Elliptic Curve Generation

Peter Manohar, Xingyou Song

November 18, 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:

$$x_3 = s^2 - 2x_1 y_3 = \tag{4}$$

TODO

1.3 Pairings and Isogenies

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,

$$(y')^2 = (x')^3 + \mu^4 A x' + \mu^6 B \implies (y')^2 = (x')^3 + A'x' + B' \tag{5}$$

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

$$j(E) = 1728 \frac{4A^3}{4A^3 + 27B^2} \tag{6}$$

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

$$y^2 = x^3 + \frac{3j}{1728 - j}x + \frac{2j}{1728 - j} \tag{7}$$

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.

2 Motivations and Applications

2.1 Discrete Log Problem

3 Generating Curves