Elliptic Curves Recitation Notes

1 Introduction

These are the notes for recitation 8 on elliptic curves. They are essentially the same as Prof. Rivest's notes from the following link:
http://courses.csail.mit.edu/6.857/2016/files/L13-groups-DH-key-exchange-elliptic-curves.pdf

2 Definition of Elliptic Curves

Let p be a prime number and let a and b be elements of Z_p such that $4a^3 + 27b^2 \neq 0$ (mod p) (*).
The equation (where x,y elements of Z_p) $y^2 = x^3 + ax + b$(mod p) (**) defines an algebraic curve.
If point (x,y) belongs on the curve, then point (x,-y) also belongs on the curve. Also, if r_1, r_2, r_3 are roots of the equation then it is true that:
$[(r_1 - r_2)(r_2 - r_3)(r_3 - r_1)]^2 = -(4a^3 + 27b^2)$ which from the condition (*) means that the roots are distinct.

Definition 1. *The points on the curve (**) are:*
E=$\{(x, y) : y^2 = x^3 + ax + b(\text{mod } p)\} \cup \{\infty\}$*. Here "$\infty$" denotes the "point at infinity".*

Fact 1. $|E| = p + 1 + t$ *where* $|t| \leq 2\sqrt{p}$

Fact 2. $|E|$ *can be computed efficiently.*

Fact 3. *A binary operation "+" can be defined on E such that (E,+) is a finite abelian group. In this group ∞ is the identity element (P+∞=P). The inverse of (x,y) is (x,-y) (which as we said also belongs in the curve). The inverse of ∞ is ∞ itself.*

3 Operations in Elliptic Curves

Let $P = (x_1, y_1)$, $Q = (x_2, y_2)$ and $R = P + Q = (x_3, y_3)$. Intuitively P and Q define a line. Let -R be the third point in the curve on this line. Then the symmetric R is defined to be P+Q.