Finding Points on Elliptic Curves in Deterministic Polynomial Time (odd characteristic)

Christiaan van de Woestijne, Technische Universität Graz

ANTS VII
TU Berlin
23 July 2006

The Question

We are given a finite field $\mathbb{F}$ with $q = p^e$ elements, and an equation

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

with coefficients $a_i \in \mathbb{F}$ (a cubic Weierstrass equation).

Question: compute $x, y \in \mathbb{F}$ that satisfy the equation.

Well-known: if the curve defined by the equation is nonsingular, its projective closure is an elliptic curve over $\mathbb{F}$, i.e., a curve of genus 1 with a specified $\mathbb{F}$-rational point — which is at infinity.

Answers

First try:

1. Guess a value for X.
2. See if the resulting quadratic equation in Y is solvable.
   If not, go to step 1.
3. Solve it using a probabilistic root taking algorithm (Tonelli-Shanks, or Cantor-Zassenhaus).

Question (Schoof 1985): is there an efficient deterministic algorithm?

Answer: yes, there is! The algorithm I will present

- is long and complicated...
- uses group theory, theory of algebras and some geometry
- takes about cubic time in $\log q$ when using fast arithmetic

Reductions

We assume $\operatorname{char} \mathbb{F} \neq 2$ — for the case of characteristic 2, listen to the next talk.

Now we can complete the square, and get a simpler Weierstrass equation

$$Y^2 = X^3 + aX^2 + bX + c =_{\text{def}} f(X).$$

This equation is singular iff $f(X)$ has a double root in $\mathbb{F}$.

In the singular case, it is easy to compute the coordinates of the singular point; and in fact, we can use this point to parametrise the entire curve.

For the rest of the talk, the equation $Y^2 = f(X)$ is supposed to be nonsingular.

Geometric setting

Let E be an elliptic curve over $\mathbb{F}$, and consider the threefold

$$E \times E \times E.$$

The curve E possesses an elliptic involution

$$-1 : E \to E : (x, y) \mapsto (x, -y), \mathcal{O} \mapsto \mathcal{O}.$$

Thus, on E^3, there is an action of $G = \{\pm 1\}^3$. Consider the subgroup H of G consisting of

$$\{(1, 1, 1), (-1, -1, 1), (-1, 1, -1), (1, -1, -1)\},$$

a Klein 4-group.

Geometric setting (II)

We construct the quotient of E^3 with respect to the action of H, and get a (very singular) threefold

$$V = E^3/H.$$

Doing some Galois theory on the function field of E^3, we find an affine model of V:

$$V : f(X_1)f(X_2)f(X_3) = Y^2.$$

(The idea of using this threefold is due to Mariusz Skałba.)
(In characteristic 2, there is a comparable model — see next talk.)

We will solve two subproblems:

1. Show how to construct points on V;
2. Show how every point P on V leads to a point on E.

On square roots

We first treat the latter question. Observe that if

$$f(x_1)f(x_2)f(x_3)$$

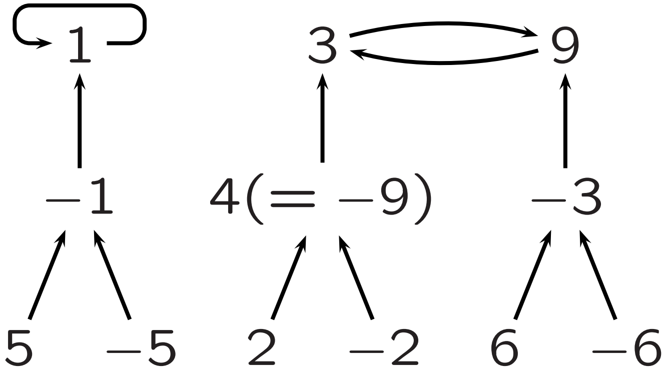
is a square y^2, then at least one of the $f(x_i)$ is a square itself.

Lemma. If $a, b \in \mathbb{F}^*$ are such that ord(b) has more factors 2 than ord(a), then a deterministic variant of the Tonelli-Shanks algorithm can compute a square root of a using b.

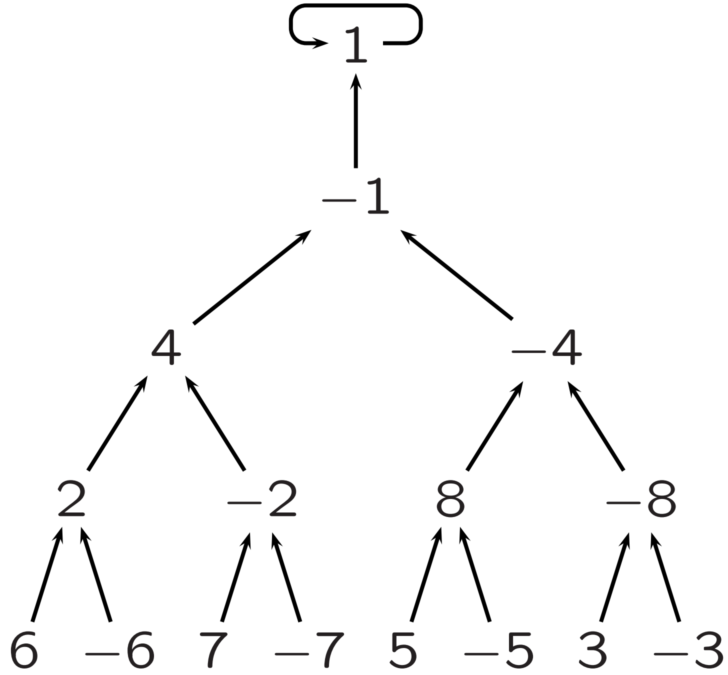
But even if all three of ord$(f(x_i))$ have equally many factors 2, then ord y must have more! So in any case, we can get a square root of at least one of the $f(x_i)$.

Squaring in $\mathbb{F}_{13}^*$ and $\mathbb{F}_{17}^*$

$13 - 1 = 2^2 \cdot 3$:



$17 - 1 = 2^4$:



The level of an element in the tree (where the root has level 0) is equal to the number of factors 2 in its order!

A rationally ruled surface

The first step to finding points on the threefold V is a rational map

$$\phi : S \to V$$

where S is a rationally ruled surface over $\mathbb{F}$.

Most of the ruling curves on S are conic sections over $\mathbb{F}$, and we have

Theorem. There exists a deterministic efficient algorithm that can solve an equation

$$ax^2 + by^2 = c$$

over a finite field.

Having a rational point, we can easily parametrise the conic section, and thus parametrise a genus 0 curve on the threefold V.

Solving quadratic equations

Given an equation $ax^2 + by^2 = c$, with $abc \neq 0$, we first divide by c to get

$$ax^2 + by^2 = 1.$$

If ord(a) has more factors 2 than ord(b), we can take a square root of b.

If the levels of a and b are equal, then this common level is:

0: we can take square roots of a and b anyway

>1: we can take a square root of $-a/b$ and get $ax^2 - ay^2 = 1$

1: we can take square roots of $-a$ and $-b$ and get $x^2 + y^2 = -1$.

The last one is tricky; I use a "bisection" to solve it.

Geometric details

The surface S is given by

$$y^2 h(u,v) = -f(u)$$

where

$$h(u,v) = u^2 + uv + v^2 + a(u+v) + b$$

is such that $h(u,u) = f'(u)$.

Computations in the étale algebra $\mathbb{F}[X]/(f)$ show that the rational map

$$(u,v,y) \mapsto \left(u, -a-u-v, u+y^2, -\frac{f(u)f(u+y^2)}{y^3}\right)$$

sends points on S to V (see the proceedings article).

Norms in the elliptic algebra

Consider $R = \mathbb{F}[X]/(f) = \mathbb{F}[\theta]$. Using the norm from R to $\mathbb{F}$, we see that, for any $a \in \mathbb{F}$,

$$\text{Norm}(a - \theta) = f(a).$$

Thus, we consider

$$\phi(u, v, w) = (u - \theta)(v - \theta)(w - \theta)$$

and hope that its norm will be a square.
If we stipulate $a + u + v + w = 0$, then

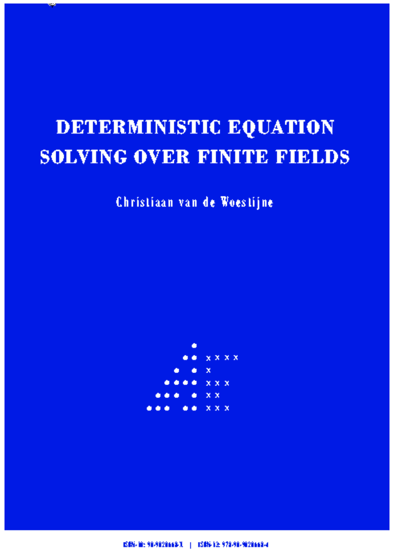
$$f(u)f(v)f(w) = \text{Norm}\,\phi(u, v, w) = -h(u, v)^3 f\left(u - \frac{f(u)}{h(u, v}\right).$$

So, if we restrict ourselves to the surface S defined by

$$-f(u) = y^2 h(u, v)...$$

Proofs...

of the results on square roots and quadratic equations are in my Ph.D. thesis



Deterministic equation
solving over finite fields
(U. Leiden, 2006)

which you are welcome to take a copy of (just ask me).

The End