Lecture 11

Jose Capco (jcapco@risc.jku.at)

Recall the following result from the last lecture

Theorem 1. Let E, E_1, E_2 be elliptic curves over K then

a.) $\mathrm{Hom}(E_1, E_2)$ is a torsion-free $\mathbb{Z}$-module.

b.) The endomorphism ring $\mathrm{End}(E)$ has no zero-divisors and is of characteristic 0.

c.) The map $\mathrm{End}(E) \times \mathrm{End}(E) \to \mathbb{Z}$ defined by

$$(\psi, \phi) \mapsto \deg(\psi + \phi) - \deg \psi - \deg \phi$$

is $\mathbb{Z}$-bilinear i.e. we have the identity

$$\deg(m\phi + n\psi) = m^2 \deg \phi + n^2 \deg \psi + mn(\deg(\phi + \psi) - \deg \phi - \deg \psi)$$

for all $\phi, \psi \in \mathrm{End}(E)$ and $m, n \in \mathbb{Z}$

d.) Let $K = \mathbb{F}_p$ and $m, n \in \mathbb{Z}$ such that $(m, n) \neq (0, 0)$ then $m\phi_p + n$ is separable iff $p \nmid n$.

Proposition 2. Let $\phi \neq 0$ be a non-trivial separable isogeny, then

$$\deg \phi = \#\ker(\phi)$$

Exercise 1. Modify the proof of the above without knowing that ϕ is surjective (this is not needed to prove it). Also, suppose we do not know that ϕ is separable, show that $\ker \phi$ is finite in fact show

$$\#\ker(\phi) \leq \deg \phi$$

Hint: The proof is the same as previous lecture (only one line of argument is different).

In some of the proofs we may have used the fact that non-trivial isogenies are surjective, we will give the proof of this here

Proposition 3. Any non-trivial isogeny $\phi : E_1 \to E_2$ between two elliptic curves (over the same field) is surjective

Proof. Let $\phi : E_1 \to E_2$ be a non-trivial isogeny with $E_1 : y^2 = f_1(x)$ and $E_2 : y^2 = f_2(x)$ and write $\phi(x, y) = (r_1(x), yr_2(x))$ with $r_1(x) = p(x)/q(x)$ such that the polynomials p and q are coprime. Assume now $(\alpha, \beta) \in E_2(\bar{K})\backslash\{O_2\}$. We have two cases $p - \alpha q$ is a constant or otherwise.

Suppose $p - \alpha q \in \bar{K}[x]\backslash K$ then it has a root $\alpha_0 \in \bar{K}$ and so $q(\alpha_0) \neq 0$ (because p and q are coprime). So by a previous exercise we know that $r_2(\alpha_0)$ is defined. Let β_0 be the square root of $f_1(\alpha_0)$, so $(\alpha_0, \beta_0) \in E_1(\bar{K})$. Since ϕ is an isogeny $(\alpha, \beta_0 r_2(\alpha_0)) \in E_2(\bar{K})\backslash\{O_2\}$. So if $\beta_0 r_2(\alpha_0) \neq \beta$ we must have $-\beta_0 r_2(\alpha_0) = \beta$. Either way we have

$$\phi(\alpha_0, \beta_0) = (\alpha, \beta) \quad \text{or} \quad \phi(\alpha_0, -\beta_0) = (\alpha, \beta)$$

Suppose now that $p - \alpha q$ is a constant. Then either p or q is nonconstant, because there are only finitely many points (α_0, β_0) mapping to E_2 with first coordinate α (we assume from the exercise above that we proved $\deg \phi \leq \#\ker \phi$ without knowing that ϕ is surjective). But this means that p and q must have the same degree and are both non-constant. So $p - \alpha q$ can only be a constant for at most one $\alpha \in \bar{K}$. In this particular case, ϕ may not map to at most two points (α, β) or $(\alpha, -\beta)$ of $E_2(\bar{K})$. To other points (infinite choices) of $E_2(\bar{K})$ we have a pre-image of ϕ. So let

$$Q \in E_2(\bar{K})\backslash\{O_2, (\alpha, \pm\beta), (\alpha, \pm\beta) - (\alpha, \beta)\}$$

and assume $\phi(P_1) = Q$ for some $P_1 \in E_1(\bar{K})$. Because $Q + (\alpha, \beta) \neq (\alpha, \pm\beta)$ we have a P_2 such that

$$\phi(P_2) = Q + (\alpha, \beta)$$

In particular $\phi(P_2 - P_1) = (\alpha, \beta)$ and $\phi(P_1 - P_2) = (\alpha, -\beta)$. □

Now we are ready to prove Hasse's theorem ...

Theorem 4. Let p be a prime number

1. We have $\ker(\phi_p - 1) = E$ for any elliptic curve $E = E(\mathbb{F}_p)$ over $\mathbb{F}_p$. Furthermore
$$\#E = \deg(\phi_p - 1)$$
2. Let $m, n \in \mathbb{Z}$ then $\deg(m\phi_p - n) = m^2 p + n^2 - mna$ where
$$a := p + 1 - \#E(\mathbb{F}_p) = p + 1 - \deg(\phi_p - 1)$$

Proof. 1. Because $\mathbb{F}_p \subset \overline{\mathbb{F}_p}$ is the set of zeros of $x^p - x$ (Fermat's Little Theorem) and the p-th root in a characteristic p field is unique, we conclude that $\phi_p(\alpha, \beta) \in E$ iff $(\alpha, \beta) \in E$. This just means that $\ker(\phi_p - 1) = E$.

By the last item in Theorem 1 we know that $\phi_p - 1$ is a separable isogeny and so the result follows from Proposition 2.

2. We use the bilinearity of the map in Theorem 1 part d.) and note that $\deg \phi_p = p$ and $\deg(-1) = 1$ to get
$$\deg(m\phi_p - n) = m^2 p + n^2 + mn(p + 1 - \deg(\phi_p - 1))$$
and the result follows

□

From the above theorem, Hasse's Theorem follows immediately

Hasse's Theorem. Let $E : y^2 = f(x)$ be an elliptic curve over a finite field $\mathbb{F}_p$, then $\#E$ is in the interval
$$[p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}]$$

Proof. The degree map is a nonnegative map, so if we divide the equality in the identity of the above theorem by n^2 we get
$$\deg(m\phi_p - n)/n^2 = p\frac{m^2}{n^2} - a\frac{m}{n} + 1 \geq 0$$
And this holds for any rational number $\frac{m}{n} \in \mathbb{Q}$. And so this follows for all numbers $r \in \mathbb{R}$ i.e.
$$pr^2 - ar + 1 \geq 0 \quad \forall r \in \mathbb{R}$$
This is equivalent to saying that the polynomial $px^3 - ax + 1$ has at most one real root iff the discriminant is non-positive i.e. $a^2 - 4p \leq 0$ and so $|a| \leq 2\sqrt{p}$. We thus have the inequality
$$|p + 1 - \deg(\phi_p - 1)| \leq 2\sqrt{p}$$
We also so from the above theorem that $\#E = \deg(\phi_p - 1)$ so Hasse's bound follows from that. □

Remark 5. Almost all of the result stated for elliptic curves over $\mathbb{F}_p$, p a prime, holds for any elliptic curve over $\mathbb{F}_q$, q a prime power. In particular Hasse's theorem for elliptic curves $E = E(\mathbb{F}_q)$ generalizes to
$$q + 1 - 2\sqrt{q} \leq \#E \leq q + 1 + 2\sqrt{q}$$

We finally discuss Lenstra's elliptic curve factorization algorithm.

Algorithm 1: Elliptic Curve Method (Lenstra)

Input: $n \in 2\mathbb{N}+1$ such that $\gcd(6,n)=1$, $B \in \mathbb{N}$ (power-smooth bound), `trials`$\in \mathbb{N}$
Output: A factor of n if it is composite and ECM is successful using B and `trials`

1 Choose Random a, α, β in $\{0, 1, \ldots, n-1\}$
2 Solve $b := \beta^2 - (\alpha^3 - a\alpha)$
3 Solve $\Delta := 4a^3 + 27b^2$
4 **if** $\Delta = 0$ *(rare)* **then goto** Line 1
5 Let $g := \gcd(n, \Delta)$
6 **if** $g = n$ *(rare)* **then goto** Line 1
7 **else if** $g > 1$ **then return** g
8 Fetch all prime numbers $p_1, \ldots, p_k$ less or equal to B
9 Fetch all $e_1, \ldots, e_k \in \mathbb{N}$ such that $p_i^{e_i}$ is highest p_i power less or equal B.
10 **for** i *from* 1 *to* k **do**
11 | **for** j *from* 1 *to* e_i **do**
12 | | **try**
13 | | | Set $P = p_i P$
14 | | **on error** *The denominator of the slope $d \in \mathbb{Z}$ in the addition formula is not invertible mod n*
15 | | **return** $\gcd(d, n)$
16 | |
17 | **end**
18 **end**
19 **return** No Result

Let us analyse this algorithm comparing it with Pollard's $p-1$:

- Given $n \in 2\mathbb{N}+1$ such that $6 \nmid n$ that we want to factorize we randomly choose a, b such that $n \nmid 4a^3 + 27b^2$ and $P = (\alpha, \beta) \in (\mathbb{Z}/n)^2$ satisfying

  $$\beta^2 = \alpha^3 + \alpha a + b$$

  Then for any prime divisor p of n the curve

  $$G_p := E_{a,b}(p) : y^2 = x^3 + ax + b$$

  is an elliptic curve over $\mathbb{F}_p$ and the reduction of P to $\mathbb{F}_p^2$ is a point in G_p.

- We now consider for such an n the group

  $$G_n := \prod_{p|n} E_{a,b}(p)$$

  There is a natural surjection $\phi_p : G_n \to G_p$

- We do not know the prime divisors p of n and do not exactly know G_n

- However, provided we do not get O, in one of the $E_{a,b}(p)$ we can do duplication and k-multiples of elements in G_n by using k-multiple formula in $E_{a,b}(n)$ (i.e. modulo n). So if reduction mod p is not O for any $p \mid n$, kP reduced to $\mathbb{F}_p^2$ is exactly the k-multiple of P reduced to $\mathbb{F}_p^2$

- Taking k-multiples like above is illegal (upon computation of slope μ we have a division by a number d not coprime to n) if the k-multiple of reduction of P to a $p \mid n$ is O. In other words, we are saying that if we know a non-trivial element in $\ker \phi_p$ then we can find a divisor of n. We are hoping for this!

- The strategy is to have an elliptic curve such that one of the G_p is B-smooth or B-power-smooth. But what are the chances??

The chances are based on a result by Deuring and of Lenstra:

1. Deuring 1941: Given a prime number p such that $p > 3$ and any number k in the Hasse interval
$$[p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}]$$
There is an elliptic curve E over $\mathbb{F}_p$ such that $\#E = k$

2. Lenstra Jr 1986: Probability of finding an elliptic curve E over $\mathbb{F}_p$ in the Hasse interval that is B-power-smooth (or B-smooth) is roughly the same as the probability finding a random number in the Hasse interval that is B-power-smooth (or B-smooth). So we can use the ψ in the estimates of Dickmann, Pomerance, Konyagin etc. to find this probability.

Exercise 2. Extend ECM such that you can collect which elliptic curves $E_{a,b}$ and which point $P \in E_{a,b}$ yields a factor $p \mid n$. Write a function that gives the order of such $E_{a,b}$ over $\mathbb{F}_p$ and provide some sample computation from your new algorithm.

Let us compare the results with Pollard's $p - 1$ method:

- In the $p - 1$ method we rely on the power-smoothness of $p - 1$ for some prime factor p of n
- In the elliptic curve method we rely on the choice of any power-smooth number in the interval
$$[p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p}]$$
for some prime factor p of n.

If one random elliptic curve does not work in the factorization we have the luxury of choosing another random elliptic curve. Lentra computed the complexity of finding a factor to be subexponential in terms of the log of the lowest prime divisor of n (so complexity does not depend on n, rather on the smallest divisor of it).

Example 6. The 10-th Fermat number
$$F_{10} := 2^{2^{10}} + 1$$
is a composite number and the two smallest prime factors were first found (by trial division) in the 50's and 60's. Only in 1995 did we had a complete factorization of this number by Richard Brent. This was one of the first successes of ECM over other factorization methods. F_{10} is factored as follows:
$$F_{10} = p_8 \cdot p_{10} \cdot p_{40} \cdot p_{252}$$
where there subscripts represent the number of the digits of the prime numbers. Imagine one wants to factor the composite $c_{291} := p_{40}p_{252}$ using the $p - 1$ method, then one has to deal with a prime factor of $p_{40} - 1$ with 23 digits and this exceed the bound B of B-power-smooth numbers that we can easily compute (6 digits are still feasible). Consider now the proposed elliptic curve by Brent that eventually factored this c_{291}:
$$E : 5y^2 = x^3 + ax + x \qquad \log_{10} a \sim 40$$
i.e. $a = 1597447308290318352284957343172858403618$. For this particular curve we have the following order
$$\#E = 2^2 \cdot 3^2 \cdot 5 \cdot 149 \cdot 197 \cdot 7187 \cdot 18311 \cdot 123677 \cdot 226133 \cdot 314263 \cdot 4677853$$
So the largest prime factor of $\#E$ has only 7 digits.

For those who are looking for a challenge: to this date, we have not fully factored F_{12}.