Tutorial on Elliptic and Hyperelliptic Curve Cryptography, Dublin 2007
Lecture notes for talk by Tanja Lange, Tuesday September 4, 2007

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

Big example on isogenies, for details see Silverman/Tate Chapter III.4.
$E : y^2 = x^3 + x^2 + bx$ is elliptic curve if $\operatorname{disc}(f) = b^2(a^2 - 4b) \neq 0$. Put $\bar{E} : v^2 = u^3 + \bar{a}u^2 + \bar{b}u$, with $\bar{a} = -2a, \bar{b} = a^2 - 4$. Note that $\operatorname{disc}(f) = \operatorname{disc}(\bar{f})$.
The map φ defined by $\varphi(0,0) = P_{\infty,\bar{E}}$, $\varphi(P_{\infty,E}) = P_{\infty,\bar{E}}$, and $\varphi(x,y) = (u,v)$ with $u = x + a + b/x = y^2/x^2$ and $v = y(x^2 - b)/x^2$ maps points on E to points on $\bar{E}$.
Check by hand that $\varphi(x,y) \in \bar{E}$; we do not show that φ is actually a homomorphism and that $\operatorname{Im}(\varphi) = \bar{E}$. Obviously $\ker(\varphi) = \{(0,0), P_{\infty,E}\}$ is finite.
$\bar{E}$ is of the same shape as E, so iterate procedure; this leads to $\bar{\bar{E}} : \bar{y}^2 = \bar{x}^3 + \bar{\bar{a}}\bar{x}^2 + \bar{\bar{b}}\bar{x}$, where $\bar{\bar{a}} = -2\bar{a} = 4a$ and $\bar{\bar{b}}\bar{a}^2 - 4\bar{b} = 4a^2 - 4a^2 + 16b = 16b$.
$\bar{\bar{E}}$ isomorphic to E with $\bar{y} = 8y, \bar{x} = 4x$.

What happened to point $(x_0, y_0) \in E$ under composition $\psi \circ \bar{\varphi} \circ \varphi : E \to E$? We have $\psi \circ \bar{\varphi}(u_0, v_0) = (v_0^2/(4u_0^2), v_0(u_0^2 - \bar{b})/(8u_0^2))$, so

$$\begin{aligned}
\psi \circ \bar{\varphi} \circ \varphi(x_0, y_0) &= \psi \circ \bar{\varphi}\left(\frac{y_0^2}{x_0^2}, \frac{y_0(x_0^2 - b)}{x_0^2}\right) = \left(\frac{\left(\frac{y_0(x_0^2-b)}{x_0^2}\right)^2}{4\left(\frac{y_0^2}{x_0^2}\right)^2}, \frac{\frac{y_0(x_0^2-b)}{x_0^2}\left(\left(\frac{y_0^2}{x_0^2}\right)^2 - (a^2 - 4b)\right)}{8\left(\frac{y_0^2}{x_0^2}\right)^2}\right) \\
&= \left(\frac{(x_0^2 - b)^2}{4y_0^2}, \frac{(x_0^2 - b)(y_0^4 - a^2x_0^4 + 4bx_0^4)}{8y_0^3}\right)
\end{aligned}$$

Compare this with $[2](x_0, y_0) = (\lambda^2 - 2x_0 - a, \lambda(x_0 - x_3) - y_0)$, where $\lambda = (3x_0^2 + 2ax_0 + b)/(2y_0)$. First coordinate

$$\begin{aligned}
\lambda^2 - 2x_0 - a &= \left(\frac{3x_0^2 + 2ax_0 + b}{2y_0}\right)^2 - 2x_0 - a = \frac{(3x_0^2 + 2ax_0 + b)^2 - 8x_0y_0^2 - 4ay_0^2}{4y_0^2} \\
&= \frac{(3x_0^2 + 2ax_0 + b)^2 - 8x_0(x_0^3 + ax_0^2 + bx_0) - 4a(x_0^3 + ax_0^2 + bx_0)}{4y_0^2} = \frac{(x_0^2 - b)^2}{4y_0^2}.
\end{aligned}$$

Since the resulting point is on E it can be either $[2](x_0, y_0)$ or $[-2](x_0, y_0)$; check leads to $\psi \circ \bar{\varphi} \circ \varphi(x_0, y_0) = [2](x_0, y_0)$

For $\frac{m}{n} \in \mathbb{Q}$ define *height* $H\left(\frac{m}{n}\right) = \max\{|m|, |n|\}$. So $H : \mathbb{Q} \to \mathbb{N}$.

Note that for any r the cardinality of $\{\frac{m}{n} \in \mathbb{Q} \,\big|\, H\left(\frac{m}{n}\right) < r\}$ is finite.

Definition: Let $P = (x_0, y_0) \in E(\mathbb{Q})$. Define $H(P) = H(x_0)$ and $H(P_\infty) = 1$. The *small height* or *logarithmic height* is given by $h(P) = \log H(P)$, $h(P_\infty) = 0$.

Properties of the height function for sums of points:
There exist κ_0 depending only on P_0 and coefficients of f and κ depending only on coefficients of f so that

$$h(P \oplus P_0) \leq 2h(P) + \kappa_0 \text{ and } h([2]P) \geq 4h(P) - \kappa.$$

Let E be defined over $\mathbb{Z}$ by $E : y^2 = f(x)$. Consider reduction of each coefficient modulo $p > 3$:

$$\tilde{E} : \tilde{y}^2 = \tilde{x}^3 + \tilde{a_2}\tilde{x}^2 + \tilde{a_4}\tilde{x} + \tilde{a_6} = \tilde{f}(\tilde{x}),$$

where $a_i \equiv \tilde{a_i} \bmod p$.

$\tilde{E}$ non-singular $\Leftrightarrow$ $\mathrm{disc}(\tilde{f}) \neq 0 \Leftrightarrow \mathrm{disc}(f) \not\equiv 0 \bmod p \Leftrightarrow p \nmid \mathrm{disc}(f)$. Since for $E/\mathbb{Z}$ also $\mathrm{disc}(f)$ there are only finitely many primes p of bad reduction (those dividing the discriminant of f).
Let $P = (x_0, y_0) \in E(\mathbb{Z}) \Rightarrow \tilde{P} = (\tilde{x_0}, \tilde{y_0}) \in \tilde{E}(\mathbb{F}_p)$, where $x_0 \equiv \tilde{x_0} \bmod p$ and $y_0 \equiv \tilde{y_0} \bmod p$. To extend this to a map on all of $E(\mathbb{Q})$ we need to work with the projective model. Easy to see: rational points can be reduced modulo p if denominators are not divisible by p.

Lifting: Start with curve $\tilde{E}$ over $\mathbb{F}_p$, find curve E over $\mathbb{Q}$ so that reduction of E modulo p is $\tilde{E}$. What are good choices for E? See Joe Silverman's talk.

The rest of this talk is well covered by the slides posted online. The slides are a short version of my talk at the "ECRYPT PhD Summer School on Emerging Topics in Cryptographic Design and Cryptanalysis", see my homepage
`www.hyperelliptic.org/tanja`.