CS 681: Computational Number Theory and Algebra **Lecture 35**
Lecturer: Manindra Agrawal **Notes by: Ashwini Aroskar**

November 18, 2005.

Elliptic Curves on Finite Fields (contd)

Let $E(F_p)$ be the elliptic curve $y^2 = x^3 + Ax + B (mod\ p)$
We also use $E(F_p)$ to denote the set of points on the curve over F_p.

We will study $E(\bar{F}_p)$ where $\bar{F}_p$ is the algebraic closure of F_p.
We want to characterize points of $E(F_p)$ in $E(\bar{F}_p)$. As $\bar{F}_p$ is a field of characteristic p, we can raise the coordinates to the p_{th} power and we derive the following test.

Define $\phi_p(x, y) = (x^p, y^p)$
Observation: ϕ_p is identity on (x, y) *iff* $(x, y) \in E(F_p)$
Equivalently, $\phi_p - 1$ is 0 on (x, y) *iff* $(x, y) \in E(F_p)$.

Note: When we write $\phi_p - 1$, the subtraction is the one defined on the elliptic curve.

Observation: $\phi_p - 1$ is a homomorphism from $E(\bar{F}_p)$ to $E(\bar{F}_p)$.

Proof:
$\phi_p - 1[(x_1, y_1) + (x_2, y_2)] = \phi_p[(x_1, y_1) + (x_2, y_2)] - (x_1, y_1) - (x_2, y_2)$
Denote the sum of the two points on the curve as (x_3, y_3)
Let $m = \frac{y_2^p - y_1^p}{x_2^p - x_1^p}$

$$\begin{aligned}
\phi_p(x_3, y_3) &= (x_3^p, y_3^p) \\
&= [(m^2 - x_1 - x_2)^p, -y_1 - m(x_3 - x_1)^p] \\
&= [m^{2p} - x_1^p - x_2^p, -y_1^p - m^p(x_3^p - x_1^p)] \quad (mod p) \\
&= \phi_p(x_1, y_1) + \phi_p(x_2, y_2)
\end{aligned}$$

Also note that each coordinate of the image of a point under this homomorphism is a rational function in x and y.

$$\begin{aligned}
\phi_p - 1(x, y) &= (x^p, y^p) - (x, y) \\
&= (x^p, y^p) + (x, -y) \\
&= (\frac{y^p + y}{x^p - x}^2 - x^p - x, ...)
\end{aligned}$$

Let $\psi : E(\bar{F}_p) \longrightarrow E(\bar{F}_p)$ be a homomorphism given by $\psi(x,y) = (r_1(x,y), r_2(x,y))$, where r_1 and r_2 are rational functions in x and y.
Such a ψ is called an endomorphism.
Thus, $\phi_p - 1$ is called an endomorphism.

So, we can state the previous observation as follows:
Observation: $Ker(\phi_p - 1) = E(F_p)$

Let $\psi(x,y) = (\frac{p(x,y)}{q(x,y)}, \frac{r(x,y)}{s(x,y)})$ $\quad p, q, r, s$ polynomials in x and y
Replacing $y^2 = x^3 + Ax + B$, we get
$\psi(x,y) = (\frac{p_1(x)+yp_2(x)}{q_1(x)+yq_2(x)}, \frac{r_1(x)+yr_2(x)}{s_1(x)+ys_2(x)})$
For the first coordinate, multiply both numerator and denominator by $q_1(x) - yq_2(x)$ and replace y^2 in terms of x again. Similarly for thr second coordinate. So we get
$\psi(x,y) = (\frac{p_3(x)+yp_4(x)}{q_3(x)}, \frac{r_3(x)+yr_4(x)}{s_3(x)})$

If $\psi(x,y) = (u,v)$. As $\psi(O) = O$, $\psi(x,-y) = (u,-v)$
Therefore $y \longrightarrow -y$ must leave u changed and change the sign of v.
$\Longrightarrow p_4(x) = 0, r_3(x) = 0$

Thus we can write ψ in the standard or normal form as
$\psi(x,y) = (\frac{p(x)}{q(x)}, y\frac{r(x)}{s(x)})$

Further we may also assume $(p(x), q(x)) = 1 = (r(x), s(x))$

Therefore we have $\frac{y^2r^2}{s^2} = \frac{p^3}{q^3} + A\frac{p}{q} + B$

So, $s^2(p^3 + Apq^2 + Bq^3) = q^3r^2(x^3 + Ax + B)$

A root of q is obviously a root of s since it cannot be a root if p.

Conversely let α be a root of s.
Assume the elliptic curve is non-singular, that is, $x^3 + Ax + B$ has no repeated root.
$(x-\alpha)^2$ divides the R.H.S. r cannot have α as a root. As the curve is non-singular, $(x-\alpha)^2 | q^3(x)$, α is a root of q.
So, q and s have the same roots.

The curve is singular is $x^3 + Ax + B$ has repeated roots, that is,
$\Longleftrightarrow (x^3 + Ax + B, 3x^2 + A) \neq 1$
$\Longleftrightarrow (\frac{2}{3}Ax + B, 3x^2 + A) \neq 1$
$\Longleftrightarrow (\frac{2}{3}Ax + B, \frac{27B^2}{4A^2} + A) \neq 1$

The curve is singular *iff* $4A^3 + 27B^2 = 0$

We define the degree of ψ as the maximum of the degree of p and q.

Endomorphism ψ is said to be *separable* if $p'q - pq'$ is not identically zero. Obviously $\phi_p(x, y)$ is not separable as the computations are modulo p.

Theorem: Let $\psi(x, y) = (\frac{p(x)}{q(x)}, y\frac{r(x)}{s(x)})$ be any separable endomorphism. Then $|Ker\psi| = deg(\psi)$