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 $E(\overline{F}_p)$ where $\overline{F}_p$ is the algebraic closure of $F_p$.
We want to characterize points of $E(F_p)$ in $E(\overline{F}_p)$. As $\overline{F}_p$ 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: $\phi_p$ 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 $E(\overline{F}_p)$ to $E(\overline{F}_p)$.

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 $m = \frac{y_2^p - y_1^p}{x_2^p - x_1^p}$

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

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

$\phi_p - 1(x, y) = (x^p, y^p) - (x, y)$
$= (x^p, y^p) + (x, -y)$
$= \left(\frac{y^p + y^2}{x^p - x} - x^p - x, \ldots\right)$
Let $\psi : E(F_p) \rightarrow E(F_p)$ 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 $\psi$ is called an endomorphism.

Thus, $\phi_p - 1$ is called an endomorphism.

So, we can state the previous observation as follows:

**Observation:** $\text{Ker}(\phi_p - 1) = E(F_p)$

Let $\psi(x, y) = (p(x, y), r(x, y))$. Replacing $y^2 = x^3 + Ax + B$, we get $\psi(x, y) = \left(\frac{p(x,y)}{q(x,y)}, \frac{r(x,y)}{s(x,y)}\right)$. Further we may also assume $(p(x), q(x)) = (r(x), s(x))$.

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

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

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

Conversely let $\alpha$ 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 $\alpha$ as a root. As the curve is non-singular, $(x - \alpha)^2|q^3(x)$, $\alpha$ is a root of $q$.

So, $q, s$ have the same roots.

The curve is singular is $x^3 + Ax + B$ has repeated roots, that is,

$\iff (x^3 + Ax + B, 3x^2 + A) \neq 1$

$\iff (\frac{2}{3}Ax + B, 3x^2 + A) \neq 1$

$\iff (\frac{2}{3}Ax + B, 27B^2 + A) \neq 1$

The curve is singular iff $4A^3 + 27B^2 = 0$
We define the degree of $\psi$ as the maximum of the degree of $p$ and $q$.

Endomorphism $\psi$ 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 $|\text{Ker}\psi| = \text{deg}(\psi)$