On the Divisibility of Certain Polynomials over Finite Fields

Pascale Charpin

INRIA, Codes
Domaine de Voluceau - Rocquencourt,
BP 105 - 78153, Le Chesnay, FRANCE

Aimo Tietäväinen

Department of Mathematics, University of Turku,
FIN - 20014 Turku, FINLAND

Victor Zinoviev

Institute for Problems of Information Transmission
Russian Academy of Sciences
Bol'shoi Karetnyi 19, GSP-4,
Moscow, 101447, RUSSIA

TUCS

Turku Centre for Computer Science
TUCS Technical Report No 82
December 1996

ISBN 951-650-925-8
ISSN 1239-1891

On the Divisibility of Certain Polynomials over Finite Fields

Pascale Charpin

INRIA, Codes
Domaine de Voluceau - Rocquencourt,
BP 105 - 78153, Le Chesnay, FRANCE

Aimo Tietäväinen

Department of Mathematics, University of Turku,
FIN - 20014 Turku, FINLAND

Victor Zinoviev

Institute for Problems of Information Transmission
Russian Academy of Sciences
Bol'shoi Karetnyi 19, GSP-4,
Moscow, 101447, RUSSIA

Turku Centre for Computer Science
TUCS Technical Report No 82
December 1996

ISBN 951-650-925-8
ISSN 1239-1891

Abstract

We use subfields of the splitting field of $f(x)$ in order to obtain several statements concerning the divisibility of some polynomials of the form $f(x^u)$. Sometimes we obtain the complete factorization.

TUCS Research Group
Coding Theory Group

Let $q = 2^m$, let F_q be the finite field of order q and let g be a factor of m. Then F_{2^g} is a subfield of F_q. Let γ be a primitive element of F_q and $u = (2^m - 1)/(2^g - 1)$. Then $\beta = \gamma^u$ is a primitive element of F_{2^g}. Denote by $m_s(x)$ the minimal polynomial of γ^s over F_2. The notation above will be used throughout this paper.

In general, it is difficult to find the conditions under which $m_s(x)$ divides a given polynomial $f(x) \in \mathbf{F}_2[x]$. Perhaps the most interesting case is the one when $f(x)$ is a trinomial (i.e., a polynomial with exactly three nonzero terms). There is an extensive literature on the factorization of polynomials over finite fields; for good surveys, see ([1], Ch. V), ([2], Ch. 3 and 4) and ([3], Ch. 2). In this paper we give several simple and natural statements which we could not find in the references above.

Definition 1 *Let g be fixed. For $f(x) = \sum_{i=0}^{2^g-2} a_i x^i \in \mathbf{F}_2[x]$ and $r \in \{1, 2, ..., 2^g - 2\}$, where $gcd(r, 2^g - 1) = 1$, define*

$$f^{[1/r]}(x) = \sum_{i=0}^{2^g-2} a_i x^{i/r}$$

where the quotients i/r in the exponents are calculated in the ring $\mathbf{Z}_{2^g-1}$. Further, denote by $f^{[u/r]}(x)$ the polynomial obtained from $f^{[1/r]}(x)$ by replacing x by x^u.

Theorem 1 *Let $r \in \{1, 2, ..., 2^g - 2\}$, let $gcd(r, 2^g - 1) = 1$ and let i be any integer, $0 < i < 2^m - 1$, such that $2^j i \equiv r(mod\ 2^g - 1)$ for some j. Let $f(x) \in \mathbf{F}_2[x]$ be a polynomial of degree at most $2^g - 2$. If now $m_u(x)$ divides $f(x)$ then $m_i(x)$ divides $f^{[u/r]}(x)$.*

Proof. We have to prove that γ^i (or as well $\gamma^{2^j i}$) is a zero of $f^{[u/r]}(x)$. By the assumption, there is an s such that $2^j i = r + s(2^g - 1)$. Thus

$$f^{[u/r]}(\gamma^{2^j i}) = f^{[1/r]}(\beta^{2^j i}) = f^{[1/r]}(\beta^r) = f(\beta)$$

and $f(\beta) = 0$ because the minimal polynomial $m_u(x)$ of β divides $f(x)$. □

We could write Theorem 1 in the following slightly different form.

Theorem 2 *Let $r \in \{0, 1, ..., 2^g-2\}$ and let i be any integer, $0 \leq i \leq 2^m-2$, such that $2^j i \equiv r(mod\ 2^g-1)$ for some j. Let $f(x) \in \mathbf{F}_2[x]$ be a polynomial of degree at most $2^g - 2$. If now $m_{ur}(x)$ divides $f(x)$ then $m_i(x)$ divides $f(x^u)$.*

Proof. We can easily see that

$$f(\gamma^{2^j iu}) = f(\gamma^{u(2^g-1)s} \cdot \gamma^{ur}) = f(\gamma^{ur}) = 0$$

and so $m_{2^j i}(x) = m_i(x)$ divides $f(x^u)$. □

Example 1 *Let* $m = 6, g = 3$ *and* $m_1(x) = x^6 + x + 1$. *Then* $u = 9$ *and* $m_9(x) = x^3 + x^2 + 1$. *If* $f(x) = m_9(x)$ *and* $r = 1$ *then, by Theorem 1,* $m_i(x)$ *divides* $x^{27} + x^{18} + 1$ *for* $i = 1, 9, 11, 15, 23$. *In fact, in this case we have the complete decomposition:*

$$x^{27} + x^{18} + 1 = m_1(x)m_9(x)m_{11}(x)m_{15}(x)m_{23}(x).$$

If $f(x) = x^5 + x + 1$ *then again* $m_9(x)$ *divides* $f(x)$. *If* $r = 3$, *we thus have* $f^{[u/r]}(x) = (x^4)^9 + (x^5)^9 + 1$ *and so* $m_i(x)$ *divides* $x^{45} + x^{36} + 1$ *for* $i = 3, 5, 13, 27, 31$. *Of course, in this case the decomposition is not complete, i.e.,* $x^{45} + x^{36} + 1$ *has also other factors. If* $f(x) = m_{27}(x) = x^3 + x + 1$ *then, by Theorem 2,* $m_i(x)$ *divides* $f(x^u) = x^{27} + x^9 + 1$ *for* $i = 3, 5, 13, 27, 31$. *The case* $r = 0$ *is exceptionally simple. If* $f(x) = m_0(x) = x + 1$ *then we know by Theorem 2 that* $f(x^u) = x^9 + 1$ *is divisible by* $m_i(x)$ *for any* $i \equiv 0(mod 7)$. *Hence* $x^9 + 1 = m_0(x)m_7(x)m_{21}(x)$.

In fact, also the following inverse statement of Theorem 2 is valid.

Theorem 3 *If* $m_i(x)$ *divides* $f(x^u)$ *and* $r \equiv 2^j i(mod\ 2^g - 1)$ *for some* j *then* $m_r(x)$ *divides* $f(x^u)$ *and* $m_{ur}(x)$ *divides* $f(x)$.

Proof. By the second assumption, we may write $r = 2^j i + k(2^g - 1)$, where k is an integer. Thus $ur = u2^j i + k(2^m - 1)$ and so

$$f(\gamma^{ur}) = f(\gamma^{ui2^j}) = (f(\gamma^{ui}))^{2^j}.$$

On the other hand, $f(\gamma^{ui}) = 0$ because γ^i is a zero of $f(x^u)$. Hence $f(\gamma^{ur}) = 0$ and so γ^r is a zero of $f(x^u)$ and γ^{ur} is a zero of $f(x)$. □

Example 2 *Let* $a(x) = x^{18} + x^9 + 1$. *Then* $ord(a(x))$, *the order of* $a(x)$, *is* 27. *Let* $b(x)$ *be an irreducible factor of* $a(x)$ *of lowest degree. Thus* $ord(b(x))$ *is either* 3 *or* 9 *or* 27. *If* $ord(b(x)) = 3$ *then* $b(x) = x^2 + x + 1$ *which is impossible. Let* $ord(b(x))$ *be* 27. *Since* 18 *is the smallest positive* m *such that* 27 *divides* $2^m - 1$, *the degree of* $b(x)$ *is* 18 *and therefore* $b(x) = a(x)$. *Consider then the case where* $ord(b(x)) = 9$. *Then the degree of* $b(x)$ *is* 6 *and therefore* $b(x)$ *is* $m_i(x)$, *the minimal polynomial of an element* γ^i *where* γ *is a primitive element of* F_{64}. *If* $i \equiv 0(mod\ 7)$ *then by Theorem 3* $m_r(x)$ *divides* $a(x)$ *for any* $r \equiv 0(mod\ 7)$. *This is impossible because* $m_0(x) = x + 1$ *does not divide* $a(x)$. *If* $i \not\equiv 0(mod\ 7)$ *then* $m_r(x)$ *divides* $a(x)$ *for all* r *congruent to* $2^j i$ *modulo* 7 *for some* j. *But this shows that the degree of* $a(x)$ *should be at least* 27, *a contradiction. Thus* $a(x)$ *is irreducible over* F_2.

Definition 2 *Let I_m be a set of representatives of 2-cosets of the set $\{0, 1, ..., 2^m - 2\}$ modulo $2^m - 1$.*

Theorem 4 *If $r \in \{0, 1, ..., 2^g - 2\}$ then*

$$m_{ur}(x^u) = \prod_i m_i(x)$$

where the multiplication is over all i in the set I_m such that $2^j i \equiv r(mod\ 2^g - 1)$ for some j.

Proof. The fact that the right hand side divides the left hand side follows from Theorem 2. Since the both sides are monic polynomials, it is enough to prove that the degrees are equal. The degree of $m_{ur}(x^u)$ is u times the degree of $m_{ur}(x)$, and the latter is the number of elements in the cyclotomic coset C_r modulo $2^g - 1$ determined by r. On the other hand, the degree of the right hand side is the number of elements i in the set $\{0, 1, ..., 2^m - 2\}$ such that $2^j i \equiv r(mod\ 2^g - 1)$ for some j, and so also it is u times the number of elements in C_r. □

Considering the problem from a different point of view we may write Theorem 4 in the following form.

Theorem 5 *If $f(x)$ is an irreducible polynomial of degree g, m any multiple of g and, as always, $u = (2^m - 1)/(2^g - 1)$, then $f(x^u)$ is reducible. If, further, $f(x)$ is of order $(2^g - 1)/r$ and we choose a primitive element γ of F_{2^m} in such a way that γ^{ur} is a zero of $f(x)$ then*

$$f(x^u) = \prod_i m_i(x) \tag{1}$$

where the multiplication is again over all i in the set I_m such that $2^j i \equiv r(mod\ 2^g - 1)$ for some j.

Proof. Since $f(x)$ is irreducible and $f(\gamma^{ur}) = 0$, we have $f(x) = m_{ur}(x)$. Thus it follows from Theorem 4 that Eq. (1) is valid. □

Example 3 *Let $m = 8, g = 4, m_1(x) = x^8 + x^7 + x^6 + x + 1$ and $r = 7$. Then $u = 17$ and $m_{119}(x) = m_{7 \cdot 17}(x) = x^4 + x + 1$. By Theorem 4,*

$$x^{68} + x^{17} + 1 = m_{119}(x^{17}) = \prod_i m_i(x)$$

where i runs over the set

$$\{i \in I_8 : \exists j : 2^j i \equiv 7(mod\ 15)\} = \{7, 11, 13, 29, 37, 43, 59, 119, 127\}.$$

Example 4 *Let $f(x) = x^5 + x^2 + 1 \in \mathbf{F}_2[x]$. Then the degree and the order of $f(x)$ are 5 and 31, respectively. Thus $g = 5$ and $r = 1$. If we take $m = 10$ (and so $u = 33$) and choose a primitive element γ of the field F_{2^m} in such a way that γ^{33} is a zero of $f(x)$ then, by Theorem 5,*

$$x^{165} + x^{66} + 1 = \prod_i m_i(x)$$

where the multiplication is over all i in the set I_{10} such that $2^j i \equiv 1 (mod\ 31)$ for some j.

References

1. S. W. Golomb, "Shift Register Sequences", Aegean Park Press, Revised Edition, 1982.

2. R. Lidl and H. Niederreiter, "Finite Fields", Encyclopedia of Mathematics and its Applications, Addison-Wesley Publishing Company, London / Amsterdam / Don Mills, Ontario / Sydney / Tokyo, 1983.

2. I. E. Shparlinski, "Computational and Algorithmic Problems in Finite Fields", Kluwer Academic Publishers, Dordrecht / Boston / London, 1992.

Turku Centre for Computer Science
Lemminkäisenkatu 14
FIN-20520 Turku
Finland

http://www.tucs.abo.fi

University of Turku
- **Department of Mathematical Sciences**

Åbo Akademi University
- **Department of Computer Science**
- **Institute for Advanced Management Systems Research**

Turku School of Economics and Business Administration
- **Institute of Information Systems Science**