Edoardo Persichetti Lecture 7: Elliptic Curves 01/04/2014

Notes written by Marcin Andrychowicz

Frobenius

Definition 1 (Frobenius endomorphism) $\phi_q : \overline{\mathbb{F}}_q \to \overline{\mathbb{F}}_q$ is defined by the formula $\phi_q(x) = x^q$.

Remark 1 $\phi_q(x) = x$ for all $x \in \mathbb{F}_q$.

Theorem 1 *Let E be an elliptic curve over $\mathbb{F}_q$ and $(x, y) \in E(\overline{\mathbb{F}}_q)$. Then,*

1. $\phi_q(x, y) \in E(\overline{\mathbb{F}}_q)$
2. $(x, y) \in E(\mathbb{F}_q) \iff \phi_q(x, y) = (x, y)$

Endomorphisms All endomorphisms of an elliptic curve form a monoid. Examples of endomorphisms are:

$0 : (x, y) \to \infty$

$1 : (x, y) \to (x, y)$

$-1 : (x, y) \to -(x, y)$

$\alpha : (x, y) \to \alpha(x, y)$

Theorem 2 *Let E be an elliptic curve over $\mathbb{F}_q$ and $a = q + 1 - \#E(\mathbb{F}_q)$. Then*

$$\phi_q^2 - a\phi_q + q = 0. \tag{1}$$

Moreover, a is the only integer such that (1) holds.

Theorem 3 *Let E be an elliptic curve over $\mathbb{F}_q$ and $a = q + 1 - \#E(\mathbb{F}_q)$. Then,*

1. $E(\mathbb{F}_{q^n}) = Ker(\phi_q^n - 1)$
2. $\#E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n)$ *for α, β such that $x^2 - ax + q = (x - \alpha)(x - \beta)$.*

Proof Point 1 follows directly from Theorem 1, since $\phi_q^n = \phi_{q^n}$. For point 2, consider the function $f(x) = (x^n - \alpha^n)(x^n - \beta^n) = x^{2n} - (\alpha^n + \beta^n)x^n + q^n$. Notice that $f(\alpha) = f(\beta) = 0$, so $x^2 - ax + q | f(x)$ and hence $f(x) = (x^2 - ax + q)Q(x)$ for some polynomial $Q(x)$. Moreover,

$$(\phi_q^n)^2 - (\alpha^n + \beta^n)\phi_q^n + q^n = f(\phi_q) = Q(\phi_q)(\phi_q^2 - a\phi_q + q) = 0.$$

Remember, by Theorem 2, that $q^n + 1 - \#E(\mathbb{F}_{q^n})$ is the *unique* k such that $(\phi_q^n)^2 - k\phi_q^n + q^n = 0$, so $q^n + 1 - \#E(\mathbb{F}_{q^n}) = \alpha^n + \beta^n$, which concludes the proof.

Counting points on specific curves

Theorem 4 *Let $E : y^2 = x^3 - kx$ be an elliptic curve over $\mathbb{F}_q$ and $k \not\equiv 0 \mod q$.*

1. *If $q \equiv 3 \mod q$, then $\#E(\mathbb{F}_q) = q + 1$.*
2. *If $q \equiv 1 \mod 4$, then*

$$\#E(\mathbb{F}_q) = \begin{cases} q + 1 - 2a & \text{if } k \text{ is 4th power mod } q \\ q + 1 + 2a & \text{if } k \text{ is a square (but not a 4th power) mod } q \\ q + 1 \pm 2b & \text{if } k \text{ is not a square mod } q \end{cases}$$

for $a, b \in \mathbb{Z}$ s.t. $2|a$, $a + b \equiv 1 \mod 4$ and $q = a^2 + b^2$.

Example $E : y^2 = x^3 - x$ over $\mathbb{F}_q$ for $q = 61$. Then $a = -5$ and $b = 6$, k is a 4th power mod q, so $\#E(\mathbb{F}_q) = 61 + 1 - 2 \cdot (-5) = 72$.

Theorem 5 *Let E be an elliptic curve over $\overline{\mathbb{F}}_q$ for $q = p^k$ and $a = q + 1 - \#E(\mathbb{F}_q)$. Then, $E(\overline{\mathbb{F}}_q)$ is supersingular (i.e. $E[q] = \{\infty\}$) $\iff a \equiv 0 \mod p \iff \#E(\mathbb{F}_q) \equiv 1 \mod p$.*

Proof The last equivalence is immediate, since $a = q + 1 - \#E(\mathbb{F}_q)$. ($\Leftarrow$)
Remember that $\#E(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n)$ for α, β s.t. $x^2 - ax + q = (x - \alpha)(x - \beta)$. Let $S_n = \alpha^n + \beta^n$. Notice, that it can be also defined by $S_0 = 2, S_1 = a, S_{n+1} = aS_n - qS_{n-1}$. All the equivalences will be mod p. From the latter definition we notice that $S_n \equiv 0$ for all $n \geq 1$. Moreover, $\#E(\mathbb{F}_q) = q^n + 1 - S_n \equiv 1$, so there are no points of order p in $E(\mathbb{F}_{q^n})$. $\overline{\mathbb{F}}_q = \bigcup_{n \geq 1} \mathbb{F}_{q^n}$, so there are no points of order p in $E(\overline{\mathbb{F}}_q)$, hence it is supersingular.
($\Rightarrow$)
We prove the contrapositive. Suppose $a \not\equiv 0$. Then, $S_1 \equiv a$ and $S_{n+1} \equiv aS_n$, so $S_n \equiv a^n$. Consequently, $\#E(\mathbb{F}_{q^n}) \equiv 1 - a^n \equiv 0$ for $n = p - 1$ from the Fermat's little theorem. Therefore, there are points of order p in $E(\mathbb{F}_{q^{p-1}})$ and $E(\overline{\mathbb{F}}_q)$ is not singular.

Elliptic curves in cryptography

Definition 2 ECDLP Given $P, Q \in E$ compute $n \in \mathbb{Z}$ such that $nP = Q$. Such n is denoted $\log_P(Q)$.

Remark 2 Notice that $\log_P(Q)$ may not always exist, however for cryptographic applications it is well defined since usually the point P is chosen first, and then Q is generated as a multiple.

Remark 3 Let k be the order of P. Then $\log_P(Q)$ is defined over $\mathbb{Z}_k$. Therefore, it follows that $\log_P : E(\mathbb{F}_q) \to \mathbb{Z}_k$ is a group homomorphism.

Cryptographic primitives based on the DLP in $\mathbb{Z}_q$ directly *translate* to the elliptic curves' setting. For example the DSA signature algorithm (refined version of ElGamal) is called ECDSA (currently one of the most efficient signature schemes available). Most attacks also translate to elliptic curves, e.g. collision attacks such as Pollard's ρ algorithm. What makes elliptic curves special is that there is no index calculus-like attack, which is the most efficient attack against DLP in $\mathbb{Z}_q$. Hence most efficient attack against general ECDLP has complexity $\approx \mathcal{O}(\sqrt{q})$.

However, just like for DLP (Pohlig-Hellman algorithm), in some instances the ECDLP is easier. In particular, for supersingular curves, there exists an attack called Menezes-Okamoto-Vanstone (MOV) that reduces ECDLP($\mathbb{F}_q$) to DLP($\mathbb{F}_{q^k}$) for some integer k, where k is called *embedding degree*. If k is small, it is then possible to efficiently attack DLP using fast algorithms such as index calculus. For supersingular curves, k is very small: for $a = 0$ we have $k = 2$ and in general $k \leq 6$.

Lenstra's factorization algorithm

It is the fastest known integer factorization algorithm in the class of algorithms whose complexity depends on the size of the factors (such as Pollard's $p-1$ algorithm). The algorithm goes as follows. Suppose we are trying to factor $N = pq$. Then:

1. Choose E_i and $P_i \in E_i(\mathbb{Z}_N)$ for $i = 1 \dots 20$ (in practice, we sample a point first and than sample a curve containing that point).

2. Choose $B \in \mathbb{Z}$ and compute $(B!)P_i$ for each i. This can fail if during the computation we have to compute the inverse of an element $a \in \mathbb{Z}_N$ s.t. $(a, N) \neq 1$. In this case though, the gcd gives us a factor of N.

3. If all computations of $(B!)P_i$ succeeded, then we start over again choosing new curves or increasing B.

The idea behind the algorithm is that $E(\mathbb{Z}_{pq}) = E(\mathbb{Z}_p) \oplus E(\mathbb{Z}_q)$. If the curve $E(\mathbb{Z}_p)$ has B-smooth order, than $(B!)P = \infty$ in $E(\mathbb{Z}_p)$. In such cases the algorithm finds a factor if only if $(B!)P \neq \infty$ in $E(\mathbb{Z}_q)$. This happens with very high probability.

When applied to singular curves, the algorithm yields classical factorization methods. In particular, for the special case of curve $y^2 = x^2(x + 1)$ this algorithm turns out to be equivalent to Pollard's $p-1$ factoring algorithm, while for $y^2 = x^2(x+a)$, where $a \neq 1$, it is equivalent to the $p+1$ method. Finally, for the curve $y^2 = x^3$, the attack is equivalent to a brute force algorithm.

The complexity of Lenstra's algorithm is $L_p(1/2, \sqrt{2} + o(1))$. For comparison, the quadratic sieve has a complexity of $L_N(1/2, 1 + o(1))$, so in the worst case the elliptic curve factoring method is as efficient as the quadratic sieve.