Elliptic Curve Generation

Peter Manohar, Xingyou Song

November 24, 2015

Abstract

The goal of this report is to....

Contents

1 Introduction

In this section, we will introduce some of the properties of elliptic curves and their mathematical properties.

1.1 Elliptic Curves

The simplest explanation of an elliptic curve is using the Weierstrass Equation; i.e. assume we have a field K, and consider the equation (in Weierstrass Form)

$$y^2 = x^3 + Ax + B \tag{1}$$

Note that here, because (through Vieta formulas),

$$((r_1 - r_2)(r_1 - r_3)(r_2 - r_3))^2 = -(4A^3 + 27B^2) \tag{2}$$

We do not consider curves with multiple roots, and so we take the constraint $4A^3 + 27B^2 \neq 0$.

1.2 Group Law

A property of elliptic curves is an abelian group law which forms on its points, which we will describe below. (A more general proof over all curves is by Reimann-Roch) Geometrically, consider two points $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$. Define the operation of

$$P_3 = P_1 \oplus P_2 \tag{3}$$

where we draw a line in between P_1, P_2 that hits the elliptic curve again at a new point P', then reflect P' about the x-axis to obtain P_3.

More specifically, we can write this explicitly in terms of algebra:

$$x_3 = s^2 - 2x_1y_3 = \tag{4}$$

TODO

1.3 Pairings and Isogenies

Due to the abelian group law on curves, we introduce the concept of an isogeny, i.e. a homomorphism between the elliptic curve groups, that is also algebraic in nature. More formally, an isogeny ϕ is a homomorphism with respect to the group laws

$$\phi : E_1 \to E_2, \quad \phi(O) = O$$

An example of an isogeny from E_1 to itself is multiplication by m, i.e.

$$[m] : E_1 \to E_1, \qquad [m]P = P + P + P + ... + P \text{ (m times)} \tag{5}$$

Then we can define $E[m] = \{P \in E(\bar{K}) | mP = O\}$, i.e. the set of $m-$torsion points of the curve.

Theorem 1. *If K is a field of characteristic 0 or does not divide m, then $E[m] \simeq Z_m \oplus Z_m$.*

The proof of this is mainly using the fundamental theorem of abelian groups, and analyzing the decomposition of the torsion group (TODO?)

Then the Weil-Pairing e_r is defined as a bilinear map,

$$e_r : E[r] \times E[r] \to \mu_r \tag{6}$$

where μ_r is the set of primitive roots of unity in $\bar{K}$, i.e. $\mu_r = \{x | x^r = 1\}$. In other words, instead of working with the r-torsion group of $E(K)$, we may work with the much simpler objects in the extension field of K.

Then we may define the embedding degree to be the degree of the extension field $K(\mu_r)$, or in other words, $[K(\mu_r) : K]$. It is shown that then, if k is the embedding degree with respect to r, then k is the smallest integer such that r divides $q^k - 1$.

1.4 j-invariant

A question arises when two elliptic curves over a field $E_1(K), E_2(K)$ are have a bijective isogeny, i.e. are isomorphic with respect to the group law. An intuitive answer is that the points on elliptic curves be transformed algebraically, which will use different Weierstrass Equations

Note the transformation

$$x' = \mu^2 x$$
$$y' = \mu^3 y$$

implies, after plugging into the Weierstrass equation,

$$(y')^2 = (x')^3 + \mu^4 Ax' + \mu^6 B \implies (y')^2 = (x')^3 + A'x' + B' \tag{7}$$

where $A' = \mu^4 A, B' = \mu_6 B$. μ may not exist in the field K, but only in its closure $\bar{K}$.

From here, we define the j-invariant j of a Weierstrass Form to be

$$j(E) = 1728\frac{4A^3}{4A^3 + 27B^2} \tag{8}$$

Note that the j invariant is homogenous; scalings of the form from (5) will still leave j constant. Given a j, then the canonical elliptic curve associated with this j-invariant will be

$$y^2 = x^3 + \frac{3j}{1728 - j}x + \frac{2j}{1728 - j} \tag{9}$$

Going back to the concept of closed field, note that for non-closed fields, we may have non-isomorphic curves with the same j-invariant.

For instance, $y^2 = x^3 - 25x$, $y^2 = x^3 - 4x$ have $j = 1728$. The first curve has infinitely many pointts in Q, but the second has only finite. The transformation $(x, y) \to (\mu^2 x, \mu^3 y)$ only exists when we consider $Q\sqrt{10}$, since $\mu = \sqrt{10}/2$ is the scaling factor.

Specifically, however, from this example, we do not need the full closure $\bar{K}$; we only need $d = \mu^2$, which means we only need $K(\sqrt{d})$.

1.5 Twist

From the above, we can give different "twists" of curves that are isomorphic in the closed field $\bar{K}$, but not in K. Then if D is a square free integer, then for a elliptic curve $E : y^2 = x^3 + Ax + B$, the given twist $E(D)$, from the above, will be

$$E(D) : y^2 = x^3 + AD^2x + BD^3 \tag{10}$$

1.6 The Complex Lattice

Theorem 2. *Let ω_1, ω_2 be linearly independent points in C. Then define the lattice*

$$L = Z\omega_1 + Z\omega_2$$

Then there exists an elliptic curve that is isomorphic to C/L.

Define $G_k(L) = \sum_{\omega \in L} \omega^{-k}$. Then define the Weierstrass $\wp(z)$ function as follows:

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega \in L}\left(\frac{1}{(z - \omega)^2} - \frac{1}{\omega^2}\right) \tag{11}$$

Then this function can easily be shown, by applications of complex analysis, to be convergent and meromorphic, as well as periodic. Then the derivative $\wp(z)$ is

$$\wp'(z) = -2\sum_{\omega \in L}\frac{1}{(z - \omega)^2} \tag{12}$$

Now we have a isomorphism from the additive group on C/L to the the group of elliptic points on $E(C)$, by the map

$$z \to (\wp(z), \wp'(z)), \quad 0 \to O$$

with E being defined as

$$E : y^2 = 4x^3 - g_2x - g_3 \tag{13}$$

where $g_2 = 60_4, g_3 = 140G_6$ Note that the periodicity will give:

$$(\wp(z_1), \wp'(z_1)) \oplus (\wp(z_2), \wp'(z_2)) = (\wp(z_1 + z_2), \wp'(z_1 + z_2)) \tag{14}$$

which gives rise to the corresponding group law on elliptic curves.

Now we relate the j-invariant on curves to the $j-$function of a complex lattice. First, let rescale our lattice L to $Z\tau + Z$ where $\tau = \frac{w_1}{w_2}$. First, define $q = e^{2\pi 1\tau}$. Then the j-invariant related to the lattice parameter is

$$j(\tau) = 1728\frac{g_2^3}{g_2^3 - 27g_3^2} \tag{15}$$

The proof of all of this we won't go into detail in this paper, but this gives rise to the relationship between the complex lattice and isogenies, mainly integer endomorphisms $[m]$ give rise to $z \to mz$, and for multiplication by a complex number c, we have $z \to cz$, which will induce a endormorphism on the corresponding elliptic curve.

For curves defined on a field K, there is a homomorphism $K \to C$ if we linearly map the finite basis elements of K, $\alpha_1, ..., \alpha_n$ respectively to any algebraically independent set of elements in C, $\tau_1, ..., \tau_n$, so we can regard $E(K)$ as a curve in C.

1.6.1 Using Quadratic Lattices

Consider the case when our lattice $L = O_D$ for some discriminant D, where the basis elements will be $[1, \sqrt{D}/2]$ or $[1, \sqrt{D}]$ depending on D is $1, 3(\mod 4)$ (????? casework)

Then define the Hilbert Class polynomial $H_D \in Z[X]$ that is the minimal polynomial that contains the $j(L)$ as a root. There are many ways to calculate this, but we won't get to that in this paper. Thus, we can define an elliptic curve based on a square free discriminant D.

2 Motivations and Applications

2.1 Discrete Log Problem

In the discrete log problem, we are given any group G, with a base generator element P, with a ciphertext Q, where the problem involves finding k such that $P^k = Q$ in G.

For elliptic curves, this becomes using a base point P with high degree, in a finite field F_p. However, note that by the theorem of finite abelian groups, the elliptic curve group is isomorphic to ————

2.1.1 Pohlig-Hellman Attack

For an element P, assume it has order N in the group G. Then the prime factorization of N, is important to the adversary; i.e. if

$$N = \prod_i q_i^{e_i}$$

then if we need to find k such that $P^k = Q$, then all we need to do is find k in its base $q_1, q_2, ...$ expansions and then construct k using the Chinese Remainder Method. We can do so on each q_i by successively iteration. Thus the difficulty of attacking this problem relies on the largest prime dividing N. TODO(too long)

This implies that we will need to find elliptic curves that have large- prime order torsion groups

3 Generating Curves

3.1 CM Method

The general method of generating curves is the CM - method. The method involves, given (p, N), take $t = p + 1 - N$, with $4p = t^2 + s^2|D|$, where D is square free. Then compute the Hilbert class polynomial $H_D(X)$, and find j such that $H_D(j) = 0 \mod p$. Using (9), we can then construct the explicit formula of the curve.

References