

# ALGORITHMS FOR FINITE FIELDS

Lecture notes - September 26<sup>th</sup>, 28<sup>th</sup> 2006.

**Problem.** Given  $a \in \mathbb{F}_q$  (with  $q$  odd) such that  $a$  is a square; find  $x$  such that  $x^2 = a$ . This is equivalent to factoring the polynomial  $x^2 - a$ . Note that  $a \in \mathbb{F}_q^*$  is a square if and only if  $a^{\frac{q-1}{2}} = 1$ .

The general techniques for polynomial solving give probabilistic polynomial time algorithms. For example, we can take the greatest common divisor

$$(x^2 - a, (x - b)^{\frac{q-1}{2}} - 1)$$

for random  $b$ . (See last lecture).

Today we will see some algorithms that are specific for square roots and outperform the general polynomial solving algorithms in some situations.

## 1 An algorithm

Let  $q \equiv 3 \pmod{4}$ . If  $a^{\frac{q-1}{2}} = 1$  then  $a^{\frac{q-1}{2}} a = a$  but  $a^{\frac{q-1}{2}} a = a^{\frac{q+1}{2}} = (a^{\frac{q+1}{4}})^2$ . Hence  $x = \pm a^{\frac{q+1}{4}}$  are the square roots of  $a$  in  $\mathbb{F}_q$ .

Note that this is a consequence of a fact that holds for every group of odd cardinality:  $|G| = m \equiv 1 \pmod{2} \Rightarrow (g^{\frac{m+1}{2}})^2 = g \forall g \in G$ . Now  $q \equiv 3 \pmod{4} \Rightarrow \#[(\mathbb{F}_q^*)^2] = \frac{q-1}{2}$  is odd.

This is a nice way to take square roots in groups of odd order. We can try to generalize this idea. Write  $q - 1 = 2^r m$  with  $m$  odd.

Since  $\mathbb{F}_q^*$  is a cyclic group, it has a unique subgroup of order  $m$ , let's call it  $G$  :

$$G = \{x \in \mathbb{F}_q^* \mid x^m = 1\}.$$

Then the following sequence is exact, and  $|\mathbb{F}_q^*/G| = 2^r$  :

$$0 \rightarrow G \hookrightarrow \mathbb{F}_q^* \rightarrow \mathbb{F}_q^*/G \rightarrow 0$$

$|\mathbb{F}_q^*/G| = 2^r$  and  $\mathbb{F}_q^* \simeq G \times \mathbb{F}_q^*/G$ .

Suppose  $c \in \mathbb{F}_q^*$  is not a square. Then using  $c$  we will have a deterministic algorithm for taking square roots in  $\mathbb{F}_q^*$  which is good if  $r$  is small. We discuss how to find  $c$  below.

Given  $a \in \mathbb{F}_q^*$  set  $e_0 = 0$ , and for  $i = 1, \dots, r$  do: if  $(ac^{-e_{i-1}})^{\frac{q-1}{2^i-1}} \neq 1$  put  $e_i = e_{i-1} + 2^{i-1}$ , otherwise,  $e_i = e_{i-1}$ . We will show below that  $ac^{-e_r} \in G$ , i.e.  $(ac^{-e_r})^m = 1$ .

**Claim.**  $e_r$  even  $\Rightarrow (ac^{-e_r})^{\frac{m+1}{2}} c^{\frac{e_r}{2}}$  is a square root of  $a$ .

*Proof.* Since  $m$  is odd and  $e_r$  is even, all the exponents in the expression are integers. Now let's take the square:

$$\begin{aligned} [(ac^{-e_r})^{\frac{m+1}{2}} c^{\frac{e_r}{2}}]^2 &= \\ (ac^{-e_r})^{m+1} c^{e_r} &= \\ (ac^{-e_r})^m (ac^{-e_r}) c^{e_r} &= \\ a(c^{-e_r} c^{e_r}) &= a \end{aligned}$$

□

**Claim.** For all  $i = 0, \dots, r$   $(ac^{-e_i})^{\frac{q-1}{2^i}} = 1$ .

*Proof.* By induction.

$i = 0$ :  $(ac^{-e_0})^{q-1} = 1$  automatically. (Nothing to be checked).

$1 \leq i \leq r-1$ :  $(ac^{-e_{i-1}})^{\frac{q-1}{2^{i-1}}} = 1$  by our inductive hypothesis. Taking square roots on both sides we obtain:

$$(ac^{-e_{i-1}})^{\frac{q-1}{2^i}} = \pm 1,$$

so there are two cases to check.

Case 1:  $= +1$ . Here  $e_i = e_{i-1}$ , so  $(ac^{-e_i})^{\frac{q-1}{2^i}} = 1$ .

Case 2:  $= -1$ . Here  $e_i = e_{i-1} + 2^{i-1}$ , so

$$\begin{aligned}
(ac^{-e_i})^{\frac{q-1}{2^i}} &= (ac^{-e_{i-1}-2^{i-1}})^{\frac{q-1}{2^i}} \\
&= (ac^{-e_{i-1}})^{\frac{q-1}{2^i}} (c^{-2^{i-1}})^{\frac{q-1}{2^i}} \\
&= (-1)c^{-\frac{q-1}{2}} \\
&= (-1)\frac{1}{-1} \quad (\text{since } c \text{ is not a square}). \\
&= 1
\end{aligned}$$

$i = r$ :  $1 = (ac^{-e_r})^{\frac{q-1}{2^r}} = (ac^{-e_r})^m$ , hence  $ac^{-e_r} \in G$ .

□

Note that we get an isomorphism

$$\begin{array}{ccc}
\mathbb{F}_q^*/G & \xrightarrow{\sim} & \mathbb{Z}/2^r\mathbb{Z} \\
a & \mapsto & e_r
\end{array}$$

The problem with this algorithm is finding  $c$ . If we assume the generalized Riemann hypothesis, for  $q$  an odd prime there exists  $c$ ,  $1 \leq c \leq 4(\log q)^2$ , with  $c^{\frac{q-1}{2}} \not\equiv 1 \pmod{q}$ . Note that if for a given  $q$  such a  $c$  doesn't exist, then this would be a counterexample to GRH. Alternatively, we can do a random search for  $c$  and each try will have a 0.5 probability of success.

Now suppose  $a \in \mathbb{F}_q$  is a square, and let  $t \in \mathbb{F}_q$  such that  $f(x) = x^2 - tx + a$  is irreducible in  $\mathbb{F}_q[x]$ . Then for  $\alpha$  a root of  $f$ ,  $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^2}$  and the norm of  $\alpha$  is given by the product of  $\alpha$  itself and its image under the Frobenius morphism, hence:

$$N_{\mathbb{F}_{q^2}/\mathbb{F}_q}(\alpha) = \alpha^{q+1} = a.$$

So  $\alpha^{\frac{q+1}{2}}$  is a square root of  $a$  in  $\mathbb{F}_{q^2}$ . Since we are assuming that  $a$  has a square root in  $\mathbb{F}_q$ , we conclude that  $\alpha^{\frac{q+1}{2}} \in \mathbb{F}_q$ .

When is  $f$  irreducible?  $x^2 - tx + a$  is irreducible iff  $t^2 - 4a$  is not a square. So again we need to find a non square in  $\mathbb{F}_q$ . We can proceed randomly to find it or sequentially if we believe GRH.

This algorithm is much faster than the previous one when  $r$ , (the 2-adic valuation of  $q$ ), is large.

## 2 Schoof's algorithm

Given  $a \in \mathbb{Z}$  and a prime  $p$ , Schoof's algorithm is a deterministic algorithm to compute a square root of  $d \pmod p$  in polynomial time in  $|d| \log p$ . It is based on a method to count rational points on elliptic curves over finite fields.

Let  $a, b \in \mathbb{F}_q$ , with  $(b, q) = 1$  and let's consider the elliptic curve over the finite field  $\mathbb{F}_q$  given by the equation  $y^2 = x^3 + ax + b$ . Thus

$$E(\mathbb{F}_{q^n}) = \{(x, y) \in \mathbb{F}_{q^n} \times \mathbb{F}_{q^n} \mid y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$$

Elliptic curves have a group structure where  $P + Q + R = \mathcal{O} \Leftrightarrow P, Q, R$  are colinear.

We know  $\#E(\mathbb{F}_q) = q + 1 - t$  where  $|t| \leq 2\sqrt{q}$ .

Schoof's algorithm computes  $\#E(\mathbb{F}_q)$  in polynomial time in  $\log q$ .

Let's say we compute the square root of  $d \pmod p$ ,  $d \in \mathbb{Z}$  and  $p$  prime. For simplicity, let's assume  $d < 0$ . (Think of  $0 < d < p$  and take  $d := d - p$ ).

We need to find an elliptic curve with complex multiplication <sup>1</sup>by  $\mathbb{Q}(\sqrt{d})$  and reduce it modulo  $p$ . We won't see here how to find such a curve, but it exists. Unfortunately, such a curve is hard to find and that's why the running time depends badly on  $|d|$ . Assume that  $E$  is such a curve.

Let  $f(x) = x^2 - tx + q$  where  $\#E(\mathbb{F}_q) = q + 1 - t$ . Let  $\alpha$  be a root of  $f$ . Then

$$\begin{cases} \alpha \bar{\alpha} = q \\ \alpha + \bar{\alpha} = t \end{cases}$$

The complex multiplication hypothesis is essentially equivalent to  $\alpha, \bar{\alpha} \in \mathbb{Q}(\sqrt{d})$  and this is all we will use of it. Let's write  $\alpha = u + \sqrt{d}v$  where  $2u, 2v \in \mathbb{Z}$ . Then:

$$\begin{cases} t = 2u (= \alpha + \bar{\alpha}) \\ p = u^2 - dv^2 \end{cases}$$

We will compute  $u$  using Schoof, and from that we compute  $v = \sqrt{(u^2 - p)/d}$ . Now  $p = u^2 - dv^2 \Rightarrow (\frac{u}{v})^2 \equiv d \pmod p$ . Hence we would have found a square root of  $d \pmod p$ , namely  $\frac{u}{v}$ .

EXAMPLE.

$$d = -1$$

$$E: y^2 = x^3 - x \pmod p.$$

$E$  has complex multiplication by  $\mathbb{Q}(i)$ . If  $p \equiv 1 \pmod 4$ , then the number of points on the curve is  $p + 1 - 2u$ , and  $u^2 + v^2 = p$ . This gives a square root of  $-1$  modulo

---

<sup>1</sup>See Silverman's *Advanced topics in the arithmetic of elliptic curves*.

$p$ . As an aside,  $(\frac{p-1}{2})!$  is also a square root of  $-1$  modulo  $p$  but is a horrible way to compute it.

EXAMPLE.

$$E : y^2 = x^3 - 1$$

$E$  has complex multiplication by  $\mathbb{Q}(\sqrt{-3})$ .

How do we count the points? Let's consider the Frobenius morphism and its square.

$$\begin{array}{ccc} E & \xrightarrow{Fr} & E \\ (x, y) & \mapsto & (x^q, y^q) \end{array} \quad \begin{array}{ccc} E & \xrightarrow{Fr^2} & E \\ (x, y) & \mapsto & (x^{q^2}, y^{q^2}) \end{array}$$

It can be proved that  $Fr$  satisfies  $x^2 - tx + q = 0$ , hence

$$Fr^2 - tFr + qI = 0.$$

$$(x^{q^2}, y^{q^2}) + [q](x, y) = [t](x^q, y^q)$$

We don't know  $t$ . We will compute it modulo  $l$  for every  $l \leq L$ , where  $L$  is chosen as the smallest such that  $M := \prod_{\text{primes } l \leq L} l > 4\sqrt{q}$ . Once we know  $t \pmod l$  for every  $l \leq L$ , then we know  $t \pmod M$  by the Chinese Remainder Theorem. But we also know that  $|t| \leq 2\sqrt{q} < M/2$ , hence  $|t| < \frac{M}{2}$ . This uniquely determines  $t$ .

Note that the Prime Number Theorem implies that  $M \sim e^L$ .

Since we want  $M > 4\sqrt{q}$  it is enough to take  $L = O(\log q)$ . There are  $O(\log q)$  primes  $l \leq O(\log q)$ . Remember that the  $l$ -**torsion** of the elliptic curve is given by the elements whose order is divisible by  $l$ :

$$E[l] = \{p \in E(\overline{\mathbb{F}}_q) \mid lp = 0\}$$

$$Fr^2 - tFr + qI = 0 \text{ on } E[l].$$

For each  $l$ , the algorithm computes  $Fr^2 + qI$  on  $E[l]$  and then, for each  $\tau = 0, \dots, l-1$ , it computes  $\tau Fr$  on  $E[l]$  until  $Fr^2 + qI = \tau Fr$  in  $E[l]$ . Once a match is found, we get  $\tau \equiv t \pmod l$ .

Using the algebraic description of the group law we can write

$$[n](x, y) = \left( \frac{u_n(x)}{f_n(x)^2}, \frac{v_n(x)y}{f_n(x)^3} \right),$$

where  $u_n, v_n, f_n$  are certain polynomials. This implies that

$$(x, y) \in E[l] \Leftrightarrow f_l(x) = 0.$$

To test the equation  $(x^{q^2}, y^{q^2}) + [q](x, y) = [\tau](x^q, y^q)$  in  $E[l]$  can be tested by computing in  $\mathbb{F}_q[x]/(f_l(x))$ .

For instance, compute  $\frac{u_n(x)}{f_n(x)^2} \bmod f_l$  where  $n \equiv q \pmod{l}$  will give the  $x$  coordinate of  $[q](x, y)$  in  $E[l]$ . Likewise,  $(\frac{u_\tau(x)}{f_\tau(x)^2})^q$  is the  $x$  coordinate of  $[\tau](x^q, y^q)$ .

We know that  $\deg f_l = \frac{l^2-1}{2}$  if  $l$  is odd.  $O(\log q^{\frac{l^2-1}{2}}) = O(l^2 \log q) = O((\log q)^3)$  is required for doing one computation on the ring  $\mathbb{F}_q[x]/(f_l(x))$ .

The case  $l = 2$  is a little special but it can be done directly.

$\#E(\mathbb{F}_q) = q + 1 - t$  and since  $q$  is odd,  $\#E(\mathbb{F}_q) \equiv t \pmod{2}$ . Hence  $\#E(\mathbb{F}_q)$  is even  $\Leftrightarrow (E[2] \setminus \{\mathcal{O}\}) \cap E(\mathbb{F}_q) \neq \emptyset$ .

Note that the points of odd order come in pairs, whereas  $E[2] - \{\mathcal{O}\}$  has odd cardinality, since its elements correspond to the roots of  $x^3 + ax + b$  in  $\mathbb{F}_q$ .

We will do an example next week.