

CS559 Curve Based Cryptography - Prof. Ming-Deh Huang
Scribe: Iftikhar A Burhanuddin
burhanud@usc.edu
Classes #10 - March 19, 2002

Administrivia: Scribe notes for class #9 are online at the course webpage:
<http://www-rcf.usc.edu/~mdhuang/cs599>

Today's class:

1. Possible Project Topics
2. Frobenius Endomorphism
3. Schoof's Point Counting Algorithm

I. Possible Project Topics:

1. ECDSA vs DSA
2. Counting points on elliptic curves - constructive aspects of ECC
3. E/\mathbf{F}_q , where q is a large prime vs E/\mathbf{F}_{p^n} , where p is a small prime 2, 3, ... such that $q \approx p^n$
4. Industrial trends - wireless/smart cards
5. Constructive use of Weil Pairing in cryptography
6. Quantum computing
7. What quantum cryptography says about hard problems like integer factoring, DLP, ECDLP, etc.
8. Hyper elliptic curves, Hyperelliptic curve DLP
9. Experimental projects on representation of \mathbf{F}_{p^n} , choice of suitable basis for E/\mathbf{F}_{p^n} computation, etc.

Send an email to Prof. Ming Deh-Huang at huang@pollux.usc.edu before 03/26/02 with project topic and url of the project webpage.

II. Frobenius Endomorphism:

The point counting algorithm we'll discuss today is not restricted to prime finite fields, the field may have $q = p^n$ elements, but we'll restrict our talk to the case when q is a large prime.

Suppose $E : y^2 = x^3 + ax + b$ is an elliptic curve over \mathbf{F}_q with $a, b \in \mathbf{F}_q$. We are interested in computing in an efficient time the cardinality of the \mathbf{F}_q rational points

$$|E(\mathbf{F}_q)| = \#\{(x, y) \mid x, y \in \mathbf{F}_q, y^2 = x^3 + ax + b\} \cup \{O\}$$

By *efficient* we mean that the running time is polynomial $\log q$, so we'll rule out naive counting which will take $O(q)$ time. The algorithm we'll discuss involves computing the characteristic polynomial of the Frobenius endomorphism [1].

Let's look at $E(\overline{\mathbf{F}}_q)$, that is all possible solutions of $E : y^2 = x^3 + ax + b$ over $\overline{\mathbf{F}}_q$ the algebraic closure of \mathbf{F}_q . Say $P = (x, y) \in E(\overline{\mathbf{F}}_q)$, so $x, y \in \overline{\mathbf{F}}_q$. Consider the map $(x, y) \rightarrow (x^q, y^q)$ which preserves the point at infinity.

Claim: The resulting point (x^q, y^q) is still a point on $E(\overline{\mathbf{F}}_q)$

Proof: Consider

$$y^2 = x^3 + ax + b$$

Raising the RHS to the q -th power we note that as $a, b \in \mathbf{F}_q$ and $a^q = a$ and $b^q = b$ by Flt

$$\begin{aligned} (x^3 + ax + b)^q &= x^{3q} + a^q x^q + b^q \quad \text{char } \mathbf{F}_q = q \\ &= x^{3q} + ax^q + b \end{aligned}$$

Raising the LHS to the q -th power gives y^{2q} . Hence $(y^q)^2 = (x^q)^3 + ax^q + b$ and $(x^q, y^q) \in E(\overline{\mathbf{F}}_q)$ \diamond .

We'll see that this map $\rho : E(\overline{\mathbf{F}}_q) \rightarrow E(\overline{\mathbf{F}}_q)$ is a group homomorphism and is called the *Frobenius endomorphism*. In fact the set of endomorphisms forms a ring with addition and composition as the ring operations.

Remark: More generally, if you have a set of m polynomials in n variables over \mathbf{F}_q : $F_i(x_1, \dots, x_n)$, $1 \leq i \leq m$ (*) and we are interested in the solutions to this system of polynomials. Say (x_1, \dots, x_n) is a solution to (*) that is $F_i(x_1, \dots, x_n) = 0$, $1 \leq i \leq m$. Using an argument similar to the one polynomial case, we know that

$$F_i(x_1^q, \dots, x_n^q) = (F_i(x_1, \dots, x_n))^q, \quad 1 \leq i \leq m$$

As $F_i(x_1^q, \dots, x_n^q) = 0$, $1 \leq i \leq m$, we see that (x_1^q, \dots, x_n^q) is a solution to (*) \diamond

Claim: Say $T_1, T_2 \in E(\overline{\mathbf{F}}_q)$, $\rho(T_1 \oplus T_2) = \rho(T_1) \oplus \rho(T_2)$.

Proof: Suppose $T_1 = (x_1, y_1)$, $T_2 = (x_2, y_2)$ and $T_1 \oplus T_2 = (x_3, y_3)$

Once the curve is defined over \mathbf{F}_q , then the addition is defined over \mathbf{F}_q . So by the addition law formulae say $x_3 = \frac{h_1(x_1, y_1, x_2, y_2)}{h_2(x_1, y_1, x_2, y_2)}$ and h_1, h_2 are polynomials with coefficients in \mathbf{F}_q . We know that by definition $\rho(T_1) = (x_1^q, y_1^q)$ and $\rho(T_2) = (x_2^q, y_2^q)$ and that the x -coordinate of $\rho(T_1) \oplus \rho(T_2)$ is given by $\frac{h_1(x_1^q, y_1^q, x_2^q, y_2^q)}{h_2(x_1^q, y_1^q, x_2^q, y_2^q)}$

Our *Remark* tells us that for a function g defined over \mathbf{F}_q $g(x_1^q, \dots, x_n^q)$ is equal to $[g(x_1, \dots, x_n)]^q$.

So the x -coordinate of $\rho(T_1) \oplus \rho(T_2) = \frac{[h_1(x_1, y_1, x_2, y_2)]^q}{[h_2(x_1, y_1, x_2, y_2)]^q} = x_3^q$. A similar argument for the y -coordinate completes the proof for the following lemma.

Lemma: Suppose $T_1 = (x_1, y_1), T_2 = (x_2, y_2)$ and $T_1 \oplus T_2 = (x_3, y_3)$ then $\rho(T_1) = (x_1^q, y_1^q), \rho(T_2) = (x_2^q, y_2^q)$ and $\rho(T_1) \oplus \rho(T_2) = (x_3^q, y_3^q)$

III. Schoof's Point Counting Algorithm:

Let's consider the action of the Frobenius map on the l -torsion points, where l is a prime. Say $T = (x_1, y_1) \in E[l]$, we know that $\rho(T) \in E(\overline{\mathbf{F}}_q)$. Infact we'll show that $\rho(T) \in E[l]$. Recall that ρ is a group homomorphism so

$$O = \rho(O) = \rho(l.T) = \rho(T \oplus \dots \oplus T) = \rho(T) \oplus \dots \oplus \rho(T) = l.\rho(T)$$

Therefore $\rho(T)$ is also an l -torsion point. Moreover this ρ map is an isomorphism on $E[l]$

$$\rho : E[l] \xrightarrow{\cong} E[l]$$

The intuition for this isomorphism is that the map $\rho : E(\overline{\mathbf{F}}_q) \rightarrow E(\overline{\mathbf{F}}_q)$ is a 1-1 map and it doesn't send a non-zero point to zero and the same holds for the ρ map restricted to the l -torsion points.

$E[l]$ is a vector space over $\mathbf{Z}/l\mathbf{Z}$ of dimension 2, that is there exist $S, T \in E[l]$ such that $E[l] = \{a.S \oplus b.T \mid 0 \leq a, b \leq l-1\} = \mathbf{Z}/l\mathbf{Z}S \oplus \mathbf{Z}/l\mathbf{Z}T$. It is a direct sum as a point can be uniquely written using S and T .

Recall that a linear map on a vector space has a characteristic polynomial. Say $\rho(S) = a.S \oplus b.T, \rho(T) = c.S \oplus d.T$ for some $a, b, c, d \in \mathbf{Z}/l\mathbf{Z}$

$$\rho : \begin{matrix} S \\ T \end{matrix} \rightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Then the *unique* characteristic polynomial of ρ on $E[l]$ is given by $(x-a)(x-d) - bc = x^2 - tx + \delta$ where $t = a + d$ is the trace of the matrix and $\delta = ad - bc$ is determinant of the matrix. By definition of the characteristic polynomial, $\rho^2 - (a+d)\rho + (ad-bc)$ kills everybody in the vector space,

$$[\rho^2 - (a+d)\rho + (ad-bc)](v) = 0 \text{ for all } v \in \mathbf{Z}/l\mathbf{Z}$$

S and T are not linearly dependent $S = k.T$, where $1 \leq k \leq l-1$. l is small so it is not solving the *DLP*

Remark: $E[l] \subset E[l^2] \subset E[l^3] \subset \dots$

Pick $T_0 \in E(\overline{\mathbf{F}}_q)$ and choose T_1 such that $l.T_1 = T_0$. Notice that there are l^2 ways of choosing T_1 as

$$l.T_1 = T_0 \Rightarrow l.(T_1 \oplus R) = T_0 \Rightarrow R \in E[l]$$

Similarly choose T_2, T_3, \dots such that $l.T_2 = T_1, l.T_3 = T_2, \dots$

Now consider the set

$$\{(T_0, T_1, T_2, \dots) \mid T_0 \in E(\overline{\mathbf{F}}_q), l.T_i = T_{i-1}, i \geq 1\}$$

This set is a 2-dimensional vector space over the l -adic field \mathbf{Q}_l . Applying the ρ map coordinate wise,

$$\rho(T_0, T_1, T_2, \dots) := (\rho(T_0), \rho(T_1), \rho(T_2), \dots)$$

The image stays in the set as $l.\rho(T_i) = \rho(l.T_i) = \rho(T_{i-1})$, $i \geq 1$

1. It turns out that the characteristic of ρ which is defined over \mathbf{Q}_l , is a rational polynomial χ_ρ (recall that $\mathbf{Q}[x] \hookrightarrow \mathbf{Q}_l[x]$)
2. For all but finitely many l , $\chi_\rho \bmod l =$ characteristic polynomial of ρ on $E[l]$
3. In the case of elliptic curves $\chi_\rho = x^2 - tx + q$ where t is called the trace of the Frobenius and $t \leq 2\sqrt{q}$ [Hasse's Theorem]
4. $|E(\mathbf{F}_q)| = q + 1 - t = \chi_\rho(1)$

According to [3] $\chi_\rho \bmod l \equiv x^2 - \bar{t}x + \bar{q}$ where $\bar{t} = t \bmod l$, $\bar{q} = q \bmod l$. For primes $l = 5, 7, \dots, \log q$ we construct the characteristic polynomial of ρ acting on $E[l]$ and compute the trace which is $t \bmod l$. Using the Chinese Remainder Theorem on $t \bmod l$'s for the different primes l , we can recover the unique *unique* t modulo $4\sqrt{q}$ and the Hasse theorem that tells us this is the t we need to compute $|E(\mathbf{F}_q)| = q + 1 - t$. Schoof's algorithm runs in $O(\log^8 q)$ and with refinements it can be made to run in $O(\log^5 q)$

Bibliography:

1. R. Schoof, Counting points on elliptic curves over finite fields, Journal Theorie des Nombres de Bordeaux, vol. 7, 1995, pp. 219-254