Cryptology Fall 2017

Chloe Martindale
TU/e

October 12, 2017

These notes are based on notes by Tanja Lange. Recall from last time that we defined an Edwards curve to be a curve of the form

$$x^2 + y^2 = 1 + dx^2y^2,$$

where $d \in \mathbb{F}_q^*$ is a non-square, and gave a group law on the set of $\mathbb{F}_q$ points of this curve. You can do exactly the same thing with *twisted Edwards curves*, which are curves of the form

$$ax^2 + y^2 = 1 + dx^2y^2,$$

where $a, d \in \mathbb{F}_q^*$ and d is a non-square. Both Edwards curves and twisted Edwards curves are examples of *elliptic curves*, which will be the topic of this lecture.

1 Elliptic curves in Weierstrass form

The most common representation of an elliptic curve over a field K (i.e. with coefficients in K) is *Weierstrass form*:

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_0,$$

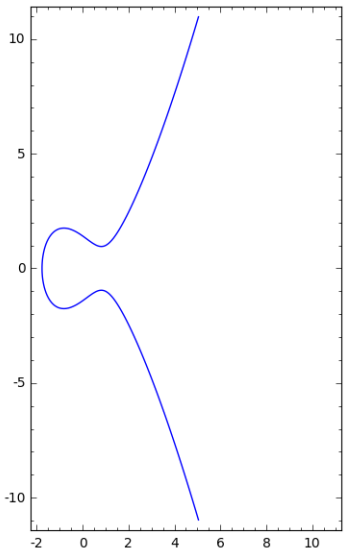
where $a_i \in K$. This is the most common form as every elliptic curve can be written in this way. Although the Edwards and twisted Edwards curves we saw before have an x^2y^2 term which does not appear in the Weierstrass model, there is a transformation to take an Edwards curve to a Weierstrass curve; more on that later.

If K has characteristic different from 2 or 3 (for $K = \mathbb{F}_{p^r}$ this means that $p \neq 2$ or 3), then every elliptic curve can be written in *short Weierstrass form*

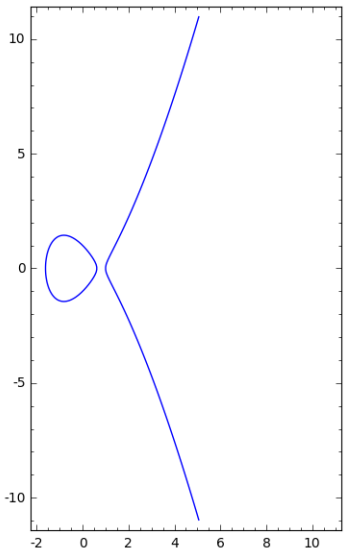
$$E : y^2 = x^3 + ax + b,$$

with $a, b \in K$ and $4a^3 + 27b^2 \neq 0$. Many people consider this to be the definition of an elliptic curve.

Examples. Here is an example with $a = -2$ and $b = 2$, i.e., the curve $y^2 = x^3 - 2x + 2$:

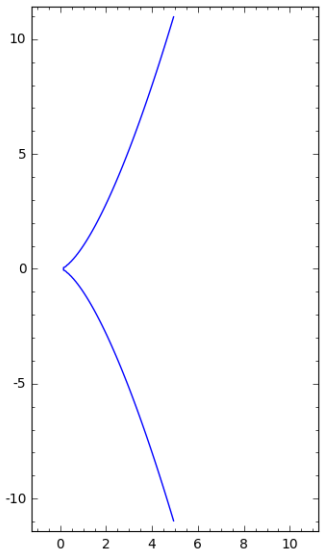


Here is an example with $a = -2$ and $b = 1$, i.e., the curve $y^2 = x^3 - 2x + 1$:

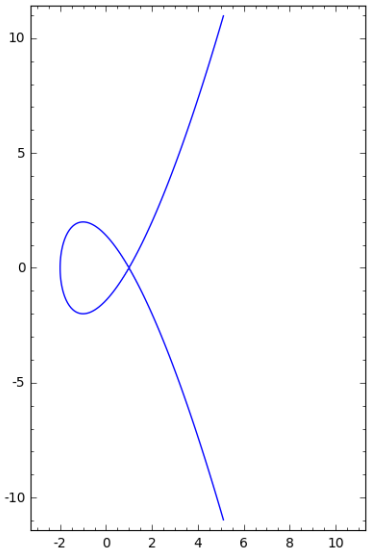


To see why we have excluded a and b such that $4a^3 + 27b^2 = 0$, consider the following non-examples of elliptic curves:

- $a = b = 0$, the curve $y^2 = x^3$:



- $a = -3$, $b = 2$, the curve $y^2 = x^3 - 3x + 2$:

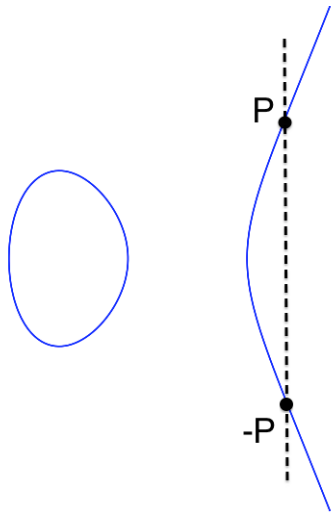


So we include the condition $4a^3 + 27b^2 = 0$ to avoid curves with 'sharp' points or curves that cross themselves. Now we would like to make a group from the points on an elliptic curve as we did with circles and with Edwards curves. So define

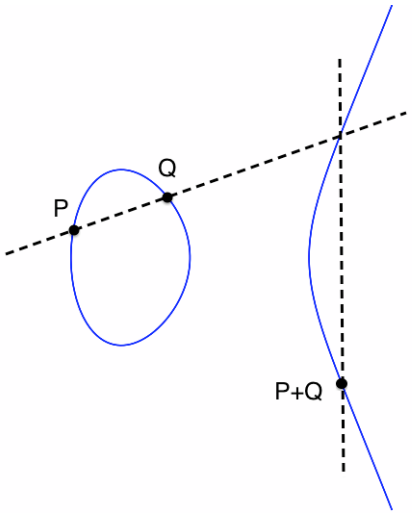
$$G = \{(x, y) \in \mathbb{Q} \times \mathbb{Q} : y^2 = x^3 + ax + b\}$$

for some $a, b \in \mathbb{Q}$. We can 'almost' make a group from G. The group law on Weierstrass curves has a nice geometric definition.

- We define the inverse of a point (x, y) to be $(x, -y)$.



- We define every vertical line to have an invisible point P_∞, 'the point at infinity', and this is the neutral element of the group.
- We define a straight line that is tangent to the curve to intersect the curve twice at that point.
- With the above conventions, every straight line passing through at least 2 points on the curve intersects the curve in exactly 3 points. We define the sum of 3 points on a straight line to be P_∞, hence addition looks like this:



We made quite a few choices in defining our group law $+$, so we need to check the group axioms to make sure that it is really a group law for $G \cup \{P_\infty\}$:

(G1) To check (G1), we need to make sure that given P and Q in $G \cup \{P_\infty\}$, $P + Q \in G \cup \{P_\infty\}$. If P or $Q = P_\infty$ this is trivial, so assume otherwise. $P + Q$ is on the curve by definition, so we only need to check that the coordinates are rational. The coordinates of $P + Q$ are rational if and only if the coordinates of $-(P + Q)$ are rational, which was the third point of intersection between the line through P and Q and the elliptic curve. Suppose that the the equation of the line through P and Q is given by $y = mx + c$. Then as P and Q have rational coordinates, m and $c \in \mathbb{Q}$. To get the third point of intersection of $y = mx + c$ with $y^2 = x^3 + ax + b$, we just plug y into E to get a cubic in x with rational coefficients, 2 roots of which (x_P and x_Q) are known to be rational, hence the third is also rational. So the x-coordinate of $-(P + Q)$ is rational, hence also the y coordinate as $y = mx + c$.

(G2) To check (G2), we need to check that given P, Q, and $R \in G \cup \{P_\infty\}$, $P + (Q + R) = (P + Q) + R$. Checking this by writing out the formulae is easy but long, so we skip it.

(G3) Axiom (G3) states that there exists a neutral element, which is P_∞ by definition.

(G4) Axiom (G4) states that every element has an inverse, which we saw already was given by reflecting about the x-axis.

Remark 1. Another way to think of P_∞ is the following. When we study elliptic curves and their associated groups, the $y^2 = x^3 + ax + b$ (with a and b in K) comes from setting $x = X/Z$ and $y = Y/Z$ in the equation

$$Y^2Z = X^3 + aXZ^2 + bZ^3.$$

Note that every term in this equation has degree 3, so that if (X_0, Y_0, Z_0) is a solution of this equation, then (nX_0, nY_0, nZ_0) is also a solution of the equation for every n in K. For this reason, if $(nX_0, nY_0, nZ_0) = (X_0, Y_0, Z_0)$ then we say that the 2 solutions are *equivalent*. Observe that these solutions all correspond to a unique x and y! The point at infinity is

$$P_\infty = (0, 1, 0)$$

in (X, Y, Z)-coordinates, which gets 'sent to infinity' when we switch to (x, y)-coordinates. Note that this is always on the curve!

Having intuitively constructed a geometric group law elliptic curves over $\mathbb{Q}$, if we now write down the formulae for adding points, we can get a group law for elliptic curves over $\mathbb{F}_q$. So what are the formulae for adding?

Write $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$, and define $(x_R, y_R) = R = P + Q$. We want to write down a formula for x_R and for y_R. We know that P, Q, and $-R$ all lie on the straight line passing through P and Q, so we first calculate the formula of this line. The equation of this line is $y = mx + c$ where

$$m = \begin{cases} (y_Q - y_P)/(x_Q - x_P) & P \neq Q \\ (3x_P^2 + a)/(2y_P) & P = Q \end{cases}$$

and

$$c = y_P - mx_P.$$

(Recall that the gradient of a tangent line to a curve at a point P is the value of $\frac{dy}{dx}$ at P.) We plug in $y = mx + c$ with m and c as above to the equation for E and solve to find the intersection points:

$$(mx + c)^2 = x^3 + ax + b.$$

We know that the roots of this cubic are x_P, x_Q, and x_R, so

$$x^3 - (mx + c)^2 + ax + b = (x - x_P)(x - x_Q)(x - x_R).$$

Then by comparing coefficients of x^2, we see that

$$x_R = m^2 - x_P - x_Q.$$

Then we can just use the equation of the line to compute y_R:

$$y_R = -y_{-R} = -(mx_R + c).$$

With these explicit formulae, we can define, for any $a, b \in \mathbb{F}_q$ such that $4a^3 + 27b^2 \neq 0$, a group law on

$$G = \{(x, y) \in \mathbb{F}_q \times \mathbb{F}_q : y^2 = x^3 + ax + b\} \cup \{P_\infty\}$$

as

$$(x_P, y_P) + (x_Q, y_Q) = (m^2 - x_P - x_Q, -m(m^2 - x_P - x_Q) - c),$$

where

$$m = \begin{cases} (y_Q - y_P)/(x_Q - x_P) & P \neq Q \\ (3x_P^2 + a)/(2y_P) & P = Q \end{cases}$$

and

$$c = y_P - mx_P.$$

All the case distinctions with P_∞ mean that with this group law we have a lot more checks than with Edward's curves, so it can be nicer to work with Edwards curves and then transform to Weierstrass if necessary. Before seeing how to do this, we define one more curve shape.

2 Montgomery curves

Definition 1. A *Montgomery curve* is a curve of the form

$$M_{A,B} : Bv^2 = u^3 + Au^2 + u$$

for $B(A^2 - 4) \neq 0$. The group law looks very similar to the group law for Weierstrass curves:

$$(u_1, v_1) \oplus (u_2, v_2) = (Bm^2 - A - u_1 - u_2, m(u_1 - u_3) - v_1),$$

where $u_3 = Bm^2 - A - u_1 - u_2$, and

$$m = \begin{cases} (v_1 - v_2)/(u_1 - u_2) & (u_1, v_1) \neq (u_2, v_2) \\ (3u_1^2 + 2Au_1 + 1)/(2Bv_1) & (u_1, v_1) = (u_2, v_2). \end{cases}$$

The neutral element is again P_∞.

We have now mentioned a few times a 'transformation' that relates different curve shapes. We would like a way to say when 2 curves are 'the same', or at least a way to say what 'the same' means! Let's think about what this would mean in an ideal world..

Remember that last time we thought about how to do Diffie-Hellman in curve groups:

- Setup: Alice and Bob agree on a curve C_d or $M_{A,B}$ over a field $\mathbb{F}_q$ and a point P on the curve that generates a large group.
- Alice chooses a secret key $a \in \mathbb{Z}$, computes her public key aP, and sends it to Bob.
- Bob chooses a secret key $b \in \mathbb{Z}$, computes his public key bP, and sends it to Alice.
- Alice computes the shared secret as $a(bP) = (ab)P$ and Bob computes it as $b(aP) = (ab)P$.

Suppose that we have some map from the Edwards curve

$$C_d : x^2 + y^2 = 1 + dx^2y^2$$

to the Montgomery curve $M_{A,B}$ above given by

$$f : C_d \longrightarrow M_{A,B}.$$

Suppose that we know some way to break the DLP for curves, i.e., to find n given nQ, on a Montgomery curve, but that Alice and Bob have used an Edwards curve. It would be nice if for all points P on C_d and for all $a \in \mathbb{Z}$, we had that $f(aP) = af(P)$, as $f(P) = Q$ and $af(P) = aQ$ are points on a Montgomery curve, so then we can find a (if we can break DLP on a Montgomery curve). That is, if f satisfies this nice property of $f(aP) = af(P)$, we can somehow translate the discrete logarithm on C_d to a discrete logarithm on $M_{A,B}$. It would also be nice to be able to go the other direction, that is if there's a map

$$g : M_{A,B} \longrightarrow C_d$$

that is the inverse of f. Some other nice properties to require of f:

- $f(P + Q) = f(P) + f(Q)$
- $f((0, 1)) = P_\infty$ (remember that the neutral point on C_d was $(0, 1)$.

We can write down a nice map from a twisted Edwards curve to a Montgomery curve:

$$\begin{array}{ccc} ax^2 + y^2 = 1 + dx^2y^2 & \longrightarrow & Bv^2 = u^3 + Au^2 + u \\ (x, y) & \longmapsto & (u, v) = ((1 + y)/(1 - y), (1 + y)/(x(1 - y))) \\ (a, d) & \longmapsto & (A, B) = (2(a + d)/(a - d), B = 4/(a - d). \end{array}$$

In other direction we have the map:

$$\begin{array}{ccc} Bv^2 = u^3 + Au^2 + u & \longrightarrow & ax^2 + y^2 = 1 + dx^2y^2 \\ (u, v) & \longmapsto & (x, y) = (u/v, (u - 1)/(u + 1)) \\ (A, B) & \longmapsto & (a, d) = ((A + 2)/B, (A - 2)/B). \end{array}$$

By a similar transformation we can go from Montgomery to Weierstrass, but not necessarily back! All elliptic curves are Weierstrass, but not all can be written in Edwards/Montgomery form. There is a quick way to see this: Edwards curves (and hence Montgomery curves) always have a point $(1, 0)$ of order 4, and there are examples of Weierstrass curves that do not. To see that $(1, 0)$ is a point of order 4, recall the doubling formula for Edwards curves from last time:

$$2 \cdot (x, y) = \left(\frac{2xy}{x^2 + y^2}, \frac{y^2 - x^2}{2 - x^2 - y^2} \right).$$

Then we can easily compute

$$2 \cdot (1, 0) = (0, -1)$$

and hence

$$4 \cdot (1, 0) = 2 \cdot (0, -1) = (0, 1).$$

(Recall that $(0, 1)$ is the neutral element.)

Some final observations on elliptic curves:

- Computations on Edwards curves are faster than on curves in Weierstrass form, so you should use Edwards curves for implementations when possible.
- Weierstrass curves are much older than Edwards curves, and much more widely studied, which acts as a security argument for the newer Edwards curves (from 2007) - as for example the Discrete Logarithm problem can be translated along transformations.
- More formulae for addition/doubling on elliptic curves in various shapes are available at `hyperelliptic.org/EFD`.