Elliptic curves over finite fields

The ground field

Let $p > 3$ be a prime. We shall work throughout over the field with p elements, $\mathbb{F}_p$. One can easily generalize things to work over an arbitrary finite field, including characteristics 2 and 3, but prime fields (the integers mod p) are more familiar, and the formulae are simpler when the characteristic is at least 5. Moreover, some results are easier to formulate when the number of elements in the field is a prime, rather than a prime power.

Definition of an elliptic curve

An **elliptic curve** over $\mathbb{F}_p$ is the set of points $(x, y) \in \mathbb{F}_p^2$ satisfying an equation of the form

$$y^2 = x^3 + ax + b$$

(where $a, b \in \mathbb{F}_p$ and $4a^3 + 27b^2 \neq 0$), together with "the point at infinity" denoted by $\mathbf{O}$.

Examples

Take $p = 5$. then

$$y^2 = x^3 + 3x$$

defines an elliptic curve over $\mathbb{F}_5$ (with $a = 3$, $b = 0$ and $4.3^3 + 27.0^2 \neq 0$), having 10 points namely

$$\mathbf{O}, (0,0), (1,2), (1,3), (2,2), (3,1), (3,4), (4,1), (4,4).$$

Similarly

$$y^2 = x^3 + 2x$$

gives an elliptic curve over $\mathbb{F}_5$ with just two points $\mathbf{O}$ and $(0, 0)$.

The number of points

For a given value of x the number of $y \in \mathbb{F}_p$ for which $y^2 = x^3 + ax + b$ could be 0, or 1, or 2 (the second case arising when $x^3 + ax + b = 0$). The number of values of y will be

$$1 + \left(\frac{x^3 + ax + b}{p}\right)$$

in each case, so that, including the point at infinity, the number of points on the elliptic curve will be

$$1 + \sum_{x \in \mathbb{F}_p} \left(1 + \left(\frac{x^3 + ax + b}{p}\right)\right) = p + 1 + \sum_{x \in \mathbb{F}_p} \left(\frac{x^3 + ax + b}{p}\right) = p + 1 + \varepsilon,$$

say. If the values of the Legendre symbol were $+1$ and -1 at random one would expect ε to show quite a bit of cancellation. In fact there is the following result.

Hasse's Theorem (1933)
For any elliptic curve over $\mathbb{F}_p$ one has $|\varepsilon| \leq 2\sqrt{p}$. Thus if the number of points on the curve (including the point at infinity) is N then

$$|N - (p+1)| \leq 2\sqrt{p}.$$

Examples If $p = 5$, then we have $|\varepsilon| \leq 4$, so that $2 \leq N \leq 10$. In fact all possibilities occur:

ε	N	Equation
-4	2	$y^2 = x^3 + 2x$
-3	3	$y^2 = x^3 + 4x + 2$
-2	4	$y^2 = x^3 + x$
-1	5	$y^2 = x^3 + 3x + 2$
0	6	$y^2 = x^3 + 1$
1	7	$y^2 = x^3 + 2x + 2$
2	8	$y^2 = x^3 + 4x$
3	9	$y^2 = x^3 + x + 1$
4	10	$y^2 = x^3 + 3x$

It is useful to know not only that the number of points is close to $p + 1$, but also that there are "many" possibilities for the number of points. It can be shown that every number of points in Hasse's range is possible.

The group law

An abelian group law, written additively, is defined on the set of points of an elliptic curve E by

- $\mathbf{O}$ is the identity;
- $P + Q + R = \mathbf{O}$ if and only if there is a line meeting E at P, Q and R, counted properly. (Any vertical line $x =$constant passes through $\mathbf{O}$, and if $P = Q$ the line will be tangent at P.)

Inverses

We have $-(x, y) = (x, -y)$. For if $P = (x, y)$ is on E then so is $Q = (x, -y)$ and the line through Q and Q is vertical and so passes through $\mathbf{O}$. Hence $P + Q + \mathbf{O} = \mathbf{O}$, and so $Q = -P$. Note that this argument, suitably interpreted, remains correct even when $y = 0$.

P+Q

The line through P and Q (or the tangent at P if $P = Q$) meets E at a third point, R say. then $P + Q + R = \mathbf{O}$, whence $P + Q = -R$. So to add P and Q we take the third point of intersection of the line PQ with E, and change the sign of its y coordinate.

Explicit formulae

(i) $-\mathbf{O} = \mathbf{O}$; $\mathbf{O} + \mathbf{O} = \mathbf{O}$.

(ii) $(-x, y) = (x, -y)$; $(x, y) + (x, -y) = \mathbf{O}$.

(iii) If (x_1, y_1) and (x_2, y_2) are on E and $x_1 \neq x_2$, then $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$ where

$$x_3 = \left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2 - x_1 - x_2$$

and

$$y_3 = -y_1 + \left(\frac{y_1 - y_2}{x_1 - x_2}\right)(x_1 - x_3).$$

(iv) If (x_1, y_1) is on E and $y_1 \neq 0$, then $2(x_1, y_1) = (x_3, y_3)$ where

$$x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1$$

and

$$y_3 = -y_1 + \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3).$$

Is this an abelian group law?

Addition is plainly commutative, since the line through P and Q is the same as the line through Q and P; we have an identity element, and inverses exist. Thus all the axioms for an abelian group are satisfied apart possibly from associativity. This can in principle be checked from the above formulae, separating several special cases, or one can refer to the various textbooks.

An example

Consider $E : y^2 = x^3 + 3x$ over $\mathbb{F}_5$. Suppose we wish to add $P = (0, 0)$ and $Q = (1, 2)$, which both lie on E. The line through P and Q is $y = 2x$. If (u, v) lies both on E and on this line we will have $v^2 = u^3 + 3u$ and $v = 2u$, so that $(2u)^2 = u^3 + 3u$. This cubic has roots $u = 0, 1$ and 3 over $\mathbb{F}_5$, corresponding to $v = 0, 2$ and 1 respectively. Thus the line meets E at $P = (0, 0)$, $Q = (1, 2)$ and $(3, 1)$. It follows that $P + Q = -(3, 1) = (3, -1)$.

To compute $2Q$ for example, we need the tangent line at Q. This passes through $Q = (1, 2)$ and has slope dy/dx. Since

$$2y\frac{dy}{dx} = \frac{d}{dx}(x^3 + 3x) = 3x^2 + 3$$

we have $4(dy/dx) = 6$, so that the slope of the tangent line at Q will be -1. The tangent line is therefore $y = 4x + 3$, which meets E at Q, with multiplicity 2, and at $(4, 4)$, via a calculation analogous to that used above for $P + Q$. It follows that $2Q = -(4, 4) = (4, -4) = (4, 1)$.

Points of order two Points of order two are easy to spot. If $2(x, y) = \mathbf{O}$ then $(x, y) = -(x, y) = (x, -y)$, which holds if and only if $y = 0$. (It was for reasons such as this that we insisted at the outset that $p \geq 5$.)

Examples of groups
Take $p = 5$ and consider the curves $E_1 : y^2 = x^3 + x + 2$ and $E_2 : y^2 = x^3 + x$. Both curves have four points

$$E_1 : \ \mathbf{O}, (1, 2), (1, 3), (4, 0),$$

$$E_2 : \ \mathbf{O}, (0, 0), (2, 0), (3, 0),$$

so in each case we have an abelian group of order 4, which can only be C_4 or $C_2 \times C_2$. For E_1 there is exactly one point of order 2, so the group must be C_4, while for C_2 there are three points of order 2 and the group is $C_2 \times C_2$.

Possible group types
For an elliptic curve over a finite field, the group is either cyclic or a product of two cyclic groups. If $C_m \times C_m$ is a subgroup then $p = 1 (\text{mod } m)$. Thus, for example, if an elliptic curve over $\mathbb{F}_5$ has 9 points the group must be C_9.

Computing multiples of points
To compute kP for large k we can use a repeated doubling technique. Find $2P$, $4P$, $8P$,... successively, and add together whichever of these correspond to the binary expansion of k. Thus kP can be found in $O(\log k)$ steps. The process mimics modular exponentiation closely, and can be rearranged so as to avoid storing all the various points $2^r P$.