ELLIPTIC CURVE CRYPTOGRAPHY (CONTINUED)

MATH 195

A Review

A summary of all we have seen: An elliptic curve over a field k is given by an equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

for $a_i \in k$, $\Delta \neq 0$. We denote $E(k)$ as the set of points (x, y) satisfying this equation together with the point at infinity, O. $E(k)$ is an (additively written) abelian group.

To compute $P + Q$, for $P, Q \in E(k)$:

- If $P = O$ then $P + Q = Q$;
- If $Q = O$ then $P + Q = P$;
- Else $P = (x_1, y_1)$ and $Q = (x_2, y_2)$; $P + Q = O$ if $x_1 = x_2$ and $y_1 + y_2 = -a_1x_1 - a_3$;
- Else let

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & x_1 \neq x_2 \\ \dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, & x_1 = x_2; \end{cases}$$

and $\nu = y_1 - \lambda x_1$, $x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2$, $y_4 = \lambda x_3 + \nu$, $y_3 = a_1x_3 - a_3 - y_4$, and then $P + Q = (x_3, y_3)$.

We characterize this group law as follows: To add $P \neq Q$, draw the (unique) line $y = \lambda x + \nu$ through these two points, the line will intersect the curve E at another (unique) point R, then we take $P + Q = -R$, its negative.

Doubling

To double P, draw the tangent line to E at P. This must be understood in a formal sense: Let $F(x, y)$ be any polynomial in two variables

$$F(x, y) = \sum_{i,j \geq 0}^{<\infty} a_{ij}x^iy^j$$

(with only finitely many terms). For example, we would take

$$F(x, y) = y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6.$$

Suppose $F(x_0, y_0) = 0$. What is the tangent line to "$F = 0$" at (x_0, y_0)? We let $x = x_0 + (x - x_0)$ and $y = y_0 + (y - y_0)$ so that we can approximate F by a linear polynomial.

This is some of the material covered May 7–9, in Math 195: Cryptography, taught by Hendrik Lenstra, prepared by John Voight jvoight@math.berkeley.edu.

Recall the Taylor expansion of a polynomial $f(x)$ at a point x:

$$f(x) = f(x_0) + (x - x_0)f'(x_0) + (x - x_0)^2 \frac{f''(x_0)}{2} + \cdots \approx f(x_0) + (x - x_0)f'(x_0)$$

We mimic this in the two variable case, and again throw out any terms of degree ≥ 2: first we write

$$F(x, y) = \sum_{i,j \geq 0}^{<\infty} a_{ij}(x_0 + (x - x_0))^i (y_0 + (y - y_0))^j;$$

since by the binomial formula

$$\begin{aligned}(x_0 + (x - x_0))^i &= x_0^i + ix_0^{i-1}(x - x_0) + \frac{i(i-1)}{2} x_0^{i-2}(x - x_0)^2 + \dots \\ &\approx x_0^i + ix_0^{i-1}(x - x_0)\end{aligned}$$

this gives

$$\begin{aligned}F(x, y) &\approx \sum_{i,j \geq 0}^{<\infty} a_{ij}(x_0^i + ix_0^{i-1}(x - x_0))(y_0^j + jy_0^{j-1}(y - y_0)) \\ &\approx \sum_{i,j \geq 0}^{<\infty} a_{ij} \left(x_0^i y_0^j + ix_0^{i-1} y_0^j (x - x_0) + jx_0^i y_0^{j-1}(y - y_0) \right) \\ &= F(x_0, y_0) + \left.\frac{\partial F}{\partial x}\right|_{(x_0,y_0)} (x - x_0) + \left.\frac{\partial F}{\partial y}\right|_{(x_0,y_0)} (y - y_0).\end{aligned}$$

We also write $\partial F / \partial x = F_x$ and $\partial F / \partial y = F_y$.

Since $F(x_0, y_0) = 0$ (the point is on the curve), we call

$$\left.\frac{\partial F}{\partial x}\right|_{(x_0,y_0)} (x - x_0) + \left.\frac{\partial F}{\partial y}\right|_{(x_0,y_0)} (y - y_0)$$

the *tangent line* to F at (x_0, y_0).

Example. Take $F = y^2 - x^3 - 1$, representing the curve $E : y^2 = x^3 + 1$. The point $(x_0, y_0) = (0, -1)$ is on the curve. We compute $F_x(x_0, y_0) = 3x_0^2 = 0$, $fF_y(x_0, y_0) = 2y_0 = -2$, so the tangent line is $0(x - x_0) + (-2)(y - y_0) = 0$, or simply $y = -1$. This is a horizontal line!

If $F_x(x_0, y_0) = F(x_0, y_0) = 0$, then (x_0, y_0) is called a *singular point* of the curve $F = 0$. Our requirement $\Delta = 0$ provides that the elliptic curve has no singular points.

Note that we can also write it (when $F_y(x_0, y_0) \neq 0$):

$$y = -\frac{F_x(x_0, y_0)}{F_y(x_0, y_0)} x + \frac{F_x(x_0, y_0)x_0 + F_y(x_0, y_0)y_0}{F_y(x_0, y_0)}.$$

Now for our equation,

$$F(x, y) = y^2 + a_1 xy + a_3 y - x^3 - a_2 x^2 - a_4 x - a_6,$$

we have

$$-\frac{F_x(x_1, y_1)}{F_y(x_1, y_1)} = \lambda = \frac{3x_1^2 + 2a_2 x_1 + a_4 - a_1 y_1}{2y_1 + a_1 x_1 + a_3}.$$

This is how one gets this λ: it is the slope of the tangent line at (x_1, y_1).

Definition of Δ

We want our elliptic curves to be *nonsingular*. This is the condition that $\Delta \neq 0$. Define:

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 \\ b_4 &= 2a_4 + a_1a_3 \\ b_6 &= a_3^2 + 4a_6 \\ b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \end{aligned}$$

Then

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6.$$

These coefficients have a meaning: if $2 \neq 0$ in k, we multiply our equation F by 4 and complete the square:

$$(2y + a_1x + a_3)^2 = 4x^3 + b_2x^2 + 2b_4x + b_6;$$

treating the expression in parentheses as a new y, we get a new elliptic curve of a simpler form.

Then we may treat $a_1 = a_3 = 0$, and so we have $y^2 = x^3 + a_2x^2 + a_4x + a_6$. Then

$$\Delta = 16(a_2^2a_4^2 - 4a_4^3 - 4a_2^3a_6 - 27a_6^2 + 18a_2a_4a_6).$$

This is none other than the discriminant of the polynomial $x^3 + a_2x^2 + a_4x + a_6$: if the roots of this polynomial are α, β, γ, then this is equal to

$$16(\alpha - \beta)^2(\beta - \gamma)^2(\gamma - \alpha)^2.$$

Other Ways of Defining Elliptic Curves

We have given an elliptic curve (when the characteristic of our field is not 2) as

$$y^2 = x^3 + a_2x^2 + a_4x + a_6,$$

which can be achieved by a change of variable (completing the square). When the characteristic is not 3, one can "complete the cube": replace x with $(x + a_2/3)^3$, to get a curve of the form

$$y^2 = x^3 + a_4x + a_6$$

(with different a_4 and a_6).

On occasion, we may have a curve

$$uy^2 + a_1xy + a_3y = vx^3 + a_2x^2 + a_4x + a_6$$

where $u, v \neq 0$. Multiply this equation by u^3v^2 to obtain

$$u^4v^2y^2 + a_1u^3v^2xy + a_3u^3v^2y = u^3v^3x^3 + a_2u^3v^2x^2 + a_4u^3v^2x + a_6u^3v^2$$

and then replace y by u^2vy and x by uvx to get

$$y^2 + a_1xy + a_3uvy = x^3 + a_2ux^2 + a_4u^2vx + a_6u^3v^2.$$

Third, we supplement each term in our curve with z so that the degree of every term is 3:

$$y^2z + a_1xyz + a_3yz^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3.$$

It then becomes what we call a *homogeneous* equation of degree 3. By adding these, we then care only about the ratio $(x : y : z)$. Therefore we write

$$(x : y : z) = (x' : y' : z')$$

if and only if there exists a $c \in k^*$ such that $x' = cx, y' = cy, z' = cz$. Note that if you take a solution to the equation and multiply each variable c, each term in the equation is scaled by c^3, so it is again zero. "Most of the time", $z \neq 0$, so it has an inverse in the field, and then we may scale by z^{-1} to get

$$(x : y : z) = (x/z : y/z : 1)$$

and we get back to the original equation (we substitute $z = 1$). We exclude the trivial point $(x : y : z) = (0 : 0 : 0)$. We have extended the plane to what is known as the projective plane $\mathbb{P}^2(k)$ as the set of all such ratios,

$$\mathbb{P}^2(k) = ((k \times k \times k) \setminus (0, 0, 0))/\sim$$

where the equivalence relation

$$(x, y, z) \sim (x', y', z')$$

if and only if there is $c \in k^*$ such that $x' = cx$, $y' = cy$, $z' = cz$.

This explains where the point at infinity comes from: we let $z = 0$, and substituting this into the equation we get $x = 0$, so the only point, which we denote as O, is $O = (0 : y : 0) = (0 : 1 : 0)$.

To avoid divisions in computing the addition of two points, using projective coordinates we can avoid denominators: $(x/d, y/d) = (x/d : y/d : 1) = (x : y : d)$, for any denominator d.

In fact, we may (in general) take any projective cubic curve C, defined by a homogeneous equation $F(x, y, z) = 0$ of degree 3, subject to the requirements that F is 'non-singular' (so, in particular, F is irreducible), and one is given a point $P_0 \in C(k)$. In this case, P_0 is the zero element, and if two lines L_1, L_2 intersect the curve C in $\{P_1, Q_1, R_1\}$ and $\{P_2, Q_2, R_2\}$, then

$$P_1 + Q_1 + R_1 = P_2 + Q_2 + R_2.$$

After awhile, you define an elliptic curve as a nonsingular projective one-dimensional variety of genus one, together with a point on it. (Think of this as analogous to the abstraction of $\mathbb{R}^n$ as a vector space over $\mathbb{R}$ with a basis.)