CONTRUCTION OF ELLIPTIC CURVES ON FINITE FIELD

UNIVERSITY OF HYDERABAD

सा विद्या या विमुक्तये

NAME	REG. NO
1.MUKESH KUMAR MISHRA	11MCMC20
2.ANUKUAR KUMAR	11MCMC18
3. GUNIKHAN SONOWAL	11MCMC33

Construction of Rational Points

on Elliptic

Curves over Finite Fields

INTRODUCTION

Elliptic curves over finite fields
Have been in the centre of
attention of Cryptographers since
the invention of
“ Elliptic curves cryptography ”.

Continue(introduction)

It is not very hard to show that, unless the base field is extremely small such curves always have rational points other than O , the point at infinity .

Continue(introduction)

Until now, this was possible only using an obvious probabilistic method:given an equation for the curve, substitute random values for all coordinates but one and see if the remaining univariate equation can be solved for the last coordinate.

Continue(introduction)

M. Skalba proved that,

given a cubic polynomial

$$\mathbf{f(x) = x^3 + Ax + B}$$

over a field F with characteristic unequal to 2 or 3, with $A \neq 0$,

we have the identity

$$f(X_1(t^2))f(X_2(t^2))f(X_3(t^2)) = U(t)^2 \quad \text{...........(1)}$$

for some nonconstant univariate rational functions X_1, X_2, X_3, U over F

Continue(introduction)

Now assume that F is a finite field and that the curve E is defined over F by the equation $y^2=f(x)$, with f (as last side). The multiplicative Group F is cyclic,

The multiplicative group F is cyclic , and Therefore , as Skalba notes , if we specialise t in (1) to some value t_0 in F , we find that at least one of the $f(X_i(t_0^2))$ is a square in F*.

However, no efficient deterministic algorithm is known to date to take the square root .

Continue(introduction)

we show how to go on from this point to obtain a complete efficient deterministic

algorithm for constructing rational points

on curves given by cubic Weierstrass equations over finite fields. We will reprove Skalba’s Result to obtain, for the case of finite fields of odd characteristic, a parametrisation as in (1) that is invertible as a rational map

Continue(introduction)

The construction of this parametrisation in the

case of odd characteristic rests on the ability

to solve deterministically and efficiently

equations of the form

$$ax^2 + by^2 = c \text{ ....}(2)$$

over finite fields.

Quadratic Equations

Lemma 2. There exists a deterministic algorithm that, given a finite field F of q elements, and nonzero elements a and z of F such that either

(i) v_2 (ord a) < v_2 (ord z),

or

(ii) ord a is odd,

computes a square root of a, in time polynomial in log q.

Theorem 3 .

There exists a deterministic algorithm that, given a finite field F

of q elements, and nonzero elements a0 , a1 , a2 , b of F such that a0 a1 a2 = b2 ,

returns an i in {0, 1, 2} and a square root of ai , in time polynomial in log q.

Theorem 4.

There exists a deterministic algorithm that, given a finite field F

of q elements, and nonzero elements a, b, c of F, computes x, y ∈ F such that

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

continue(Weierstrass Equations)

If E is nonsingular, then the projective closure È of E is a smooth projective curve of genus 1 over F with a specified rational point, so it is an elliptic curve over F, and every elliptic curve over F may be given in this way. The set of rational points on E has a natural abelian group structure , with the point O as identity element.

continue(Weierstrass Equations)

We will be interested in methods to construct rational points on E other than O, or to show that no other points exist.

By Hasse's bound , we know that the number N of rational points on É satisfies

$$|q + 1 - N| \leq 2\sqrt{q}.$$

continue(Weierstrass Equations)

From this, it is easily verified that É has at least 2 rational points whenever $q \geq 5$.

On the other hand, if $q \leq 4$, curves over F exist with only the trivial

rational point O, such as the curve $y^2 = x^3 - x - 1$ over F_3 , and the curve

$y^2 + y = x^3 + \alpha$ over $F_4 = F_2(\alpha)$.

Normal Forms.

The equation (3) may be simplified depending on the characteristic of the base field. We give these forms in detail as we will use their properties

If the characteristic of F is not 2 or 3, then a linear change of coordinates transforms (3) into

$y^2 = x^3 + Bx + C =_{def} f(x)$..........................(4)

Continue(normal form)

For this form of the equation, the important associated quantities Δ (the dis-criminant) and j (the j-invariant) are easily computed: we have

$$\Delta = -16(4B^3 + 27C^2) \quad , j = -1728(4B)^3/\Delta.$$

Now E is singular if and only if $\Delta = 0$, and thus if and only if the right hand side f (x) of (4) has a repeated zero; it has j-invariant 0 if and only if $\Delta = 0$ and

$B = 0$.

Continue(normal form)

In characteristic 3, we must admit a third coefficient; we can transform (3)

into

$$y^2 = x^3 + Ax^2 + Bx + C =_{def} f(x) \text{ ....(5)}$$

with associated quantities

$$\Delta = A^2 B^2 - A^3 C - B^3 \quad , \quad j = A^2 / \Delta.$$

Again, E is singular if and only if f has a double zero. Also, we find that for a nonsingular equation we have

$$j = 0 \text{ if and only if } A = 0.$$

Continue(normal form)

In characteristic 2, no coefficient of (3) can be omitted in all cases. However,

we can obtain one of the following two normal forms, depending on whether a_1 is zero:

$Y^2 + a_3 Y = X^3 + a_4 X + a_6$ if a1 = 0 initially........(6)

$Y^2 + XY = X^3 + a_2 X^2 + a_6$ ifa1= 0 initially......... (7)

Continue(normal form)

In these normal forms, we have $\Delta = (a_3)^4$ and $\Delta = a_6$, respectively, which gives

an easy criterion for singularity of E. Furthermore, for nonsingular equations,

the two cases correspond to j being respectively zero or nonzero.

Elliptic Curves in Odd Characteristic

Lemma 5

For any $u, v, w \in F$ satisfying $u + v + w + A = 0$,

we have

$$f(u)f(v)f(w) = (uv + uw + vw - B)^3$$

$$f((uvw + C)/(uv + uw + vw - B)$$

..........................(9)

Lemma 6.

Put $h(u, v) = u^2 + uv + v^2 + A(u + v) + B$, and define

$S : y^2 h(u, v) = -f(u)$ ....(12)

$\psi : (u,v,y) \rightarrow (v, -A - u - v, u + y^2, f(u + y^2) h(u, v) y^{-1}$

..........................(13)

Then ψ is a rational map from the surface S to V that is invertible on its image.

Lemma 7

There exists a deterministic algorithm that, given a finite field F of

q elements, where q is odd, a nonsingular cubic Weierstrass equation y 2 = f (x)

over F, and an element $u \in F$ such that

$f(u) \neq 0$ and ${}^{3}/_{2}u^{2} + {}^{1}/_{2}Au + B - {}^{1}/_{4}A^{2} \neq 0$

Continue(lemma 7)

computes a rational map,

$$\varphi : A^1 \rightarrow S$$

defined over F that is invertible on its image, in time polynomial in log q. Here

the surface S is as defined in (12).

Lemma 9

Let F be a finite field of q elements, let $u_0 \in F$ satisfy the requirements of Lemma 7, and let $\varphi : A^1 \to S$ be the corresponding map. Let ψ be the

map from Lemma 6.

Then there is a subset $T \subseteq F$ of cardinality at least $(q - 4)/16$, such that for

all distinct $t, t' \in T$, the points $\psi \circ \varphi(t)$ and $\psi \circ \varphi(t')$ are disjoint.

Elliptic Curves in Characteristic 2

Lemma 10.

If f is linear in X, then there exists a deterministic polynomial-time algorithm that returns a point of $Y^2 + Y = f(X)$ over a finite field F.

Lemma 11

Let F be a field of characteristic 2. There exist rational maps φ_1 :

$S_1 \to V_1$ and $\varphi_2 : S_2 \to V_2$ over F which are invertible on their images, given by

$$\varphi_1 : (x, y, w) \to (x, y, xy(x + y)^{-1}, w)$$

$$\varphi_2 : (x, y, w) \to (x, y, x + y, w) .$$

Theorem 12

There exists a deterministic polynomial-time algorithm that,

given a finite field F of characteristic 2 with more than 4 elements and an elliptic

curve E over F, computes a nontrivial rational point on E.

Theorem 13

Let F be a finite field of order $q = 2^r$ with $q > 4$. The number of

disjoint points of V1 that arise from Theorem 12 is at least $(q - 4)/6$.

Theorem 1.

There exists a deterministic algorithm that, given a finite field F of q elements and a cubic Weierstrass equation f(x, y) over F:

Continue (Theorem 1)

(i) detects if $f(x, y)$ is singular, and if so, computes the singular points and gives A rational parametrisation of all rational points on the curve $f(x, y) = 0$;

Continue (Theorem 1)

(ii) if $f(x, y)$ is nonsingular and

$|F| > 5$, computes an explicit rational map from the affine line over F to an affine threefold V

that is given explicitly in terms of the coefficients of f;

Continue (Theorem 1)

(iii) given a rational point on the threefold V , computes a rational point on the

elliptic curve $E : f(x, y) = 0$, in such a way that at

least $(q - 4)/8$ rational points on E are obtained

from the image of the map , and at least $(q-4)/3$

if F has characteristic 2;

and performs all these tasks in time

polynomial in $\log q$.