ON THE DISTRIBUTION OF IRREDUCIBLE TRINOMIALS OVER $\mathbb{F}_3$

OMRAN AHMADI

Abstract. We present some results about irreducible polynomials over finite fields and use them to prove a conjecture of von zur Gathen concerning the distribution of irreducible trinomials over $\mathbb{F}_3$.

1. Introduction

Let $\mathbb{F}_{q^n}$ be the degree n extension of $\mathbb{F}_q$. Then we have $\mathbb{F}_{q^n} = \mathbb{F}_q[x]/(f(x))$ where $f(x)$ is an irreducible polynomial of degree n over $\mathbb{F}_q$. The weight of $f(x)$ is the number of its coefficients that are non-zero. If the weight of $f(x)$ is three, then $f(x)$ is called a trinomial. It is well known that multiplication in $\mathbb{F}_{q^n}$ can be sped up considerably if $f(x)$ is a trinomial (e.g. see [7]).

Fast arithmetic in finite fields is important for the efficient implementation of error-correcting codes and discrete logarithm cryptosystems. Finite fields of characteristic two have received special attention because their arithmetic can be efficiently implemented in both hardware and software, and there has been a significant amount of work done on the distribution of irreducible trinomials over $\mathbb{F}_2$ (e.g. see [2, 3, 12, 15]). More recently, there has been increased interest in fast arithmetic for finite fields of characteristic 3 (e.g. see [8, 9, 13, 14]) because there are two supersingular elliptic curves over $\mathbb{F}_3$ with embedding degree six that are very well suited to the implementation of pairing-based cryptographic protocols [1, 5].

Von zur Gathen [6] (see also Loidreau [10]) proved some interesting results about irreducible trinomials over $\mathbb{F}_3$, and made some conjectures about their distribution. The conjectures were supported by extensive experiments. In Section 2 of this paper we present some results about the irreducibility of trinomials that are related to each other. Our results can be used to speed up the search and enumeration of irreducible polynomials over finite fields. We then use these results in Section 3 to prove one of von zur Gathen's conjectures.

2. Main Result

The order of an irreducible polynomial $f(x)$ over $\mathbb{F}_q$ is the smallest positive integer e such that $f(x) \mid x^e - 1$ in $\mathbb{F}_q[x]$.

Date: June 26, 2005.

Key words and phrases. Finite Fields, Irreducible Polynomials.

Theorem 1. [11, Theorem 3.9] Let $f(x) \in \mathbb{F}_q[x]$ be an irreducible polynomial over $\mathbb{F}_q$ of degree n and order e and let t be a positive integer. Then $f(x^t)$ is irreducible over $\mathbb{F}_q$ if and only if

(i) $\gcd(t, \frac{q^n-1}{e}) = 1$;
(ii) each prime factor of t divides e; and
(iii) if $4 \mid t$, then $4 \mid q^n - 1$.

An immediate corollary is the following:

Corollary 2. Let q be a prime power where $q \equiv 3 \pmod 4$, and let $f(x) \in \mathbb{F}_q[x]$ be a polynomial of odd degree. Then $f(x^{2^r})$ where $r \geq 2$ is always reducible over $\mathbb{F}_q$.

It is well known that if $f(x) \in \mathbb{F}_q[x]$ is an irreducible polynomial over $\mathbb{F}_q$ and $\alpha \in \mathbb{F}_q^*$, then $f(\alpha x) \in \mathbb{F}_q[x]$ is also irreducible over $\mathbb{F}_q$. In the following we generalize this fact.

Theorem 3. Let $f(x)$ be an irreducible polynomial of degree n over $\mathbb{F}_q$. Let $\theta \in \mathbb{F}_{q^n}^*$ be such that $f(\theta x) \in \mathbb{F}_q[x]$. Then $f(\theta x)$ is the product of irreducible polynomials over $\mathbb{F}_q$ whose degrees divide n.

Proof. Let $f(\theta x) = f_1(x) \cdots f_l(x)$ where $f_i(x)$ is an irreducible polynomial of degree n_i over $\mathbb{F}_q$. Let $\alpha_i \in \mathbb{F}_{q^{n_i}}$ be a root of f_i, and let $\beta_i = \theta\alpha_i$. Then $f(\beta_i) = 0$. Now $\beta_i \in \mathbb{F}_{q^n}$ since $f(x)$ is an irreducible polynomial of degree n over $\mathbb{F}_q$. On the other hand we have $\theta^{-1} \in \mathbb{F}_{q^n}^*$. Thus $\theta^{-1}\beta_i = \alpha_i \in \mathbb{F}_{q^n}$ and hence n_i divides n. □

It is easy to see that if $f(x)$ and θ are as above and β is a root of $f(x)$ in $\mathbb{F}_{q^n}$, then $f(\theta x)$ is irreducible over $\mathbb{F}_q$ if and only if $\theta^{-1}\beta$ is not in any proper subfield of $\mathbb{F}_{q^n}$. Notice that this latter condition is always satisfied if $\theta \in \mathbb{F}_q^*$. Because if $\theta \in \mathbb{F}_q^*$ and $\beta \in \mathbb{F}_{q^n}$ is not in any proper subfield of $\mathbb{F}_{q^n}$, then since $(\theta^{-1})^{q^c-1} = 1$ for every $c \geq 1$, we have $(\theta^{-1}\beta)^{q^c-1} = \beta^{q^c-1} = 1$ if and only if n divides c. Thus $\theta^{-1}\beta$ is in $\mathbb{F}_{q^n}$ and not in any proper subfield of $\mathbb{F}_{q^n}$.

In the following we use the ideas presented above to obtain the main result of this paper. First we need the following elementary lemmas.

Lemma 4. Let q be an odd prime power and let $n = 2^r n'$ where n' is an odd number and $r \geq 1$. Then $2^{r+2} \mid q^n - 1$ and $2^r \mid \frac{q^n-1}{q-1}$.

Proof. The case $r = 1$ is easy. For $r \geq 2$ we have

$$q^n - 1 = (q^2 - 1)\left(\prod_{i=1}^{r-1}(q^{2^i} + 1)\right)\left(\sum_{i=0}^{n'-1}(q^{2^r})^i\right).$$

The result now follows because $q^2 \equiv 1 \pmod 8$. □

Lemma 5. Let q be an odd prime power and $n = 2^r n'$ where n' is an odd number, and let $r \geq s \geq 0$. Then for any $\alpha \in \mathbb{F}_q^*$ there exists $\theta \in \mathbb{F}_{q^n}$ such that $\theta^{2^s} = \alpha$.

Proof. The statement is trivial when $r = 0$, so let us suppose that $r \geq 1$. Let γ be a generator of $\mathbb{F}_{q^n}^*$ and $\alpha \in \mathbb{F}_q^*$. Then there exists a unique integer d such that $\gamma^d = \alpha$ and $0 \leq d \leq q^n - 2$. Thus $(\gamma^d)^{q-1} = \alpha^{q-1} = 1$. Now since γ is a generator of $\mathbb{F}_{q^n}^*$, we have $q^n - 1 \mid d(q-1)$ and hence $\frac{q^n-1}{q-1} \mid d$. By Lemma 4 we get $2^r \mid d$, and since $r \geq s$, if we take $\theta = \gamma^{\frac{d}{2^s}}$, then $\theta^{2^s} = \alpha$. □

Theorem 6. Let $n = 2^r n'$ and $k = 2^s k'$ where n' and k' are odd numbers and $r > s \geq 0$, and let q be an odd prime power and $\alpha \in \mathbb{F}_q^*$. Then $x^n + ax^k + b \in \mathbb{F}_q[x]$ is irreducible over $\mathbb{F}_q$ if and only if

$$\alpha^{2^{r-s}n'} x^n + a\alpha^{k'} x^k + b \in \mathbb{F}_q[x]$$

is irreducible over $\mathbb{F}_q$.

Proof. Suppose that $f(x) = x^n + ax^k + b \in \mathbb{F}_q[x]$ is irreducible over $\mathbb{F}_q$. By Lemma 5, there exists $\theta \in \mathbb{F}_{q^n}^*$ such that $\theta^{2^s} = \alpha$. We claim that $g(x) = f(\theta x) = \alpha^{2^{r-s}n'} x^n + a\alpha^{k'} x^k + b \in \mathbb{F}_q[x]$ is irreducible over $\mathbb{F}_q$. Using the comments made after Theorem 3, it suffices to show that $\alpha = \theta^{-1}\beta$ is not in any proper subfield of $\mathbb{F}_{q^n}$ where β is a root of $f(x)$ in $\mathbb{F}_{q^n}$.

Suppose by the way of contradiction that $\alpha^{q^l - 1} = 1$ where l is a proper divisor of n, and let $l = 2^v l'$, where $v \leq r$ and $l' \mid n'$. From Lemma 4, we know $2^{v+2} \mid q^l - 1$. Now if $v \geq s$, then

$$\beta^{q^l-1} = \theta^{q^l-1} = \theta^{2^s(q-1)t} = 1$$

and this is a contradiction since β is not in any proper subfield of $\mathbb{F}_{q^n}$. Thus suppose $v < s$ and let $w = s - v$. Now, $q^l - 1 \mid q^{2^w l} - 1$. Since $\beta^{q^l-1} = \theta^{q^l-1}$, we have

$$\beta^{q^{2^w l}-1} = \theta^{q^{2^w l}-1} = \theta^{q^{2^s l'}-1} = \theta^{2^s(q-1)t'} = 1,$$

and hence we must have $n \mid 2^w l$. But this cannot hold since the largest power of 2 which divides $2^w l$ and n are s and r, respectively, and we have $r > s$. The converse is similarly true since $f(x) = g(\theta^{-1}x)$ and $\theta^{-2^s} = \alpha^{-1} \in \mathbb{F}_q^*$. □

By taking $\alpha = -1$ in Theorem 6, we obtain the following.

Corollary 7. Let n, k, r, s be as in the above theorem. Then $x^n + ax^k + b$ is irreducible over $\mathbb{F}_q$ if and only if $x^n - ax^k + b$ is irreducible over $\mathbb{F}_q$.

Specializing Theorem 6 to some finite fields yields interesting results. The following results are of this flavour.

Corollary 8. Let n be a positive integer divisible by 4. Then the degree n trinomial $f(x) = x^n - x^k + 1$ is always reducible over $\mathbb{F}_3$.

Proof. If the power of 2 which divides k is not less than that of n, then it follows from Corollary 2 that $f(x)$ is reducible. Suppose then that the power of 2 which divides n is greater than that of k. Since $x^n + x^k + 1$ is reducible over $\mathbb{F}_3$, it follows from Corollary 7 that $f(x)$ is also reducible. □

Corollary 9. Let n, k, r, s be as in the above theorem, and furthermore let $r > s+1$ and c be a non-zero element of $\mathbb{F}_5$. Then $x^n + ax^k + b$ is irreducible over $\mathbb{F}_5$ if and only if $x^n + cax^k + b$ is irreducible over $\mathbb{F}_5$.

Theorem 6 can easily be generalized to polynomials of any weight. The proof of Theorem 10 is similar to the proof of Theorem 6 and is omitted.

Theorem 10. Let $f(x) = \sum_{i=0}^{t} a_i x^{n_i} \in \mathbb{F}_q[x]$ where q is an odd prime power, $n = n_t > n_{t-1} > \cdots > n_1 > n_0 = 0$, $a_t = 1$ and $a_i \neq 0$ for every $0 \leq i \leq t-1$. Let s be the largest power of 2 which divides $d = \gcd(n_0, n_1, \cdots, n_t)$, let r_i be the largest power of 2 dividing n_i, and suppose that $r_t > s$. Furthermore let $\alpha \in \mathbb{F}_q^*$. Then $f(x)$ is irreducible over $\mathbb{F}_q$ if and only if

$$g(x) = \sum_{i=0}^{t} \alpha^{2^{-s} n_i} a_i x^{n_i}$$

is irreducible over $\mathbb{F}_q$.

3. Applying our results to trinomials over $\mathbb{F}_3$

Joachim von zur Gathen studied the distribution of irreducible trinomials over $\mathbb{F}_3$ and made two conjectures based on some experimental data. The first conjecture was proven by Stephen Cohen [4]. We provide a proof for the sake of completeness.

Theorem 11. If $n \equiv 0 \pmod 4$, $k \equiv 2 \pmod 6$, and $x^n + ax^k + b \in \mathbb{F}_3[x]$ is irreducible over $\mathbb{F}_3$, then the largest power of 2 which divides n is greater than the largest power of 2 which divides k.

Proof. Let $x^n + ax^k + b \in \mathbb{F}_3[x]$ where $n = 2^r n'$, $k = 2^s k'$, n' and k' are odd numbers, and $s \geq r \geq 2$. Then if we let $f(x) = x^{n'} + ax^{2^{s-r}k'} + b$, we have $x^n + ax^k + b = f(x^{2^r})$ and from Corollary 2 it follows that $x^n + ax^k + b$ is reducible over $\mathbb{F}_3$. □

The second conjecture of von zur Gathen that we proved is the following. Recall that the reciprocal of a degree-n polynomial $f(x)$ whose constant term is non-zero is defined to be $f^*(x) = x^n f(1/x)$, and if $f(x)$ is irreducible over $\mathbb{F}_q$, then so is $f^*(x)$.

Theorem 12. Let m be a fixed positive integer. For given $a, b \in \mathbb{F}_3$, $p \in \{0, 4, 8\}$ and $0 \leq c \leq 5$, the number of irreducible trinomials $x^n + ax^k + b \in \mathbb{F}_3[x]$ where $n \equiv p \pmod{12}$, $k \equiv c \pmod 6$, and $n \leq m$ is equal to the number of irreducible trinomials $x^n + ax^k + b \in \mathbb{F}_3[x]$ where $n \equiv p \pmod{12}$, $k \equiv p - c \pmod 6$ and $n \leq m$.

Proof. The case where $a = b = 1$ is trivial since there is no irreducible trinomial $x^n + x^k + 1$ over $\mathbb{F}_3$. Now we assume $a = 1$, $b = -1$. The other cases can be dealt with similarly. Let $x^n + x^k - 1$ be an irreducible trinomial over $\mathbb{F}_3$ where $n \equiv p \pmod{12}$, $k \equiv c \pmod 6$ for given $p \in \{0, 4, 8\}$ and

$0 \leq c \leq 5$. Then from Theorem 11 the largest power of 2 which divides n is greater than the largest power of 2 which divides k. Thus by Corollary 7, $x^n - x^k - 1$ is irreducible over $\mathbb{F}_3$. Now the reciprocal of $x^n - x^k - 1$, namely $-x^n - x^{n-k} + 1$, is also irreducible over $\mathbb{F}_3$, so it follows that $x^n + x^{n-k} - 1$ is irreducible over $\mathbb{F}_3$. But in this case we have $n \equiv p \pmod{12}$ and $n-k \equiv p-c \pmod{6}$. This establishes a bijection between the two sets of irreducible polynomials and hence proves the theorem. □

References

[1] P. Barreto, H. Yim, B. Lynn and M. Scott, "Efficient algorithms for pairing-based cryptosystems", *Proceedings of CRYPTO 2002*, Lecture Notes in Computer Science 2442 (2002), 354-368.

[2] I. Blake, S. Gao and R. Lambert, "Constructive problems for irreducible polynomials over finite fields", *Information Theory and Applications*, Lecture Notes in Computer Science 793 (1994), 1-23.

[3] I. Blake, S. Gao and R. Lambert, "Construction and distribution problems for irreducible polynomials over finite fields", *Applications of Finite Field* (D. Gollmann, Ed.), Clarendon Press, (1996), 19-32.

[4] S. D. Cohen, *Mathematical Reviews*, MR 1986817 (2004c:11229).

[5] S. Galbraith, K. Harrison and D. Soldera, "Implementing the Tate pairing", *ANTS-V* (C. Fieker and D. Kohel, Eds), Lecture Notes in Computer Science 2369 (2002), 324-337.

[6] J. von zur Gathen, "Irreducible trinomials over finite fields", *Mathematics of Computation*, 72 (2003), 1987-2000.

[7] J. von zur Gathen and M. Nöcker, "Polynomial and normal bases for finite fields", *Journal of Cryptology*, to appear.

[8] P. Grabher and D. Page, "Hardware acceleration of the Tate pairing in characteristic three", *Proceedings of CHES 2005*, to appear.

[9] T. Kerins, W. Marnane, E. Popovici and P. Barreto, "Efficient hardware for the Tate pairing calculation in characteristic three", *Proceedings of CHES 2005*, to appear.

[10] P. Loidreau, "On the factorization of trinomials over $\mathbb{F}_3$", Technical Report 3918, Institut National de Recherche en Informatique et en Automatique (INRIA), http://www.inria.fr/rrrt/rr-3918.html, 2000.

[11] A. J. Menezes, I. F. Blake, X. Gao, R. C. Mullin, S. A. Vanstone and T. Yaghoobian *Applications of Finite Fields*, Kluwer, 1993.

[12] G. Seroussi, "Table of low-weight binary irreducible polynomials", Hewlett-Packard Technical Report HPL-98-135, 1998.

[13] K. Harrison, D. Page and N. P. Smart, "Software implementation of finite fields of characteristic three", *LMS Journal of Computation and Mathematics*, 5 (2002), 181-193.

[14] D. Page and N. P. Smart, "Hardware implementation of finite fields of characteristic three", *Proceedings of CHES 2002*, Lecture Notes in Computer Science 2523 (2002), 529-539.

[15] R. Swan, "Factorization of polynomials over finite fields", *Pacific Journal of Mathematics*, 12 (1962), 1099-1106.

Dept. of Combinatorics and Optimization, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1

E-mail address: `oahmadid@math.uwaterloo.ca`