Noname manuscript No.
(will be inserted by the editor)

Efficient pth Root Computations in Finite Fields of Characteristic p

D. Panario† · D. Thomson

December 24, 2009

Abstract We present a method for computing pth roots using a polynomial basis over finite fields $\mathbb{F}_q$ of odd characteristic p, $p \geq 5$, by taking advantage of a binomial reduction polynomial. For a finite field extension $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$ our method requires $p-1$ scalar multiplication of elements in $\mathbb{F}_{q^m}$ by elements in $\mathbb{F}_q$. In addition, our method requires at most $(p-1)\lceil m/p \rceil$ additions in the extension field. In certain cases, these additions are not required. If z is a root of the irreducible reduction polynomial, then the number of terms in the polynomial basis expansion of $z^{1/p}$, defined as the *Hamming weight* of $z^{1/p}$ or $\mathrm{wt}\left(z^{1/p}\right)$, is directly related to the computational cost of the pth root computation. Using trinomials in characteristic 3, Ahmadi et al. [1] give $\mathrm{wt}\left(z^{1/3}\right)$ is greater than 1 in nearly all cases. Using a binomial reduction polynomial over odd characteristic p, $p \geq 5$, we find $\mathrm{wt}\left(z^{1/p}\right) = 1$ always.

Keywords Finite field arithmetic · irreducible binomials · pth roots.

Mathematics Subject Classification (2000) 12E30

1 Introduction

The problem of efficient root extraction is motivated by the pairing computation problem in cryptography, see [3,4], for example. In addition, computing pth roots of elements expressed as polynomials is used in factorization algorithms, see [8, Algorithm 3.110] and [5], for example. Barreto [2] uses the so-called folklore algorithm for computing cube roots over finite fields of characteristic 3. He simplifies the computation using a trinomial reduction polynomial, and eliminates the use of multiplications in the extension field to compute the cube roots. Barreto's methods work for trinomials $x^m + ax^k + b$

† The author is supported in part by NSERC of Canada.

School of Mathematics and Statistics, Carleton University
1125 Colonel By Drive, Ottawa, ON, K1S 5B6 E-mail: {daniel,dthomson}@math.carleton.ca

where $m \equiv k \pmod 3$. In particular, for a root z of the reduction trinomial, he shows

$$\mathrm{wt}\left(z^{1/3}\right) = \begin{cases} 3 & \text{if } m \equiv k \equiv 1 \pmod 3, \\ 2 & \text{if } m \equiv k \equiv 2 \pmod 3, \end{cases}$$

where $\mathrm{wt}\left(z^{1/3}\right)$ is the *Hamming weight* (the number of non-zero terms under the polynomial basis) of the expansion of $z^{1/3}$. The Hamming weight of $z^{1/3}$ is directly related to the computational cost of the root extraction problem. Barreto [2] presents a comparison of timings for the Duursma-Lee algorithm [4] for computing the Tate pairing and notes an approximate 10% decrease in the overall pairing time. Ahmadi et al. [1] generalize Barreto's results by giving $\mathrm{wt}\left(z^{1/3}\right)$ where z is a root of the irreducible trinomial over $\mathbb{F}_3$ used to define an extension field. Table 1 summarizes the results in [1].

Table 1 Hamming weight of $z^{1/3}$, where z is a root of $x^m + ax^k + b$; $l = \lceil (m-1)/3k \rceil + \lceil (m-1-k)/3k \rceil$ and $l' = \lceil (2m-1)/3k \rceil + \lceil (2m-1-k)/3k \rceil + \lceil (2m-1-2k)/3k \rceil$.

$\mathrm{wt}\left(z^{1/3}\right)$	Condition
$m \not\equiv -k \pmod 3$	
3	$m \equiv k \equiv 1 \pmod 3$
2	$m \equiv k \equiv 2 \pmod 3$
3	$m \neq 3k$, $k \neq 1$
1	$m = 3k$, $a = 1$
2	$m = 3k$, $a = -1$
2	$k = 1$
≤ 5	$m \equiv 0 \pmod 3$, $k \equiv 2 \pmod 3$
$\in \{l, l+1, l+2\}$	$m \equiv 1 \pmod 3$, $k \equiv 0 \pmod 3$
$\in \{l', l'+1, l'+2, l'+3\}$	$m \equiv 2 \pmod 3$, $k \equiv 0 \pmod 3$
$m \equiv -k \pmod 3$	
$\in \{m/d-2, m/d-1, m/d\}$	$d = \gcd(m, k)$

In this paper, we consider the pth root computation using a polynomial basis in finite fields of odd characteristic p, $p \geq 5$, by using a binomial reduction polynomial[1]. There appears to be some recent interest in cryptographic applications using characteristic p, $p \geq 5$, see [6, 11]. Since we use binomials, we begin by providing a condition on the existence of irreducible binomials over $\mathbb{F}_q$, where q is a power of an odd prime p, $p \geq 5$. Then we explicitly compute the 5th root of an element in extensions of $\mathbb{F}_5$ formed by using an irreducible binomial. We generalize our results to compute pth roots in any finite field $\mathbb{F}_q^m$ of odd characteristic p such that an irreducible binomial of degree m over $\mathbb{F}_q$ exists. In every case we show that $\mathrm{wt}\left(z^{1/p}\right) = 1$, where z is a root of the irreducible binomial.

2 Existence of Irreducible Binomials

For efficient finite field arithmetic using a polynomial representation it is desirable to use reduction polynomials with as few non-zero terms as possible. In characteristic two

[1] Without loss of generality, all binomials considered in this paper are monic.

there is only one irreducible binomial, $x+1$, and therefore the use of trinomials is desirable. Swan [10] showed that irreducible trinomials are permitted in characteristic two for approximately half of all degrees, see also [9]. In higher characteristic, in principle it is possible for irreducible binomials to exist. The following is a sufficient and necessary condition on the existence of irreducible binomials in finite fields of odd characteristic, see [7, Theorem 3.75].

Theorem 1 *Let q be a prime power, let $f(x) = x^m - a$ be a binomial over $\mathbb{F}_q$, $m \geq 2$, and let e be the multiplicative order of a. Then f is irreducible if and only if*

(1) $\gcd((q-1)/e, m) = 1$*,*
(2) each prime factor of m divides e,
(3) if $m \equiv 0 \pmod 4$ then $q \equiv 1 \pmod 4$.

We observe that irreducible binomials over $\mathbb{F}_q$ may only exist for certain degrees m. Consider an irreducible binomial $f(x) = x^m - a$, $m \geq 2$, over $\mathbb{F}_3$. Then, $a \neq 1$ since otherwise 1 is a root of f. We apply Theorem 1 with $q = 3$ and $a = 2$. Condition (1) is always satisfied and Condition (2) gives that m is a power of two. Combining this with Condition (3) gives that there is only one nonlinear irreducible binomial over $\mathbb{F}_3$, namely $x^2 - 2$.

We now consider Theorem 1 for a general q to determine for which degrees m we find irreducible binomials over $\mathbb{F}_q$.

Theorem 2 *Let $\mathbb{F}_q$ be a finite field of odd characteristic p, $p \geq 5$. There exists an irreducible binomial over $\mathbb{F}_q$ of degree m, $m \not\equiv 0 \pmod 4$, if and only if every prime factor of m is also a prime factor of $q-1$. For $m \equiv 0 \pmod 4$ then there exists an irreducible binomial over $\mathbb{F}_q$ of degree m if and only if $q \equiv 1 \pmod 4$ and every prime factor of m is also a prime factor of $q-1$.*

Proof Let $\mathbb{F}_q$ be a finite field of odd characteristic p, $p \geq 5$. We analyze the conditions of Theorem 1 to determine for which degrees m there exist an irreducible binomial. Condition (3) of Theorem 1 gives that irreducible binomials of degree $m \equiv 0 \pmod 4$ exist only for $q \equiv 1 \pmod 4$. Since $\mathbb{F}_q^*$ is cyclic, for every divisor e of $q-1$ there is an element of multiplicative order e, namely $\alpha^{(q-1)/e}$ where α is a primitive element of $\mathbb{F}_q^*$. By Condition (2) each prime factor of m must divide the multiplicative order of the constant term $a \in \mathbb{F}_q$, $a \neq 0$, so we need only consider degrees m whose prime factors divide $q-1$. Let $q-1 = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$, then $m = p_{s_1}^{l_1} \cdots p_{s_t}^{l_t}$ where $t \leq r$ and $\{p_{s_1}, p_{s_2}, \ldots, p_{s_t}\} \subseteq \{p_1, p_2, \ldots, p_r\}$. We construct the element

$$a = \alpha^{\frac{q-1}{p_{s_1}^{e_{s_1}} \cdots p_{s_t}^{e_{s_t}}}},$$

where α is a primitive element of $\mathbb{F}_q^*$. Then a has order $e = p_{s_1}^{e_{s_1}} \cdots p_{s_t}^{e_{s_t}}$ so $\gcd(q-1/e, m) = 1$ and Condition (1) of Theorem 1 is satisfied. ■

Table 2 gives a list of degrees m for which irreducible binomials over $\mathbb{F}_q$ exist, for $q < 50$. We observe that the proof of Theorem 2 not only provides the possible degrees m such that irreducible binomials exist but also gives the elements $a \in \mathbb{F}_q$ such that $x^m - a$ is an irreducible binomial. Using Theorem 2, it is trivial to find infinite families of irreducible binomials for finite fields $\mathbb{F}_q$ with odd characteristic $p \geq 5$ and $q > 50$.

Table 2 Degrees m for which there exists an irreducible binomial over $\mathbb{F}_q$, $q < 50$.

q	m	q	m
3	2	25	$2^{k_1}3^{k_2}$
5	2^k	27	$2^{k_1}13^{k_2}$, $m \not\equiv 0 \pmod 4$
7	$2^{k_1}3^{k_2}$, $m \not\equiv 0 \pmod 4$	29	$2^{k_1}7^{k_2}$
9	2^k	31	$2^{k_1}3^{k_2}5^{k_3}$, $m \not\equiv 0 \pmod 4$
11	$2^{k_1}5^{k_2}$, $m \not\equiv 0 \pmod 4$	37	$2^{k_1}3^{k_2}$
13	$2^{k_1}3^{k_2}$	41	$2^{k_1}5^{k_2}$
17	2^{k_1}	43	$2^{k_1}3^{k_2}7^{k_3}$, $m \not\equiv 0 \pmod 4$
19	$2^{k_1}3^{k_2}$, $m \not\equiv 0 \pmod 4$	47	$2^{k_1}23^{k_2}$, $m \not\equiv 0 \pmod 4$
23	$2^{k_1}11^{k_2}$, $m \not\equiv 0 \pmod 4$	49	$2^{k_1}3^{k_2}$

However, we note that for any odd characteristic p there are many degrees m for which there are no irreducible binomial over $\mathbb{F}_q$. We return to this issue in the conclusions.

We use irreducible binomials as reduction polynomials to develop a method for efficient pth root computation in finite fields $\mathbb{F}_q$ of odd characteristic p, $p \geq 5$, using a polynomial basis. Our method can be employed in any extension $\mathbb{F}_{q^m}$ of $\mathbb{F}_q$ such that an irreducible binomial of degree m over $\mathbb{F}_q$ exists, as given by Theorem 2.

3 Using Binomials to Compute pth Roots in Finite Fields of Odd Characteristic p.

3.1 Computing 5th roots in $\mathbb{F}_{5^m}$

By Theorem 2 for $q = p = 5$, irreducible binomials over $\mathbb{F}_5$ only exist of the form $x^m - a$ for $m = 2^k$. To compute the fifth root of an element in finite fields of characteristic five we follow the folklore algorithm, as in [2]. Let $m = 2^k, k \geq 1$ and let $c \in \mathbb{F}_{5^m}$, then $c = c^{5^m} = \left(c^{5^{m-1}}\right)^5$. We denote the fifth root of c by α, then $\alpha = c^{5^{m-1}}$, which requires at most $2(m-1)\log 5$ multiplications using repeated squaring.

Let $\{z_0, z_1, \ldots, z_{m-1}\}$ be a basis of $\mathbb{F}_{5^m}$ over $\mathbb{F}_5$ and write $c = \sum_{i=0}^{m-1} c_i z_i, c_i \in \mathbb{F}_5$. Then, we have

$$\alpha = \left(\sum_{i=0}^{m-1} c_i z_i\right)^{5^{m-1}} = \sum_{i=0}^{m-1} c_i z_i^{5^{m-1}}.$$

Using a polynomial basis we write $z_i = z^i$ and then

$$\alpha = \sum_{i=0}^{m-1} c_i \left(z^{5^{m-1}}\right)^i.$$

We split the summation into five, where each summation is over one coset modulo 5. First, let $m \equiv 1 \pmod 5$, then

$$
\begin{aligned}
\alpha = & \sum_{i=0}^{(m-1)/5} c_{5i}\left(z^{5^{m-1}}\right)^{5i} + \sum_{i=0}^{(m-6)/5} c_{5i+1}\left(z^{5^{m-1}}\right)^{5i+1} \\
& + \sum_{i=0}^{(m-6)/5} c_{5i+2}\left(z^{5^{m-1}}\right)^{5i+2} \sum_{i=0}^{(m-6)/5} c_{5i+3}\left(z^{5^{m-1}}\right)^{5i+3} \\
& + \sum_{i=0}^{(m-6)/5} c_{5i+4}\left(z^{5^{m-1}}\right)^{5i+4} \\
= & \sum_{i=0}^{(m-1)/5} c_{5i} z^i + \sum_{i=0}^{(m-6)/5} c_{5i+1}\left(z^{5^{m-1}}\right) z^i + \sum_{i=0}^{(m-6)/5} c_{5i+2}\left(z^{5^{m-1}}\right)^2 z^i \\
& + \sum_{i=0}^{(m-6)/5} c_{5i+3}\left(z^{5^{m-1}}\right)^3 z^i + \sum_{i=0}^{(m-6)/5} c_{5i+4}\left(z^{5^{m-1}}\right)^4 z^i \\
= & \sum_{i \equiv 0 \bmod 5} c_i z^{i/5} + z^{1/5}\left(\sum_{i \equiv 1 \bmod 5} c_i z^{(i-1)/5}\right) + z^{2/5}\left(\sum_{i \equiv 2 \bmod 5} c_i z^{(i-2)/5}\right) \\
& + z^{3/5}\left(\sum_{i \equiv 3 \bmod 5} c_i z^{(i-3)/5}\right) + z^{4/5}\left(\sum_{i \equiv 4 \bmod 5} c_i z^{(i-4)/5}\right).
\end{aligned}
$$

For $m \equiv 2,3,4 \pmod 5$ the computation is similar, with the only change being over the range of the summation. We define the vectors d_0, d_1, d_2, d_3, d_4 to be each respective summation so that $\alpha = d_0 + z^{1/5}d_1 + \cdots + z^{4/5}d_4$. We show how to precompute $z^{1/5}, z^{2/5}, z^{3/5}, z^{4/5}$ exploiting the binomial reduction polynomial f.

Let $f(x) = x^m - b$ be an irreducible binomial over $\mathbb{F}_5$. Then $b = 2,3$ by Theorem 2. If $m \equiv j \pmod 5$ then $m = 5u + j$ and $z^m - b = z^{5u+j} - b = 0$. Thus, $z^u z^{j/5} = b$, and $-bz^u = z^{-j/5}$ since for $b = 2,3 \in \mathbb{F}_5, (b)^{-1} = -b$. Let e be the smallest positive integer such that $ej \equiv -1 \pmod 5$, then $(-b)^e z^{eu} = z^{-ej/5}$, and

$$z^{1/5} = (-b)^e z^{eu+(ej+1)/5}.$$

The Hamming weight of $z^{1/5}$ is 1 in all cases. We give all values of e and j and note, in particular, that $eu + (ej+1)/5 < m$:

e	j	$(ej+1)/5$
1	4	1
2	2	1
3	3	2
4	1	1

We follow the notation and language introduced by Ahmadi et al. [1]: we denote by $\gg s$ a cyclic right bit shift by s positions. Let $\gamma = eu + (ej+1)/5$. Since $z^m = b$, the shift introduces a new scaling by b every time a bit cycles from the $(m-1)$th to the 0th position. We express α by

$$\alpha = d_0 + (-b)^e d_1^{\gg\gamma} + (-b)^{2e} d_2^{\gg 2\gamma} + (-b)^{3e} d_3^{\gg 3\gamma} + (-b)^{4e} d_4^{\gg 4\gamma}. \tag{1}$$

The computation of α is sped by the precomputation and storage of the coefficients introduced before each d_k term in Equation (1). The precise value of these coefficients is determined by the value of γ, that is, by the total number of shifts introduced.

Example 1 Let $q = p = 5$, then Theorem 2 gives that there exists an irreducible binomial for $m = 32 = 6 \cdot 5 + 2$. In this case $\gamma = 13$. Let $c \in \mathbb{F}_{5^{32}}$, and let $\alpha = c^{1/5}$. In the computation of α we need to perform shifts by $k\gamma$ elements, for $k = 1, 2, 3, 4$, as shown in Equation (1). For $k = 1$ the shift by γ elements introduces a scaling by b for the last γ elements of d_1. For $k = 2$ the shift by 2γ requires a single scaling by b for the last 2γ elements of d_2, since $2\gamma = 26 < m$. For $k = 3$, we need to scale each element of d_3 by b and the final $3\gamma - m$ elements of d_3 by an additional factor of b. The $k = 4$ case is the same, where each element of d_4 needs to be scaled by a factor of b and the final $4\gamma - m$ elements need to be scaled by an additional b.

In total, we need to store $(-b)^e, (-b)^{e+1}, (-b)^{2e}, (-b)^{2e+1}, (-b)^{3e+1}, (-b)^{3e+2}, (-b)^{4e+1}, (-b)^{4e+2}$, or a total of 8 elements of $\mathbb{F}_5$.

We always have a storage requirement associated with 8 computations of elements in $\mathbb{F}_5$, though the precise values needed depend on the value of γ.

The fifth-root computation of c, $c \in \mathbb{F}_{5^m}$, requires in total, after a precomputation of 8 elements, at most $4\lceil m/5 \rceil$ additions in $\mathbb{F}_{5^m}$ in the case where the shifts cause every vector to be aligned in the same position modulo 5, and 4 scalar multiplications of elements in $\mathbb{F}_{5^m}$ by elements in $\mathbb{F}_5$. If $\gamma \equiv 0 \pmod 5$ no addition is required.

3.2 The General Case

The technique presented for the $q = p = 5$ case generalizes naturally to all $q \geq 5$.

Theorem 3 *Let q be a power of an odd prime p and let m be a positive integer such that there exists an irreducible binomial $x^m - b$ over $\mathbb{F}_q$, as given by Theorem 2. Let e be the multiplicative order of $b \in \mathbb{F}_q$. After a precomputation of $2(p-1)$ elements in $\mathbb{F}_q$, the pth root of an element $c \in \mathbb{F}_{q^m}$ requires $p-1$ scalar multiplications of elements in $\mathbb{F}_{q^m}$ by elements in $\mathbb{F}_q$. In addition, the computation requires at most $(p-1)\lceil m/p \rceil$ additions in $\mathbb{F}_{q^m}$.*

Proof Let q be a power of an odd prime p and let m be a positive integer such that there exists an irreducible binomial of degree m over $\mathbb{F}_q$. Suppose we know the factorization of m; this is not a problem in practice since m is small in applications. Then using Theorem 2 we find an irreducible binomial over $\mathbb{F}_q$ of degree m.

Suppose $f(x) = x^m - b$ is irreducible over $\mathbb{F}_q$. Let $c \in \mathbb{F}_{q^m}$, and let $\alpha = c^{1/p}$. Let z be a root of f; then $\{1, z, z^2, \ldots, z^{m-1}\}$ form a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$. We write

$$c = \sum_{i=0}^{m-1} c_i z^i$$

and follow the same process as above. If C_j is the jth coset of $\mathbb{Z}_m$ modulo p, so that for $i \in C_j$, $i - j \equiv 0 \pmod p$, then

$$\alpha = \sum_{j=0}^{p-1} z^{j/p} \sum_{i \in C_j} c_i z^{(i-j)/p}.$$

Let $d_i = \sum_{i \in C_j} c_i z^{(i-j)/p}$ and hence we have

$$\alpha = d_0 + z^{1/p} d_1 + \cdots + z^{(p-1)/p} d_{p-1}.$$

What remains is to precompute $z^{1/p}, z^{2/p}, \ldots, z^{(p-1)/p}$.

If $m \equiv j \pmod p$ then $m = pu + j$ and $z^m - b = z^{pu+j} - b = 0$. Thus, $z^u z^{j/p} = b$. Then, $b^{-1} z^u = z^{-j/p}$. Let e be the smallest positive integer such that $ej \equiv -1 \pmod p$, then $b^{-e} z^{eu} = z^{-ej/p}$, and

$$z^{1/p} = b^{-e} z^{eu+(ej+1)/p}.$$

The Hamming weight of $z^{1/p}$ is 1 in all cases.

As before, we denote $\gg s$ to be a right bit shift by s positions. Let $\gamma = eu+(ej+1)/p$, then

$$\alpha = d_0 + b^{-e} d_1^{\gg\gamma} + \cdots + b^{-(p-1)e} d_{p-1}^{\gg(p-1)\gamma}.$$

Since $z^m = b$, as before, the shift introduces a new scaling by b for each time a bit cycles from the $(m-1)$th to the 0th position. Since $\gamma = eu + (ej+1)/p$, we have that

$$p\gamma = peu + ej + 1 = e(pu + j) + 1 = em + 1,$$

and so $\gamma = (em+1)/p < m$. For any positive integer $k \leq p-1$, if $k\gamma = tm + i$, where $0 \leq i < m$, then the shift of d_k by $k\gamma$ elements introduces a scalar multiplication by b^t for the first $m - i$ elements of d_k and a multiplication by b^{t+1} for the final i elements of d_k. The computation of α is sped by the precomputation of all the b^{-ke+t} and $b^{-ke+t+1}$, where $1 \leq k \leq p-1$ and t is given by $k\gamma = tm + i$. Hence, this requires in total a precomputation of $2(p-1)$ elements in $\mathbb{F}_q$.

Each sum d_j has non-zero terms only on the $j \pmod p$ positions, so if $\gamma \equiv 0 \pmod p$, no additions are performed. Otherwise, in the worst case we can assume that each sum is shifted to align with the first position, creating $p-1$ additions of sums with at most $\lceil m/p \rceil$ terms. The ceiling function is used to cover every case regardless of the value of $m \pmod p$.

Thus, after precomputation, the pth root operation using a binomial reduction polynomial requires $p-1$ scalar multiplications of elements in $\mathbb{F}_{q^m}$ by elements in $\mathbb{F}_q$. In addition, the computation requires at most $(p-1)\lceil m/p \rceil$ additions in the extension field. If $\gamma \equiv 0 \pmod p$ then there is no addition required. ∎

4 Conclusions

We present a method for computing pth roots of elements in finite fields $\mathbb{F}_{q^m}$ of odd characteristic p, $p \geq 5$, by taking advantage of the structure introduced by using an irreducible binomial of degree m as the reduction polynomial. The computational cost of our method requires $p-1$ scalar multiplications of elements in $\mathbb{F}_{q^m}$ by elements in $\mathbb{F}_q$. In addition, the computation requires at most $p-1\lceil m/p \rceil$ additions in the extension field. Our method also requires a precomputation of $2(p-1)$ elements in $\mathbb{F}_q$.

We relate our result in higher characteristic to the work of Barreto [2] and Ahmadi et al. [1] using trinomials in characteristic 3. Ahmadi et al. show that the Hamming weight of $x^{1/3}$, where x is a root of an irreducible trinomial over $\mathbb{F}_3$, is greater than

1 in almost all cases. In every case we show that the Hamming weight of $z^{1/p}$, where z is a root of an irreducible binomial over a finite field of odd characteristic $p \geq 5$, is always equal to 1.

Theorem 2 determines for which degrees m we have irreducible binomials over $\mathbb{F}_q$. Our method of root computation is applicable wherever such a binomial exists. In the absence of irreducible binomials over $\mathbb{F}_q$, what remains for further work is to find the lowest weight irreducible polynomial of a given degree m. In these cases, the pth roots may be computed using the so-called folklore algorithm, as above and in [1, 2]. Then, explicit forms for $z^{1/p}$ can be found, where z is a root of the irreducible polynomial. When there are many irreducible polynomials with the smallest number of nonzero terms, the one the one which yields the lowest weight of $z^{1/p}$ is preferred to minimize the computational cost.

References

1. O. Ahmadi, A. Menezes and D. Hankerson, Formulas for cube roots in $\mathbb{F}_{3^m}$, Discrete Applied Mathematics, Vol. 155 (2007), pp. 260-270.
2. P. S. L. M. Barreto, A note on efficient computation of cube roots in characteristic 3, Cryptology ePrint Archive, no. 2004/305 (2004).
3. P. S. L. M. Barreto, B. Lynn and M. Scott, Efficient implementation of pairing-based cryptosystems, Journal of Cryptology, Vol. 17 (2004), pp. 321-334.
4. I. M. Duursma and H.-S. Lee, Tate pairing implementation for Hyperelliptic Curves $y^2 = x^p - x + d$, Asiacrypt 2003, LNCS 2894, Springer-Verlag (2003), pp 111-123.
5. J. von zur Gathen and D. Panario, A survey on factoring polynomials over finite fields, Journal of Symbolic Computation, Vol. 31, (2001), pp 3-17.
6. R. Harasawa, Y. Sueyoshi and A. Kudo, Ate pairing for $y^2 = x^5 - \alpha x$ in characteristic five, Cryptology ePrint archive, no. 2006/202 (2006).
7. R. Lidl and H. Neiderreiter, Finite Fields (2nd ed.), Cambridge University Press, Cambridge UK. 1997.
8. A. Menezes, P. van Oorschot and S. Vanstone, Handbook of Applied Cryptography, CRC Press, 1996.
9. G. Seroussi, Table of low-weight irreducible polynomials, HP Labs Technical Report, no. HPL-98-135 (1998).
10. R. G. Swan, Factorization of polynomials over finite fields, Pacific Journal of Mathematics, Vol. 12, no. 3 (1962), pp 1099-1106.
11. K. Wang and B. Li, Computation of Tate pairing for supersingular curves over characteristic 5 and 7, Cryptology ePrint Archive, no. 2005/374 (2005).