Designs, Codes and Cryptography, 28, 33–44, 2003

Short Polynomial Representations for Square Roots Modulo *p*

SIMON JOSEPH AGOU sjagou@aviion.univ-lemans.fr
Département de Mathématiques, Université du Maine, Avenue Olivier Messiaen, F-72085 Le Mans Cédex, France

MARC DELÉGLISE deleglis@desargues.univ-lyon1.fr
Institut Girard Desargues, Mathématiques, Bâtiment J. Braconnier, Université Claude Bernard (Lyon 1), F-69622 Villeurbanne Cédex, France

JEAN-LOUIS NICOLAS* jlnicola@in2p3.fr
Institut Girard Desargues, Mathématiques, Bâtiment J. Braconnier, Université Claude Bernard (Lyon 1), F-69622 Villeurbanne Cédex, France

Communicated by: S. Gao

Received February 15, 2001; Revised October 3, 2001; Accepted October 24, 2001

Abstract. Let p be an odd prime number and a a square modulo p. It is well known that the simple formula $a^{\frac{p+1}{4}} \bmod p$ gives a square root of a when $p \equiv 3 \bmod 4$. Let us write $p-1 = 2^n s$ with s odd. A fast algorithm due to Shanks, with n steps, allows us to compute a square root of a modulo p. It will be shown that there exists a polynomial of at most 2^{n-1} terms giving a square root of a. Moreover, if there exists a polynomial in a representing a square root of a modulo p, it will be proved that this polynomial would have at least 2^{n-1} terms, except for a finite set $\mathcal{P}_n$ of primes p depending on n.

Résumé. Soit p un nombre premier impair et a un carré modulo p. La formule très simple $a^{\frac{p+1}{4}} \bmod p$ fournit une valeur de la racine carrée de a lorsque $p \equiv 3 \bmod 4$. Plus généralement, si l'on écrit $p-1 = 2^n s$ avec s impair, un algorithme dû à Shanks, comprenant n étapes, permet de calculer la racine carrée de a modulo p. Nous montrerons qu'il existe un polynôme d'au plus 2^{n-1} termes et dont la valeur est une racine carrée de a pour tout carré a. De plus, pour n fixé, nous démontrons que tout polynôme en a représentant la racine carrée de a modulo p a au moins 2^{n-1} termes, excepté pour un ensemble fini $\mathcal{P}_n$ de nombres premiers $p \equiv 1 \pmod{2^n}$.

Keywords: square root mod p, Shanks algorithm, finite fields

AMS Classification: 12E20, 68W40

1. Introduction

Any function f from a finite field K into itself is a polynomial the value of which can be obtained by Lagrange interpolation formula or by Chevalley's trick (cf. [7], p. 272):

$$f(X) = \sum_{t \in K} f(t)(1-(X-t)^{q-1})$$

*Research partially supported by CNRS, Institut Girard Desargues, UPRES-A 5028 and Région Rhône-Alpes, contract 99 029744.

where q is the number of elements of K. In [9] and [10], the authors considered polynomials representing the discrete logarithm on a finite field $GF(q)$. In the present paper, we wish to investigate the function *square root;* we shall restrict ourselves to the fields $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, with p an odd prime. It would be possible to study, in the same way, cubic roots and more generally, k-th roots, for $k > 2$ (cf. [1]).

Let $p \neq 2$ be a prime number. It is well known that there are $\frac{p-1}{2}$ quadratic residues a in $\mathbb{F}_p^* = \{1, 2, \ldots, p-1\}$ which can be obtained by the congruence involving the Legendre symbol

$$1 = \left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}. \tag{1}$$

We shall denote by $\sqrt{a}$ to be one of the square roots of a. The two square roots of a square $a \neq 0$ will be denoted by $\pm\sqrt{a}$.

We shall say that a polynomial $P(X) \in \mathbb{F}_p[X]$ represents the square root in $\mathbb{F}_p^*$ if, for all quadratic residues $a \in \mathbb{F}_p^*$, the relation $(P(a))^2 = a$ (i.e., $P(a) = \pm\sqrt{a}$) holds or, equivalently

$$\forall t \in \mathbb{F}_p^*, \qquad (P(t^2))^2 = t^2. \tag{2}$$

It is easy to see that $\mathbb{F}_p^*$ can be replaced by $\mathbb{F}_p$ in (2). This means that an additional restriction on P, namely $P(0) = 0$ is to be imposed. However this is not a serious restriction: if P satisfies (2), the polynomial

$$\hat{P}(X) = P(X) + \left(X^{\frac{p-1}{2}} - 1\right) P(0) \tag{3}$$

also satisfies (2) and moreover $\hat{P}(0) = 0$.

In Section 2, we shall prove the following theorem.

THEOREM 1. *Let p be an odd prime number. Let us call S_p the set of vectors $\boldsymbol{\sigma} = (\sigma_1, \sigma_2, \ldots, \sigma_{\frac{p-1}{2}})$ such that $\sigma_i \in \{-1, +1\}$ for all i (so, there are $2^{(p-1)/2}$ vectors $\boldsymbol{\sigma} \in S_p$).*

(i) For every vector $\boldsymbol{\sigma} \in S_p$, there exists one and only one polynomial $P_{\boldsymbol{\sigma}} \in \mathbb{F}_p[X]$ such that

$$\text{for } 1 \leq i \leq \frac{p-1}{2}, \quad P_{\boldsymbol{\sigma}}(i^2) = \sigma_i i \tag{4}$$

and

$$\deg(P_{\boldsymbol{\sigma}}) \leq \frac{p-3}{2}. \tag{5}$$

The value of $P_{\boldsymbol{\sigma}}$ is given by

$$P_{\boldsymbol{\sigma}}(X) = -2 \sum_{k=0}^{(p-3)/2} \left(\sum_{j=1}^{(p-1)/2} \sigma_j j^{1-2k} \right) X^k \bmod p. \tag{6}$$

(ii) Let $P(X) = \sum_{k=0}^{(p-3)/2} c_k X^k$ be a polynomial in $\mathbb{F}_p[X]$ of degree at most $(p-3)/2$ and representing the square root in $\mathbb{F}_p^*$. Then there exists a vector $\boldsymbol{\sigma} \in S_p$ such that $P = P_{\boldsymbol{\sigma}}$.

Moreover, for $1 \le i \le (p-1)/2$,

$$\sigma_i \equiv i \sum_{k=0}^{(p-3)/2} (\tau(i))^{2-2k} c_k \pmod{p} \tag{7}$$

where $\tau(i)$ *is the only integer* j *such that* $(ij)^2 \equiv 1 \pmod{p}$ *and* $1 \le j \le (p-1)/2$.

(iii) Any polynomial $\hat{P} \in \mathbb{F}_p[X]$ *representing the square root in* $\mathbb{F}_p^*$ *can be written as*

$$\hat{P}(X) = P_{\sigma}(X) + \left(X^{\frac{p-1}{2}} - 1\right) H(X) \tag{8}$$

where σ *belongs to* S_p *and* H *is some polynomial in* $\mathbb{F}_p(X)$. *Conversely, any polynomial* $\hat{P}$ *defined by (8) where* H *is any polynomial in* $\mathbb{F}_p(X)$ *represents the square root in* $\mathbb{F}_p^*$.

The computation of polynomials P_{σ} for small primes shows that most of these polynomials do have many non zero coefficients. However, there exist a few exceptions. To study this phenomenon, we introduce the following:

Definition. The length of a polynomial P denoted by $\ell(P)$ is the number of non zero terms occuring in the polynomial. So, the monomials are the polynomials of length 1, the binomials the polynomials of length 2, and so on.

The following Lemma will be useful; for instance, from (8), (5), and Lemma 1, it follows that $\ell(\hat{P}) \ge \ell(P_{\sigma})$.

LEMMA 1. *Let* $m \ge 1$ *be an integer, and* K *be a field. Then, for any polynomial* $A \in K[X]$, *the inequality* $\ell(A) \ge \ell(R)$ *holds, where* R *is the remainder in the Euclidean division of* $A(X)$ *by* $X^m - 1$.

Proof of Lemma 1. First, we observe that the remainder in the division of X^k by $X^m - 1$ is $X^{\bar{k}}$ where $\bar{k}$ is the remainder in the division of k by m. Therefore, if $A(X) = \sum_i a_{k_i} X^{k_i}$, we shall have $R(X) = \sum_i a_{k_i} X^{\overline{k_i}}$, and clearly, $\ell(R) \le \ell(A)$ holds which completes the proof of Lemma 1. ∎

The explicit calculation of the square root in $\mathbb{F}_p^*$ plays nowadays an important role in cryptography (cf. [5] or [11]). Up to now, there does not seem to exist a good deterministic algorithm to compute a square root modulo p (cf. [12]) but there is a very fast probabilistic algorithm which was established by Lehmer (cf. [6]) and whose present form is due to Shanks (cf. [3] and [2]).

When $p \equiv 3 \pmod 4$ this algorithm works as follows: if a is a square modulo p then $a^{\frac{p+1}{4}} \bmod p$ is a square root of a modulo p. So, in this case, there is a monomial which does represent the square root in $\mathbb{F}_p^*$ (see the application at the end of Section 2).

More generally, let us write

$$p - 1 = 2^n s \quad \text{with } s \text{ odd.} \tag{9}$$

The case $n = 1$ corresponds to $p \equiv 3 \pmod 4$. For larger n, Shanks's algorithm encompasses n steps, and works as follows (cf. [2] or [11]). Let b be a non residue modulo p. The

following sequence of congruences is built

$$a^{\alpha_i} b^{\beta_i} \equiv 1 \pmod{p}, \quad i = 1, \ldots, n$$

with $\alpha_i = (p-1)/2^i$, β_i even, $\beta_1 = 0$ and n is defined by (9). Whenever $i < n$, the value of β_{i+1} is obtained in the following way: the value of

$$\varepsilon_i = a^{\alpha_i/2} b^{\beta_i/2}$$

is equal to ± 1. If $\varepsilon_i = +1$, then $\beta_{i+1} = \beta_i/2$. If $\varepsilon_i = -1$, then $\beta_{i+1} = \beta_i/2 + (p-1)/2$. From the definition of n, α_n is odd, and the square roots of a are $\pm a^{\frac{\alpha_n+1}{2}} b^{\beta_n/2}$.

It is possible to modify this algorithm to find a polynomial of length at most 2^{n-1} and representing the square root in $\mathbb{F}_p^*$. For instance, if $n = 2$ (then, it follows from (9) that $p \equiv 5 \pmod 8$), the above algorithm distinguishes two cases: $\varepsilon_1 = a^{\frac{p-1}{4}} = \pm 1$. If $\varepsilon_1 = +1$, the square root is equal to $a^{\frac{\alpha_2+1}{2}} = a^{\frac{p+3}{8}}$, while, if $\varepsilon_1 = -1$, it is equal to $a^{\frac{\alpha_2+1}{2}} b^{\beta_2/2} = a^{\frac{p+3}{8}} b^{\frac{p-1}{4}}$. Both cases are covered in the formula:

$$\begin{aligned}\sqrt{a} &= \pm\frac{1}{2}\left(a^{\frac{p+3}{8}}\left(a^{\frac{p-1}{4}}+1\right) + a^{\frac{p+3}{8}} b^{\frac{p-1}{4}}\left(a^{\frac{p-1}{4}}-1\right)\right) \\ &= \pm\left(\left(\frac{1+b^{\frac{p-1}{4}}}{2}\right) a^{\frac{3p+1}{8}} + \left(\frac{1-b^{\frac{p-1}{4}}}{2}\right) a^{\frac{p+3}{8}}\right) \end{aligned} \tag{10}$$

which is a binomial on a. Let us observe that $b^{\frac{p-1}{4}}$ is a primitive fourth root of unity. It can take two different values, so that, formula (10) yields 4 binomials representing the square root in $\mathbb{F}_p^*$.

We shall prove in Section 3.

THEOREM 2. *Let $r \geq 1$ and p be a prime such that*

$$p \equiv 2r + 1 \pmod{4r}. \tag{11}$$

Then there exists at least 2^r polynomials $P \in \mathbb{F}_p[X]$ of degree $\deg(P) \leq \frac{p-3}{2}$, of length $\ell(P) \leq r$ and representing the square root in $\mathbb{F}_p^*$.

Setting $r = 2^{n-1}$ in Theorem 2 gives Theorem 3.

THEOREM 3. *Let p be an odd prime number, and n the 2-adic valuation of $p-1$ defined by (9). Then there exists at least $2^{2^{n-1}}$ polynomials $P \in \mathbb{F}_p[X]$ of degree $\deg(P) \leq \frac{p-3}{2}$, of length $\ell(P) \leq 2^{n-1}$ and representing the square root in $\mathbb{F}_p^*$.*

In some sense, the following theorem is a converse of Theorem 3.

THEOREM 4. *Let $n \geq 1$. There exists a finite set $\mathcal{P}_n$ of prime numbers such that, for all prime p, $p \notin \mathcal{P}_n$ and $2^n \mid (p-1)$, and all $P \in \mathbb{F}_p[X]$ representing the square root in $\mathbb{F}_p^*$ (i.e., satisfying (2)), $\ell(P) \geq 2^{n-1}$ holds.*

One has: $\mathcal{P}_1 = \mathcal{P}_2 = \mathcal{P}_3 = \emptyset$; $\mathcal{P}_4 = \{17\}$.

$\mathcal{P}_5$ is much bigger; its elements will be given in Section 4 together with the proof of Theorem 4.

It is easy to show that the only monomials representing the square root in $\mathbb{F}_p^*$ and of degree at most $(p-3)/2$ are $\pm X^{(p+1)/4}$ with $p \equiv 3 \pmod 4$. It is also possible to show that the only binomials representing the square root in $\mathbb{F}_p^*$ and of degree at most $(p-3)/2$ are the four binomials given by (10) when $p \equiv 5 \pmod 8$ (the proof is similar to that of Theorem 5 below, but much easier). In Section 5, we shall prove Theorem 5 which answers a similar question about trinomials.

THEOREM 5. *Let us assume that there exists a trinomial $Q(x) \in \mathbb{F}_p[x]$ representing the square root in $\mathbb{F}_p^*$ satisfying $Q(x) = ax^\alpha + bx^\beta + cx^\gamma$ with*

$$0 \le \alpha < \beta < \gamma < (p-1)/2 \tag{12}$$

and $abc \neq 0$; then p should be of the form $12m+7$ ($m \ge 1$). Conversely, for such a prime p, there exist exactly six such trinomials given by the formulae

$$Q = \pm\tfrac{1}{3}\left[2x^{(p+5)/12} - x^{(p+1)/4} + 2x^{(5p+1)/12}\right] \tag{13}$$

or

$$Q = \pm\tfrac{1}{3}\left[(1 \mp \sqrt{-3})x^{(p+5)/12} + x^{(p+1)/4} + (1 \pm \sqrt{-3})x^{(5p+1)/12}\right] \tag{14}$$

where $\sqrt{-3}$ is any of the two square roots of -3 modulo p; for instance $\sqrt{-3} \equiv (-3)^{\frac{p+1}{4}} = (-3)^{3m+2} \pmod p$.

In [8] a somewhat similar question has been investigated.

Remark. We have not succeeded yet in extending Theorem 5 to polynomials with more than three terms. We guess that the 2^r polynomials of length at most r which are announced in Theorem 2 as representing the square root in $\mathbb{F}_p^*$ are the only ones, but our method of proving Theorem 5 becomes too technical for $r \ge 4$.

2. The Polynomials P_σ

Proof of Theorem 1, (i). Polynomials P_σ are interpolation polynomials at the points i^2, $1 \le i \le \frac{p-1}{2}$. Their existence and uniqueness are given by Lagrange's Theorem.

To prove formula (6), it suffices to prove it for $X = i^2$, $1 \le i \le \frac{p-1}{2}$. By changing the order of the summation, we get

$$-2\sum_{k=0}^{(p-3)/2}\left(\sum_{j=1}^{(p-1)/2}\sigma_j j^{1-2k}\right) i^{2k} = -2\sum_{j=1}^{(p-1)/2} j\sigma_j \sum_{k=0}^{(p-3)/2}(i/j)^{2k}.$$

But the sum in k is a sum of terms in geometric progression. For $j \neq i$, it vanishes (by Fermat's Theorem) while, for $j = i$, it is equal to $(p-1)/2$. The value of the above expression is thus $-2i\sigma_i(p-1)/2 = i\sigma_i$, in agreement with (4). ∎

Proof of Theorem 1, (ii). As P represents the square root in $\mathbb{F}_p^*$, then for all $i, 1 \le i \le \frac{p-1}{2}$, we should have $P(i^2) = \pm i$; therefore, from (i), as the degree of P is at most $(p-3)/2$, there exists $\boldsymbol{\sigma} \in S_p$ with $P = P_{\boldsymbol{\sigma}}$.

So, we have $P_{\boldsymbol{\sigma}}(X) = P(X) = \sum_{k=0}^{(p-3)/2} c_k X^k$. Let us associate to $P_{\boldsymbol{\sigma}}$ the column vector

$$D = \begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_{\frac{p-1}{2}} \end{pmatrix} = \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{\frac{p-3}{2}} \end{pmatrix}.$$

Further, let us introduce the square matrix $M = (m_{i,j})$, $1 \le i, j \le \frac{p-1}{2}$ defined by

$$m_{i,j} = -2j^{3-2i} \mod p. \tag{15}$$

It follows from (6) that

$$D = \begin{pmatrix} d_1 \\ d_2 \\ \vdots \\ d_{\frac{p-1}{2}} \end{pmatrix} = \begin{pmatrix} c_0 \\ c_1 \\ \vdots \\ c_{\frac{p-3}{2}} \end{pmatrix} = M \begin{pmatrix} \sigma_1 \\ \sigma_2 \\ \vdots \\ \sigma_{\frac{p-1}{2}} \end{pmatrix} = M\, {}^t\boldsymbol{\sigma}. \tag{16}$$

Now, let us set $A = {}^tMM = (a_{i,j})$. A simple calculation shows that

$$a_{i,j} = 4 \sum_{k=1}^{(p-1)/2} (ij)^{3-2k} \mod p. \tag{17}$$

With the definition of $\tau(i)$, it follows from (17) that

$$\text{for } j \ne \tau(i), \quad a_{i,j} = 0$$

while

$$a_{i,\tau(i)} = 4\left(\frac{p-1}{2}\right) i\tau(i) \equiv -2i\tau(i) \pmod p.$$

So, for any column vector V with components in $\mathbb{F}_p$, we have

$$AV = {}^tMM \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_{\frac{p-1}{2}} \end{pmatrix} = -2i\tau(i) \begin{pmatrix} v_{\tau(1)} \\ v_{\tau(2)} \\ \vdots \\ v_{\tau\left(\frac{p-1}{2}\right)} \end{pmatrix}. \tag{18}$$

Further, (16) and (18) yield

$${}^tMD = {}^tMM\, {}^t\boldsymbol{\sigma} = -2i\tau(i) \begin{pmatrix} \sigma_{\tau(1)} \\ \sigma_{\tau(2)} \\ \vdots \\ \sigma_{\tau\left(\frac{p-1}{2}\right)} \end{pmatrix} \tag{19}$$

which allows us to calculate

$$\sigma_{\tau(i)} = \frac{-1}{2i\tau(i)} \sum_{j=1}^{(p-1)/2} m_{j,i} d_j = \frac{-1}{2i\tau(i)} \sum_{k=0}^{(p-3)/2} m_{k+1,i} c_k$$

Observing that $\tau(\tau(i)) = i$ and $i\tau(i) = \pm 1$, the above formula in conjunction with (15) becomes

$$\sigma_i \equiv \frac{-i\tau(i)}{2} \sum_{k=0}^{(p-3)/2} m_{k+1,\tau(i)} c_k \equiv i\tau(i) \sum_{k=0}^{(p-3)/2} \tau(i)^{1-2k} c_k \pmod{p}.$$

which yields (7). ∎

Application. As an application of (7), let us try to determine the vector $\boldsymbol{\sigma}$ corresponding to the polynomial $P(a) = a^{\frac{p+1}{4}}$ when $p \equiv 3 \pmod 4$. We have, from (7),

$$\sigma_i \equiv i\tau(i)^{2-\frac{p+1}{2}} \equiv i\tau(i)\tau(i)^{-\frac{p-1}{2}} \pmod{p}$$

and since $i\tau(i) = \pm 1$ and $p \equiv 3 \pmod 4$, the Legendre symbol satisfies

$$\left(\frac{i}{p}\right)\left(\frac{\tau(i)}{p}\right) = \left(\frac{i\tau(i)}{p}\right) = i\tau(i)$$

so that

$$\sigma_i = \left(\frac{i}{p}\right)\left(\frac{\tau(i)}{p}\right)\tau(i)^{-\frac{p-1}{2}} = \left(\frac{i}{p}\right).$$

Proof of Theorem 1, (iii). By the Euclidean division

$$\hat{P}(X) = \left(X^{\frac{p-1}{2}} - 1\right)H(X) + R(X), \quad \deg(R) \le \frac{p-3}{2}.$$

By Fermat's Theorem, we have $\hat{P}(i^2) = R(i^2) = \pm i$, and so, from (i), there exists $\boldsymbol{\sigma}$ with $R = P_{\boldsymbol{\sigma}}$. Conversely, for any polynomials H and $P_{\boldsymbol{\sigma}}$, polynomial $\hat{P}$ defined by (8) represents the square root in $\mathbb{F}_p^*$. ∎

3. Existence of Short Polynomials

Proof of Theorem 2. First we observe that, since $p \equiv 1 \pmod{2r}$, there are $2r$ $2r$-th roots of unity in $\mathbb{F}_p^*$: if g is a primitive root in $\mathbb{F}_p^*$, these roots of unity are $g^s, g^{2s}, g^{3s}, \ldots, g^{2rs} = 1$, where s is equal to $(p-1)/(2r)$. Let us introduce now a family $\mathcal{Q} \subset \mathbb{F}_p[X]$ of polynomials. A polynomial Q belongs to $\mathcal{Q}$ if its degree is at most $r-1$, and if, when x is a r-th root of unity (i.e., $x = g^{2js}$ with $1 \le j \le r$), its value $Q(x)$ is the inverse of one of the square roots of x (i.e., $Q(x) = \pm g^{-js}$). From the Lagrange interpolation Theorem, there are 2^r polynomials $Q \in \mathcal{Q}$ and they satisfy

$$\text{for } x \in \mathbb{F}_p^* \quad \text{such that} \quad x^r = 1, \quad Q(x)^2 = 1/x. \tag{20}$$

Now, for $Q \in \mathcal{Q}$, let us consider the polynomial

$$P(X) = X^{\frac{p+2r-1}{4r}} Q\left(X^{\frac{p-1}{2r}}\right).$$

From (11), the exponents are integers, and

$$\deg(P) \le \frac{p+2r-1}{4r} + (r-1)\frac{p-1}{2r} = \frac{p-1}{2} - \frac{p-2r-1}{4r}. \tag{21}$$

If $p > 2r+1$, it follows from (21) that $\deg(P) \le \frac{p-3}{2}$. In the case $p = 2r+1$, we replace P by the remainder in the division of P by $X^{\frac{p-1}{2}} - 1$, which, from Lemma 1, does not increase the length. Moreover, if t belongs to $\mathbb{F}_p^*$, and $a = t^2$, then $a^{\frac{p-1}{2r}}$ is a r-th root of unity since

$$\left(a^{\frac{p-1}{2r}}\right)^r = a^{\frac{p-1}{2}} = t^{p-1} = 1$$

and, by (20),

$$(P(t^2))^2 = (P(a))^2 = a^{\frac{p+2r-1}{2r}} Q\left(a^{\frac{p-1}{2r}}\right)^2 = a^{\frac{p+2r-1}{2r}} a^{-\frac{p-1}{2r}} = a = t^2$$

so that, by (2), P represents the square root in $\mathbb{F}_p^*$, and, obviously, $\ell(P) = \ell(Q) \le r$, which completes the proof of Theorem 2. ∎

Remark. If Q belongs to the family $\mathcal{Q}$, then trivially, $-Q$ also belongs to it. This family possesses another symmetry: if

$$Q(X) = q_0 + q_1 X + q_2 X^2 + \cdots + q_{r-1} X^{r-1}$$

belongs to $\mathcal{Q}$, then the polynomial

$$\tilde{Q}(X) = q_{r-1} + q_{r-2} X + \cdots + q_1 X + q_0 = X^{r-1} Q\left(\frac{1}{X}\right)$$

by (20) also belongs to $\mathcal{Q}$.

4. Not Too Short Polynomials

Proof of Theorem 4. Let $P \in \mathbb{F}_p[X]$ be a polynomial representing the square root in $\mathbb{F}_p^*$, i.e., satisfying (2). Let w be a primitive 2^n-th root of unity in $\mathbb{F}_p$ (since $2^n \mid (p-1)$, such a root does exist). From (2), we have

$$(P(w^{2i}))^2 = w^{2i}, \quad 0 \le i \le 2^{n-1} - 1 \tag{22}$$

whence $P(w^{2i}) = \varepsilon_i w^i$ with $\varepsilon_i \in \{-1, 1\}$. Let us define $R(X)$ as the interpolation polynomial of the polynomial P on the points w^{2i}, $0 \le i \le 2^{n-1} - 1$. The classical Lagrange's calculation gives

$$R(X) = \sum_{i=0}^{2^{n-1}-1} \frac{X^{2^{n-1}} - 1}{X - w^{2i}} \frac{w^{2i}}{2^{n-1}} \varepsilon_i w^i. \tag{23}$$

As both polynomials P and R coincide on the 2^{n-1}-th roots of unity, there exists a polynomial H such that

$$P(X) = R(X) + \left(X^{2^{n-1}} - 1\right) H(X). \tag{24}$$

From Lemma 1 with $m = 2^{n-1}$, we have $\ell(P) \geq \ell(R)$, and, in order to prove Theorem 4, it suffices to show

$$\ell(R) \geq 2^{n-1}. \tag{25}$$

Further, let us calculate, from (23), the coefficients of R. By expanding

$$X^{2^{n-1}} - 1 = X^{2^{n-1}} - (w^{2i})^{2^{n-1}} = (X - w^{2i}) \sum_{h=0}^{2^{n-1}-1} X^h w^{2i(2^{n-1}-1-h)}$$

we get

$$R(X) = \frac{1}{2^{n-1}} \sum_{h=0}^{2^{n-1}-1} \sum_{i=0}^{2^{n-1}-1} X^h \varepsilon_i w^{i(1-2h)} = \frac{1}{2^{n-1}} \sum_{h=0}^{2^{n-1}-1} a_h X^h \tag{26}$$

with

$$a_h = \sum_{i=0}^{2^{n-1}-1} \varepsilon_i w^{i(1-2h)} = A_\varepsilon \left(w^{(1-2h)}\right) \tag{27}$$

where ε denotes the vector $\varepsilon = (\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{2^{n-1}-1})$ and A_ε the polynomial

$$A_\varepsilon(X) = \sum_{i=0}^{2^{n-1}-1} \varepsilon_i X^i. \tag{28}$$

Let $\Phi_{2^n}(X) = X^{2^{n-1}} + 1$ be the cyclotomic polynomial of index 2^n. It is well known that cyclotomic polynomials are irreducible in $\mathbb{Q}(X)$, and since the degree of A_ε is, from (28), smaller than the degree of Φ_{2^n}, the resultant $\mathrm{Res}(A_\varepsilon, \Phi_{2^n})$, calculated in $\mathbb{Z}$, is a non zero constant K_ε. If the coefficient a_h vanishes in $\mathbb{F}_p$, $w^{(1-2h)}$, which is a root of Φ_{2^n}, is also, by (27), a root of A_ε in $\mathbb{F}_p$. So, $\mathrm{Res}(A_\varepsilon, \Phi_{2^n})$ calculated in $\mathbb{F}_p$ should vanish and this means that p divides K_ε . So, we have to consider the product, or more precisely the least common multiple, of all these constants K_ε for all the 2^{n-1} possible values of ε:

$$\begin{aligned}\Pi_n &= \mathrm{l\,cm}\left\{K_\varepsilon;\, \varepsilon = (\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{2^{n-1}-1}) \in \{-1, +1\}^{2^{n-1}}\right\} \\ &= \mathrm{l\,cm}\left\{\mathrm{Res}(A_\varepsilon, \Phi_{2^n});\, \varepsilon = (\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{2^{n-1}-1}) \in \{-1, +1\}^{2^{n-1}}\right\}.\end{aligned}$$

If p does not divide Π_n, no coefficient a_h, $0 \leq h \leq 2^{n-1} - 1$, can vanish in $\mathbb{F}_p$ and, from (26), formula (25) holds. So, Theorem 4 is proved, by choosing for $\mathcal{P}_n$ the set of prime factors p of Π_n satisfying $p \equiv 1 \pmod{2^n}$.

With MAPLE, we have computed Π_n for $n = 2, 3, 4, 5$:

$$\begin{aligned}
\Pi_1 &= 1\\
\Pi_2 &= 2\\
\Pi_3 &= 2^3\\
\Pi_4 &= 2^7 \times 17\\
\Pi_5 &= 2^{15} \times 17^2 \times 31^2 \times 97^2 \times 127^2 \times 193 \times 257 \times\\
&\quad 353 \times 449 \times 577 \times 641 \times 673 \times 769 \times 929 \times\\
&\quad 1153 \times 1217 \times 1249 \times 1409 \times 1601 \times 1697 \times 2017 \times\\
&\quad 2081 \times 2113 \times 2273 \times 2593 \times 2657 \times 2753 \times 3041 \times\\
&\quad 3137 \times 3329 \times 3361 \times 3457 \times 4129 \times 4481 \times 4673 \times\\
&\quad 4801 \times 4993 \times 5153 \times 5281 \times 5441 \times 6113 \times 6337 \times\\
&\quad 7297 \times 7393 \times 8513 \times 8609 \times 8737 \times 9857 \times 10273 \times\\
&\quad 11681 \times 12097 \times 12161 \times 13121 \times 13217 \times 13441 \times 13633 \times\\
&\quad 14401 \times 16417 \times 16673 \times 16993 \times 17569 \times 17761 \times 19073 \times\\
&\quad 21121 \times 21313 \times 31489 \times 35393 \times 49121 \times 49409 \times 53441 \times\\
&\quad 70529
\end{aligned}$$

The set $\mathcal{P}_5$ is the set of all prime factors of Π_5 excluding 2, 17, 31, and 127. ■

5. The Trinomials

Proof of Theorem 5. First, by setting $r = 3$ in Theorem 2, it is not difficult to see that, for $p \equiv 7 \pmod{12}$, there are at least $2^r = 8$ trinomials representing the square root in $\mathbb{F}_p^*$. Actually, if we carry out the calculation of polynomials Q used in the proof of Proposition 1, we find exactly the 6 trinomials (13) and (14), and the two last ones are the monomials $\pm X^{\frac{p+1}{4}}$. It remains to show that there are no other trinomials representing the square root in $\mathbb{F}_p^*$.

Let us suppose that $Q(X) = aX^\alpha + bX^\beta + cX^\gamma$ represents the square root in $\mathbb{F}_p^*$, we have by (2)

$$\forall t \in \mathbb{F}_p^*, \qquad (Q(t^2))^2 = t^2$$

which implies that the polynomial $(Q(X^2))^2 - X^2$ is a multiple of $X^{p-1} - 1$. The polynomial $(Q(X^2))^2 - X^2$ on expansion writes

$$a^2X^{4\alpha} + b^2X^{4\beta} + c^2X^{4\gamma} + 2abX^{2\alpha+2\beta} + 2acX^{2\alpha+2\gamma} + 2bcX^{2\beta+2\gamma} - X^2.$$

But, in the division of the monomial X^k by the binomial $X^{p-1} - 1$, the remainder is $X^{\bar{k}}$ where $\bar{k}$ is the remainder in the division of k by $p - 1$. As a consequence,

$$a^2X^{\overline{4\alpha}} + b^2X^{\overline{4\beta}} + c^2X^{\overline{4\gamma}} + 2abX^{\overline{2\alpha+2\beta}} + 2acX^{\overline{2\alpha+2\gamma}} + 2bcX^{\overline{2\beta+2\gamma}} - X^2 = 0 \tag{29}$$

Now, from (12), the three numbers $\overline{2\alpha+2\beta}$, $\overline{2\alpha+2\gamma}$ and $\overline{2\beta+2\gamma}$ are distinct. Further, among the seven terms of the left hand side of (29) there should be at most three different degrees since none of these terms vanishes and their sum does vanish. So, among these seven terms there are exactly three different degrees, $\overline{2\alpha+2\beta}$, $\overline{2\beta+2\gamma}$ and $\overline{2\beta+2\gamma}$, and

one of them is equal to 2. From (12), $\overline{4\alpha}$ cannot be equal to $\overline{2\alpha+2\beta}$ or $\overline{2\alpha+2\gamma}$; thus, we should have

$$\overline{4\alpha} = \overline{2\beta+2\gamma}$$

and, similarly,

$$\overline{4\beta} = \overline{2\alpha+2\gamma} \quad \text{and} \quad \overline{4\gamma} = \overline{2\alpha+2\beta}.$$

Finally, there is a permutation (u, v, w) of (α, β, γ) such that $\overline{4v} = \overline{2u+2w} = 2$, $\overline{4u} = \overline{2v+2w}$ and $\overline{4w} = \overline{2u+2v}$ which, after dividing by 2 can be written as a system of congruences

$$\begin{cases} u & +v & -2w \equiv 0 & \left(\text{mod } \frac{p-1}{2}\right) \\ 2u & -v & -w \equiv 0 & \left(\text{mod } \frac{p-1}{2}\right) \\ & 2v & \equiv 1 & \left(\text{mod } \frac{p-1}{2}\right) \\ u & & +w \equiv 1 & \left(\text{mod } \frac{p-1}{2}\right). \end{cases}$$

The third congruence implies that $\frac{p-1}{2}$ is odd (so that $p \equiv 3 \pmod 4$). By substracting the first congruence from the second twice we get the equivalent system

$$\begin{cases} u & +v & -2w & \equiv 0 & \left(\text{mod } \frac{p-1}{2}\right) \\ & -3v & +3w & \equiv 0 & \left(\text{mod } \frac{p-1}{2}\right) \\ & 2v & & \equiv 1 & \left(\text{mod } \frac{p-1}{2}\right) \\ u & & +w & \equiv 1 & \left(\text{mod } \frac{p-1}{2}\right) \end{cases}$$

The second congruence implies that $\frac{p-1}{2}$ is a multiple of 3. Indeed, if 3 does not divide $\frac{p-1}{2}$, we should have $v \equiv w \pmod{\frac{p-1}{2}}$, which, from (12), would imply $v = w$. So, $p \equiv 1 \pmod 6$, and since $p \equiv 3 \pmod 4$, we can write $p = 12m+7$. After simplification, the above system becomes

$$\begin{cases} u & +v & -2w \equiv 0 & (\text{mod } 6m+3) \\ & -v & +w \equiv 0 & (\text{mod } 2m+1) \\ & 2v & \equiv 1 & (\text{mod } 6m+3) \\ u & & +w \equiv 1 & (\text{mod } 6m+3) \end{cases} \tag{30}$$

The solution of (30) is $v \equiv 3m+2 \pmod{6m+3}$, $w \equiv m+1 \pmod{2m+1}$, $u \equiv 1-w \pmod{6m+3}$ and taking (12) into account, the only possibility is

$$\alpha = m+1, \quad \beta = 3m+2, \quad \gamma = 5m+3.$$

This implies $m \geq 1$, because $m = 0$ would yield $p = 7$ and $\deg Q = 3 = (p-1)/2$.

Further, in (29), let us find the sums of the monomials of degree $\overline{4\alpha}, \overline{4\gamma}$ and $\overline{4\beta}$ respectively which vanish. We get

$$a^2 + 2bc = 0, \quad c^2 + 2ab = 0, \quad b^2 + 2ac = 1. \tag{31}$$

It remains to check that, when $p = 12m+7$ (with $m \geq 1$), the system (31) on the unknowns a, b, c in $\mathbb{F}_p$, always has solutions satisfying $abc \neq 0$. By adding the three equations of (31)

we see that $a+b+c=\pm 1$. Moreover, (a, b, c) is a solution if and only if $(-a, -b, -c)$ is a solution. So, it is enough to look for solutions satisfying $a+b+c=1$, which drives us to the system

$$\begin{cases} a^2-2ab-2b^2+2b=0 \\ -2a^2-2ab+b^2+2a=1. \end{cases}$$

The resultant on a of these two equations is

$$27b^4-36b^3+6b^2+4b-1=(3b-1)^2(b-1)(3b+1).$$

For $b=1$ we get $a=0$, which does not fit, since $abc\neq 0$. For $b=-1/3$ we get $a=c=2/3$ which gives (13). For $b=1/3$ we get $\{a, c\}=\{(1-\sqrt{-3})/3, (1+\sqrt{-3})/3\}$ which gives (14). ■

References

1. S. J. Agou, *On Explicit Formulas for r-th Roots in Galois Fields GF(q)*. Rump session, Eurocrypt 1999, Praha, 2–6 May (1999).
2. L. Adleman, K. Manders and G. Miller, On taking roots in finite fields, In *Proceedings of the 20-th Annual Symposium on the Foundation of Computer Science* (1979) pp. 175–178.
3. H. Cohen, *A Course in Computational Algebraic Number Theory, Graduate Texts in Mathematics,* Vol. 138, Springer-Verlag (1993).
4. G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers,* 4th ed., Oxford, Clarendon Press (1960).
5. N. Koblitz, *A Course in Number Theory and Cryptography, Graduate Texts in Mathematics,* Vol. 114, Springer-Verlag (1987).
6. D. H. Lehmer, Computer technology applied to the theory of numbers—studies in number theory, Math. Assoc. Amer. (distributed by Prentice Hall), (1969) pp. 117–151.
7. R. Lidl and H. Niederreiter, *Finite Fields,* 2nd ed., Cambridge University Press (1997).
8. D. J. Madden and W. Y. Vélez, Polynomials that represent quadratic residues at primitive roots, *Pacific J. of Math.,* Vol. 98 (1982) pp. 123–137.
9. G. L. Mullen and D. White, A polynomial representation for logarithms in $GF(q)$, *Acta Arithmetica,* Vol. 47 (1986) pp. 255–261.
10. H. Niederreiter, A short proof for explicit formulas for discrete logarithms in finite fields, *Applicable Algebra,* Vol. 1 (1990) pp. 55–57.
11. G. Robin, *Algorithmique et cryptographie, Mathématiques et Applications,* Vol. 8, Ellipses, Paris (1991).
12. R. Schoof, Elliptic curves over finite fields and the computation of square roots modulo p, *Math. Comp.,* Vol. 44 (1985) pp. 483–494.