Tutorial on Elliptic and Hyperelliptic Curve Cryptography, Dublin 2007
Lecture notes for talk by Tanja Lange, Monday September 3, 2007

Background elliptic curves over $\mathbb{Q}$ and $\mathbb{F}_q$

References: See online, we will use Silverman/Tate a lot during the talk.

Definition: Affine curves C, $\bar{C}$ given by $F(x,y) = 0, \bar{F}(u,v) = 0$ over the same field k are *birationally equivalent* if there exist rational functions $G_x, G_y, \bar{G}_u, \bar{G}_v$ such that $(G_x(u_0,v_0), G_y(u_0,v_0)) \in C$ and $(\bar{G}_u(x_0,y_0), \bar{G}_v(x_0,y_0)) \in \bar{C}$ for $(x_0,y_0) \in C$ and $(u_0,v_0) \in \bar{C}$ whenever the expressions are defined.

Example: Circle $C : x^2 + y^2 = 1$ and line $\bar{C} : u = 0$ are isomorphic.

For elliptic curves consider maps that preserve group structure, i.e. homomorphisms $\varphi : E \to \bar{E}$ with $\varphi(P \oplus_E Q) = \varphi(P) \oplus_{\bar{E}} \varphi(Q)$. Obviously need $\varphi(P_{\infty,E}) = P_{\infty,\bar{E}}$.

Definition: Elliptic curves $E, \bar{E}$ over k are *isogenous* if there exists a homomorphism $\varphi : E \to \bar{E}$ with $\mathrm{Im}(\varphi) = \bar{E}$ and finite kernel $\ker(\varphi)$.

Definition: An isogeny of the curve with itself is called an *endomorphism*.

Example: Examples of endomorphisms are $[2] : E \to E, P \mapsto [2]P$, $[n] : E \to E, P \mapsto [n]P$. If E is defined over $\mathbb{F}_2$ then $\sigma : E \to E$ with $\sigma(x,y) = (x^2, y^2), \sigma(P_\infty) = P_\infty$ is endomorphism. (Exercise!)

Definition: Elliptic curves $E, \bar{E}$ over k are *isomorphic* if there exist homomorphisms $\varphi : E \to \bar{E}, \psi : \bar{E} \to E$ with

$$\psi \circ \varphi = \mathrm{Id}_E \text{ and } \varphi \circ \psi = \mathrm{Id}_{barE}.$$

Example: $E, \bar{E}$ in Weierstrass form

$$E : y^2 + \underbrace{(a_1x + a_3)}_{h(x)} = \underbrace{x^3 + a_2x^2 + a_4x + a_6}_{f(x)}, \ \bar{E} : v^2 + \bar{h}(u)v = \bar{f}(u)$$

are isomorphic if $u = a^2x + b$, $v = a^3y + cx + d$ with $a, b, c, d \in k$.

Example: $\mathrm{char}(k) \neq 2$, each elliptic curve is isomorphic to one in *short Weierstrass form* $E : y^2 = f(x)$.

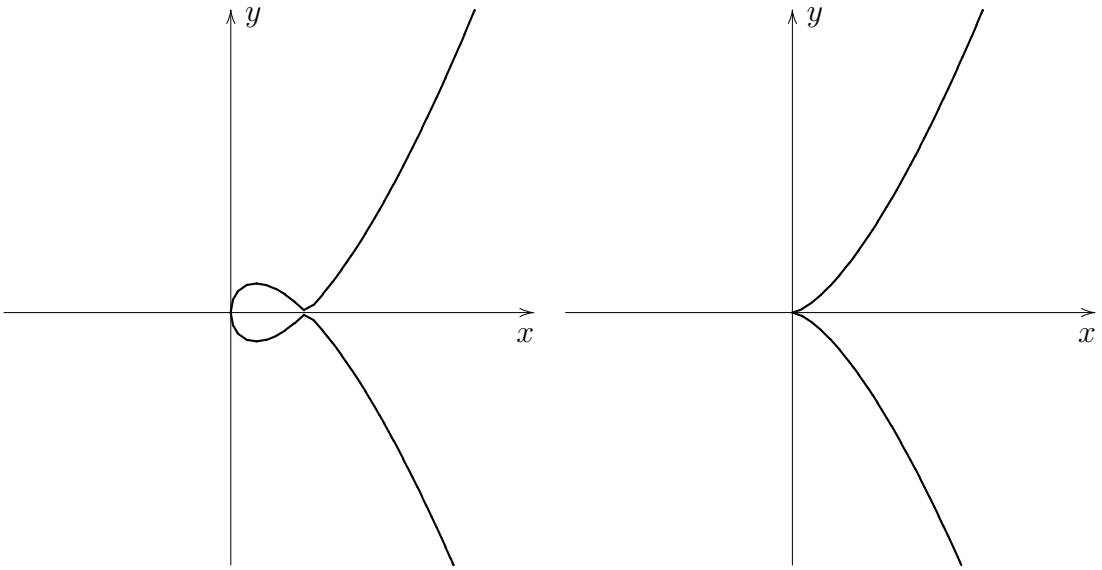
Group law on ECC relies on tangents. Let more generally the curve C be given by $F(x,y) = 0$. Calculus tells us that the tangent (if defined) to F at (x_0,y_0) is given by

$$\frac{\partial F}{\partial x}(x_0,y_0)(x - x_0) + \frac{\partial F}{\partial y}(x_0,y_0)(y - y_0) = 0.$$

This defines a line unless $\frac{\partial F}{\partial x}(x_0, y_0) = \frac{\partial F}{\partial y}(x_0, y_0) = 0$ for some point $(x_0, y_0) \in C$.

Definition: $P = (x_0, y_0) \in C$ is *singular* if and only if $\frac{\partial F}{\partial x}(x_0, y_0) = \frac{\partial F}{\partial y}(x_0, y_0) = 0$.

Prominent examples:
The first picture shows a node, characterized by having two candidate tangents at that point. The second picture shows a cusp. The tangents at points next to the singularity have opposite slopes.



On the left-hand side we draw the graph of $y^2 = (x-1)^2 x$ which has a node, the right curve is $y^2 = x^3$ having a cusp.

Definition: Curve C is *non-singular* if and only if there is no singular point $(x_0, y_0) \in C(\bar{k})$. Note that the coordinates can come from an algebraic closure.
These concepts can be extended to projective curves; we actually use that them on projective curves.

Definition: An elliptic curve is a nonsingular curve of genus 1 with at least one k-rational point.

Example: Let $\mathrm{char}(k) = 2$, $C : y^2 = f(x)$ is singular.

The following was moved to the exercise session; don't read further if you don't want to spoil your exercises.

Example: Let $\mathrm{char}(k) \neq 2$, so we can transform any curve in Weierstrass form to $C : y^2 = f(x)$, so $F(x, y) = y^2 - f(x)$. When is this curve nonsingular?
We have $\frac{\partial F}{\partial x} = -(3x^2 + a_2 x + a_4)$ and $\frac{\partial F}{\partial y} = 2y$. A singular point (x_0, y_0) must thus have

$y_0 = 0$. So, x_0 must satisfy $f(x_0) = 0$ and $3x_0^2 + a_2x_0 + a_4 = f'(x_0) = 0$. So x_0 is common root of f and f', so x_0 is a multiple root of f (Exercise).
C is non-singular if and only if f has only simple roots over $\bar{k}$.

Definition: Let $f \in k[x]$ split as $f(x) = (x - a_1)(x - a_2)\cdots(x - a_n)$ over $\bar{k}$. The *discriminant* of f is given by $\text{disc}(f) = \prod_{1 \le i < j \le n}(a_i - a_j)^2$.

Lemma: $\text{disc}(f) \neq 0 \Leftrightarrow f$ has only simple roots $\Leftrightarrow E : y^2 = f(x)$ is elliptic curve.