CS 681: Computational Number Theory and Algebra **Lecture 33**

Elliptic Curves

Lecturer: Manindra Agrawal **Scribe: Sudeepa Roy**

November 11, 2005

1 Introduction

Elliptic Curves are *cubic polynomials in two variables.* Two of their uses are in

1. Factoring Integers and in
2. Cryptosystem

2 Form of Elliptic Curve

The general form of the elliptic curve is

$$y^2 + a_1xy + a_2y = x^3 + a_3x^2 + a_4x + a_5$$

The coefficients $a_i \in F$, where F is a field. If the characteristic of the field is not 2 or 3 this can be written as *Weierstrass Equation*

$$y^2 = x^3 + Ax + B, \qquad A, B \in F$$

We will discuss only the Weierstrass form.

3 Examples

Example 3.1 *Let $y^2 = x^3 + x + 1$ over $\Re$. It has only 1 real root between -1 and $-\frac{1}{2}$. It will be of the form as shown in Figure 1.*

Example 3.2 *Let $y^2 = x^3 - x$ over $\Re$. It has 3 real roots, ± 1 and 0. It will be of the form as shown in Figure 2.*

Example 3.3 *Make a pyramid of balls with $n \times n$ grid at the base. For what n is the total no. of balls used perfect square?*

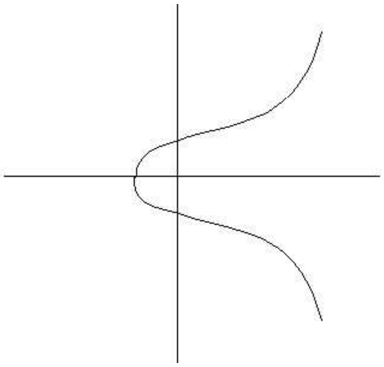

Figure 1: Elliptic Curve with one real root

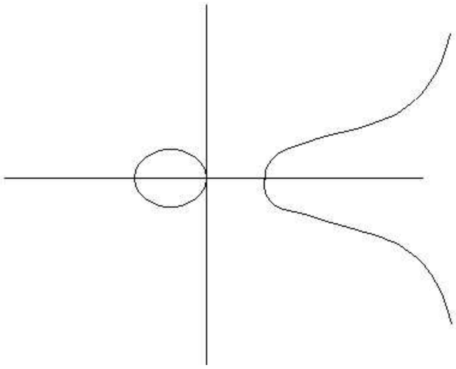

Figure 2: Elliptic Curve with three real roots

For Example 3.3 total no. of balls $= \frac{1}{6}n(n+1)(2n+1)$. Let $y^2 = \frac{1}{6}x(x+1)(2x+1)$. Hence the solution n is all integral points on this elliptic curve. Two trivial solutions are $(0,0)$ and $(1,1)$. We join these two points and consider the third point on the curve where this straight line intersects the curve.

The equation of the straight line is $y = x$. Solving $x^2 = \frac{1}{6}x(x+1)(2x+1)$ we get the third point $(\frac{1}{2}, \frac{1}{2})$ which is not an integral solution. We won't get any new point on the curve by joining any two of these three points. We try with the reflection of the third point $(\frac{1}{2}, \frac{1}{2})$ about x-axis, i.e. $(\frac{1}{2}, -\frac{1}{2})$ and draw the straight line joining $(\frac{1}{2}, -\frac{1}{2})$ and $(1,1)$. Equation of the straight line is $y = 3x - 2$. Solving $(3x-2)^2 = \frac{1}{6}x(x+1)(2x+1)$ we get integral solution $(24, 70)$. By analysis with elliptic curve it can be shown that this is the only integral solution of this problem.

4 Defining Group on Elliptic Curve

Let $(x_0, y_0), (x_1, y_1) \in E(F)$, where $E(F)$ is the elliptic curve E over field F. Let (x_2, y_2) be the third point on $E(F)$ that lie on the line passing through $(x_0, y_0), (x_1, y_1)$.
Define operation '+'

$$(x_0, y_0) + (x_1, y_1) = (x_2, -y_2)$$

Theorem 4.1 *The set of points on $E(F)$ form an abelian group under '+'.*

It is easy to see that the operation '+' is commutative.
To define the identity point we suitably choose a *"point at infinity"*, denoted as O to be in $E(F)$. For a point (x_1, y_1), we draw a vertical line through it and define a point outside $E(F)$ as O.
It can be checked that inverse of (x_1, y_1) is $(x_1, -y_1)$ according to this definition. This operation can also be proved to be associative.