CS 681: Computational Number Theory and Algebra **Lecture 37: Elliptic Curves (Continued)**
Lecturer: Manindra Agrawal **Notes by: Arun Iyer**
November 24, 2005.

1 Last Lecture Recap

Let $\psi(x,y) = \left(\frac{p(x)}{q(x)} \quad , \quad y\frac{u(x)}{v(x)} \right)$ be an endomorphism on $E(\overline{F_p})$.

Definition 1.1 *Degree of the endomorphism ψ, deg(ψ), is defined as max(deg(p),deg(q)).*

Definition 1.2 *Endomorphism ψ is said to be separable if $p'q - pq'$ is not identically zero.*

The following theorem was then proved in the last lecture,

Theorem 1.1 *Let $\psi(x,y) = \left(\frac{p(x)}{q(x)} \quad y\frac{u(x)}{v(x)} \right)$ be any separable endomorphism. Then,*

$$|ker(\psi)| = deg(\psi)$$

Let $E[n] \subseteq E(\overline{F_p})$ be the set of points P in $E(\overline{F_p})$ such that $nP = 0$. Then, it was shown that,

$$E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n, \quad p \not| \ n$$

2 The Weil Pairing

Let η be a primitive n^{th} root of unity ($\eta \in \overline{F_p}$), there is a function

$$e_n : E[n] \times E[n] \rightarrow \{1, \eta, \ldots, \eta^{n-1}\}$$

called **the Weil Pairing** such that,

1. e_n is bilinear. This means that

   $$e_n(P + S, Q) = e_n(P, Q)e_n(S, Q)$$

   and

   $$e_n(P, S + Q) = e_n(P, S)e_n(P, Q)$$

   $\forall P, Q, S \in E[n]$

2. If $e_n(P, Q) = 1$ for all Q, then $P = \bigcirc$. Similarly, if $e_n(P, Q) = 1$ for all P, then $Q = \bigcirc$

3. $e_n(P,P) = 1, \forall P \in E[n]$
4. $e_n(P,Q) = e_n^{-1}(Q,P)$
5. For any automorphism ϕ of $\overline{F_p}$, if $\phi(A) = A$ and $\phi(B) = B$, then $\phi(e_n(P,Q)) = e_n(\phi(P), \phi(Q))$
6. For any endomorphism ψ of $E(\overline{F_p})$, $e_n(\psi(P), \psi(Q)) = e_n(P,Q)^{deg(\psi)}$

3 Hasse's Theorem

Theorem 3.1 *Let E be an elliptic curve over the finite field F_p. Then the order of $E(F_p)$ satisfies,*

$$|p + 1 - \#E(F_p)| \leq 2\sqrt{p}$$

Proof: Consider the action of endomorphism ψ on $E[n]$ ($p \not| n$ and $E[n] \cong \mathbb{Z}_n \oplus \mathbb{Z}_n$). There exists two points $T_1, T_2 \in E[n]$ such that,

$$E[n] : (\mathbb{Z}_n)T_1 + (\mathbb{Z}_n)T_2$$

Let $\alpha T_1 + \beta T_2 \in E[n]$.
$\psi(\alpha T_1 + \beta T_2) = \alpha\psi(T_1) + \beta\psi(T_2)$
Let $\psi(T_1) = aT_1 + bT_2$ and $\psi(T_2) = cT_1 + dT_2$
If we view $\alpha T_1 + \beta T_2$ as vector $\begin{bmatrix} \alpha \\ \beta \end{bmatrix}$, then

$$\psi \begin{bmatrix} \alpha \\ \beta \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \alpha \\ \beta \end{bmatrix} (mod\ n)$$

Let

$$M_n^{\psi} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$$

We have from the Weil Pairing Property 6,

$$\begin{aligned} e_n(T_1,T_2)^{deg(\psi)} &= e_n(\psi(T_1), \psi(T_2)) \\ &= e_n(aT_1 + bT_2, cT_1 + bT_2) \\ &= e_n(aT_1, cT_1)e_n(aT_1, dT_2)e_n(bT_2, cT_1)e_n(bT_2, dT_2) && \text{[Property (1)]} \\ &= e_n(T_1,T_1)^{ac}e_n(T_1,T_2)^{ad}e_n(T_2,T_1)^{bc}e_n(T_2,T_2)^{bd} && \text{[Property (1)]} \\ &= e_n(T_1,T_2)^{ad-bc} && \text{[Property (3) and (4)]} \end{aligned}$$

Therefore,

$$deg(\psi) = (ad - bc) = |M_n^{\psi}|(mod\ n) \tag{1}$$

Letting $\psi = \phi_p - 1$, we get,

$$|M_n^{\phi_p}| = p(mod\ n)$$
$$|M_n^1| = 1(mod\ n)$$

Now, $M_n^{r\phi_p+s} = M_n^{r\phi_p} - M_n^s = rM_n^{\phi_p} - sI$ for $(r,s) = 1$

Claim 3.1 *Given M and N are two 2×2 matrices, then*

$$|\alpha M + \beta N| = \alpha^2|M| + \beta^2|N| + \alpha\beta(|M+N| - |M| - |N|)$$

Using claim 3.1,

$$\begin{aligned} |rM_n^{\phi_p} - sI| &= r^2p + s^2 - rs(|M_n^{\phi_p} - I| - p - 1) \\ &= r^2p + s^2 - rs(|E(F_p)| - p - 1) \end{aligned}$$

Let $|E(F_p)| = p + 1 + a$.
Therefore, $|rM_n^{\phi_p} - sI| = r^2p + s^2 - rsa$.
¿From equation 1,

$$deg(r\phi_p - s) = |rM_n^{\phi_p} - sI| = r^2p + s^2 - rsa(mod\ n)$$

However,

$$\begin{array}{llll} & deg(r\phi_p - s) & \geq & 0 \\ \Rightarrow & r^2p + s^2 - rsa & \geq & 0 \\ \Rightarrow & x^2p - ax + 1 & \geq & 0 & \text{where x} = \frac{r}{s} \text{ i.e } x \in \mathbb{Q} \\ \Rightarrow & x^2p - ax + 1 & \geq & 0 & \text{for all } x \text{ reals, since } \mathbb{Q} \text{ is dense in } \mathbb{R} \\ \Rightarrow & a^2 - 4p & \leq & 0 \\ \Rightarrow & a & \leq & 2\sqrt{p} \\ \Rightarrow & |p + 1 - \#E(F_p)| & \leq & 2\sqrt{p} \end{array}$$

Hence proved. ■