The University of Sydney
Math3925 Public Key Cryptography

Semester 2 **Exercises and Solutions for Week 10** 2004

Let E be an elliptic curve of the form

$$E : y^2 = x^3 + ax + b.$$

Let O denote the point at infinity, which is defined to be the identity element for the group law on E. The addition law on E is defined by the rule that any three points of E meeting a line L sum to O. Given points P_1 and P_2, a line through these points meets at one additional point Q_3 such that $P_1 + P_2 + Q_3 = O$. The sum of P_1 and P_2 is then the point $-Q_3$, the additive inverse of Q_3.

Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be two points on E, such that $x_1 \neq x_2$. Then the sum $P_1 + P_2 = P_3 = (x_3, y_3)$ given by the formulas:

$$x_3 := \frac{(x_1x_2 + a)(x_1 + x_2) - 2y_1y_2 + 2b}{(x_1 - x_2)^2},$$
$$y_3 := \frac{\big((3x_1^2 + a)x_2 + x_1^3 + 3ax_1 + 4b\big)y_2 - \big((3x_2^2 + a)x_1 + x_2^3 + 3ax_2 + 4b\big)y_1}{(x_1 - x_2)^3},$$

is determined by solving for the third point $-P_3$ meeting the line through P_1 and P_2.

1. For an elliptic curve E with equation as above, explain why the definition $-P = (x_0, -y_0)$, where $P = (x_0, y_0)$, is consistent with the rule that three points on a line sum to O.

Solution The points P and $-P$ (as defined above) pass through a vertical line $x = x_0$, which must also meet the projective point at infinity, hence sum to zero.

2. Let E be the elliptic curve $y^2 = x^3 + x + 2$ over $\mathbb{F}_{13}$, and let $P_1 = (1, 2)$ and $P_2 = (2, 5)$. Solve for the line L through P_1 and P_2 and use this to solve for the third point of $L \cap E$. Use this to show that $P_1 + P_2 = (6, 9)$ and verify your result using the addition formula.

Solution The line L through $(1, 2)$ and $(2, 5)$ is $y = 3x - 1$. The intersection with E gives $(3x - 1)^2 = x^3 + x + 2$ having $x = 1$, $x = 2$, and $x = 6$ as solutions. The latter corresponds to the third (new) point $(6, 4)$ on $L \cap E$. The reflection $(6, -4) = (6, 9)$ is the sum $P_1 + P_2$.

3. In order to use the group of points $E(\mathbb{F}_p)$ for cryptographic purposes, it is essential to be able to find those curves whose number of points, the group order, is prime or is divisible by a large prime.

a. Choose a prime $p > 3$, and use `Magma` to form random elliptic curves E and determine their number of points, e.g.:

```
F := FiniteField(101);
a := Random(F); b := Random(F);
E := EllipticCurve([a,b]);
#E;
```

Show that the number of points $|E(\mathbb{F}_p)|$ is always within $2\sqrt{p}$ of the value $p+1$.

b. For a fixed curve $E/\mathbb{F}_p$ determine the number of points on $E(\mathbb{F}_{p^n})$ for $n = 1, 2, 3, \ldots$. Can you find any pattern to the number of points?

Solution

a. The number of points is experimentally verified to fall in this range.

b. Yes. (For the pattern, see lectures and tutorial 11.)