Lecture 12 Elliptic Curves over Finite Fields

Def. Given a prime number *p* an elliptic curve over a finite field $\mathbf{F}_p$ is a curve with an equation $y^2 = x^3 + Ax + B$ where $4A^3 + 27B^2 \neq 0$. Note: all computations are done mod *p*.

The following theorem is essentially the same as with elliptic curves in the previous lecture.

Theorem: Let *E* be the elliptic curve $y^2 = x^3 + Ax + B$. Let *O* be the point at infinity.
(a) Let *P* be any point on E. Then $P + O = O + P = P$.

(b) Let *P* be any point on E. Then $P + P' = O$..

(c) If $P = (x_1, y_1),\ Q = (x_2, y_2)$, define

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} \pmod{n} & \text{if } P \neq Q \\[2ex] \dfrac{3x_1^2 + A}{2y_1} \pmod{n} & \text{if } P = Q \end{cases}$$

Let $x_3 = (\lambda^2 - x_1 - x_2) \pmod{n},\ y_3 = (\lambda(x_1 - x_3) - y_1) \pmod{n}$. Then $P + Q = (x_3, y_3)$

Example:
(1) Consider the elliptic curve $y^2 = x^3 + 12x + 15$ over $\mathbf{F}_{23}$. Let $P = (9,1),\ \ Q = (16,18)$

Compute

$$P + Q$$
$$(x_1, y_1) = (9,1),\ (x_2, y_2) = (16,18)$$
$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \pmod{23} \equiv \frac{17}{7} \equiv 17 * 7^{-1} \equiv 17 * 10 \equiv 9 \pmod{23}$$
$$x_3 = \lambda^2 - x_1 - x_2 = 9^2 - 9 - 16 = 56 \equiv 10 \pmod{23}$$
$$y_3 = \lambda(x_1 - x_3) - y_1 = -10 \equiv 13 \pmod{23}$$
$$P + Q = (10,13)$$

Note: We used $7^{-1} \equiv 10 \pmod{23}$. This would be computed by the extended Euclidean Algorithm.

Namely,

$$\begin{aligned}
&23 = 3*7+2 \\
&7 = 3*2+1 \\
&1 = 7-3*2 = 7-3*(23-3*7) = 10*7-3*23 \Rightarrow 7^{-1} \equiv 10 \pmod{23}
\end{aligned}$$

Compute

$$\begin{aligned}
&2P = P+P \ ((x_1, y_1) = (x_2, y_2) = (9,1)) \\
&\lambda = \frac{3x_1^2 + A}{2y_1} = \frac{255}{2} = 255*2^{-1} \pmod{23} \equiv 255*12 \equiv 1 \pmod{23} \\
&x_3 = \lambda^2 - x_1 - x_2 = 1^2 - 9 - 9 \equiv 6 \pmod{23} \\
&y_3 = \lambda(x_1 - x_3) - y_1 = 1*(9-6) - 1 \equiv 2 \pmod{23} \\
&2P = (6,2)
\end{aligned}$$

Note: We used $2^{-1} \equiv 12 \pmod{23}$. This would be computed by the extended Euclidean Algorithm.

$$\begin{aligned}
&23 = 11*2+1 \\
&1 = 23-11*2 \\
&2^{-1} \equiv -11 \equiv 12 \pmod{23}
\end{aligned}$$

The Elliptic Curve Discrete Logarithm Problem

Def. Let E be an elliptic curve over $\mathbf{F}_p$ and P, Q be points on *E*. The Elliptic Curve Discrete Logarithm Problem (ECDLP) is the problem of finding an integer *n* such that $Q = nP$, in this case we write $n = \log_p(Q)$.

There are a couple of possible problems with this.

(1) There is not always a solution to this problem, depending on *P*, *Q*, n, and *p*.

(2) Since *E* only has finitely many points, the sequence $P, 2P, 3P, \ldots$ cannot all be different values. There must be a smallest integer $s \geq 1$ such that $sP \equiv 0 \pmod{p}$. The number *s* is called the order of *P*. The order of a point must be the divisor of the order of the elliptic curve (i.e., of the number of points on *E*).

Example:

$E: y^2 = x^3 + 3x + 8$ over $\mathbf{F}_{13}$

First of all *E* has 9 points: $\{0, (1,5), (1,8), (2,3), (2,10), (9,6), (9,7), (12,2), (2,11)\}$

$$
\begin{aligned}
&x = 0: y^2 = 8 \quad \text{No Solution} \\
&x = 1: y^2 = 12 \Rightarrow y = 5\ (5^2 \equiv 25 \equiv 12 \pmod{23}),\ \text{or}\ \ y = 8\ (8^2 \equiv 64 \equiv 12\ ) \\
&x = 2: y^2 = 9 \pmod{13} \Rightarrow y \equiv 3 \pmod{13}\ \ \text{or}\ \ y \equiv -3 \equiv 10 \pmod{13} \\
&x = 3: y^2 = 5 \pmod{13} \quad \text{No solution} \\
&x = 4: y^2 = 6 \pmod{13} \quad \text{No solution} \\
&x = 5: y^2 \equiv 5 \pmod{13} \quad \text{No solution} \\
&x = 6: y^2 \equiv 8 \pmod{13} \quad \text{No solution} \\
&x = 7: y^2 \equiv 8 \pmod{13} \quad \text{No solution} \\
&x = 8: y^2 \equiv 11 \pmod{13} \quad \text{No solution} \\
&x = 9: y^2 \equiv 10 \pmod{13} \Rightarrow y \equiv 6 \pmod{13}\ \ \text{or}\ \ y \equiv 7 \pmod{13} \\
&x = 10: y^2 \equiv 11 \pmod{13} \quad \text{No solution} \\
&x = 11: y^2 \equiv 7 \pmod{13} \quad \text{No solution} \\
&x = 12: y^2 \equiv 4 \pmod{13} \Rightarrow y \equiv 2 \pmod{13}\ \ \text{or}\ \ y \equiv -2 \equiv 11 \pmod{13}
\end{aligned}
$$

The point (2, 3) has order 9. The point (9, 6) has order 3. Let's see why the latter is true.

Compute

$$
\begin{aligned}
&(9,6) + (9,6) \\
&(x_1, y_1) = (x_2, y_2) = (9,6) \\
&\lambda = \frac{3x_1^2 + A}{2y_1} = \frac{41}{2} \equiv (41 * 2^{-1}) \equiv 1 \pmod{13}\ \ (2^{-1} \equiv 7 \pmod{13},\ \text{since}\ 2*7 \equiv 14 \equiv 1) \\
&x_3 = \lambda^2 - x_1 - x_2 = 9,\ \ y_3 = \lambda(x_1 - x_3) - y_1 = 7 \\
&(9,6) + (9,6) = (9,7) \\
&3P = (9,6) + (9,7) = 0 \\
&\text{Since}\ \ \lambda = \frac{y_2 - y_1}{x_2 - x_1} = \frac{1}{0} \Rightarrow 9,6) + (9,7) = 0
\end{aligned}
$$

In this example 3*(9,6) = 0, so only 3 points are multiples of (9,6) $(\ 0*(9,6) = 0,\ \ 1*(9,6) = (9,6),\ \ 2*(9,6) = (9,7)\ )$. The other 6 points on *E* are not multiples of (9,6).

The Double and Add Algorithm

This is analogous to the Fast Power Algorithm. In Elliptic Curve Cryptography the method of encryption and decryption involves computing multiples of a point. The faster one can do this, the better.

Algorithm: For an elliptic curve *E* and a point *P* on *E*, compute *nP*.

Step 1: Let *Q = P. R = 0*
Step 2: While *n* > 0
Step 3: If *n* is odd then let R = R + Q
Step 4: Let Q = 2Q, n = n/2

Example: $y^2 = x^3 + 23x + 13$ over $\mathbf{F}_{83}$. For the point $P = (24,14)$ compute $19P$

Compute the following table. In each row the value for *Q* is the result of computing 2*Q* (note: without using software one would have to compute 2*Q* using the formulas for elliptic curve addition). Also, every time the value of *n* is odd, the value of *R* in the next row is computed as *R* + *Q* (by elliptic curve addition).

n	*Q*	*R*
19	(24,14)	0
9	(30,8)	(24,14)
4	(24,69)	(30,75)
2	(30,75)	(30,75)
1	(24,14)	(30,75)
0	(30,8)	(24,69)

The final answer is the final value for *R*: $19P = (24,69)$