ can appear: it seems that the series is not always the sum of a polynomial in values of $\zeta(s)$ (with s odd) and of a linear combination of antisymmetric MZVs $\zeta^{\mathrm{as}}(s_1, \ldots, s_q)$ with $s_1, \ldots, s_q$ odd.

When $A \leq 2$, we necessarily have $q' = 0$ in all the products, which implies the following corollary.

Corollary 1. *Under the hypotheses of Theorem 4, if $A \leq 2$, then the series* (0.6) *is a polynomial in $\zeta(3)$ with rationals coefficients.*

Theorem 4 also contains, for example, the following special case.

Corollary 2. *Consider integers $n, r, t, \varepsilon \geq 0$ and $A, p \geq 1$, with n even, such that*

$$\varepsilon \equiv (A+1)(n+1) + 1 \bmod 2$$

and

$$\varepsilon + (4r+2)p + 2t \leq (A-1)(n+1) + 4r.$$

Then, the convergent series

$$\sum_{k_1 \geq \ldots \geq k_p \geq 1} \Bigg[\prod_{i=1}^{p} (k_i + \frac{n}{2})\Bigg]^{\varepsilon} \times \frac{\Big[\prod\limits_{1 \leq i < j \leq p} (k_i - k_j - r)_{2r+1} (k_i + k_j + n - r)_{2r+1}\Big]\Big[\prod\limits_{i=1}^{p} (k_i - t)_{2t+n+1}\Big]}{(k_1)_{n+1}^{A} \ldots (k_p)_{n+1}^{A}}$$

is a linear combination as described in Theorem 4.

An example of application of this corollary is the following series (in which we take $t = 0$ and the Pochhammer symbols $(k_i)_{n+1}$ at the numerator cancel out with those at the denominator):

$$\sum_{k_1 \geq k_2 \geq k_3 \geq 1} \big(k_1 + \frac{1}{2}\big)\big(k_2 + \frac{1}{2}\big)\big(k_3 + \frac{1}{2}\big) \times \frac{(k_1 - k_2)(k_2 - k_3)(k_1 - k_3)(k_1 + k_2 + 1)(k_1 + k_3 + 1)(k_2 + k_3 + 1)}{(k_1)_2^4\,(k_2)_2^4\,(k_3)_2^4} = -\frac{1}{4} - \zeta(3) + \frac{1}{4}\,\zeta(5) + \zeta(3)^2 - \frac{1}{4}\,\zeta(7).$$

$$\sum_{k_1 \geq k_2 \geq 1} \big(k_1 + \frac{1}{2}\big)\big(k_2 + \frac{1}{2}\big) \frac{(k_1 - k_2 - 1)_3 (k_1 + k_2)_3 (k_1 - 1)_4 (k_2 - 1)_4}{(k_1)_2^7\,(k_2)_2^7} = -1156 + 891\,\zeta(3) + \frac{189}{2}\,\zeta(5) + 78\big(\zeta(5,3) - \zeta(3,5)\big).$$

Finally, let us mention that the series described in the above theorems are related to the multiple hypergeometric series that can be associated to root systems: see [3, 4] for example as well as the discussion in [7].

References

[1] R. Apéry, *Irrationalité de $\zeta(2)$ et $\zeta(3)$*, Journées Arithmétiques (Luminy, 1978), Astérisque, no. **61**, 1979, p. 11–13.

[2] K. Ball and T. Rivoal, *Irrationalité d'une infinité de valeurs de la fonction zêta aux entiers impairs*, Invent. Math. **146** (2001), no. 1, p. 193–207.

[3] G. Bhatnagar and M. Schlosser, *C_n and D_n very well-poised ${}_{10}\phi_9$ transformations*, Constr. Approx. **14** (1998), p. 531–567.

[4] H. Coksun, *An Elliptic BC_n Bailey Lemma, Multiple Rogers–Ramanujan Identities and Euler's Pentagonal Number Theorems*, Trans. AMS, to appear

[5] J. Cresson, S. Fischler and T. Rivoal, Algorithm available at `http//www.math.u-psud.fr/~fischler/algo.html`.

[6] J. Cresson, S. Fischler and T. Rivoal *Séries hypergéométriques multiples et polyzêtas*, Bulletin de la Soc. Math. de France, to appear.

[7] J. Cresson, S. Fischler and T. Rivoal, *Phénomènes de symétrie dans des formes linéaires en polyzêtas*, J. reine angew. Math., to appear.

[8] S. Fischler, *Irrationalité de valeurs de zêta (d'après Apéry, Rivoal, ...)*, Sém. Bourbaki 2002/03, Astérisque **294**, 2004, exp. no. 910, p. 27–62.

[9] A. Goncharov, *Multiple polylogarithms and mixed Tate motives*, preprint available at `http//front.math.ucdavis.edu/math.AG/0103059`, 2001.

[10] M. Hoffman, *Multiple harmonic series*, Pacific J. of Math. **152** (1992), p. 275–290.

[11] C. Krattenthaler and T. Rivoal, *Hypergéométrie et fonction zêta de Riemann*, Memoirs of the AMS **186** (2007), 93 pages.

[12] T. Rivoal, *La fonction zêta de Riemann prend une infinité de valeurs irrationnelles aux entiers impairs*, C. R. Acad. Sci. Paris, Ser. I **331** (2000), no. 4, p. 267–270.

[13] V. Sorokin, *Apéry's theorem*, Vestnik Moskov. Univ. Ser. I Mat. Mekh. [Moscow Univ. Math. Bull.] **53** (1998), no. 3, p. 48–53 [48–52].

[14] T. Terasoma, *Mixed Tate motives and multiple zeta values*, Invent. Math. **149** (2002), no. 2, p. 339–369.

[15] D. Vasilyev, *Approximations of zero by linear forms in values of the Riemann zeta-function*, Doklady Nats. Akad. Nauk Belarusi **45** (2001), no. 5, p. 36–40, in russian ; extended version in english anglais : *On small linear forms for the values of the Riemann zeta-function at odd points*, preprint no.1 (558), Nat. Acad. Sci. Belarus, Institute Math., Minsk (2001), 14 pages.

[16] M. Waldschmidt, *Valeurs zêta multiples : une introduction*, J. Théor. Nombres Bordeaux **12** (2000), no. 2, p. 581–595.

[17] S. Zlobin, *Expansion of multiple integrals in linear forms*, Mat. Zametki [Math. Notes] **77** (2005), no. 5, 683–706 [630–652].

[18] S. Zlobin, *Properties of coefficients of certain linear forms in generalized polylogarithms*, Fundamentalnaya i Prikladnaya Matematika [Fundamental and Applied Mathemetics] **11** (2005), no. 6, p. 41–58,

[19] W. Zudilin, *One of the numbers* $\zeta(5)$, $\zeta(7)$, $\zeta(9)$, $\zeta(11)$ *is irrational*, Uspekhi Mat. Nauk [Russian Math. Surveys] **56** (2001), no. 4, p. 149–150 [774–776].

[20] W. Zudilin, *Well-poised hypergeometric service for diophantine problems of zeta values*, J. Théor. Nombres Bordeaux **15** (2003), no. 2, p. 593–626.

Is n a prime number? *

Nitin Saxena

Centrum voor Wiskunde en Informatica
Amsterdam, The Netherlands

Abstract

In this talk we survey the various efficient primality tests known by classifying them according to the rings they work on.

1 Introduction

The problem of primality testing is to check whether a given positive integer n is a prime number or not. Ideally, we would like to do this in time polynomial in $\log n$. This problem appears in the literature atleast as early as 500 B.C. (ancient Chinese) and 200 B.C. (ancient Greek: Eratosthenes Sieve) but the question of finding an "efficient" primality test was probably first raised by Kurt Gödel in a letter to John von Neumann in 1956. Eratosthenes sieve is a primality test almost derived from the definition of prime numbers : divide n by all prime numbers between 2 to $\sqrt{n}$ and declare n prime iff n is not divisible by any of them. In the last century many more advanced primality tests were introduced (refer [3]) and we will survey some of them here.

2 Primality and Rings

All the advanced methods associate a ring R to the given integer n and try to relate the properties of the ring with the properties of the integer n.

2.1 Ring $\mathbb{Z}_n$

The most natural ring to work with is integers modulo n: $\mathbb{Z}_n$. There are many primality tests that work in this ring:

1. *Fermat Test:* Pick a random $a \in \mathbb{Z}_n$ and declare n prime iff $a^n = a$. This was proposed by Fermat in 1660s. It was shown by Carmichael in 1910 that there are n when this test will fail for all choices of a.

2. *Lucas Test:* Pick a random $a \in \mathbb{Z}_n$ and declare n prime iff $a^{n-1} = 1$ and $a^{\frac{n-1}{p}} \neq 1$ for all primes $p|(n-1)$. This was proposed in 1891. This is an efficient randomized test if $(n-1)$ is smooth.

*An extended abstract of the talk given in University of Turku, Finland on 10th May 2007.

3. *Pocklington-Lehmer Test:* Pick a random $a \in \mathbb{Z}_n$ and declare n prime iff $a^{n-1} = 1$ and $\gcd(a^{\frac{n-1}{p_i}} - 1, n) = 1$ for any distinct primes $p_1, \ldots, p_t | (n-1)$. This was proposed in 1914. This is an efficient randomized primality test if we know distinct primes $p_1, \ldots, p_t | (n-1)$ such that $p_1 \cdots p_t \geq \sqrt{n}$.

4. *Pépin's Test:* Declare n prime iff $3^{\frac{n-1}{2}} = -1 \pmod{n}$. This was proposed in 1877. It is an efficient deterministic primality test for Fermat numbers $n = 2^{2^k} + 1$.

5. *Solovay-Strassen Test:* Pick a random $a \in \mathbb{Z}_n$ and declare n prime iff $a^{\frac{n-1}{2}} = \left(\frac{a}{n}\right)$. This was proposed in 1973. It is an efficient randomized primality test for all numbers n.

6. *Miller-Rabin Test:* Given an odd number $n = 1 + 2^s \cdot t$ where $s, t \in \mathbb{N}$ and t is odd. Pick a random $a \in \mathbb{Z}_n$ and declare n prime iff the sequence $a^{2^{s-1} \cdot t}$, $a^{2^{s-2} \cdot t}$, $\ldots, a^t$ has either a -1 or all 1's. This was proposed in 1975. It is the most popular efficient randomized primality test for all numbers n.

2.2 Quadratic Extension Ring $\mathbb{Z}_n[\sqrt{D}]$

Computing in the quadratic extension ring $\mathbb{Z}_n[\sqrt{3}]$ Lucas proved in 1876 that the Mersenne number $2^{127} - 1$ is prime; this would remain the largest known Mersenne prime for three-quarters of a century. Lehmer generalized this method in the 1930s to test primality of numbers n when $(n+1)$ is smooth and by working in $\mathbb{Z}_n[\sqrt{D}]$ where $\left(\frac{D}{n}\right) = -1$.

The idea of doing computations in a ring extension of $\mathbb{Z}_n$ is a promising one. For example, whenever $(n^2 \pm n + 1)$ is smooth one can test n for primality by going to *cubic extensions* (Williams 1978). The next section presents primality tests that use even higher ring extensions.

2.3 Coordinate Ring of Elliptic Curves $\mathbb{Z}_n[x, y]/(y^2 - x^3 - ax - b)$

An *elliptic curve* over $\mathbb{Z}_n$ is the set of points:

$$E_{a,b}(\mathbb{Z}_n) = \left\{(x, y) \in \mathbb{Z}_n^2 \mid y^2 = x^3 + ax + b\right\}$$

In 1986 Goldwasser-Kilian gave an efficient randomized primality test that never errs when n is composite. Its time complexity, conditional on a conjecture on the distribution of primes, is $O^{\sim}(\log^4 n)$ (Atkin-Morain 1993).

In 1992 Adleman-Huang made Goldwasser-Kilian test unconditional using hyperelliptic curves. But the time complexity rose upto $O(\log^c n)$ where $c > 30$.

2.4 Cyclotomic Ring $\mathbb{Z}_n[x]/(x^r - 1)$

The cyclotomic extension rings have been the most successful in deriving primality of n without using randomness.

1. *Adleman-Pomerance-Rumely Test:* Recall how Lucas-Lehmer-Williams tested n for primality when $(n-1), (n+1), (n^2 - n + 1)$ or $(n^2 + n + 1)$ is smooth. What can we do when $(n^m - 1)$ is smooth? Maybe go to some m-th extension of $\mathbb{Z}_n$? This question inspired the APR test (1980). It is a deterministic algorithm with time complexity $\log^{O(\log\log\log n)} n$. It was speeded up and

made practical by Cohen and Lenstra (1981). It attempts to find a prime factor of n using higher reciprocity laws in cyclotomic extensions of $\mathbb{Z}_n$ and is conceptually the most complex algorithm of all.

2. *Agrawal-Kayal-Saxena Test:* Pick an r such that $\text{ord}_r(n) > 4\log^2 n$ and work in the cyclotomic ring $R := \mathbb{Z}_n[x]/(x^r - 1)$. Declare n prime iff for each a, $1 \leq a \leq \lceil 2\sqrt{r}\log n \rceil$, $(x+a)^n = (x^n + a)$. This test, colloquially called the AKS test, was proposed in 2002. It is the only known unconditionally efficient deterministic primality test. It was speeded up by Lenstra-Pomerance (2003) to run in time $O^{\sim}(\log^6 n)$.

3 Questions

Can we reduce the number of a's for which the AKS test is performed? We end the talk with the following conjecture followed by some evidence (refer [1, 2]).

Conjecture. *[Bhattacharjee-Pandey 2001; AKS 2004)] Let $r > \log n$ be a prime number that does not divide $(n^3 - n)$. Then $(x-1)^n \equiv (x^n - 1)$ (mod $n, x^r - 1$) iff n is prime.*

Evidence:

1. Even for $r = 5$ the above conjecture holds for all $n \leq 10^{11}$.
2. The above conjecture holds for all primes $r \leq 100$ and $n \leq 10^{10}$.
3. It can be proved that an odd r passing the above congruence satisfies:

$$r^{\frac{n-1}{2}} = \left(\frac{r}{n}\right) \pmod{n}$$

References

[1] M. Agrawal, N. Kayal, and N. Saxena. *Primes is in P.* Annals of Mathematics, 160(2):781–793, 2004.

[2] N. Kayal, and N. Saxena. *Towards a deterministic polynomial-time test.* Technical report, IIT Kanpur, 2002. Available at http://www.cse.iitk.ac.in/research/btp2002/primality.html.

[3] R. Crandall, and C. Pomerance. *Prime Numbers: A Computational Perspective.* New York: Springer-Verlag, 2002.

Finding maximal torsion cosets on varieties

Iskander Aliev *Chris Smyth*

School of Mathematics and Maxwell Institute for Mathematical Sciences
University of Edinburgh
James Clerk Maxwell Building
King's Buildings
Mayfield Road
Edinburgh EH9 3JZ
UK

Abstract

We describe a new algorithm for finding all maximal torsion cosets on varieties of $\mathbb{G}_{\mathrm{m}}^n$. We illustrate the algorithm with some examples.

The starting point for this study is the search for points on a given variety whose coordinates are roots of unity. Sometimes these points are isolated, but often they are part of larger families of such points, called torsion cosets. (These are in fact elements of finite order in some quotient group of $\mathbb{G}_{\mathrm{m}}^n$.) Of greatest interest are maximal torsion cosets, not contained in any larger ones. The number of maximal torsion cosets on a variety is known to be finite, and it of interest to find upper bounds for the number of these, in terms of the dimension and the total degree of the variety. We summarise what is known about such bounds.

1 Introduction

Here we are concerned with finding *cyclotomic points* on a given variety, that is, points whose coordinates are roots of unity. One place where finding cyclotomic points on varieties arose was in [18], where the problem was to factorize polynomials

$$R_{d,m}(z) = z^{2d}(z^2 - z - 1) + z^{2(d-m)} + z^{2(m+1)} - z^2 - z + 1.$$

These can readily be shown to have at most one zero in $|z| > 1$, so, for a fixed d, m, all irreducible factors of $R_{d,m}(z)$, except perhaps one, are cyclotomic polynomials. Putting $x = z^{2d}$, $y = z^{2m}$, this leads to the problem of seeking cyclotomic points on the surface

$$x(z^2 - z - 1) + xy^{-1} + yz^2 - z^2 - z + 1 = 0. \tag{1.1}$$

For a given variety $\mathcal{V}$, we denote by n its number of variables, by d its total degree, and by h the number of hypersurfaces whose intersection defines $\mathcal{V}$.

A fundamental result needed, as in Beukers and Smyth [2], is the following.

Lemma 1 ([2, Lemma 1])**.** *(i) If $g(x) \in \mathbb{C}[x], g(0) \neq 0$, is a polynomial with the property that for every zero α of g, at least one of $\pm\alpha^2$ is also a zero, then all zeroes of g are roots of unity.*

(ii) If ω is a root of unity, then it is conjugate to exactly one of $-\omega, \omega^2$ and $-\omega^2$.

Conversely, if $\alpha \neq 0$ and either α^2 or $-\alpha^2$ is conjugate to α, then α is a root of unity.

The value of this lemma for our purposes lies in the fact that, for a variety $\mathcal{V}(H)$ defined by a set H of hypersurfaces, the lemma enables us to enlarge H to obtain a collection of (in general smaller) varieties $\mathcal{V}(H')$ with the property that the cyclotomic points on $\cup\mathcal{V}(H')$ are the same as those on $\mathcal{V}(H)$. In particular, for hypersurfaces we have the following.

Lemma 2 ([1, Theorem 1.3])**.** *Let $f \in \mathbb{C}[X_1, \ldots, X_n]$ be an irreducible polynomial with $L(f) = \mathbb{Z}^n$. Then there exist $m \leq 2^{n+1} - 1$ polynomials $f_1, f_2, \ldots, f_m$ with the following properties:*

(i) $\deg(f_i) \leq 2\deg(f)$ *for* $i = 1, \ldots, m$*;*

(ii) *For $1 \leq i \leq m$ the polynomials f and f_i have no common factor;*

(iii) *For any torsion coset C lying on the hypersurface $f = 0$ there exists some $1 \leq i \leq m$ such that the coset C also lies on the hypersurface $f_i = 0$.*

When f is in fact defined over $\mathbb{Q}$, the polynomials f_i are a subset of $f(\pm x_1, \ldots, \pm x_n)$ (not all + signs) and $f(\pm x_1^2, \ldots, \pm x_n^2)$. We also need the following simple lemma.

Lemma 3. *Suppose that L is a full (i.e. n-dimensional) sublattice of $\mathbb{Z}^n$, with determinant $D > 1$. Then there is a basis of L, and a factor $m > 1$ of D with the property that one of the basis vectors has all its components divisible by m.*

Proof. Consider an $n \times n$ matrix whose rows are a basis of L. Now put this matrix in Hermite Normal Form ([4, Section 2.4.2]), so that the rows of this new matrix are again a basis for L. Then it is upper triangular with diagonal elements $d_1, \ldots, d_n$ say, with all elements in a column being nonnegative and strictly less than the diagonal element in that column. Since $\prod_i d_i = D$, not all the d_i are 1. Let i' be the largest index i such that $d_i > 1$. Then $d_{i'} > 1$ is the only nonzero entry in row i' of the matrix. □

1.1 Definitions and earlier results.

Let $\mathbb{G}_{\mathrm{m}}$ denote the multiplicative group of $\mathbb{C}$, as a variety, and let $\mathbb{G}_{\mathrm{m}}^n = (\mathbb{G}_{\mathrm{m}})^n$ be the direct product consisting of n-tuples $\boldsymbol{x} = (x_1, \ldots, x_n)$ with $x_i \in \mathbb{G}_{\mathrm{m}}$. By a *subtorus* H of $\mathbb{G}_{\mathrm{m}}^n$ we mean an irreducible algebraic subgroup. By *torsion coset* we will understand a coset $\boldsymbol{u}H$, where H is a subtorus of $\mathbb{G}_{\mathrm{m}}^n$ and $\boldsymbol{u} = (u_1, \ldots, u_n)$ is a *torsion point*, that is all u_i are roots of unity. Let V be an algebraic subvariety of $\mathbb{G}_{\mathrm{m}}^n$. A torsion coset $\boldsymbol{u}H \subset V$ will be called *maximal* in V if there is no torsion coset $\boldsymbol{u}H'$ with $\boldsymbol{u}H \subsetneqq \boldsymbol{u}H' \subset V$. By the *dimension* of a torsion coset $\boldsymbol{u}H$ we understand the dimension of the torus H. A maximal 0–dimensional torsion coset will be also called *isolated* torsion point. Let $V^{\cup}(H)$ be the union of all maximal cosets $\boldsymbol{u}H$ contained in V and let

$$V^{\cup} = \bigcup_H V^{\cup}(H)\,,$$

where the union being over all subtori H of $\mathbb{G}_{\mathrm{m}}^n$.

Lang [8] conjectured that if V is a subvariety of $\mathbb{G}_{\mathrm{m}}^n$ defined over $\overline{\mathbb{Q}}$ then $V^{\cup}$ is the union of a finite number of torsion cosets. This conjecture was proved by Ihara, Serre and Tate (see §8.6 of Lang [8]) when $\dim V = 1$, and by Laurent [9] if $\dim V > 1$. Different proofs of this result were also given by Sarnak and Adams [15]. In Zhang [19] and in Bombieri and Zannier [3] it has been shown that $V^{\cup}$ is the union of at most $c(d, n, [K : \mathbb{Q}], M)$ torsion cosets when the defining polynomials of V had coefficients in a number field K and had degrees $\leq d$ and heights $\leq M$. Furthermore, in [17] Schmidt has given a bound of this kind.

Let $\mathcal{T}(V)$ denote the number of maximal torsion cosets lying on the subvariety V and let

$$\mathcal{T}(n, d) = \max_{V} \mathcal{T}(V)\,,$$

where the maximum is being over all subvarieties $V \subset \mathbb{G}_{\mathrm{m}}^n$ defined by the polynomial equations of degree at most d. Schmidt [17] has shown that

$$\mathcal{T}(n, d) \leq (11d)^{n^2} \exp\left(4\binom{n+d}{d}!\right)\,. \tag{1.2}$$

The proof of this bound is based on a result of Schlickewei [16] about the number of nondegenerate solutions of a linear equation in roots of unity. The latter result was significantly improved by Evertse [6]. Because of his result, the bound (1.2) can be replaced then by

$$\mathcal{T}(n, d) \leq (11d)^{n^2} \binom{n+d}{d}^{3\binom{n+d}{d}^2}\,. \tag{1.3}$$

Although the estimate (1.3) is much better than (1.2), it is still of exponential growth in d. Recently, such bounds that are polynomial in d have been obtained for varieties defined over $\mathbb{Q}$ by de Piro [14], using methods and results from model theory. Earlier, David and Philippon proved a result [13, Proposition 5.6] from which such a bound can follows, for varieties defined over $\overline{\mathbb{Q}}$. We have also obtained such a bound in [1], improving on these bounds. The main result of [1] asserts that, for any fixed dimension n, the number of maximal torsion cosets on subvarieties of $\mathbb{G}_{\mathrm{m}}^n$ is polynomially bounded in d. First, our bound for maximal torsion cosets on hypersurfaces.

Theorem 1 ([1])**.** *Let $f \in \mathbb{C}[X_1, \ldots, X_n]$, $n \geq 2$, be a polynomial of total degree d, and let $\mathcal{H} = \mathcal{H}(f)$ be the hypersurface in $\mathbb{G}_{\mathrm{m}}^n$ defined by f. Then*

$$N_{tor}(\mathcal{H}) \leq c_1(n)\, d^{\,c_2(n)}\,, \tag{1.4}$$

where $c_1(n)$ and $c_2(n)$ are effectively computable constants. Indeed we can take

$$c_1(n) = n^{1.5(2+n)5^n} \quad \textit{and} \quad c_2(n) = \frac{1}{16}(49 \cdot 5^{n-2} - 4n - 9)..$$

1.2 Examples

The following family of examples shows that the upper bound on the number of maximal torsion cosets on a hypersurface cannot be too small. In particular, a general bound must be exponential in the dimension n.

Define the following hypersurfaces $\mathcal{H}_k : f_k(x_1, \ldots, x_n) = 0$ in $\mathbb{G}_{\mathrm{m}}^n$:

- In general for $k = 1, 2, \ldots, n$ f_k is the kth elementary symmetric function of the n terms $(x_1^d - 1), \ldots, (x_n^d - 1)$. In general the hypersurface $\mathcal{H}_k$ has degree kd and $\binom{n}{k-1} d^{n-(k-1)}$ $(k-1)$-dimensional maximal torsion cosets obtained by choosing $n-(k-1)$ of $x_1, \ldots, x_n$ to be dth roots of unity.

  In particular

- $f_1(x_1, \ldots, x_n) = (x_1^d - 1) + \cdots + (x_n^d - 1)$.

  The hypersurface $\mathcal{H}_1$ has degree d and d^n isolated torsion points. They are its only torsion cosets.

- $f_2(x_1, \ldots, x_n) = \sum_{i<j} (x_i^d - 1)(x_j^d - 1)$.

  The hypersurface $\mathcal{H}_2$ has degree $2d$ and $\binom{n}{1} d^{n-1}$ 1-dimensional torsion cosets obtained by choosing $n-1$ of $x_1, \ldots, x_n$ to be dth roots of unity. They are its only maximal torsion cosets.

- $f_{n-1}(x_1, \ldots, x_n) = \sum_{i=1}^n \prod_{j \neq i} (x_j^d - 1)$.

  The hypersurface $\mathcal{H}_{n-1}$ has degree $(n-1)d$ and $\binom{n}{n-2} d^2$ $(n-2)$-dimensional maximal torsion cosets obtained by choosing two of $x_1, \ldots, x_n$ to be dth roots of unity.

1.3 General varieties

Concerning general varieties, we obtained the following result.

Theorem 2 ([1]). *There are effective constants $c_3(n)$ and $c_4(n)$ such that*

$$\mathcal{T}(n, d) \leq c_1(n)\, d^{\, c_2(n)}\,. \tag{1.5}$$

Indeed we can take

$$c_3(n) = n^{n+2) 2^{n-2} \sum_{i=2}^{n-1} c_2(i)} \prod_{i=2}^{n} c_1(i) \quad \textit{and} \quad c_4(n) = \sum_{i=2}^{n} c_2(i) 2^{n-i} + 2^{n-1}\,.$$

2 The algorithm

To motivate our algorithm, we first study a specific example.

2.1 Example: Maximal torsion cosets on a surface.

Consider the surface $f(x, y, z) = 0$, where

$$f(x, y, z) := (z + 1 + y)x - z - 1 - zy^{-1}. \tag{2.6}$$

Let $\alpha := e^{2\pi i/30}$ and $\omega := e^{2\pi i/3}$. Then the maximal torsion cosets on this surface are the 1-dimensional cosets

$$\{(1, t, t^2), (-1/t^2, t, -1), (t, 1/t^2, 1/t), (t, -1, 1/t), (t, -t, t), (t, 1/t, t), (t, \omega, \omega^2), (t, \omega^2, \omega),$$
$$(-\omega, \omega, t), (-\omega^2, \omega^2, t), (t, -\omega^2/t, \omega), (t, -\omega/t, \omega^2), (-\omega^2, t, \omega t), (-\omega, t, \omega^2 t)\},$$

where t is a free parameter, and the isolated points

$\{(\alpha^8,\alpha^6,\alpha^{17}),(\alpha^{22},\alpha^{24},\alpha^{13}),\ (\alpha^{14},\alpha^{13},\alpha^{19}),(\alpha^{26},\alpha^6,\alpha^{29}),\ (\alpha^3,\alpha^{29},\alpha^6),(\alpha^{28},\alpha^{11},\alpha^{23}),$
$(\alpha^{22},\alpha^{29},\alpha^{17}),(\alpha^9,\alpha^{17},\alpha^{18}),\ (\alpha^{22},\alpha^{11},\alpha^{17}),(\alpha^4,\alpha^{24},\alpha^1),\ (\alpha^2,\alpha^{12},\alpha^{23}),(\alpha^9,\alpha^7,\alpha^{18}),$
$(\alpha^{16},\alpha^6,\alpha^{19}),(\alpha^{22},\alpha^{12},\alpha^{13}),\ (\alpha^{21},\alpha^{13},\alpha^{12}),(\alpha^{14},\alpha^{18},\alpha^{11}),\ (\alpha^{16},\alpha^{12},\alpha^{19}),(\alpha^2,\alpha^{24},\alpha^{23}),$
$(\alpha^{21},\alpha^1,\alpha^{18}),(\alpha^{16},\alpha^{23},\alpha^{11}),\ (\alpha^{27},\alpha^1,\alpha^{24}),(\alpha^{27},\alpha^{11},\alpha^{24}),\ (\alpha^3,\alpha^{19},\alpha^6),(\alpha^{26},\alpha^{12},\alpha^{29}),$
$(\alpha^{27},\alpha^7,\alpha^6),(\alpha^2,\alpha^{19},\alpha^7),\ (\alpha^{28},\alpha^{18},\alpha^7),(\alpha^3,\alpha^{13},\alpha^{24}),\ (\alpha^{21},\alpha^{23},\alpha^{12}),(\alpha^8,\alpha^{18},\alpha^{17}),$
$(\alpha^4,\alpha^{23},\alpha^{29}),(\alpha^9,\alpha^{29},\alpha^{12}),\ (\alpha^8,\alpha^{19},\alpha^{13}),(\alpha^4,\alpha^{17},\alpha^{29}),\ (\alpha^{21},\alpha^{11},\alpha^{18}),(\alpha^4,\alpha^{18},\alpha^1),$
$(\alpha^{26},\alpha^{13},\alpha^1),(\alpha^2,\alpha^1,\alpha^7),\ (\alpha^3,\alpha^{23},\alpha^{24}),(\alpha^8,\alpha^1,\alpha^{13}),\ (\alpha^{28},\alpha^6,\alpha^7),(\alpha^9,\alpha^{19},\alpha^{12}),$
$(\alpha^{27},\alpha^{17},\alpha^6),(\alpha^{28},\alpha^{29},\alpha^{23}),\ (\alpha^{14},\alpha^7,\alpha^{19}),(\alpha^{16},\alpha^{17},\alpha^{11}),\ (\alpha^{14},\alpha^{24},\alpha^{11}),(\alpha^{26},\alpha^7,\alpha^1)\}.$

How are these found? Well, generalising from the case of curves, we compute the resultant of $f(x,y,z)$ with each of the 7 polynomials $f(\pm x,\pm y,\pm z)\neq f(x,y,z)$ and the 8 polynomials $f(\pm x^2,\pm y^2,\pm z^2)$. By Lemma 1, all cyclotomic points of f also lie on at least one of these 15 surfaces. We then take further resultants, on the same principle, as necessary.

Techniques such as this led us to formalise the process for finding all torsion cosets on a subvariety of $\mathbb{G}_{\rm m}^n$ as an algorithm. We now give this algorithm . A different algorithm for this purpose was given in [1]. We denote by n the number of variables of the polynomials describing our variety. Of course this is an upper bound for its dimension. We also denote by $V_n(f_1,\ldots,f_h)$ the union of all maximal torsion cosets on the variety defined by the h polynomials $f_1,\ldots,f_h$ in $\mathbb{Z}[x_1,\ldots,x_n]$.

The algorithm is recursive. We can clearly assume that all hypersurfaces considered are irreducible. For instance, if $f=\prod_\ell g_\ell^{k_\ell}$, then $V_n(f)=\cup_\ell V_n(g_\ell)$. Further, where more than one hypersurface is considered, we can assume that they are distinct, that is, their defining polynomials are not simply rational multiples of one another. In the algorithm, the notation x^A for $x=(x_i)\in\mathbb{G}_m^n$ and $A=(a_{ij})\in\mathbb{Z}^{n\times r}$ denotes $(\prod_i {x_i}^{a_{i1}},\ldots,\prod_i {x_i}^{a_{ir}})\in\mathbb{G}_{\rm m}^r$.

We start with hypersurfaces, computing $V_n(g)$. We then proceed to the 2-hypersurface case, followed by the general case.

1. **One hypersurface.**

   (a) $n=1$. Use the 1-variable algorithm in [2]. Alternatively, write $g(x)=g_1(x^r)$ with r maximal, and put $g_2(x)=\gcd(g_1(y),g_1(y^2),g_1(-y^2))$. Then $V_1(g_1)$ is the set of roots of g_2 and so $V_1(g)$ is the set of k-th roots of these roots.

   (b) $n\geq 2$.

      (b1) If g r-dimensional with $r<n$, say $x^A=t$, where A is $n\times r$ and, for some c, $x^c g(x)=g_1(t)$, where $t=(t_1,\ldots,t_r)$ and g_1 is again irreducible. Then maximal torsion cosets of g_1 readily give maximal torsion cosets of g.

      (b2) If g is n-dimensional and $D>1$ is the determinant of its lattice, then for some factor $m>1$ of D we can, by Lemma 3, find $B\in\mathbb{Z}^{n\times n}$ of determinant D/m such that if $y=x^B$ then and $c\in\mathbb{Z}^n$ we have $x^c g(x)=g_2(y_1^m,y_2,\ldots,y_n)$. Then maximal torsion cosets of g_2 readily give maximal torsion cosets of g.

      (b3) If g is n-dimensional and $D=1$ is the determinant of its lattice (so its lattice is $\mathbb{Z}^n$), then from Lemma 2 there are polynomials f_i with $\gcd(g,f_i)=1$ such that $V_n(g)=\cup_i V_n(g,f_i)$.

2. **Two hypersurfaces.** $V_n(g, f)$, where $g(x_1, \ldots, x_n)$ is irreducible and n-dimensional, and $f(x_1, \ldots, x_n)$ is at most n-dimensional.

   (a) If f is r-dimensional, where $r < n$, find $V_n(f)$ and then, for each maximal torsion coset in $V_n(f)$, write each variable x_i as a monomial in $t_1, \ldots, t_s$, where $s \leq r - 1 \leq n - 2$. Thus the dimension of the problem is reduced.

   (b) If f is n-dimensional, then $V_n(g, f) = V_n(g, f, s)$, where $s = \mathrm{Res}_{x_1}(g, f)$. We then proceed as in (a) to reduce the number of variables.

3. **General case.** To compute $V_n(f_1, \ldots, f_h)$, find $V_n(f_1)$ (say). Then proceed as in part 2(a).

It is not difficult to prove that this algorithm is recursive. Indeed, consider the ordered pair (r, D), where r is the smallest dimension of any hypersurface defining the variety, and D is the determinant of its lattice. Ordering such pairs lexicographically, we see that, essentially, each step of the algorithm produces only smaller (in this ordering) such associated pairs. Here, we say 'essentially' because in step 1(b3) it is necessary to merge this step with 2(b) (i.e. replace $V_n(g, f_i)$ with $V_n(g, f_i, r)$) so that the dimension is reduced.

2.2 Example: Maximal torsion cosets on the surface (1.1)

Consider the surface $p(x, y, z) = 0$, where

$$p(x, y, z) := x(z^2 - z - 1) + x/y + yz^2 - z^2 - z + 1. \tag{2.7}$$

is the polynomial defining the surface (1.1). Let $\alpha := e^{2\pi i/30}$ as before, and put $\beta := e^{2\pi i/24}$, $\gamma := e^{2\pi i/18}$, $\delta := e^{2\pi i/12}$. Then the 1-torsion cosets on this surface are

$$\{(t, 1, 1), (t, -1, -1), (t, -t, -t), (t, t^3, t^{-1}), (t, t, 1),$$
$$(t, -t, -1), (t, -t^{-2}, -t), (t, 1, t^{-1}), (1, t, t^{-1})\},$$

where t is a free parameter. This time, the 68 isolated points are given by the representatives of their Galois orbits:

$$\{(\alpha^2, \alpha, \alpha^{26}), (\alpha^2, \alpha^9, \alpha^{26}), (\alpha^8, \alpha^2, \alpha), (\alpha^8, \alpha^4, \alpha), (\beta^{18}, \beta, \beta^2), (\gamma, \gamma^2, \gamma^{14}),$$
$$(\gamma, \gamma^3, \gamma^{13}), (\gamma, \gamma^7, \gamma^{14}), (\gamma, \gamma^8, \gamma^{13}), (-1, \delta^2, \delta)\},$$

the orbits being of sizes $8, 8, 8, 8, 8, 6, 6, 6, 6, 4$, respectively. The determination of these maximal torsion cosets enables a complete factorization of the polynomials $R_{d,m}(z)$ to be made. The details are given in [18], albeit by a somewhat more *ad hoc* version of this method. [**?**, 7, 10, 11, 12]

References

[1] I. Aliev and C. Smyth. Torsion points on subvarieties of $\mathfrak{O}_{\mathrm{m}}^n$. submitted.

[2] F. Beukers and C. J. Smyth. Cyclotomic points on curves. In *Number theory for the millennium, I (Urbana, IL, 2000)*, pages 67–85. A K Peters, Natick, MA, 2002.

[3] E. Bombieri and U. Zannier. Algebraic points on subvarieties of $\mathbf{G}_m^n$. *Internat. Math. Res. Notices*, (7):333–347, 1995.

[4] H. Cohen. *A course in computational algebraic number theory*, volume 138 of *Graduate Texts in Mathematics*. Springer-Verlag, Berlin, 1993.

[5] S. David and P. Philippon. Minorations des hauteurs normalisées des sous-variétés des tores. *Ann. Scuola Norm. Sup. Pisa Cl. Sci. (4)*, 28(3):489–543, 1999.

[6] J.-H. Evertse. The number of solutions of linear equations in roots of unity. *Acta Arith.*, 89(1):45–51, 1999.

[7] S. Lang. Division points on curves. *Ann. Mat. Pura Appl. (4)*, 70:229–234, 1965.

[8] ———— *Fundamentals of Diophantine geometry*. Springer-Verlag, New York, 1983.

[9] M. Laurent. Équations diophantiennes exponentielles. *Invent. Math.*, 78(2):299–327, 1984.

[10] P. Liardet. Sur une conjecture de Serge Lang. In *Journées Arithmétiques de Bordeaux (Conf., Univ. Bordeaux, Bordeaux, 1974)*, pages 187–210. Astérisque, Nos. 24–25. Soc. Math. France, Paris, 1975.

[11] J. McKee and C. Smyth. There are Salem numbers of every trace. *Bull. London Math. Soc.*, 37(1):25–36, 2005.

[12] M. McQuillan. Division points on semi-abelian varieties. *Invent. Math.*, 120(1):143–159, 1995.

[13] S. David, P. Philippon. Minorations des hauteurs normalisées des sous-variétés des tores. *Ann. Scuola Norm. Sup. Pisa Cl. Sci.* (4) 28, 489–543, 1999.

[14] T. de Piro. Bounding the number of maximal torsion cosets on algebraic varieties. Preprint.

[15] P. Sarnak and S. Adams. Betti numbers of congruence groups. *Israel J. Math.*, 88(1-3):31–72, 1994. With an appendix by Ze'ev Rudnick.

[16] H. P. Schlickewei. Equations in roots of unity. *Acta Arith.*, 76(2):99–108, 1996.

[17] W. M. Schmidt. Heights of points on subvarieties of $\mathbf{G}_m^n$. In *Number theory (Paris, 1993–1994)*, volume 235 of *London Math. Soc. Lecture Note Ser.*, pages 157–187. Cambridge Univ. Press, Cambridge, 1996.

[18] C. J. Smyth. Salem numbers of negative trace. *Math. Comp.*, 69(230):827–838, 2000.

[19] S. Zhang. Positive line bundles on arithmetic varieties. *J. Amer. Math. Soc.*, 8(1):187–221, 1995.

Elliptic Nets and Points on Elliptic Curves

Katherine E. Stange

Elliptic divisibility sequences were first studied by Morgan Ward in 1948 [11]. These are integer sequences $h_0, h_1, \ldots, h_n, \ldots$ satisfying the following two properties:

1. For all positive integers $m > n$,
$$h_{m+n}h_{m-n} = h_{m+1}h_{m-1}h_n^2 - h_{n+1}h_{n-1}h_m^2 \ . \tag{0.1}$$
2. h_n divides h_m whenever n divides m.

They have attracted number theoretical and combinatorial interest as some of the simplest non-linear recurrence sequences (see [3] for references), but for us their interest lives in the underlying geometry: Ward demonstrates that an elliptic divisibility sequence arises from any choice of elliptic curve over $\mathbb{Q}$ and rational point on that curve.

Theorem 26 (M. Ward, 1948, [11])**.** *Suppose E is an elliptic curve defined over $\mathbb{Q}$, $\sigma : \mathbb{C} \to \mathbb{C}$ is its Weierstrass sigma function, and $u \in \mathbb{C}$ corresponds to a rational point on E. Then there exists an integer k such that the sequence*
$$h_n := k^{n^2-1}\frac{\sigma(nu)}{\sigma(u)^{n^2}}$$
forms an elliptic divisibility sequence.

The recurrence sequence reflects the behaviour of a point under multiplication; it provides access to information about $[n]P$ via a recurrence relation instead of direct curve computations. Indeed, Rachel Shipsey used this idea to solve the elliptic curve discrete logarithm problem in certain situations [6], while Mohamad Ayad used it to develop methods of finding integer points on elliptic curves of rank one [1]. To fully exploit this paradigm, then, it is desirable to extend to additions in general. Is there a multidimensional version of the sequences "reflecting" all the possible linear combinations
$$[n_1]P_1 + \ldots + [n_k]P_k \ ?$$

To accomplish this, in place of sequences we will define *elliptic nets*.

Definition 27. *Let A be a finitely generated free abelian group, and R be an integral domain. An* elliptic net *is any map $W : A \to R$ such that the following recurrence holds for all p, q, r, $s \in A$.*

$$\begin{aligned} W(p+q+s)W(p-q)W(r+s)W(r) \\ + W(q+r+s)W(q-r)W(p+s)W(p) \\ + W(r+p+s)W(r-p)W(q+s)W(q) = 0 \end{aligned} \tag{0.2}$$

We say W is normalised *if $A = \mathbb{Z}^n$ and $W(\mathbf{z}) = 1$ whenever $\mathbf{z} = \mathbf{e}_i$ or $\mathbf{z} = \mathbf{e}_i + \mathbf{e}_j$ with $i \neq j$ (where $\mathbf{e}_i$ are the standard basis vectors).*

Elliptic nets have the symmetry property that $W(-z) = -W(z)$ for any $z \in A$ (and in particular $W(0) = 0$). When $A = R = \mathbb{Z}$ and $W(1) = 1$, the positive terms of an elliptic net satisfy Ward's equation (0.1) above. Under the further condition that $W(2)|W(4)$, these terms form an elliptic divisibility sequence.

Christine Swart studied a general class of Somos-4 sequences arising from elliptic curves and including elliptic divisibility sequences [9]. Her work, and related work of van der Poorten [10], provided the clues that the more general theory of nets existed. It has recently come to my attention that the possibility of such a definition was briefly discussed in correspondence by Noam Elkies, James Propp and Michael Somos in 2001 [5].

To extend Ward's Theorem 26 to the elliptic net case (with $R = \mathbb{C}$), we define appropriate multi-elliptic functions and show that they satisfy the recurrence (0.2).

Definition 28. *Fix a lattice $\Lambda \in \mathbb{C}$ corresponding to an elliptic curve E. For $\mathbf{v} = (v_1, \ldots, v_n) \in \mathbb{Z}^n$, define a function $\Psi_{\mathbf{v}}$ on $\mathbb{C}^n$ in variables $\mathbf{z} = (z_1, \ldots, z_n)$ as follows:*

$$\Psi_{\mathbf{v}}(\mathbf{z}; \Lambda) = \frac{\sigma(v_1 z_1 + \ldots + v_n z_n; \Lambda)}{\prod_{i=1}^{n} \sigma(z_i; \Lambda)^{2v_i^2 - \sum_{j=1}^{n} v_i v_j} \prod_{1 \le k < j \le n} \sigma(z_i + z_j; \Lambda)^{v_i v_j}}$$

In particular, we have for each $k \in \mathbb{Z}$, a function Ψ_k on $\mathbb{C}$ in the variable z:

$$\Psi_k(z; \Lambda) = \frac{\sigma(kz; \Lambda)}{\sigma(z; \Lambda)^{k^2}}$$

and for each pair $(k, l) \in \mathbb{Z} \times \mathbb{Z}$, a function $\Psi_{k,l}$ on $\mathbb{C} \times \mathbb{C}$ in variables z and w:

$$\Psi_{k,l}(z, w; \Lambda) = \frac{\sigma(kz + lw; \Lambda)}{\sigma(z; \Lambda)^{k^2 - kl} \sigma(z + w; \Lambda)^{kl} \sigma(w; \Lambda)^{l^2 - kl}}$$

These functions are elliptic in each variable.

We will now see that the $\Psi_{\mathbf{v}}$ form an elliptic net as a function of $\mathbf{v} \in \mathbb{Z}^n$ when $\mathbf{z} \in \mathbb{C}^n$ and the lattice Λ are fixed. Denote by $\pi : \mathbb{C} \to \mathbb{C}/\Lambda$ the complex uniformisation of an elliptic curve. Then for any number field $L \subset \mathbb{C}$, define the free abelian group $\hat{E}_L = \pi^{-1}(E(L))$. As a means of fixing $\mathbf{z}$, we specify a homomorphism $\phi : \mathbb{Z}^n \to \hat{E}_L$.

Definition 29. *Suppose $\phi : \mathbb{Z}^n \to \hat{E}_L$ is a homomorphism such that the images of $\pm\mathbf{e}_i$ under $\pi \circ \phi$ are all distinct. Define $W_\phi : \mathbb{Z}^n \to \mathbb{C}$ by*

$$W_\phi(\mathbf{v}) = \Psi_{\mathbf{v}}(\phi(\mathbf{e}_1), \phi(\mathbf{e}_2), \ldots, \phi(\mathbf{e}_n); \Lambda)$$

Theorem 30. *$W_\phi : \mathbb{Z}^n \to L$ is an elliptic net.*

In this way, we can associate an elliptic net to any choice of n points $P_i \in E(L)$ which, along with their negatives, are all distinct. We call W_ϕ the *elliptic net associated to* $E, P_1, \ldots, P_n$. A portion of such an example net is shown in Figure 0.1.

It can be shown that all normalised elliptic nets with $R = \mathbb{C}$ arise in this manner. In fact, the curve and points concerned can be calculated explicitly.

To extend to curves defined over other fields, it is necessary to remove the dependence on the complex analytic definition. The functions $\Psi_{\mathbf{v}}$ may be written as rational functions in the coordinates $x_i = \wp(P_i), y_i = \wp'(P_i)$. In the case of elliptic divisibility sequences, these are exactly the so-called division polynomials. In the more general case, we have the following theorem:

	4335	5959	12016	-55287	23921	1587077	-7159461
	94	479	919	-2591	13751	68428	424345
	-31	53	-33	-350	493	6627	48191
	-5	8	-19	-41	-151	989	-1466
	1	3	-1	-13	-36	181	-1535
	1	1	2	-5	7	89	-149
$\uparrow Q$	0	1	1	-3	11	38	249
	$P \rightarrow$						

over $\mathbb{Q}$

	0	4	4	3	1	2	4
	4	4	4	4	1	3	0
	4	3	2	0	3	2	1
	0	3	1	4	4	4	4
	1	3	4	2	4	1	0
	1	1	2	0	2	4	1
$\uparrow Q$	0	1	1	2	1	3	4
	$P \rightarrow$						

over $\mathbb{F}_5$

Figure 0.1: A portion of the elliptic net of $E : y^2 + y = x^3 + x^2 - 2x$, $P = (0, 0)$, $Q = (1, 0)$.

Theorem 31. *Let $n \geq 1$. Consider an elliptic curve $E : y^2 = x^3 + Ax + B$ over $\mathbb{C}$. Let $p_i : E^n \to E$ be projection maps and $s : E^n \to E$ the summation. Let*

$$U = E^n \backslash \left(\bigcup_{k=1}^{n} p_k^*(\mathcal{O}) \bigcup_{1 \leq k < j \leq n} (p_k^* \times p_j^*) s^*(\mathcal{O}) \right) .$$

The $\Psi_{\mathbf{v}}$ associated to E are regular on U and are in the subring

$$\mathbb{Z}[A, B][x_i, y_i]_{i=1}^n \left[(x_i - x_j)^{-1} \right]_{1 \leq i < j \leq n} \Big/ \left\langle y_i^2 - x_i^3 - Ax_i - B \right\rangle_{i=1}^n \subset \mathcal{O}_{E^n}(U) .$$

The geometric content of the theorem is that there are functions defined on $U_{\mathbb{Z}}$ whose restrictions to U are the $\Psi_{\mathbf{v}}$.

In particular, we may define elliptic nets over finite fields. It remains to examine the relationship between the elliptic net of a curve over a number field and its reduction modulo a prime.

Let E be an elliptic curve over a number field $L \subset \mathbb{C}$ with ring of integers R. Let $\mathfrak{p}$ be a prime of good reduction for an elliptic curve E and let δ denote both the reduction modulo $\mathfrak{p}$ on the curve E and on the ring of integers R.

Theorem 32. *Consider points $P_1, \ldots, P_n \in E(L)$ such that the reductions modulo $\mathfrak{p}$ of the $\pm P_i$ are all distinct and nonzero. Then for each $\mathbf{v} \in \mathbb{Z}$ there exists a function $\Omega_{\mathbf{v}}$ such that the following diagram commutes:*

$$\begin{array}{ccc} E_L^n(R) & \xrightarrow{\Psi_{\mathbf{v}}} & \mathbb{P}^1(L) \\ \Big\downarrow{\scriptstyle \delta} & & \Big\downarrow{\scriptstyle \delta} \\ E_{k_{\mathfrak{p}}}^n(k_{\mathfrak{p}}) & \xrightarrow{\Omega_{\mathbf{v}}} & \mathbb{P}^1(k_{\mathfrak{p}}) \end{array}$$

Furthermore $\operatorname{div}(\Omega_{\mathbf{v}}) = \delta^* \operatorname{div}(\Psi_{\mathbf{v}})$.

Figure 0.1 illustrates the relationship between an example elliptic net associated to E, P, Q over $\mathbb{Q}$ and the elliptic net associated to their reductions $\tilde{E}, \tilde{P}, \tilde{Q}$ modulo 5. The order of $\tilde{Q}$ in this example is 3, but if we let W be the elliptic divisibility sequence associted to $\tilde{E}, \tilde{Q}$, then $W(4) \not\equiv W(1) \mod \mathfrak{p}$. The exact relationship is given by the "periodicity properties" of elliptic nets. For the case of elliptic divisibility sequences it has a particularly simple statement:

Theorem 33 (M. Ward, 1948, [11]). *Let W is an elliptic divisibility sequence, and $p \geq 3$ a prime not dividing $W(2)W(3)$. Let r be the least positive integer such that $W(r) = 0$. Then there exist integers a, b such that for all n,*

$$W(kr + n) \equiv W(n)a^{nk}b^{k^2} \mod p \ .$$

In the case of elliptic nets in general, the periodicity properties relate to the Tate pairing. Choose $m \in \mathbb{Z}^+$. Let E be an elliptic curve defined over a field K containing the m-th roots of unity. Suppose $P \in E(K)[m]$ and $Q \in E(K)/mE(K)$. Since P is an m-torsion point, $m(P) - m(\mathcal{O})$ is a principal divisor, say $\mathrm{div}(f_P)$. Choose another divisor D_Q defined over K such that $D_Q \sim (Q) - (\mathcal{O})$ and with support disjoint from $\mathrm{div}(f_P)$. Then, we may define the Tate pairing

$$\tau_m : E(K)[m] \times E(K)/mE(K) \to K^*/(K^*)^m$$

by

$$\tau_m(P, Q) = f_P(D_Q)$$

This pairing is well-defined, bilinear and Galois invariant. The well-known Weil pairing e_m satisfies $e_m(P, Q) = \tau_m(P, Q)/\tau_m(Q, P)$. The Tate pairing is commonly used in implementations of pairing-based elliptic curve cryptography. In this case, it is usually considered over finite fields, where it is non-degenerate. For details, see [2, 4].

The following theorem is example of the computation of the Tate pairing using an elliptic net.

Theorem 34. *Let E be an elliptic curve defined over a finite field K, m a positive integer, $P \in E(K)[m]$ and $Q \in E(K)$. If W is the elliptic net associated to E, P, Q, then we have*

$$\tau_m(P, Q) = \frac{W(m + 1, 1)W(1, 0)}{W(m + 1, 0)W(1, 1)}$$

There are methods of computing terms of elliptic nets which allow one to compute this value in $\log(m)$ time. This method may also be used to compute the Weil pairing. For further details and more such theorems see [7] and [8].

Other work in progress includes extending the work of Ayad [1] for finding integer points on curves of higher rank.

References

[1] M. Ayad. Périodicité (mod q) des suites elliptiques et points S-entiers sur les courbes elliptiques. *Ann. Inst. Fourier (Grenoble)*, 43(3):585–618, 1993.

[2] S. Duquesne and G. Frey. Background on pairings. In *Handbook of elliptic and hyperelliptic curve cryptography*, Discrete Math. Appl. (Boca Raton), pages 115–124. Chapman & Hall/CRC, Boca Raton, FL, 2006.

[3] G. Everest, A. v. d. Poorten, I. Shparlinski, and T. Ward. *Elliptic Divisibility Sequences*, pages 163–175. American Mathematical Society, Providence, 2003.

[4] S. Galbraith. Pairings. In *Advances in elliptic curve cryptography*, volume 317 of *London Math. Soc. Lecture Note Ser.*, pages 183–213. Cambridge Univ. Press, Cambridge, 2005.

[5] J. Propp. Robbins forum. `http://www.math.wisc.edu/~propp/about-robbins`.

[6] R. Shipsey. *Elliptic Divibility Sequences*. PhD thesis, Goldsmiths, University of London, 2001.

[7] K. E. Stange. The tate pairing via elliptic nets. To appear in PAIRING 2007.

[8] K. E. Stange. *Elliptic Nets*. PhD thesis, Brown University, in preparation.

[9] C. Swart. *Elliptic curves and related sequences*. PhD thesis, Royal Holloway and Bedford New College, University of London, 2003.

[10] A. J. van der Poorten. Elliptic curves and continued fractions. *J. Integer Seq.*, 8(2):Article 05.2.5, 19 pp. (electronic), 2005.

[11] M. Ward. Memoir on elliptic divisibility sequences. *Amer. J. Math.*, 70:31–74, 1948.

How Fast Can We Multiply Polynomials Over GF(2)? [extended abstract]

Paul Zimmermann

INRIA Nancy-Grand Est/LORIA

We consider here the problem of multiplying two univariate polynomials over GF(2). We assume the given polynomials have degree less than n:

$$a = \sum_{i=0}^{n-1} a_i x^i, \qquad b = \sum_{i=0}^{n-1} b_i x^i,$$

where $a_i, b_i \in \mathrm{GF}(2)$.

On a computer with word length of w bits, such polynomials are usually represented as follows: word 0 contains the coefficients a_0 to a_{w-1}, word 1 the coefficients a_w to a_{2w-1}, and so on. This representation, usually called *binary polynomial*, coincides with the representation of the integer $A = \sum_{i=0}^{n-1} a_i 2^i$. For example, on a 8-bit computer, the polynomial $x^{19} + x^4 + 1$ is stored as follows, with the most significant word on the left:

$$\underbrace{\boxed{00001000}}_{x^3 \cdot x^{16}}\underbrace{\boxed{00000000}}_{0 \cdot x^8}\underbrace{\boxed{00010001}}_{(x^4+1)\cdot x^0}.$$

The addition of binary polynomials is trivial: it suffices to perform an exclusive-or of each pair of bits $a_i \oplus b_i$, or more efficiently $a_{i\ldots i+w-1} \oplus b_{i\ldots i+w-1}$ using the word-level parallelism. The multiplication of binary polynomials is a key operation in several domains, for example in the factorization of polynomials on GF(2), or more generally in cryptographic applications, since arithmetic on $\mathrm{GF}(2^n)$ reduces to computations modulo an irreducible polynomial of degree n of $\mathrm{GF}(2)[x]$.

Several authors have studied efficient hardware multipliers [6, 8, 5]. Other authors also considered alternate representations or Montgomery multiplication [1, 4]. Nevertheless, no current processor implements in hardware multiplication in $\mathrm{GF}(2)[x]$. One could imagine for example an assembly instruction that would multiply two binary polynomials of degree less than 64 on a 64-bit processor, and would return the low and high parts of their product in two 64-bit words. In the lack of this hardware instruction, software implementers have to use some clever algorithms to get efficient code. We summarize in this extended abstract the state-of-art in this domain.

1 The Schoolbook Method

The classical $O(n^2)$ schoolbook algorithm is usually the fastest one up to a few machine words. Since addition of binary polynomials is very efficient — using the "exclusive-or" assembly instruction —, the threshold between the schoolbook method and Karatsuba's algorithm is usually small. For example, NTL [11] uses Karatsuba's algorithm up from two words.

As a consequence, the main issue is how to multiply two binary polynomials of one word each, with a result of two words representing the low and high parts of the product. We call that instruction `mul1`. (Note that on a w-bit computer, the high part of the product only has $w-1$ bits at most, since the product has degree at most $2w-2$.)

The classical way to perform `mul1` is to cut one of the operands — say b — in chunks of k bits each, and to precompute all the multiples of a by the 2^k polynomials of degree less than k. For $k=2$ for example, one first computes $0 \cdot a$, $1 \cdot a$, $x \cdot a$ and $(x+1) \cdot a$. Then for each chunk of k bits in b, a simple lookup yields the corresponding product:

$(l,h) \leftarrow (0,0)$
to $\lceil w/k \rceil$ do
  read the next k bits c from b
  $(l,h) \leftarrow x^k(l,h)$
  $(l,h) \leftarrow (l,h) + T[c]$

In the above algorithm, l and h represent the low and high words of the result, representing the polynomial $l + x^w h$ (we identify machine words and the corresponding binary polynomial); $x^k(l,h)$ means $x^k(l + x^w h)$, which can be efficiently implemented using left shifts, and $(l,h) + T[c]$ means the addition of $l + x^w h$ and the table value $T[c]$.

The precomputation of the $T[]$ table costs 2^k, and the multiplication itself costs $\lceil w/k \rceil$ iterations, thus the total cost is $O(2^k + w/k)$. In practice, the optimal value of k is 4 or 5 on modern processors.

However, one difficulty arises in the above algorithm. Indeed, the table values $T[c]$ may have degree up to $w+k-2$, i.e., need up to $w+k-1$ bits of storage. If $k > 1$, this will not fit in general in one machine word, thus each table entry should consist of two words. Another solution is the following: only store in $T[c]$ the low part of the product $c \cdot a$. The high part can be repaired as follows. Bit j of c, $1 \leq j \leq k$, yields a contribution to the high part of $c \cdot a$ for each set bit in a of weight (degree) $w-j$ or more. Thus it suffices to consider the $k-1$ most significant bits of a — from degree $w-k+1$ to $w-1$—, and for each set bit, to consider the relevant bits of b — this can be done efficiently using a bit mask —, and to add the corresponding value to (l,h), shifted at the right position. This "repair trick" is used by Victor Shoup in the NTL library [11].

Together with Richard Brent, Pierrick Gaudry and Emmanuel Thomé, we found another improvement that reduces the size of the $T[]$ table to about $2^{k/2}$. This will be described elsewhere.

2 Karatsuba and Toom-Cook Algorithms

As said above, Karatsuba's algorithm is quite effective in GF(2)[x], since it trades multiplications — which are particularly expensive in GF(2)[x] — by additions — which are particularly inexpensive in GF(2)[x]. Another advantage over the integer case is that there are no carries here when adding the low- and high-parts of the operands to be multiplied. Karatsuba's algorithm reduces a multiplication of two n-word polynomials to three multiplications of polynomials of about $n/2$ words, more precisely:

$$K(n) = 2K(\lceil n/2 \rceil) + K(\lfloor n/2 \rfloor).$$

Weimerskirch and Paar propose in [13] a Karatsuba-like formula which reduces an n-word product to six $n/3$-word products (against five such products for Toom-Cook 3-way). This was later extended by Montgomery who proposes in [7] alternative Karatsuba-like formulae which work in any characteristic — in particular over GF(2) — since they require no division.

A common misbelief is that Toom-Cook does not work on GF(2), since one could take as evaluation points "only" 0, 1 and ∞. However, one can also take as evaluation "points" polynomials in the transcendental variable x. For example, one can implement Toom-Cook 3-way with 0, 1, x, $1/x$ and ∞ as evaluation points; even better Toom-Cook 3-way formulae were found by Bodrato [2]. Such algorithms require divisions, for example by $1 + x^2$, but those divisions are known to be exact, and can thus be efficiently performed starting from the low significant bits. For example Michel Quercia (personal communication) designed the following C program to divide an array $c[]$ of n words by $1 + x^2$ on a 32-bit computer:

```
for (i = 0, t = 0; i < n; i++) {
  t ^= c[i];
  t ^= t << 2;
  t ^= t << 4;
  t ^= t << 8;
  t ^= t << 16;
  c[i] = t;
  t >>= 30;
}
```

Another interesting remark done by Michel Quercia is the following: instead of taking as evaluation point x and x^{-1} in Toom-Cook 3-way, one could take x^w and x^{-w}, where w is the word bit-size. The advantage is that one replaces bit-shifts by word-shifts, the later being for free. A small drawback is that the size of the recursive products may be larger by one word than in the bit-variant, but computer experiments made by Richard Brent (personal communication) show that the word-variant is generally faster.

Finally, Montgomery remarks in [7] that for an odd number n of words, one can save one word product in Karatsuba's algorithm. Indeed, assume $n = 2m + 1$, and we cut the input polynomials $a(x)$ and $b(x)$ in two parts each, $a_0(x)$ and $a_1(x)$, $b_0(x)$ and $b_1(x)$, with $a_0(x), b_0(x)$ having $m + 1$ words, and $a_1(x), b_1(x)$ having m words. The product $[a_0(x) + a_1(x)][b_0(x) + b_1(x)]$ is a $(m + 1) \times (m + 1)$ word product, but the most significant word of that product was already computed in the product $a_0(x)b_0(x)$, thus we have:

$$K(2m + 1) \leq 2K(m + 1) + K(m) - 1.$$

3 FFT-Based Algorithms

There are at least three ways to use the Fast Fourier Transform to multiply binary polynomials:

- Kronecker-Schönhage trick (also called segmentation), reusing an FFT implementation to multiply integers. The idea is to multiply the *integers* $A = a(2^k)$ and $B = b(2^k)$, which have at most kn bits each. If $n \leq 2^k$ — recall the degree of $a(x)$ and $b(x)$ is bounded by n — then the products $\sum a_i b_{j-i}$ will be in $[0, n-1]$, and can thus be recovered exactly by cutting the integer product

AB into chunks of k consecutive bits, and then reducing modulo 2. One thus needs $k = \Theta(\log n)$. The cost of this algorithm is $O(M(n \log n))$, which is not optimal; however if one already has an efficient FFT integer multiplication, this method is straightforward to implement.

- Cantor's algorithm, also called "additive FFT", which was efficiently implemented by von zur Gathen and Gerhard [12] in the `BiPolAr` software tool. This algorithm has complexity $O(m^2 2^m)$ where m is the smallest integer such that $4n \leq m2^m$.

- Schönhage's special-purpose algorithm for multiplication in GF(2)[x] [9]. This algorithm is based on a ternary FFT, and has cost $O(n \log n \log\log n)$.

We did implement Schönhage's algorithm. To our best knowledge, this is the first published implementation of this algorithm. Our implementation slightly differs from the original description from [9]. Indeed, Schönhage's only focuses on the asymptotic complexity, and did not worry about the implied $O()$ constant. In short, his algorithm reduces one product modulo $x^{2N} + x^N + 1$ to $2K$ products modulo $x^{2L} + x^L + 1$, where K is a power of 3, $L \geq N/K$, and L is a multiple of K. Our variant reduces one product modulo $x^{3N} + 1$ to $3K$ products modulo $x^{2L} + x^L + 1$, with K a power of 3, $L \geq N/K$, and L a multiple of K. (The recursive calls, if any, are the same in both variants.)

In the forward and backward transforms, Schönhage's algorithm performs $O(K \log K)$ additions or shifts — multiplication by some x^ℓ — modulo $x^{2L} + x^L + 1$. While the addition is trivial to implement, the multiplication by x^ℓ modulo $x^{2L} + x^L + 1$ requires some skill to implement efficiently. The pointwise products require $2K$ or $3K$ products modulo $x^{2L} + x^L + 1$; here either the algorithm is used recursively, or a full multiplication is performed, for example using Toom-Cook 3-way or 4-way algorithm [2], following by a reduction modulo $x^{2L} + x^L + 1$.

Schönhage's algorithm is very similar to Schönhage-Strassen's algorithm for multiplying integers [10, 3]. However, one of the main differences is the following. In Schönhage-Strassen's algorithm, one multiplication modulo $2^N + 1$ reduces to K products modulo $2^L + 1$, where K is a power of two dividing L. To make the implementation of arithmetic modulo $2^L + 1$ easier, one usually forces L to be a multiple of the word size w. Since w is usually a power of two — 32 or 64 —, this gives for free the corresponding power of two dividing L. However, in Schönhage's ternary-FFT algorithm, if one forces L to be divisible by w, this gives too much constraint on L, since it must also be divisible by K, which is here a power of 3 and not of 2.[1] We thus had to implement the arithmetic modulo $x^{2L} + x^L + 1$ for a general value of L, not necessarily multiple of the word size w; this made the implementation of the arithmetic modulo $x^{2L} + x^L + 1$ even more tricky.

Here is an example showing how Schönhage's algorithm — in fact our variant — works. Assume we want to compute $a(x)b(x) \bmod (x^{15} + 1)$, where:

$$\begin{aligned} a(x) &= x^{14} + x^{13} + x^{12} + x^{11} + x^{10} + x^8 + x^6 + x^5 + x^4 + x^3 + x^2 + 1, \\ b(x) &= x^{13} + x^{11} + x^8 + x^7 + x^6 + x^2. \end{aligned}$$

We have $N = 5$ with the above notation; we choose $K = 1$ and $L = 5$, thus we will perform $3K = 3$ products modulo $x^{2L} + x^L + 1 = x^{10} + x^5 + 1$. We first split the

[1] If we had a computer where w is a power of three, say 27 or 81, forcing L to be a multiple of w would give no real constraint.

input polynomials into $3K$ parts:

$$\begin{aligned} a_2 &= x^4 + x^3 + x^2 + x + 1, \quad a_1 = x^3 + x + 1, \quad a_0 = x^4 + x^3 + x^2 + 1 \\ b_2 &= x^3 + x, \quad b_1 = x^3 + x^2 + x, \quad b_0 = x^2. \end{aligned}$$

Then we perform a forward transform with $\omega = x^5$ as primitive root of unity, which yields:

$$\begin{aligned} \hat{a}_2 &= x^9 + x^7 + x^4 + x^2 + x, \quad \hat{a}_1 = x^9 + x^7 + x, \quad \hat{a}_0 = x^3 + 1. \\ \hat{b}_2 &= x^7 + x^3 + x, \quad \hat{b}_1 = x^7 + x^3 + x^2 + x, \quad \hat{b}_0 = 0. \end{aligned}$$

The pointwise transform yields:

$$\hat{c}_2 = x^6 + x^3, \quad \hat{c}_1 = x^7 + x^6 + x^3, \quad \hat{c}_0 = 0.$$

Then the backward transform gives:

$$c_2 = x^6 + x^3, \quad c_1 = x^7 + x^6 + x^3, \quad c_0 = 0,$$

and the reconstruction yields $a(x)b(x) \bmod (x^{15} + 1)$:

$$c_2 x^{10} + c_1 x^5 + c_0 = x^{13} + x^{12} + x^{11} + x^8 + x^2 + x \bmod (x^{15} + 1).$$

Here are some timings we obtained on a Core 2 processor running at 2.66Ghz, with 4MB of cache and 3GB of main memory. The first column is the degree (plus one) of the polynomials being multiplied; for degree 6972593 this corresponds to 108947 words. The second and third columns give the time of the Toom-Cook 3-way and Toom-Cook 4-way algorithms from [2]. The fourth column gives the time of (our variant of) Schönhage's algorithm, with $3K$ being the number of recursive calls.

degree	Toom-Cook 3	Toom-Cook 4	FFTMul($3K$)
6972593	1.32s	1.01s	0.27s(6561)
24036583	7.89s	6.30s	1.77s(6561)
32582657	13.9s	8.11s	2.16s(6561)

References

[1] Bajard, J.-C., Imbert, L., and Jullien, G. A. Parallel Montgomery multiplication in GF(2^k) using trinomial residue arithmetic. In *Proceedings of the 17th IEEE Symposium on Computer Arithmetic (ARITH'17)* (2005), P. Montuschi and E. Schwarz, Eds., IEEE Computer Society, pp. 164–171.

[2] Bodrato, M. Towards optimal Toom-Cook multiplication for univariate and multivariate polynomials in characteristic 2 and 0. In *Proceedings of WAIFI'2007* (Madrid, Espana, June 21-22, 2007), C. Carlet and B. Sunar, Eds., vol. 4547 of *Lecture Notes in Computer Science*, Springer-Verlag, pp. 116–133.

[3] Gaudry, P., Kruppa, A., and Zimmermann, P. A GMP-based implementation of Schönhage-Strassen's large integer multiplication algorithm. In *Proceedings of the 2007 International Symposium on Symbolic and Algebraic Computation, ISSAC'2007, July 29-August 1st, 2007* (Waterloo, Ontario, Canada, 2007), C. W. Brown, Ed., pp. 167–174.

[4] Harris, D., Krishnamurthy, R., Anders, M., Mathew, S., and Hsu, S. An improved unified scalable radix-2 Montgomery multiplier. In *Proceedings of the 17th IEEE Symposium on Computer Arithmetic (ARITH'17)* (2005), P. Montuschi and E. Schwarz, Eds., IEEE Computer Society, pp. 172–178.

[5] Kwon, S. A low complexity and a low latency bit parallel systolic multiplier over GF(2^m) using an optimal normal basis of type II. In *Proceedings of the 16th IEEE Symposium on Computer Arithmetic (ARITH'16)* (2003), J.-C. Bajard and M. Schulte, Eds., IEEE Computer Society, pp. 196–202.

[6] Lee, C.-Y., Lu, E.-H., and Lee, J.-Y. Bit-parallel systolic modular multipliers for a class of GF(2^m). In *Proceedings of the 15th IEEE Symposium on Computer Arithmetic (ARITH'15)* (2001), N. Burgess and L. Ciminiera, Eds., IEEE Computer Society, pp. 51–58.

[7] Montgomery, P. L. Five, six, and seven-term Karatsuba-like formulae. *IEEE Trans. Comput. 54*, 3 (2005), 362–369.

[8] Reyhani-Masoleh, A., and Hasan, M. A. Low complexity sequential normal basis multipliers over GF(2^m). In *Proceedings of the 16th IEEE Symposium on Computer Arithmetic (ARITH'16)* (2003), J.-C. Bajard and M. Schulte, Eds., IEEE Computer Society, pp. 188–195.

[9] Schönhage, A. Schnelle Multiplikation von Polynomen über Körpern der Charakteristik 2. *Acta Inf. 7* (1977), 395–398.

[10] Schönhage, A., and Strassen, V. Schnelle Multiplikation großer Zahlen. *Computing 7* (1971), 281–292.

[11] Shoup, V. NTL: A library for doing number theory. `http://www.shoup.net/ntl/`.

[12] von zur Gathen, J., and Gerhard, J. Arithmetic and factorization of polynomials over GF(2) (extended abstract). Tech. Report tr-rsfb-96-018, University of Paderborn, Germany, 1996. 43 pages.

[13] Weimerskirch, A., and Paar, C. Generalizations of the Karatsuba algorithm for efficient implementations. Technical report, Rurh-University Bochum, 2003. `http://weimerskirch.org/papers/Weimerskirch_Karatsuba.pdf`.

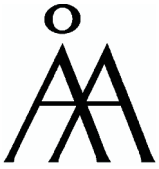
Turku Centre for Computer Science
TUCS General Publications

24. **Ralph-Johan Back and Victor Bos**, Centre for Reliable Software Technology, Progress Report 2003
25. **Pirkko Walden, Stina Störling-Sarkkila, Hannu Salmela and Eija H. Karsten (Eds.)**, ICT and Services: Combining Views from IS and Service Research
26. **Timo Järvi and Pekka Reijonen (Eds.)**, People and Computers: Twenty-one Ways of Looking at Information Systems
27. **Tero Harju and Juhani Karhumäki (Eds.)**, Proceedings of WORDS'03
28. **Mats Aspnäs, Christel Donner, Monika Eklund, Pia Le Grand, Ulrika Gustafsson, Timo Järvi and Nina Kivinen (Eds.)**, Turku Centre for Computer Science, Annual Report 2002
29. **João M. Fernandes, Johan Lilius, Ricardo J. Machado and Ivan Porres (Eds.)**, Proceedings of the 1st International Workshop on Model-Based Methodologies for Pervasive and Embedded Software
30. **Mats Aspnäs, Christel Donner, Monika Eklund, Ulrika Gustafsson, Timo Järvi and Nina Kivinen (Eds.)**, Turku Centre for Computer Science, Annual Report 2003
31. **Andrei Sabelfeld (Editor)**, Foundations of Computer Security
32. **Eugen Czeizler and Jarkko Kari (Eds.)**, Proceedings of the Workshop on Discrete Models for Complex Systems
33. **Peter Selinger (Editor)**, Proceedings of the 2nd International Workshop on Quantum Programming Languages
34. **Kai Koskimies, Johan Lilius, Ivan Porres and Kasper Østerbye (Eds.)**, Proceedings of the 11th Nordic Workshop on Programming and Software Development Tools and Techniques, NWPER'2004
35. **Kai Koskimies, Ludwik Kuzniarz, Johan Lilius and Ivan Porres (Eds.)**, Proceedings of the 2nd Nordic Workshop on the Unified Modeling Language, NWUML'2004
36. **Franca Cantoni and Hannu Salmela (Eds.)**, Proceedings of the Finnish-Italian Workshop on Information Systems, FIWIS 2004
37. **Ralph-Johan Back and Kaisa Sere**, CREST Progress Report 2002-2003
38. **Mats Aspnäs, Christel Donner, Monika Eklund, Ulrika Gustafsson, Timo Järvi and Nina Kivinen (Eds.)**, Turku Centre for Computer Science, Annual Report 2004
39. **Johan Lilius, Ricardo J. Machado, Dragos Truscan and João M. Fernandes (Eds.)**, Proceedings of MOMPES'05, 2nd International Workshop on Model-Based Methodologies for Pervasive and Embedded Software
40. **Ralph-Johan Back, Kaisa Sere and Luigia Petre**, CREST Progress Report 2004-2005
41. **Tapio Salakoski, Tomi Mäntylä and Mikko Laakso (Eds.)**, Koli Calling 2005 - Proceedings of the Fifth Koli Calling Conference on Computer Science Education
42. **Petri Paju, Nina Kivinen, Timo Järvi and Jouko Ruissalo (Eds.)**, History of Nordic Computing - HiNC2
43. **Tero Harju and Juhani Karhumäki (Eds.)**, Proceedings of the Workshop on Fibonacci Words 2006
44. **Michal Kunc and Alexander Okhotin (Eds.)**, Theory and Applications of Language Equations, Proceedings of the 1st International Workshop, Turku, Finland, 2 July 2007
45. **Mika Hirvensalo, Vesa Halava and Igor Potapov, Jarkko Kari (Eds.)**, Proceedings of the Satellite Workshops of DLT 2007
46. **Anne-Maria Ernvall-Hytönen, Matti Jutila, Juhani Karhumäki, Arto Lepistö (Eds.)**, Proceedings of Conference on Algorithmic Number Theory 2007

Turku
Centre *for*
Computer
Science

Joukahaisenkatu 3-5 B, 20520 Turku, Finland | www.tucs.fi

University of Turku
- Department of Information Technology
- Department of Mathematics



Åbo Akademi University
- Department of Information Technologies

Turku School of Economics
- Institute of Information Systems Sciences

ISBN 978-952-12-2014-2
ISSN 1239-1905

Proceedings of Conference on Algorithmic Number Theory 2007

Proceedings of Conference on Algorithmic Number Theory 2007

Proceedings of Conference on Algorithmic Number Theory 2007