Elliptic Curves

Notes from a series of lectures by

René Schoof
Università di Roma “Tor Vergata”

Guest Lecturers: Henri Darmon, Isabelle Déchène, Eyal Goren, Andrew Granville and Kiran Kedlaya

The 2008 Barbados Workshop on Computational Complexity
March 2nd – March 9th, 2008

Organizer:
Denis Thérien

Scribes:
Anil Ada, Anne Broadbent, Arkadev Chattopadhyay, Matei David, Laszlo Egri, Mark Mercer, Nitin Saxena, Valentina Settimi, John Voight.

Lecture 1. Introduction

Lecturer: René Schoof Scribe: Anne Broadbent

"The kind of computer science we do, we like to call math.
René will be showing us some real mathematics."
— Denis Thérien

1.1 Introduction

The topic of these lectures are applications of elliptic curves. The main applications we will see are:

1. factoring integers
2. primality testing
3. discrete logarithm

Scribe notes: René Schoof will give five morning lectures, each approximately 2 hours each. Late afternoon lectures last approximately 1.5 hours and will be given by different speakers each day.

1.2 Factoring, primality testing and "$p-1$" algorithms

Factoring is the jungle
— René Schoof

The *Rabin-Miller* algorithm is a very efficient "probable" primality test. Applied to $n \in \mathbb{Z}_{>0}$, it can give two answers:

1. n is not prime
2. n could be prime.

In case 1, the answer is guaranteed to be correct and so we know that n is not prime. Case 2, is not so favourable, and all we can do is repeat the test to increase our confidence level (if the test always passes, we conclude that n is "very likely" a prime). This of course, does not give a proof of primality.

Depending on the situation, we can ask the following questions:

1. If n is not prime, what are its factors?

2. If n "very likely" prime, can we have a proof of primality?

Note: There exists a deterministic polynomial time primality test by Agrawal, Kayal and Saxena.

Let p be prime, then $p-1 = \#(\mathbb{Z}/p\mathbb{Z})^*$ is the *order* of $\mathbb{Z} \mod p$. We will also write $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$; it is a finite cyclic group.

Proposition 1. *Let A be a finite multiplicative Abelian group of order n (#A =n). Then:*

1. $\forall a \in A$, $a^n = 1$
2. $\forall a \in A$, *ord(a) divides* n.

1.2.1 $p-1$ factoring

Algorithm 1 is due to Pollard and goes back to the '70ies.

Algorithm 1 $p-1$ factoring

input: $n \in \mathbb{Z}_{>0}$ to be factored
output: non-trivial factor of n or $\perp$

1. Choose a bound B which will determine the time spent running the algorithm
2. Pick a random $x \in (\mathbb{Z}/p\mathbb{Z})^*$ with $\gcd(x,n) = 1$ (use Euclidean algorithm to test this)
3. Let M be the product of all prime powers smaller than B:

$$M = \prod_{q^{e(q)} < B} q^{e(q)}\,, \tag{1.1}$$

   where q is prime and $q^{e(q)}$ is the largest power of q that is less than B. By a version of the prime number theorem, $M \sim exp(B)$
4. Compute $\gcd(x^M - 1, n) = m$ by first computing $x^M \pmod n$ using modular exponentiation
5. If $m \neq 1$, output m, otherwise output $\perp$

The work required for the modular exponentiation is in $O(B \log^2 n)$, while the rest of step 4 is in $O(\log^3 n)$. The total work of algorithm 1 is in $O(B)$.

We now have $\gcd(X^M - 1, n)$, which obviously divides n. Let's see under which circumstances this algorithm gives us something useful.

If $\gcd(X^M - 1, n) \neq 1$, it is divisible by a prime $p|n$

$$\Leftrightarrow x^M - 1 \equiv 0 \pmod p \tag{1.2}$$

$$\Leftrightarrow x^M \equiv 1 \pmod p\,. \tag{1.3}$$

By Proposition 1, $x^{p-1} \equiv 1 \pmod{p}$ (Fermat's little theorem).

$$x^M \equiv 1 \pmod{p} \tag{1.4}$$
$$\Leftrightarrow p-1 \text{ divides } M \tag{1.5}$$
$$\Leftrightarrow p-1 \text{ is } B\text{-smooth} \tag{1.6}$$

Where the before-last equivalence is "not exactly an equivalence, but true in practice". Note that we say that $p-1$ is B-*smooth* if all primes dividing $p-1$ are less than B.

Hence we have success in algorithm 1 if n is divisible by a prime p with the property that $p-1$ is B-smooth. The problem is that in practice, if you want to factor n, you do not know p, and you do not know for which B, the number $p-1$ is B-smooth! The worst case arises when $n = pq$ with $p, q \approx \sqrt{n}$, and $p-1$ not smooth for any B, i.e. $p-1 = 2r$ for r prime, $r \approx \frac{1}{2}\sqrt{n}$. The total work in this case is in $O(B) \in O(\sqrt{r})$. The naive factoring algorithm runs in the same time, hence we haven't done much better.

We can formally analyze the probability that this algorithm will work, and conclude that the algorithm almost never works!

1.2.2 $p-1$ primality test (Pocklington 1916)

We now describe an algorithm for primality testing, it is based on a proposition:

Proposition 2. *Let $n-1=QR$. If for every prime $q|Q$ there exists $a \in (\mathbb{Z}/n\mathbb{Z})^*$ with $a^Q \equiv 1 \pmod{n}$ and $\gcd(a^{\frac{Q}{q}}-1, n)=1$, then any prime divisor p of n satisfies $p \equiv 1 \pmod{Q}$ (including $p > Q$). In particular, if $Q > \sqrt{n}$, we have that n is prime.*

Proof. Let q be a prime divisor of Q, with q^m the exact power of q dividing Q.

Claim: $b = a^{\frac{Q}{q^m}} \in (\mathbb{Z}/p\mathbb{Z})^*$ has order q^m. This is because $b^{q^m} \equiv a^Q \equiv 1 \pmod{n}$, so the order of b divides q^m. Now, $b^{q^{m-1}} = a^{\frac{Q}{q}}$ in $(\mathbb{Z}/n\mathbb{Z})^*$. We also know that $b^{q^m} \equiv 1$ in $(\mathbb{Z}/p\mathbb{Z})^*$, so $b^{a^{m-1}} = a^{\frac{Q}{q}}$ in $(\mathbb{Z}/p\mathbb{Z})^*$.

Could $b^{q^{m-1}} = 1$? If so, we have $a^{\frac{Q}{q}} \equiv 1 \pmod{p}$. Since $p|(a^{\frac{Q}{q}}-1)$, $p|\gcd(a^{\frac{Q}{q}}-1, n)$ is not true. So the claim is true also in $(\mathbb{Z}/p\mathbb{Z})^*$.

Hence:

$$q^m | \#(\mathbb{Z}/p\mathbb{Z})^* = p-1 \tag{1.7}$$

$$p \equiv 1 \pmod{q^m} \forall q \tag{1.8}$$

$$p \equiv 1 \pmod{Q} \qquad \square$$

Scribe notes: in what follows, the speaker's original presentation has been modified to highlight the algorithm and its properties.

Algorithm 2 $p-1$ primality test

---

input: $n \in \mathbb{Z}_{>0}$ (suppose n passes the Miller-Rabin test)
output: "n is prime" or $\perp$

1. Using computational resources available, find all small prime factors of $n-1$. Let Q be the product of these primes. Let $n-1=QR$ (we call R the *cofactor*).
2. Now, three things can happen
   (a) (almost never) $Q > \sqrt{n}$. For each prime $q|Q$ (suppose we already have a proof of primality for q, if need be, call algorithm 2 recursively!), we need to find a corresponding a as in proposition 2. Pick a at random in $\mathbb{Z}/n\mathbb{Z}$. Check that $a^Q \equiv 1 \pmod{n}$, and that $\gcd(a^{\frac{Q}{q}}-1, n) = 1$. If all tests succeed, output "n is prime".
   (b) (usually) R not prime but cannot factor within reasonable time. Give up and output $\perp$.
   (c) (occasionally) $n-1=QR$, with $Q < \sqrt{n}$ and $R > \sqrt{n}$ passes the Miller-Rabin test. Reverse the roles of Q and R, at which point we fall back into case (a).

The goal of algorithm 2 is to check that the conditions of proposition 2 are satisfied, with $Q > \sqrt{n}$. It is clear that this is what is accomplished and that the output of the algorithm is correct.

What about the choice of a in step (a)? If n is prime, then $(\mathbb{Z}/n\mathbb{Z})^*$ is cyclic, suppose it is generated by g. Take $a = g^R$. Then $a^Q = g^{RQ} = g^{n-1} \equiv 1 \pmod{n}$ (Fermat's little theorem), and $\gcd(a^{\frac{Q}{q}} - 1, n) = 1$ because if not, $a^{\frac{Q}{q}} \equiv g^{\frac{n-1}{q}} \equiv 1 \pmod{n}$, which cannot happen. So if n is prime, our method of picking a at random should give good results.

How about the complexity of the algorithm? Computing $a^Q \pmod{n}$ (modular exponentiation) requires work in $O(\log^3 n)$. The $\gcd$ computation is also polynomial.

But will it work? In practice, because of (a), (b) and (c), we won't make much progress. For instance, taking $n \sim 10^{1000}$ gives a probability of success that is low.

1.3 Elliptic Curves

Elliptic curves are an "old" subject— much older than computers. Our study is motivated by algorithmic applications. In the previous section, we saw two $p-1$ algorithms:

- *factoring:* Success if there exists $p|n$ such that $p-1$ is B-smooth.
- *primality:* Success if $p - 1 = QR$ where the factored part Q is $> \sqrt{n}$ or $p - 1 = QR$ where the factored part $Q < \sqrt{n}$ and R is a probable prime.

These algorithms have in common the fact that they use group-theoretic statements, but they need to be lucky to actually work.

Now, our key idea will be to replace $(\mathbb{Z}/p\mathbb{Z})^*$ by groups of points on elliptic curves. The advantage here is that there are many elliptic curves to we can try, thus eliminating the need for "luck".

An *elliptic curve* over a field k ($\mathbb{R}, \mathbb{C}, \mathbb{F}_q$) is given by the cubic curve:

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6\,, \tag{1.9}$$

where $a_1, a_2, a_3, a_4, a_6 \in k$ (no, it's not a mistake that a_5 is missing). Define the following:

$$\begin{aligned}
b_2 &= a_1^2 + 4a_2 \\
b_4 &= a_1a_3 + 2a_4 \\
b_6 &= a_3^2 + 4a_6 \\
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\
c_4 &= b_2^2 - 24b_4 \\
c_6 &= -b_2^3 + 36b_2b_4 - 216b_6 \\
\Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6\,.
\end{aligned}$$

We're interested in nonsingular curves with discriminant $\Delta \neq 0$. We also have the relationship

$$1728\Delta = c_4^3 - c_6^2\,. \tag{1.10}$$

If the characteristic of the field isn't 2, we can divide by 2 and complete the square:

$$(Y + \frac{a_1X + a_3}{2})^2 = X^3 + (a_2 + \frac{a_1^2}{4})X^2 + a_4X + (\frac{a_3^2}{4} + a_6)\,, \tag{1.11}$$

which can be written as:

$$Y_1^2 = X^3 + a_2'X^2 + a_4'X + a_6'\,, \tag{1.12}$$

with $Y_1 = Y + a_1X/2 + a_3/2$. If the characteristic is also not 3, then we can let $X \leftarrow \frac{X+a_2'}{3}$ to get the curve

$$Y^2 = X^3 + AX + B\,. \tag{1.13}$$

The discriminant becomes $\Delta = -16(4A^3 + 27B^2)$, and the condition that the curve be nonsingular is of course still verified by $\Delta \neq 0$.

Some notation: elliptic curves are denoted E, and $E(k)$ denotes the set of points on E with coordinates in k, together with a special "symbolic" point (∞, ∞) called the point at infinity.

Now, we want to show our main point of this lecture, that is, that we can give $E(k)$ the structure of a group in a natural way. Our approach is a practical one; more mathematical approaches would be possible.

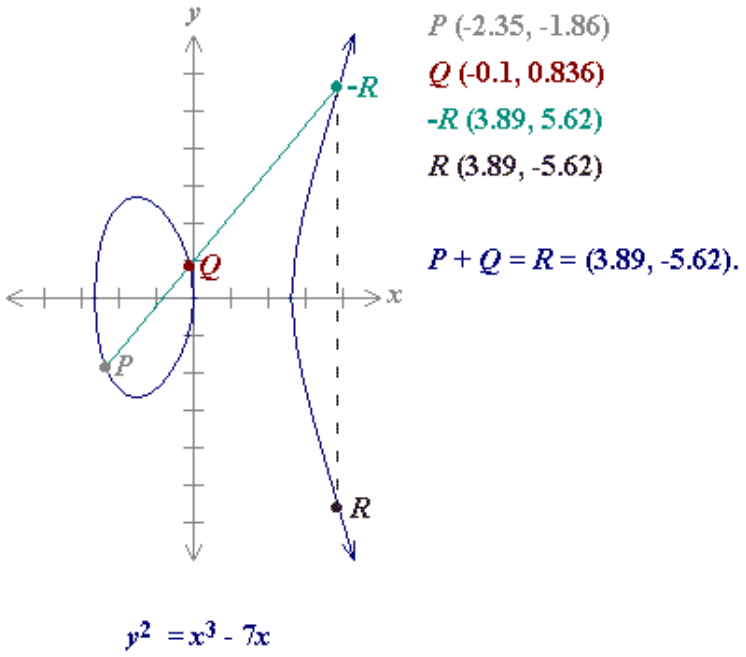


Figure 1.1: Elliptic curve addition (source: certicom.com)

1.3.1 Group Law on Elliptic Curves

Consider the right-hand side of $Y^2 = X^3 + AX + B$, which is a cubic. A cubic can have either one or two roots. When we take the square root of this cubic, we get two different families of elliptic curves, as illustrated in figures 1.1 and 1.2 (our illustrations are done with underlying field $k = \mathbb{R}$).

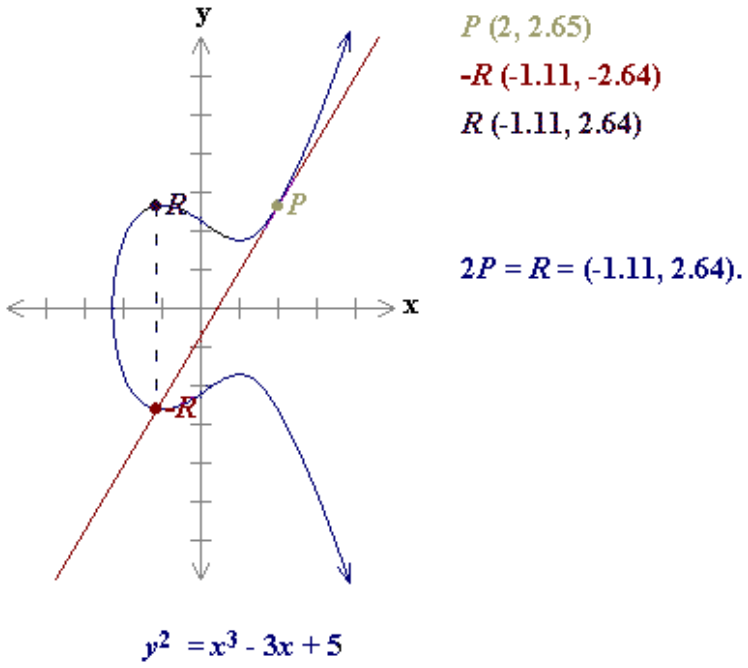


Figure 1.2: Elliptic curve doubling (source: certicom.com)

The addition of two distinct points P and Q on an elliptic curve is performed the following way: let $-R$ be the third intersection point of the line through P and Q and the curve. Then $P + Q = R$. See figure 1.1.

The doubling of a point P on an elliptic curve is performed the following way: let $-R$ be the second intersection point of the tangent to the curve at point P and the curve. Then $P+P = 2P = R$. See figure 1.2.

Now, to compute the formulas for this operation, let $P = (x_1, y_1), Q = (x_2, y_2), P + Q = (x_3, y_3)$ and so $R = (x_3, -y_3)$. In the case $P \neq Q$, we wish to compute the intersection of the line $y = \lambda x + \mu$ through P and Q with the curve $Y^2 = X^3 + AX + B$. If $P \neq Q$, this give us $\lambda = (y_2 - y_1)/(x_2 - x_1)$, while $P = Q$ yields $\lambda = (3x_1^2 + A)/2y_1$. Substituting, we get:

$$(\lambda x + \mu)^2 = X^3 + AX + B \tag{1.14}$$

$$0 = X^3 - \lambda^2 X^2 + (A - 2\lambda\mu)X + B - \mu^2 \tag{1.15}$$

$$= (X - x_1)(X - x_2)(X - x_3) \tag{1.16}$$

Hence (1.17)

$$\lambda^2 = x_1 + x_2 + x_3 \tag{1.18}$$

To find y_3:

$$\frac{-(y_3) - y_1}{x_3 - x_1} = \lambda \tag{1.19}$$

$$\Rightarrow y_3 = -y_1 - \lambda(x_3 - x_1) \tag{1.20}$$

Explicitly,

$$x_3 = -x_1 - x_2 + \lambda^2 \tag{1.21}$$
$$y_3 = -y_1 - \lambda(x_3 - x_1)\,. \tag{1.22}$$

Where either $\lambda = (y_2 - y_1)/(x_2 - x_1)$ (if $P \neq Q$) or $\lambda = (3x_1^2 + A)/(2y_1)$ (if $P = Q$).

We also add the rule that for any point $P = (x, y)$, $-P = (x, -y)$ and the $P + -P = (\infty, \infty)$.

We now have all the tools to compute on an elliptic curve, and we can indeed show that this operation forms a commutative group (associativity is harder to prove).

We now give two examples over $\mathbb{Z}/5\mathbb{Z}$:

We cannot draw a picture anymore. A picture would be quite pointless . . . literally.
— René Schoof

Example 1 (Adding points over $\mathbb{Z}/5\mathbb{Z}$)**.** *Let $E : Y^2 = X^3 + X + 1$ over $\mathbb{Z}/5\mathbb{Z}$. First, we check that this is an elliptic curve:*

$$\Delta = -16(4 \cdot 1^3 + 27 \cdot 1^2) \equiv -1(-1 + 2) \not\equiv 0 \pmod 5\,. \tag{1.23}$$

Let $P = (0, 1)$. We want to compute $P + P$. Using the given formulas, we get:

$$\lambda = \frac{3 \cdot 0^2 + 1}{2 \cdot 1} \equiv 3 \pmod 5 \tag{1.24}$$
$$x_3 = -0 - 0 + 3^2 = 9 \equiv -1 \pmod 5 \tag{1.25}$$
$$y_3 = -1 - 3(-1 - 0) \equiv 2 \pmod 5\,. \tag{1.26}$$

So $P + P = (-1, 2)$ and we can check that it sits on the curve.

Example 2 (Determining all points over $\mathbb{Z}/5\mathbb{Z}$)**.** *Consider the curve E given in the previous example. We want to list all points on E.*

First, we compute the squares in $\mathbb{Z}/5\mathbb{Z}$. We get $1^2 = 1$, $2^2 = -1$, $(-2)^2 = -1$, $(-1)^2 = 1$, so 1 and -1 are squares, with roots $\{1, -1\}$ and $\{2, -2\}$, respectively. We proceed as in table 1.1 to get the 8 points of the curve, to which we add the point at infinity.

X	X^3	$X^3 + X + 1$	points
0	0	1	$(0, 1)$, $(0, -1)$
1	1	-2	none
2	-2	1	$(2, 1)$, $(2, -1)$
-2	2	1	$(-2, 1)$, $(-2, -1)$
-1	-1	-1	$(-1, 2)$, $(-1, -2)$

Table 1.1: Finding points on the curve $Y^2 = X^3 + X + 1$ over $\mathbb{Z}/5\mathbb{Z}$

A further question we can ask is whether the group is isomorphic to $\mathbb{Z}/9\mathbb{Z}$ or $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$. The answer is $\mathbb{Z}/9\mathbb{Z}$ since we eliminate the possibility of $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ by taking $P = (0, 1)$, and finding that $p + p \neq -p$. (See example 1.)

Lecture 2. Prime and Smooth Numbers in Intervals

Lecturer: Andrew Granville Scribe: Arkadev Chattopadhyay

Here we go through a quick survey of results from analytic number theory on the asymptotic behavior of the number of primes and smooth numbers in a given interval.

2.1 Prime numbers

Gauss made the conjecture that the number of primes upto x, denoted by $\pi(x)$, is roughly $x/\log x$. Gauss's guessed estimate of $\pi(x)$, called the logarithmic integral estimate and denoted by $\mathrm{Li}(x)$, is inspired by the fact that he expected (aided by his very impressive mental calculation of the first "few" primes) the density of primes to be about $1/\log n$ around n. More precisely,

$$\mathrm{Li}(x) = \int_2^x \frac{dt}{\log t}.$$

Integrating above by parts, we get

$$\mathrm{Li}(x) = \frac{x}{\log x}\left(1 + \sum_{k=1}^{\infty} \frac{k!}{(\log x)^k}\right).$$

The first big progress towards understanding the relationship of $\pi(x)$ and $\mathrm{Li}(x)$ was made in 1896 by Hadamard and de la Vallée Poussin who proved the following:

Theorem 1 (Prime Number Theorem)**.** $\lim_{x\to\infty} \frac{\pi(x)}{x/\log x} \to 1$.

Although the Prime Number Theorem tells us that the density of primes asymptotically agree with Gauss's estimate, it does not tell us much about the error function $\pi(x) - \mathrm{Li}(x)$.

Using Fourier Analysis, we believe that 10^{316} is the right point where Gauss's estimate is inadequate. Moreover, it seems from the data that

$$\left|\pi(x) - \int_2^x \frac{dt}{\log t}\right| < 2x^{1/2}(\log x)^A \tag{2.27}$$

It is remarkable that the correctness of the above statement is equivalent to the famous Riemann Hypothesis.

Riemann defined a zeta function, denoted by ζ, by the following series for $\mathrm{Re}(s) > 1$:

$$\zeta(s) = \sum_{n\geq 1} \frac{1}{n^s}.$$

Although $\zeta(s)$ has a pole at $s = 1$, it can be analytically continued to the set of every other complex number i.e. $\mathbb{C} - \{1\}$. This analytic continuation is called the Riemann zeta function.

Conjecture 1 (Riemann's Hypothesis)**.** *If* $\zeta(s) = 0$*, then Re*$(s) \leq 1/2$.

Riemann knew that every negative even integer is a zero of the zeta function but called them the trivial zeroes. His hypothesis could be reformulated as saying "Every non-trivial zero of the zeta function occurs on the Re$(s) = 1/2$ line". The proof of the Prime Number Theorem followed by establishing the following key fact:

Fact 1 (Hadamard and de la Vallée Poussin)**.** *The Prime Number Theorem is equivalent to saying that* $\zeta(s) \neq 0$ *if Re*$(s) \geq 1$.

It was totally surprising when in 1949 Erdös/Selberg provided an elementary proof the Prime Number Theorem.

Riemann had showed also the following remarkable fact:

$$\pi(x) - \int_2^x \frac{dt}{\log t} \approx -\sum_{\rho;\zeta(\rho)=0} \frac{x^\rho}{\rho \log x} \tag{2.28}$$

In (2.28) ρ in the summation on the RHS has positive real part. Assume $\rho = \beta + i\alpha$. Note that

$$\left|\frac{x^\rho}{\rho \log x}\right| = \frac{x^\beta}{|\rho| \log x}.$$

Hence, taking absolute values on both sides of (2.28) we get

$$|\text{Error}| \leq \sum_{\rho=\beta+i\alpha} \frac{x^\beta}{|\rho| \log x}.$$

Thus,

$$|\text{Error}| \leq \frac{x^{\max\beta}}{\log x} \sum \frac{1}{|\rho|} (\log x)^A.$$

Thus, assuming the Riemann Hypothesis we see that max$\beta = 1/2$ and plugging this into the above gives us the refined estimate on $\pi(x)$ provided by (2.27).

2.1.1 Consequences for primality testing

Our guess estimate for the number of primes in the interval $[x, x+y]$ i.e. $\pi(x+y) - \pi(x)$ will be roughly $y/\log x$ where $2 < y < x^{1-\epsilon}$. However, our estimate does not give us even an integer for too small values of y. May be it is true for $x > y > (\log x)^3$. It can be proved to be true for $x > y > x^{2/3}$. On the other hand, the Riemann Hypothesis implies that it holds for $x > y > x^{1/2} \log x$.

Aside Remark 1. *In 1932 Cramer conjectured that there is always a prime in* $(x, x + (\log x)^2)$*. This conjecture is still open.*

This discussion brings us to the question on how large could the gap between consecutive primes be? Let $p_1 = 2 < p_2 = 3 < p_3 < p_4 < \cdots$ be the sequence of consecutive prime numbers with p_i denoting the ith prime. The prime number theorem tells us that on the average $p_{n+1} - p_n$ is about $\log p_n$. Erdös and others proved that the gap between consecutive primes can be arbitrarily large compared to the average. More precisely, it was shown

$$\max_{p_n \leq x} p_{n+1} - p_n \; > \; 2e^{-\gamma} \log x \frac{(\log\log x)\log\log\log\log x}{(\log\log\log x)^2} \tag{2.29}$$

In particular, (2.29) implies that

$$\lim_{n\to\infty} \sup \frac{p_{n+1} - p_n}{\log p_n} \to \infty.$$

By contrast, one can ask the question how small can the gap between consecutive primes be? In a recent breakthrough, Goldston, Pintz and Yildirim showed that the gap can be arbitrarily small compared to the average i.e.

$$\lim_{n\to\infty} \inf \frac{p_{n+1} - p_n}{\log p_n} \to 0.$$

The result above constitutes important progress to the twin prime conjecture that says there are infinitely many pairs of primes that are separated by 2 i.e. $\lim_{n\to\infty} \inf p_{n+1} - p_n \; = \; 2$.

We come back to the application to the Goldwasser-Kilian (GK) algorithm for primality testing using elliptic curves. Recall that such a curve E is given by equations of the form $y^2 = x^3 + ax + b$ mod p for some prime p. In the morning lecture, we saw that the points on such a curve form an abelian group of order $N_p(E)$ with $p - 2\sqrt{p} < N_p(E) < p + 2\sqrt{p}$. The idea of the GK algorithm is to modify Pocklington's algorithm by working with the group of points on a randomly generated curve E instead of the fixed group $\mathbb{Z}/n\mathbb{Z}$. What this modified algorithm requires (in practice) is that the number of points on the curve E be either a prime or twice a prime. In other words, we are interested in the existence of a prime q such that

$$x = \frac{p - 2\sqrt{p} + 1}{2} < q < \frac{p + 2\sqrt{p} + 1}{2} \approx x + 2\sqrt{x}.$$

What we can prove is that 100% of intervals $(x, x + x^{1/1000})$ i.e. "almost all x" have about $\frac{x^{1/1000}}{\log x}$ many primes. Consequently, Goldwasser-Kilian will prove the primality of a prime number almost all of the time. Adleman-Huang bettered GK by working with random hyperelliptic curves over $\mathbb{Z}_p$. The number of points on such a curve lies in the interval $(p^2 - cp^{3/2}, p^2 + cp^{3/2})$. Thus, we need to find primes in the interval $(x, x + x^{3/4})$ and with even higher probability than GK, Adleman-Huang (AH) succeeds. Both AH and GK tests are mostly of historical importance now as AKS provides a determinisitc poly time test for primality.

2.2 Smooth Numbers

A number n is called y-smooth if every prime that divides n is no larger than y. We denote by $\Psi(x,y)$ the number of integers less than or equal to x that are y-smooth. Obviously $\Psi(x,x)=x$.

Let us estimate $\Psi(x,x)-\Psi(x,y)$. Assume $x>y>\sqrt{x}$. Then,

$$\begin{aligned}\Psi(x,x)-\Psi(x,y) &= \#\{n=pm\le x\,:\,p>y\}\\ &= \sum_{y<p\le x}\#\{m\le\frac{x}{p}\}\\ &\approx \sum_{y<p\le x}\frac{x}{p}\end{aligned}$$

Thus,

$$\Psi(x,y)\approx x\Big(1-\sum_{y<p\le x}\frac{1}{p}\Big).$$

It can be shown that

$$\sum_{p\le x}\frac{1}{p}=\log\log x+C+O\big(\frac{1}{\log x}\big).$$

So,

$$\sum_{y<p\le x}\frac{1}{p}\approx\log\left(\frac{\log x}{\log y}\right).$$

If $x=y^u$ and $1\le u\le 2$, then

$$\Psi\big(x,x^{1/u}\big)\approx x(1-\log u).$$

If $2<u<3$, then following what we did before gets us

$$\Psi\big(x,x^{1/u}\big)\approx x\Big(1-\sum_{y<p\le x}\frac{1}{p}+\sum_{p,q>y;pq\le x}\frac{1}{pq}\Big).$$

2.2.1 Larger u

We will try to estimate $\Psi(x,y)$ recursively having established it for small values of u. Noting that

$$\Psi(x,x)-\Psi(x,y)=\sum_{y<p\le x}\#\{pm\le x\,:\,m\text{ is }p\text{-smooth}\}.$$

This immediately gives the recursive relation

$$\Psi(x,x)-\Psi(x,y)=\sum_{y<p\le x}\Psi\big(\frac{x}{p},p\big).$$

Assuming $\Psi(x, x^{1/u}) \sim x\rho(u)$, we get

$$x\big(1-\rho(u)\big) = \sum_{y<p\leq x} \frac{x}{p}\rho\bigg(\frac{\log(x/p)}{\log p}\bigg) \tag{2.30}$$

Applying the Prime Number Theorem,

$$\text{RHS of (2.30)} \approx \int_y^x \frac{x}{t\log t}\rho\bigg(\frac{\log(x/t)}{\log t}\bigg)dt \tag{2.31}$$

The RHS of (2.31) has an error term that has to be eventually taken care of. Substitute $t = y^w$ so that $\log t = w\log y$. It is easily verified then

$$\frac{dt}{t\log t} = \frac{dw}{w}.$$

Plugging this substitution into the RHS of (2.31) we get

$$\text{RHS of (2.31)} \approx x\int_{w=1}^{u} \rho\bigg(\frac{u}{w}-1\bigg)\frac{dw}{w} \tag{2.32}$$

Substitute $v = u/w$, whereby $dv/v = -dw/w$ and so we get

$$1-\rho(u) = \int_{v=1}^{u} \rho(v-1)\frac{dv}{v} \tag{2.33}$$

To summarize, what we have proved is that $\Psi(x, x^{1/u})/x \to \rho(u)$ where $\rho(u)$ is a complicated function that is given by the integral equation (2.33). The key thing to remember is that $\Psi(x, y) = x\rho(u)$ where,

$$\rho(u) \approx \frac{1}{u^u} \tag{2.34}$$

and $x = y^u$. This remains provably true for

$$y > e^{(\log\log x)^{5/3+\epsilon}} \tag{2.35}$$

Surprisingly, the Riemann Hypothesis is equivalent to the above estimate holding for $y > (\log x)^{2+\epsilon}$.

2.2.2 Lenstra's algorithm

Lenstra's algorithm modifies Pollard's $p-1$ algorithm of factoring by working with the group of points on an elliptic curve. Roughly, we estimate the time that we want the algorithm to work. Say it is B. Then let $M = \prod_{q^\epsilon < B} q^\epsilon$ be a B-smooth number. We choose a random elliptic curve E (over $\mathbb{Z}/n\mathbb{Z}$) and a point P on it. Then we compute $P + \cdots + M$ times $\cdots + P$ using the group law for adding points on E. Let p be a prime factor of n. If the curve E_p (the one E induces over $\mathbb{Z}/p\mathbb{Z}$ via reduction mod p) has an order that is B-smooth and the order of all other E_q, where $q|n$, are not B-smooth then this addition process identifies p as a factor of n. Since the order of the group of points on E_p lies between $p-2\sqrt{p}+1$ and $p+2\sqrt{p}+1$, we are interested to find B-smooth numbers in this interval[1]. The relationship between B and p is roughly given by $B = O(\log p)^c$ for some constant c if we want Lenstra's algorithm to run in polytime w.r.t its input length (which is $\log n$). Moreover the running bound of Lenstra's algorithm works if the number of B-smooth numbers in this interval is what we would expect it to be according to estimate (2.34) i.e. $4\sqrt{p}/\rho(u)^u$ where $y = x^{1/u} = (\log p)^c = \exp(c \log\log p)$. This is unfortunately smaller than the range for which estimates provably work as given by (2.35).

[1]Note that corresponding to every number in this interval, we can find an elliptic curve that has exactly that many points on it.

Lecture 3. Hasse's Theorem

Lecturer: René Schoof Scribe: László Egri

Part 1

Before René's lecture, Pavel shortly explained some probabilistic complexity classes. Primes is in coRP due to Rabin and Miller. Adleman and Huang showed that Primes is in RP and therefore Primes is in coRP $\cap$ RP $= ZPP$. Finally, in 2002 it was shown by AKS that Primes is in P. Note that the generalized Riemann hypothesis implies that primes is in P.

A problem $X \in$ ZPP if there exists a randomized polynomial time algorithm A such that

$$A(x) = 0 \to x \notin X, x \in X \to P(A(x) = 1) \geq \frac{1}{3}$$
$$A(x) = 1 \to x \in X, x \notin X \to P(A(x) = 0) \geq \frac{1}{3}.$$

More General Form

Here René shortly remarked that in general, an elliptic curve has the form $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ but usually $a_1 = a_2 = a_3 = 0$ and then we get the form which we use most of the time.

Addition can be defined in the same way. Consider $(x_1, y_1) + (x_2, y_2) = (x_3, y_3)$. The slope is

$$\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{if the two points are different} \\ \frac{3x^2 + 2a_2x + a_4x - a_1y}{24 + a_1x + a_3} & \text{if the two points are the same} \end{cases}$$

$$x_1 + x_2 + x_3 = \lambda^2 + a_1\lambda$$
$$-y_3 + a_1x_3 + a_3 = \lambda(x_3 - x_1) + y_1$$
$$-(x, y) = (x, -y + a_1x + a_3).$$

Projective Coordinates

Let K be a field and $E : y^2 = x^3 + Ax + B$ be an elliptic curve such that $char(K) \neq 2, 3$, $A, B \in K$ and $4A^3 + 27B^2 \neq 0$.

A projective plane $\mathbb{P}^2$ is defined as

$$\mathbb{P}^2 = \{(x, y, z) : (x : y : z) \neq (0, 0, 0) \text{ and } (x : y : z) \equiv (x' : y' : z') \text{ if there exists } c \in K^* \text{ such that } cx = x', cy = y', cz = z'\}$$

We can define a map from $\mathbb{A}^2$ (affine space) into $\mathbb{P}^2$ as $(x, y) \mapsto (x : y : 1)$. We can also go back:

$$\underset{\text{curve}}{\left(\frac{x}{z}, \frac{y}{z}\right)} \leftarrow \underset{\text{projective curve}}{(x : y : z) \in \mathbb{P}^2, z \neq 0}$$

We can see that the infinity point is

$$(\infty, \infty) = \begin{cases} z = 0 \\ x = 0 \\ y \neq 0 \quad y = 1. \end{cases}$$

Work on a Computer

Let $K = \mathbb{Z}/p\mathbb{Z}$. Then we can determine

$$x_3 = -x_1 - x_2 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 : y_3 : 1$$

(here the calculation of the inverse of the denominator is expensive, it can be done using the Euclidean algorithm) or equivalently,

$$(-x_1 - x_2)(x_2 - x_1)^2 + (y_2 - y_1)^2 : y_2(y_2 - x_1)^2 : (x_2 - x_1)^2$$

in $O(log^3 p)$ time.

Exercises

Let E be an elliptic curve $y^2 = x^3 + Ax + B$ over a field $K = \overline{K}$ such that $char(K) \neq 2, 3$. Let's determine the number of points of order 2 and 3.

Points of order 2

Let $P = (x, y)$. Then $P + P = 0 \leftrightarrow P = -P \leftrightarrow (x, y) = (x, -y) \rightarrow y = 0 \rightarrow x^3 + Ax + B = 0 \rightarrow$ there are three points of order 2.

Let $n \in \mathbb{N}$. Assume that K is an algebraically closed field. Define the set of n-torsion points $E[n] \subset E(K)$ to be the set of elements in $E(K)$ which have order n, i.e.

$$E[n] = \{P \in E(K) : \underbrace{P + \cdots + P}_{n} = (\infty, \infty)\}.$$

Then $E[2] \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Points of order 3

Let $P = (x, y)$. Assume that $P + P + P = 0$. Then $P + P = -P$ and $-P = (x, -y)$. So $P+P = (x_3, y_3)$. Then $x_3 = -x-x+\lambda^2$, where $\lambda = \frac{3x^2+A}{2y}$. So $(-2x+(\frac{3x^2+A}{2y})^2, y_3) = (x, -y)$. It follows that $(3x^2 + A)^2 = 3x(Ay^2) = 12x(x^3 + Ax + B)$ and $3x^4 + 6Ax^2 + 12Bx - A^2 = 0$. So there are four zeroes. In fact, $E[3] \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

Main Result

Let p be a prime and E be an elliptic curve over $\mathbb{Z}/p\mathbb{Z}$. The main result of today is:

1. $E(\mathbb{Z}/p\mathbb{Z})$ is almost cyclic, i.e. it can be generated by at most 2 elements[2];
2. $p + 1 - 2\sqrt{p} < \#E(\mathbb{Z}/p\mathbb{Z}) < p + 1 + 2\sqrt{p}$.

Let K be the field $\mathbb{F}_q$ where $q = p^m$ (p is characteristic). Here $E(K) = \{(x, y) : x, y \in K, y^2 = x^3 + Ay + B\} \cup \{\infty, \infty\}$. Let $\overline{K}$ denote the algebraic closure of K. Then $E(K) \subset E(\overline{K})$ ($E(\overline{K})$ is an infinite group).

$k(E)$ denotes a function field, $k(E) = \{\frac{f_1(x)+Yf_2(x)}{g(x)} : f_1, f_2, g \in K[x], g(x) \neq 0\}$.

Morphisms

Assume that E_1 and E_2 are two elliptic curves over a field K. Then a morphism h from E_1 to E_2 maps any $(x, y) \in E_1(\overline{K})$ to $(\varphi(x, y), \psi(x, y)) \in E_1(\overline{K})$, where φ and ψ are quotients of polynomials with coefficients in K. Morphism h must induce a group homomorphism and must map (∞, ∞) to (∞, ∞).

Examples

Let $E : y^2 = x^3 + Ax + B$. The following maps from E to E are morphisms.

$$(x, y) \mapsto (x, -y)$$
$$(x, y) \mapsto (x, y)$$
$$(x, y) \mapsto (\infty, \infty)$$

The zero morphism.

Another example is the following. Let's define $(f+g)(x, y) := f(x, y)+g(x, y)$. Assume that $f = g = id$. Then $(f+g)(P) = f(P)+g(P) = P+P$ so $(x, y)+(x, y) = (-2x+(\frac{3x^2+A}{2y})^2 : y_3)$ and the function that maps (x, y) to $(-2x + (\frac{3x^2+A}{2y})^2 : y_3)$ is a morphism.

[2]By almost cyclic we mean the following. Let ℓ be a prime. Then if $\ell \not| p - 1$ then the ℓ-part (Sylow subgroup) of $E(\mathbb{Z}/p\mathbb{Z})$ is cyclic. If $\ell | p - 1$ then the proportion of E over $(\mathbb{Z}/p\mathbb{Z})$ with ℓ-part not cyclic $\leq \frac{1}{\ell^3}$.

The Frobenius morphism. Let K be a field of characteristic p and $\alpha, \beta \in K$. Clearly, $(\alpha+\beta)^p = \alpha^p + \beta^p$. Let E be the elliptic curve $y^2 = x^3 + Ax + B$. Let $P = (x, y)$.

$$(y^2)^p = (x^3 + Ax + B)^p$$
$$(y^p)^2 = (x^p)^3 + A^p x^p + B^p$$

Then the point (x^p, y^p) is on $\tilde{E} : y^2 = x^3 + A^p x + B^p$. ($\Delta(\tilde{E}) = \Delta(E)^p$, where Δ is the discriminant.)

Let $\varphi_p : E \to \tilde{E}$ be defined as $(x, y) \mapsto (x^p, y^p)$. Then φ_p is called the *p-Frobenius morphism*. Now let $K = \mathbb{F}_q$. Then if $x \in K$ then $x^q = x$. (In particular, if $x \in \mathbb{Z}/p\mathbb{Z}$ then $x^p \equiv x \mod p$.)

Consider

$$\underbrace{E \xrightarrow{\varphi_p} \tilde{E} \xrightarrow{\varphi_p} \tilde{\tilde{E}} \xrightarrow{\varphi_p} \dots \xrightarrow{\varphi_p} \begin{array}{c}\tilde{} \\ \vdots \\ \tilde{E}\end{array}}_{m-\text{times}}.$$

The q-Frobenius morphism is defined as $\varphi_q = {\varphi_p}^m$. Observe that the curve $y^2 = x^3 + A^q x + B^q$ is the same as $y^2 = x^3 + Ax + B$, so in fact φ_q is from E to E.

Now let $K = \mathbb{F}_q \subset \overline{K} = \overline{\mathbb{F}_q}$. Then $K = \{\alpha \in \overline{K} : \alpha^q = \alpha\}$, i.e. $\mathbb{F}_q$ is the set of fixed points of the map $\alpha \mapsto \alpha^q$ (from $\overline{K}$ to $\overline{K}$). So $E(K) \subset E(\overline{K})$ where $E(K) = \{(x, y) : \varphi_q(x, y) = (x, y)\}$.

Part 2

Recall that René went over this section in finer detail in the first part of his next lecture.

Recall the following. Let $K = \mathbb{F}_q$ (or $\mathbb{Z}/p\mathbb{Z}$). Consider the elliptic curve $E : y^2 = x^3 + Ay + B$ where $A, B \in K$. Then $E(K) \subseteq E(\overline{K})$. ($E(K)$ is a finite field.) A morphism from E to itself is called an endomorphism. For example, the q-Frobenius $\varphi_q(x, y) = (x^q, y^q)$ from $E(\overline{K})$ to $E(\overline{K})$ is an endomorphism.

Let $E(K) = \{P \in E(\overline{K}) : \phi_q(P) = P\}$. Now $\varphi_q(P) = P \leftrightarrow (\varphi - id)(P) = 0 \leftrightarrow P \in ker(\varphi_q - id)$. It follows that

$$E(k) = ker(E(\overline{K}) \xrightarrow{\varphi_q - id} E(\overline{K})).$$

Question: if $E_1 \xrightarrow{f} E_2$ where f is a morphism, then what is $ker(f)$?

$\{f : E \to E$: a morphism over $K\} = End(E)$ is a ring. We can add, subtract, multiply:

$$(f + g)(P) = f(P) + g(P)$$
$$(f \cdot g)(P) = f(g(P))$$

The identity for multiplication is the identity map id. The identity for addition is the 0-morphism (sends everything to ∞). Let's define $[n] = \underbrace{id + \dots + id}_{n-\text{times}}$, where $n \in \mathbb{N}$. Observe that the map

$n \mapsto [n]$ from $\mathbb{Z}$ to $End(E)$ is an injective map. Also note that $[n] : E(\overline{K}) \to E(\overline{K})$ defined as $P \mapsto \underbrace{P + \cdots + P}_{n}$ is never the zero map.

An *isogeny* between two elliptic curves E_1 and E_2 is a morphism $\varphi : E_1 \to E_2$ such that $\varphi(0) = 0$. Two elliptic curves are *isogenous* if there is an isogeny φ between them with $\varphi(E_1) \neq \{0\}$.

Let $E_1(K)$ and $E_2(K)$ be elliptic curves and $f : E_1 \to E_2$ be a non-constant "rational map" defined over K. Then composition with f induces an injection of function fields fixing K,

$$f^* : K(E_1) \hookleftarrow K(E_2)$$

$$f^* g = f \circ g.$$

We define $deg(f) = deg(formulas)$, and $deg(f) = deg_{sep}(f) \cdot deg_{insep}(f)$ or $deg(f) = [K(E_1) : f^*K(E_2)]$ (e.g. $deg(id) = 1$ and $deg(q - Frobenius) = q$).

For example, let $y^2 = x^3 + Ax + B$ and $E \overset{[2]}{\to} E$.

$$(x, y) \to \left(-2x + \frac{(3x^2 + A)^2}{4(x^3 + Ax + B)}, yK(x) \right)$$
$$K(E) \hookleftarrow K(E) = \{a(x + Yb(x)\} \; a(x) \text{ and } b(x) \text{ are rational functions in } x$$

$\hookleftarrow$ above is a degree 4 extension.

$$-2x + \frac{(3x^2 + A)^2}{4(x^2 + Ax + B)} \leftarrow x$$
$$yK(x) \leftarrow y$$

So $deg([2])$=4.

Fact: $deg(fg) = deg(f)deg(g)$.

Let f be a morphism from E to E. If f is a p-th power where the characteristic of the field is p then f is inseparable. It is a fact that if f is separable then $\#ker(f) = deg(f)$.

Let $E \overset{f}{\to} E$. Then $I = \{f : E \to E : inseparable\} \subset End(E)$. Note that I is a two-sided ideal and I is a strict subset of $End(E)$. For example, $\phi_q \in I$.

Let $f = [p]$ where p is the characteristic of the field. Then $[p] \in I$. The formula to express $f = (x, y) + \cdots + (x, y)$ (p terms) is a p-th power.

Corollary 1.

$$p \not| n \Rightarrow [n] \notin I$$
$$\Rightarrow [n] \textit{ is separable}$$
$$\#ker([n]) = deg(n)$$

Notice that $\phi_q - id \notin I$ and it follows that $\#ker(\phi_q - id) = deg(\phi_q - id)$. (And $\#ker(\phi_q - id) = \#E(K)$.)

Let $f : E \to E$. It is a fact that $deg(f) = deg_{nonsep}(f)deg_{sep}(f)$ and therefore it is always the case that $\#ker(f) = deg_{sep}(f)|deg(f)$. $\Rightarrow deg(f)$ "kills" $ker(f)$.

Let $f : E \to E$ be an isogeny. It is a fact that there exists a unique map f^v called the dual isogeny with the property $f^v f = [deg(f)]$. These maps are in $End(E)$. Here are some properties of f^v:

$$\begin{aligned} f^{vv} &= f \\ (fg)^v &= f^v g^v \\ deg(f^v) &= deg(f) \\ (f+g)^v &= (f^v + g^v) \qquad \text{(hardest to show)} \end{aligned}$$

Let's do an example. Let $\mathbb{F}_q = \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$ and $E : y^2 + xy = x^3 + 1$. Let's compute the dual of $\phi_2(x, y) = (x^2, y^2)$, $deg(\phi_2) = 2$.

$[2] : E \to E$:

$$\begin{aligned} (x,y) + (x,y) &= \left(x^2 + \frac{1}{x^2}, (y^2+1)(1+\frac{1}{x^4}) + \frac{1}{x^2} \right) \\ &= \left(V(x)^2, W(x,y)^2 \right) \end{aligned}$$

Therefore

$$(V(x), W(x,y)) = \left(x + \frac{1}{x}, (y+1)(1+\frac{1}{x^2}) + \frac{1}{x} \right).$$

$$(x,y) \overset{g}{\mapsto} (V(x), W(x,y)).$$

Observe that $\phi_2 \circ g = [2]$ so the dual of ϕ_2 is g.

Observe that multiplication is self-dual:

$$[n]^v = [id + \ldots + id]^v = id + \ldots id = [n].$$

Then $[deg([n])] = [n]^v[n] = [n]^2 = [n^2]$ and it follows that $deg([n]) = n^2$. It follows that for every n if $p \not| n$ then $\#ker([n]) = \#E(\overline{K})[n] = n^2$. Then

$$\Rightarrow E(\overline{K})[n] = \{P \in E(\overline{K}) : \underbrace{P + \ldots + P}_{n} = \infty\} \cong \mathbb{Z}/n \times \mathbb{Z}/n$$

$$\Rightarrow E(K) \subset E(\overline{K})$$

$$\Rightarrow E(K) \qquad \text{can be generated by at most 2 points.}$$

Recall that

$$\begin{aligned} \#E(K) &= \#ker(\phi_q - id) \\ &= deg(\phi_q - id). \end{aligned}$$

We define the trace t of a function $f \in End(E)$ as follows. $t = trace = f + f^v$. Then

$$\begin{aligned} f + f^v &= (f + [1])(f^v + [1]) - ff^v - [1] \\ &= [deg(f + 1)] - [deg(f)] - [1] \end{aligned}$$

Therefore $[f + f^v]$ is in $[\mathbb{Z}] \subset End(E)$. For any f we can write that

$$\begin{aligned} f^2 - (f + f^v)f + f^v f = 0 \qquad &\text{(in } End(E)\text{)} \\ f^2 - [t]f - [deg(f)] = 0 \end{aligned}$$

t and $deg(f)$ are integers so the maps $\in End(E)$.

Proposition 3 (Analogue of Riemann Hypothesis, 1933, Hasse)**.** $t^2 \leq 4deg(f)$.

Let $m, n \in \mathbb{Z}$.

$$\begin{aligned} 0 \leq [deg([m] + [n]f)] &= ([m] + [n]f)([m]^v + [n]^v f^v) \\ &= ([m] + [n]f)([m] + [n]f^v) \\ &= ([m]^2 + [m][n](f + f^v) + [n]^2 ff^v) \\ &= [n]^2(\left(\frac{[m]}{[n]}\right)^2 + \frac{[m]}{[n]}t + deg(f)) \end{aligned}$$

It follows that $x^2 - tx + deg(f) \in \mathbb{Z}[x]$ has only ≥ 0 values. Therefore $t^2 \leq 4deg(f)$.

Corollary 2. $\#E(K) = q + 1 - t$ *with* $|t| \leq 2\sqrt{q}$.

Proof. We have

$$\begin{aligned} \#E(K) &= deg(\phi_q - id) \\ &= (\phi_q - id)(\phi_q^v - id) \\ &= q + 1 - t \end{aligned}$$

and $t^2 \leq 4deg(\phi_q) = 4q$ as required. □

Lecture 4. Constructing Elliptic Curves of Prescribed Order

Lecturer: Eyal Goren Scribe: Anil Ada

4.1 Introduction

Consider an elliptic curve E over $\mathbb{F}_p$ given by the equation $y^2 = x^3 + Ax + B$. The number of points on this elliptic curve is equal to $p + 1 - t$ where $|t| \leq 2\sqrt{p}$ (Hasse bound). Let φ denote the p-th Frobenious function: $\varphi(x, y) = (x^p, y^p)$. Then we know $[t] = \varphi + \varphi^\vee$ and φ satisfies the quadratic equation $x^2 - tx + p = 0$.

We have seen the ring $\mathrm{End}(E)$ contains $\mathbb{Z}$. In fact it contains the subring containing $\mathbb{Z}$ and φ, i.e. it contains $\mathbb{Z}[\varphi]$. The ring $\mathbb{Z}[\varphi]$ looks like a subring of $\mathbb{C}$ since

$$\varphi = \frac{t \pm \sqrt{t^2 - 4p}}{2} \in \mathbb{C}.$$

(There is an ambiguity because of "$\pm$".) This subring is not contained in $\mathbb{R}$ because $t^2 - 4p < 0$.

In this lecture we will be interested in the following three questions.

1. Given a permissible t, does there exist an elliptic curve over $\mathbb{F}_p$ with $p + 1 - t$ points?

2. If so, how many are there?

3. If so, how do you write them down?

The quick answers to these questions are as follows.

1. Yes.

2. A certain "class number". (This can be calculated rapidly for each p and t.)

3. The method is to construct elliptic curves over a number field H that is a finite extension of $\mathbb{Q}$ and a subset of $\mathbb{C}$. Then reduce these elliptic curves $\mod p$. One looks for elliptic curves E over $\mathbb{C}$ such that $\mathrm{End}(E)$ also contains $\mathbb{Z}[\varphi]$.

For this lecture, we assume that $\mathrm{End}(E)$ is imaginary quadratic, i.e. E is *ordinary*. This is equivalent to saying $t \neq 0$.

4.2 The j-invariant

Let $E_{A,B}$ be an elliptic curve over the field k with points satisfying the equation $y^2 = x^3 + Ax + B$. We can associate the j-invariant of $E_{A,B}$:

$$j(E_{A,B}) := 1728\frac{4A^3}{4A^3 + 27B^2}$$

Now we state two facts about the j-invariant.

- If k is an algebraically closed field then $E_{A,B} \cong E_{A',B'}$ if and only if $j(E_{A,B}) = j(E_{A',B'})$.
- In general, any elliptic curve $\tilde{E}$ over k with $j(\tilde{E}) = j(E_{A,B})$ is isomorphic to the elliptic curve E_d given by the equation $dy^2 = x^3 + Ax + B$, $d \neq 0$. Note that this equation can be written in standard form via simple manupilations. E_d is isomorphic to $E_{d'}$ over k if and only if d/d' is a square in $k^\times$. Therefore one can deduce that for any $j \in \mathbb{F}_p$, there exists precisely two elliptic curves up to isomorphism over $\mathbb{F}_p$ with a given j-invariant (unless $j = 0$ or $j = 1728$).

Given some $j \in k$, the elliptic curve E_j given by $y^2 = x^3 + A(x + 1)$ where $A = \frac{27j}{4(1728-j)}$ is such that the j-invariant of E_j is j. Given t, to find all the elliptic curves over $\mathbb{F}_p$ that have $p+1-t$ points, we will find all the j-invariants of the elliptic curves over $\mathbb{F}_p$ with $p + 1 - t$ points. Then given these j's, we can construct the corresponding elliptic curves. Here we have to be careful because the curve we constructed might actually have $p + 1 + t$ points. If $E_j(\mathbb{F}_p)$ has $p + 1 + t$ points than the elliptic curve given by $dy^2 = x^3 + A(x + 1)$ where d is a non-square in $\mathbb{F}_p$ (i.e. the quadratic twist) will have $p + 1 - t$ points.

We will be interested in elliptic curves over the complex numbers and the j-invariants of these elliptic curves. This is because:

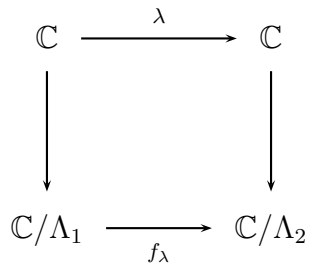
Fact 2. *The j-invariants of $E(\mathbb{C})$ with End$(E) \supseteq \mathbb{Z}\left[\frac{-t+\sqrt{t^2-4p}}{2}\right]$ reduce $\mod p$ bijectively to j-invariants of those elliptic curves over $\mathbb{F}_p$ with $p + 1 - t$ points.*

4.3 Endomorphisms of Elliptic Curves Over $\mathbb{C}$

Let E be an elliptic curver over $\mathbb{C}$ given by the equation $y^2 = x^3 + Ax + B$ where $A, B \in \mathbb{C}$. Then the endomorphism ring End$(E) = \{f : E \to E \mid \text{morphism}\}$ contains $\mathbb{Z}$. Here each f is of the form $f(x, y) = (\varphi(x, y), \psi(x, y))$ for some φ and ψ.

An elliptic curver E over $\mathbb{C}$ is a torus and every torus is isomorphic to $\mathbb{C}/\Lambda$ where Λ is a lattice. Given E, there exists a lattice $\mathbb{Z} + \mathbb{Z}\tau$, Im$(\tau) > 0$ and a surjective group homomorphism $w : \mathbb{C} \to E$ such that Ker$(w) = \{z \in \mathbb{C} \mid w(z) = 0_E\} = \Lambda$. Thus the first isomorphism theorem gives us $\mathbb{C}/\Lambda \cong E$.

Consider two elliptic curves $E_1 = \mathbb{C}/\Lambda_1$ and $E_2 = \mathbb{C}/\Lambda_2$. Suppose there exists $\lambda \in \mathbb{C}$ such that $\lambda\Lambda_1 \subseteq \Lambda_2$. Then we have the following diagram.



Here $f_\lambda(z \mod \Lambda_1) = \lambda z \mod \Lambda_2$. In fact, any morphism from E_1 to E_2 is of this form so $\mathrm{Hom}(E_1, E_2) = \{\lambda \in \mathbb{C} \mid \lambda\Lambda_1 \subseteq \Lambda_2\}$. Similarly we have $\mathrm{End}(E) = \{\lambda \in \mathcal{C} \mid \lambda\Lambda \subseteq \Lambda\}$. If we write λ using basis 1 and τ: $\lambda = \lambda 1 = a + b\tau$, $\lambda\tau = c + d\tau$, then we see that λ is actually of the form

$$\begin{pmatrix} a & c \\ b & d \end{pmatrix}$$

mapping $\alpha + \beta\tau$ to $(a\alpha + c\beta) + (b\alpha + d\beta)\tau$. So $\mathrm{End}(E) \subseteq M_2(\mathbb{Z})$.

One can conclude that

$$\mathrm{End}(E) = \begin{cases} \mathbb{Z} \\ \mathcal{O} \end{cases}$$

Here $\mathcal{O}$ is an *order* in a quadratic field $K = \mathbb{Q}(\sqrt{d})$, where d is a square-free integer. The integral closure of $\mathbb{Z}$ in K is called the *ring of integers* of K and is denoted $\mathcal{O}_K$. We have $\mathcal{O}_K = \mathbb{Z}[\delta] = \mathbb{Z} \cdot 1 + \mathbb{Z} \cdot \delta$ with integral basis $1, \delta$ where

$$\delta = \begin{cases} \sqrt{d} & \text{if } d \equiv 2, 3 \mod 4 \\ \frac{1+\sqrt{d}}{2} & \text{if } d \equiv 1 \mod 4 \end{cases}$$

An *order* $\mathcal{O} \neq \mathbb{Z}$ is a subring contained in $\mathcal{O}_K$. The discriminant of $\mathcal{O}_K$ is denoted d_K and

$$d_K = \begin{cases} 4d & \text{if } d \equiv 2, 3 \mod 4 \\ d & \text{if } d \equiv 1 \mod 4 \end{cases}$$

Any order has the shape $\mathbb{Z}[m\delta]$ for a unique positive integer m with discrimimant $m^2 d_K$.

Suppose $\mathrm{End}(E) = \mathcal{O}$. We have $\lambda \cdot 1 = a + b\tau$ and so $\tau = \frac{\lambda - a}{b} \in K$. This implies $\Lambda \subseteq K$ is a rank 2 free abelian group and $\mathcal{O}\Lambda \subseteq \Lambda$, i.e. Λ is an ideal of $\mathcal{O}$.

Fact 3. *Elliptic curves E over $\mathbb{C}$ with $\mathrm{End}(E) = \mathcal{O}$ is in bijection with ideals of $\mathcal{O}$ up to the equivalence $\Lambda \sim \alpha\Lambda$, $\alpha \in K^\times$. The latter is the class group of $\mathcal{O}$ and is denoted by $cl(\mathcal{O})$.*

Let $\mathcal{O}_o = \mathbb{Z}\left[\frac{-t+\sqrt{t^2-4p}}{2}\right]$. Recalling Fact 2 we conclude:

Theorem 2. *The number of elliptic curves over $\mathbb{F}_p$ with $p + 1 - t$ points is equal to the number of elliptic curves E over $\mathbb{C}$ with $\mathcal{O}_K \supseteq \mathrm{End}(E) \supseteq \mathcal{O}_o$, and this is equal to*

$$\sum_{K \supseteq \mathcal{O} \supseteq \mathcal{O}_o} \#cl(\mathcal{O}),$$

where $K = \mathbb{Q}(\sqrt{t^2 - 4p})$.

There is an explicit formula for $\#\text{cl}(\mathcal{O})$ and therefore the number of elliptic curves over $\mathbb{F}_p$ with $p+1-t$ points can be calculated rapidly for each p and t.

Our next goal is to find the j-invariants of the elliptic curves E over $\mathbb{F}_p$ with $p+1-t$ points. Consider the polynomial

$$f_{\mathcal{O}} = \prod_{\substack{E/\mathbb{C}: \\ \text{End}(E)=\mathcal{O}}} (x - j(E))$$

where $\mathcal{O}$ is an order with discriminant D.

Fact 4. *Let $E/\mathbb{C}$ be an elliptic curve with End$(E) \cong \mathcal{O}$. Then $j(E)$ is an algebraic integer, i.e. $f_{\mathcal{O}} \in \mathbb{Z}[X]$.*

The roots of $f_{\mathcal{O}}$ in $\mathbb{F}_p[X]$ are the j-invariants of the elliptic curves over $\mathbb{F}_p$ with endomorphism ring $\mathcal{O}$. Given a root $j \in \mathbb{F}_p$ of $f_{\mathcal{O}}$ where $\mathcal{O}$ has discriminant $D = t^2 - 4p$, the corresponding elliptic curve (or the twist) over $\mathbb{F}_p$ has $p+1-t$ points.

The rest of the lecture is devoted to showing how one can compute $f_{\mathcal{O}}$. Viewing $\mathcal{O}$ as a lattice in $\mathbb{C}$, the elliptic curve $\mathbb{C}/\mathcal{O}$ has endomorphism ring $\mathcal{O}$. Furthermore, every ideal $\Lambda \subseteq \mathcal{O}$ is a lattice in $\mathbb{C}$ and the curve $\mathbb{C}/\Lambda$ has endomorphism ring $\mathcal{O}$ if Λ is invertible $\mathcal{O}-$ideal. We will be interested in the bijection between ideal classes of $\mathcal{O}$ (i.e. cl$(\mathcal{O})$) and binary quadratic forms.

Suppose Λ is an $\mathcal{O}$-ideal where $\Lambda = \mathbb{Z}\alpha + \mathbb{Z}\beta$, $\alpha, \beta \in K = \mathbb{Q}(\sqrt{d})$. Without loss of generality $(\beta\bar{\alpha} - \alpha\bar{\beta})/\sqrt{d} > 0$. Associate to Λ the quadratic form

$$\frac{\text{Nm}(x\alpha - y\beta)}{\text{Nm}\Lambda} = ax^2 + bxy + cy^2$$

where $a = \alpha\bar{\alpha}$, $-b = \alpha\bar{\beta} + \beta\bar{\alpha}$, $c = \beta\bar{\beta}$ and we assume $\text{Nm}\Lambda = 1$. This produces positive definite primitive binary quadratic form with discriminant $D = \text{disc}(\mathcal{O})$. We write $\langle a, b, c\rangle$ for the form $ax^2 + bxy + cy^2$. A matrix $A = \begin{pmatrix} i & j \\ k & \ell \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$ acts on these forms via $f(x,y)A = f(ix + jy, kx + \ell y)$. Since $-1 \in \text{SL}_2(\mathbb{Z})$ acts trivially, we get an action of $\text{PSL}_2(\mathbb{Z})$. Each equivalence class under this action can be represented with a unique form $\langle a, b, c\rangle$ with $a > 0$, $|b| \leq a \leq c$, $b^2 - 4ac = D$ and if either $|b| = a$ or $a = c$ then $b \geq 0$. Let F_D denote these quadratic forms.

Fact 5. *The ideal classes of $\mathcal{O}$, cl$(\mathcal{O})$, is in bijection with F_D:*

$$\langle a, b, c\rangle \mapsto a\mathbb{Z} + \frac{-b + \sqrt{D}}{2}\mathbb{Z}$$

Now we can compute $f_{\mathcal{O}}$ as

$$\prod_{\langle a,b,c\rangle \in F_D} (x - j_{a,b,c})$$

where $j_{a,b,c} = j(E_\tau)$. Here $\tau = \frac{-b+\sqrt{D}}{2a}$ and $E_\tau = \mathbb{C}/(\mathbb{Z} + \mathbb{Z}\tau)$.

It is a classical result that the Fourier expansion of $j(E_\tau)$ has integral coefficients; it is a power series in $e^{2\pi i\tau}$ that we can calculate to any amount of precision. We know that $f_{\mathcal{O}}$ has integer coefficients, we only have to approximate the j-values in the product with high enough precision. The running time to calculate $f_{\mathcal{O}}$ is $O(|D|(\log|D|)^3(\log\log|D|)^3)$.

Lecture 5. Schoof's Algorithm

Lecturer: René Schoof Scribe: Mark Mercer

5.1 Review

Since many people had questions about the material in the Tuesday morning lecture, we will spend the first hour going over this material in finer detail. Following that, we will continue with the schedule topics, which is Schoof's algorithm for computing $\#E(\mathbb{F}_q)$.

The material regarding basic properties of endomorphisms on elliptic curves and their relation to the problem of counting the number of points on a curve can be found in Chapters 3 and 5 of the Silverman text. The applications can be found in the text by Lawrence C. Washington.

Recall that in the Tuesday morning lecture we showed that $\#E(\mathbb{Z}/p\mathbb{Z})$ satisfies:

$$p + 1 - 2\sqrt{p} \leq \#E(\mathbb{Z}/p\mathbb{Z}) \leq p + 1 + 2\sqrt{p}.$$

Note in particular that the value of $\#E(\mathbb{Z}/p\mathbb{Z})$ is centered around $p + 1$. There is an intuitive reason for this. Let us take for example a curve $Y^2 = X^3 + AX + B$, and we will try to count the points directly. First of all, there is always one point at infinity. There are p possible values for X, each of which contribute either two, one, or zero points to the curve. A given value x for X contributes two points if $x^3 + Ax + B$ is a nonzero square, or one point in the case that this value is zero. Otherwise, this value is a nonzero nonsquare and contributes no points to the curve.

Let us define $\chi : \mathbb{Z}/p\mathbb{Z} \to \{-1, 0, +1\}$ by:

$$\chi(a) = \begin{cases} 1 & a \text{ is nonzero square,} \\ 0 & a = 0, \\ -1 & \text{otherwise.} \end{cases}$$

You may note that this corresponds to the values of the Legendre symbol. We can rewrite the equation for $\#E(\mathbb{Z}/p\mathbb{Z})$ as:

$$\begin{aligned} \#E(\mathbb{Z}/p\mathbb{Z}) &= 1 + \sum_{x \in \mathbb{Z}/p\mathbb{Z}} (1 + \chi(X^3 + AX + B)) \\ &= 1 + p + \sum_{x \in \mathbb{Z}/p\mathbb{Z}} \chi(X^3 + AX + B). \end{aligned}$$

We will now proceed to give some background on endomorphisms of elliptic curves. Let us fix the field to be $\mathbb{F}_q$, and let us denote by $End(E)$ the set of endomorphism over $\mathbb{F}_q$. This forms

a ring with function addition $(\phi + \psi)(P) = \phi(P) + \psi(P)$ as the additive operator and function composition as the multiplicative operator. The identity of the ring is the identity mapping id, and the zero is the morphism mapping all points to zero. If $f \in End(E)$ then the morphism f can be expressed as a mapping $(x, y) \to (\phi(x, y), \psi(x, y))$, where ϕ and ψ are polynomials.

An important class of endomorphisms on curves are what we call the *mult-by-n* mappings. For $n \in \mathbb{Z}$ we define $[n]$ to be the sum of n identity mappings. Then $n \mapsto [n]$ is a morphism from $\mathbb{Z}$ to $End(E)$. Another important example is the *Frobenius morphism*, defined as $\varphi_q(x, y) = (x^q, y^q)$.

For $f \in End(E)$, the *degree of* f or $deg(f)$ is defined as $[K(E) : f^*K(E)]$. Informally, we can think of $deg(f)$ to be the degree of the formulas for f. We can factor this quantity as $deg(f) = deg(f)_{sep} \cdot deg(f)_{insep}$, the *separable* and *inseparable* degrees of f. It can be shown that $\#ker(f) = deg(f)_{sep}$. We will use this fact in several counting arguments in the sequel.

For $f \in End(E)$, we define f^v to be the (provably unique) endomorphism such that $f^v \circ f = [degf]$. Them mapping $f \mapsto f^v$ is an involution, i.e. it satisfies:

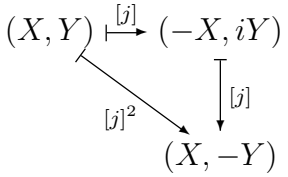
$$\begin{aligned} (f^v)^v &= f, \\ (f+g)^v &= f^v + g^v, \text{and} \\ (fg)^v &= g^v f^v. \end{aligned}$$

Here are a few easy-to-prove identities that we will use:

$$\begin{aligned} id^v &= id, \\ [n]^v &= [n], \\ f^v f &= [\deg f], \\ deg(f^v) &= deg(f). \end{aligned}$$

This implies, for example, that $deg([n]) = n^2$. This can be used to prove that $E(\mathbb{Z}/p\mathbb{Z})$ can be generated using at most two elements. The idea here is to decompose the abelian group $E(\mathbb{Z}/p\mathbb{Z})$ as a direct product of cyclic groups, and analyze $E(\mathbb{Z}/p\mathbb{Z})[\ell]$ where ℓ is the order of the group.

For some curves, the mult-by-n and Frobenius mappings are sufficient to generate $End(E)$. This is not always the case, however. We will now introduce some more endomorphisms which we haven't seen before. Consider the curve $Y^2 = X^3 - X$ over field $\mathbb{Z}/p\mathbb{Z}$ with $p \equiv 1 \mod 4$. The discriminant of this curve is -64. Let us denote by $[j]$ the endomorphism defined by $(x, y) \mapsto (-x, iy)$ (note that we use j here as a symbol to suggest the action of a complex number; is not meant to represent a positive integer). Then $[j]\,[j] = (x, -y) = -(x, y)$.



Note that $[j]^2 = [-1]$, so in particular this map cannot be equivalent to any of the mult-by-n maps. It can be shown that $End(E)$ is in fact generated by the mult-by-n maps and the $[j]$ map.

The properties of the involution $f \mapsto f^v$ are similar in some sense to complex conjugation. An arbitrary $f \in End(E)$ will, for example, satisfy:

$$\begin{aligned} f + f^v &= (f + id)(f^v + id) - ff^v - id \\ &= (f + id)(f + id)^v - ff^v - id \\ &= [deg(f + id)] - [degf] - [1] \\ &= [t] \quad \text{for some integer } t. \end{aligned}$$

We call t the *trace* of f. The endomorphisms f and $[t]$ satisfy $f^2 - [t]\, f + [\deg f] = 0$, in other words f is a zero of $X^2 - [t]X + [degf]$. We call this the characteristic polynomial of f.

In general, it is not always clear how to compute f^v. However, if the coefficients of the characteristic polynomial are known, then we can immediately plug t into the equation $f^v = [t] - f$.

Here is another example. Consider the curve $Y^2 = X^3 - X$ over $\mathbb{F}_{p^2}$, where $p \equiv 3 \mod 4$. In this case $F_p = F_p(i)$. In this case, the $End(E)$ ring is generated by the $[n]$ mappings, the $[j]$ map, and the Frobenius map φ_p, defined as usual:

$$(X, Y) \overset{[j]}{\longmapsto} (-X, iY)$$
$$(X, Y) \overset{\varphi_p}{\longmapsto} (X^p, Y^p)$$

Then:

$$\begin{array}{ccccc} (X,Y) & \overset{[j]}{\longmapsto} & (-X, iY) & \overset{\varphi_p}{\longmapsto} & (-X^p, i^p Y^p) = (-X^p, -Y^p) \\ & \searrow^{\varphi_p} & & & \\ & & (X^p, Y^p) & \overset{[j]}{\longmapsto} & (-X^p, iY^p) \end{array}$$

We observe quaternion-like behavior with respect to these morphisms:

$$\begin{aligned} \varphi_q\, [j] &= -\,[j]\, \varphi_q, \\ [j]^2 &= -1, \\ \varphi_q^2 &= -\,[p]\,, \end{aligned}$$

It can be shown that $End(E)$ is generated by the mult-by-n mappings, the $[j]$ mapping, and the φ_q mapping. Curves having this property are called *supersingular* (although this is a bit of a misnomer). They have a number of equivalent characterizations.

5.2 Hasse's Theorem

We now give a sketch of the following result:

Theorem 3. *(Hasse) For any curve E over finite field $\mathbb{F}_q$, we have*

$$\#E(\mathbb{F}_q) = q + 1 - t,$$

with $|t| \leq 2\sqrt{q}$.

Let φ_q the q-Frobenius morphism. It can be shown that all of the points in $E(\mathbb{F}_q)$ are fixed by φ_q. Therefore, $E(K) = \ker(\varphi_q - id)$. In particular,

$$\#E(K) = \#\ker(\varphi_q - id) = \deg(\varphi_q - id)_{sep}.$$

It can be shown that $\varphi_q - id$ is itself separable, so $\#E(\mathbb{F}_q) = \deg(\varphi_q - id)$. Now:

$$\begin{aligned} [\deg(\varphi_q - id)] &= (\varphi_q - id)(\varphi_q - id)^v \\ &= \varphi_q\varphi_q^v + id - \varphi_q - \varphi_q^v \\ &= [q] + [1] + [t]\,. \end{aligned}$$

5.3 Riemann-type theorems

In the last section, we showed that the number of points on an elliptic curve over $\mathbb{F}_q$ is $q + 1 - t$, with $|t| \leq 2\sqrt{q}$. Results such as these are often referred to as being analogous to the Riemann hypothesis. In this section we will give some explanation as to why this terminology is used. First, we need to understand this we will first describe two ways in which the Riemann Zeta function has been generalized. Recall that this function is defined to be the analytic continuation of the function defined by:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

on all $s \in \mathbb{C}$ such that $Re(s) > 1$. Euler showed that this function can also be formulated as:

$$\zeta(s) = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}.$$

Furthermore, the function can be reexpressed as a sum over the set of ideals I of $\mathbb{Z}$ as follows:

$$\zeta(s) = \sum_{I \subseteq \mathbb{Z}} \frac{1}{[\mathbb{Z} : I]^s}.$$

This type of expression is a special case of what is called a *Dedekind Zeta Function*. The Dedekind Zeta function over field $\mathbb{F}$ is defined by:

$$\zeta_{\mathbb{F}}(s) = \sum_{I \subseteq \mathcal{O}_{\mathbb{F}}} \frac{1}{[\mathcal{O}_{\mathbb{F}} : I]^s},$$

where $\mathcal{O}_{\mathbb{F}}$ is the ring of integers, and the sum is again taken over the set of ideals. We obtain the Riemann zeta function when $\mathbb{F} = \mathbb{Q}$. We can also write:

$$\zeta_{\mathbb{F}}(s) = \prod_{P \subseteq \mathcal{O}_{\mathbb{F}}} \frac{1}{1 - [\mathcal{O}_{\mathbb{F}} : P]^{-s}}.$$

Another type of generalization of the Riemann zeta function was introducted by Artin. He defined:

$$\zeta_{\mathbb{F}_q(X)}(s) = \sum_{I} \frac{1}{[\mathbb{F}_q[X] : I]^s},$$

where $\mathbb{F}_q[X]$ be the set of polynomial with coefficients in $\mathbb{F}_q$. Each ideal is generated by a unique monic polynomial, so to evaluate this sum we count, for each degree i, the number of monic polynomials of degree i is q^i. Thus,

$$\begin{aligned} \zeta_{\mathbb{F}_q(X)} &= 1 + \frac{q}{q^s} + \frac{q^2}{q^{2s}} + \frac{q^3}{q^{3s}} \cdots \\ &= \frac{1}{1 - q \cdot q^{-s}}. \end{aligned}$$

We want to define a zeta-type function for elliptic curves E, combining the two generalizations above. We define:

$$\zeta_E(s) = \prod \frac{1}{1 - [R : P]^s}.$$

There exists a bijection of the prime ideals of R not equal to 0 and the points P of E over $\mathbb{F}_q$. So we can rewrite this function as:

$$\zeta_E(s) = \prod_{P \in E(\mathbb{F}_q)} \frac{1}{1 - \#\mathbb{F}_q(P)^{-s}}.$$

This function can be evaluated to:

$$\zeta_E(s) = \frac{1 - tq^{-s} + q \cdot q^{-2s}}{(1 - q \cdot q^{-s})}.$$

Suppose s is a zero of ζ_E. Then q^s is a zero of $X^2 + tX + q$. This is the characteristic poly of φ_q, so we know that the discriminant is ≤ 0 so there are two roots of equal magnitude. In particular,

$|q^s| = \sqrt{q}$, and thus $q^{Re(s)} = q^{\frac{1}{2}}$ and $Re(s) = \frac{1}{2}$. All of the zeroes lie on the critical line where the points have real part equal to $1/2$, so we say that the Riemann hypothesis for $\zeta_{\mathbb{F}_q(X)}$ is true. Unlike the Riemann Zeta function however, this function is periodic modulo $\frac{2\pi i}{\log q}$.

5.4 Computing $\#E(\mathbb{F}_q)$

In this last section we address the following computational problem:

> **Input:** $Y^2 = AX + B + X^2$ over $\mathbb{F}_q$,
> **Problem:** compute $\#E(\mathbb{F}_q)$.

We focus on the particular case where $\mathbb{F}_q = \mathbb{Z}/p\mathbb{Z}$, for $p \gg 0$. In this we are helped in this case by Hasse's Theorem, and also the fact that $E(\mathbb{F}_q)$ is either cyclic or almost cyclic, in the sense that it is generated by at most two elements.

We will consider two techniques. The first technique is to directly evaluate the formula:

$$\#E(\mathbb{Z}/p\mathbb{Z}) = p + 1 - \sum_{X \in \mathbb{Z}/p\mathbb{Z}} \left(\frac{X^3 + AX + B}{p} \right).$$

Roughly, this is a feasible algorithm for $p < 100$.

For larger primes, we can use the following algorithm. This is a randomized algorithm which will be feasible for primes of size up to 10^{20} (roughly).

This algorithm uses a time-space tradeoff technique called the *baby step, giant step* technique. Let $a = \sqrt{4\sqrt{p}} \approx p^{1/4}$. The first step is to choose a random point $P = (x, y)$. We can do this by picking a random x in $\mathbb{F}_q$ and then solve for y. Our next objective then is to compute the order of this point. To do this we compute all the points in the sequence $P, 2P, 3P, \ldots, aP$. Since we can compute the inverse of each of these points by negating the Y component, we have actually computed $2a$ points. We call these points the *baby steps*. We store these points in a hash table and from here on we assume that we can check in constant time whether a given point is a baby step.

We also compute the point $(2a + 1)P$ and the point $(p + 1)P$. From this we compute, for all j, $Q_j = (p + 1)P \pm j(2a + 1)P$. We check each point Q_j in turn to see if it is one of the baby steps. Indeed by the choice of a we will find for some i, j with $-a \leq i, j \leq a$ such that $Q_j = iP$. It follows then that $mP = 0$ for $m = p + 1 + (2s + 1)i - j$. If there is exactly one (i, j) such that $Q_j = iP$, then we will have that m is the order of the group $E(\mathbb{F}_q)$, and so in this case $\#E(\mathbb{F}_q) = m$. This will be the case for most curves. The running time for this algorithm is $O(p^{\frac{1}{4}} \log^2 p)$.

In rare cases there will be two (i, j) pairs for which $Q_j = iP$. In this case, it is a fact that there are exactly two solutions. We can handle this exceptional case using some additional machinery by J.-F. Mestre.

Lecture 6. Hyperelliptic Curves Point Counting by p-adic Methods

Lecturer: Kiran Sridhara Kedlaya Scribe: Nitin Saxena

6.1 Introduction

The finite field in this lecture is $\mathbb{F}_q$ where $q = p^N$ and p is a prime. Think of p as a fixed or at least a small prime. In this lecture we will see Kedlaya's algorithm to compute the number of $\mathbb{F}_q$-points on a given curve $E(\mathbb{F}_q)$ of genus g using p-adic methods. The complexity of the algorithm is $\tilde{O}(g^4N^3)$. Elliptic curves are of genus 1 and this algorithm is better than Schoof's algorithm (remember p is fixed). For higher genus this algorithm is exponentially better than Schoof's! A *hyperelliptic* curve of genus g is given by the equation: $y^2 = f(x)$ where $f(x)$ is of degree $(2g+1)$. In this lecture we will see only a sketch of Kedlaya's algorithm in the special case of elliptic curves.

Our problem: Given an elliptic curve $E(\mathbb{F}_q)$: $y^2 = x^3 + Ax + B$. Find the number t for which $\#E(\mathbb{F}_q) = q + 1 - t$ and $|t| \leq 2\sqrt{q}$.

There are currently four ways to do this:

1. Enumerate all the $\mathbb{F}_q$ points on E. Deterministic and time taken: $\tilde{O}(q)$.

2. Since $E(\mathbb{F}_q)$ is a group of which we have a size estimate and an *oracle* access. We can use generic group algorithms (eg. baby-step giant-step). Randomized and time taken: $\tilde{O}(q^{\frac{1}{4}})$.

3. Schoof's algorithm. Deterministic and time taken: $\tilde{O}(\log^5 q)$.

4. p-adic methods. Deterministic and time taken: $poly(pN)$.

We will look at the fourth method here. But before that let us see two special instances when $\#E(\mathbb{F}_q)$ is easy to compute.

When the given equation of the elliptic curve has coefficients in $\mathbb{F}_p$ then it is easy to compute $\#E(\mathbb{F}_q)$. This is because we can trivially compute $\#E(\mathbb{F}_p)$ and then using the following lemma compute $\#E(\mathbb{F}_q)$.

Lemma 1. *Let E be an elliptic curve with coefficients in $\mathbb{F}_p$. If $\#E(\mathbb{F}_p) = p + 1 - t_0$ and α, β are the roots of $(x^2 - t_0x + p)$ then $\#E(\mathbb{F}_q) = q + 1 - \alpha^N - \beta^N$.*

Proof Sketch. We have from the theory of elliptic curves that $\#E(\mathbb{F}_p) = p + 1 - tr(\phi_p)$ and the Frobenius map ϕ_p satisfies the (endomorphism) equation: $\phi_p^2 - tr(\phi_p) \cdot \phi_p + p = 0$. Similarly, $\#E(\mathbb{F}_q) = q + 1 - tr(\phi_p^N)$ where we can now express $tr(\phi_p^N)$ in terms of the eigen values of ϕ_p. □

An elliptic curve $E(\mathbb{F}_q)$ is called *supersingular* if $t = 0 \pmod p$. There is a way to check whether an elliptic curve is supersingular and if it is then there is an explicit expression for $\#E(\mathbb{F}_q)$. Thus, we can assume that our given elliptic curve is not supersingular.

Rough Idea: In p-adic methods we compute $t \pmod{p^m}$ for large enough m's. Since we have a bound for t it will be enough to go upto $m \sim N$.

6.2 p-adic Numbers: Preliminaries

Definition 1. **p-adic numbers:** *Informally, for a prime p, $\mathbb{Z}_p$ are base-p expansions that are infinite on the left of the "decimal" unlike the natural integers. And $\mathbb{Q}_p$ are base-p expansions that are infinite on both sides of the "decimal" unlike the rationals.*

Note that a typical element a in $\mathbb{Z}_p$ looks like: $a = a_0 + a_1p + a_2p^2 + \cdots$ where $0 \leq a_i < p$ and there maybe infinitely many a_i's in the expansion. The $a_0, (a_0 + a_1p), (a_0 + a_1p + a_2p^2), \ldots$ can be seen as the values of $a \pmod p, a \pmod{p^2}, a \pmod{p^3}, \ldots$ respectively. This fact can be used to define the addition and multiplication operations in the set $\mathbb{Z}_p$.

Problem 1. *$\mathbb{Z}_p$ is a principal ideal domain and $\mathbb{Q}_p$ is a field. Both are of characteristic 0.*

A useful result about the p-adic numbers is *Hensel's lemma*. It says that if $f(x)$ is a polynomial with coefficients in $\mathbb{Z}_p$ then a root α of $f(x) \pmod p$ can be lifted to a root $\hat{\alpha}$ in $\mathbb{Z}_p$.

Problem 2. *Let p be an odd prime. If $x \in \mathbb{Z}_p$ such that x is a square modulo p then $\sqrt{x} \in \mathbb{Z}_p$. (Hint: Use Newton's iteration.)*

Quadratic extensions of $\mathbb{Q}_p$: If $x \in \mathbb{Z}_p$ is not a square modulo p then the extension ring $\mathbb{Q}_p[T]/(T^2 - x)$ is infact a field. It is a field of dimension 2 above $\mathbb{Q}_p$.

Higher extensions of $\mathbb{Q}_p$: In general, if $\mathbb{F}_q = \mathbb{F}_p[T]/(\overline{P}(T))$ is a finite field where $\overline{P}(T)$ is an irreducible polynomial with coefficients in $\mathbb{F}_p$. Then we can embed $\overline{P}(T)$ in $\mathbb{Z}_p[T]$ and call it $P(T)$. This gives us an extension ring of $\mathbb{Z}_p$:

$$\mathbb{Z}_q := \mathbb{Z}_p[T]/(P(T))$$

and a corresponding extension field of $\mathbb{Q}_p$:

$$\mathbb{Q}_q := \mathbb{Q}_p[T]/(P(T))$$

For example, the finite field $\mathbb{F}_9 = \mathbb{F}_3[T]/(T^2 + 1)$ of characteristic 3 has the corresponding infinite field $\mathbb{Q}_9 = \mathbb{Q}_3[T]/(T^2 + 1)$ of characteristic 0.

6.3 p-adic Cohomology Framework

The framework of cohomology has its roots in the theory of curves over characteristic zero. We know, for instance, that a circle in $\mathbb{R}^2$ *locally* looks like a line and we know that there are 'objects' called *differentials* that can be *integrated* on a part of the circle. Thus, the differential $r \cdot d\theta$, where (r, θ) are the polar coordinates, when integrated on the whole circle gives its circumference. The general philosophy is to associate linear data to nonlinear geometric objects. This associated linear data is called *cohomology*.

We want to bring these notions of locality and differentials to curves over characteristic $p > 0$. This is what the p-adic cohomology framework achieves and gives us a strong tool to study and to do computations in general curves over finite fields. We sketch here the main ideas of this framework in the case of elliptic curves.

Definition 2. *Let $\mathbb{F}_q(E) =$ fraction field of $\mathbb{F}_q[x, y]/(y^2 - x^3 - Ax - B)$, be the set of rational functions defined (almost everywhere) on the elliptic curve E. There is a natural* **derivation operator** *d defined on $\mathbb{F}_q(E)$. For any $f, g \in \mathbb{F}_q(E)$, d satisfies:*

- $df = 0$ *if* $f \in \mathbb{F}_q$.
- $d(f + g) = df + dg$.
- $d(f \cdot g) = f \cdot dg + g \cdot df$.

For example, $d(x^2) = 2xdx$ and $d(y^p) = py^{p-1}dy = 0$. But what are dx and dy? To give them meaning we define the following module.

Definition 3. *The set Ω of* **differential forms** *of an elliptic curve $E(\mathbb{F}_q)$ is the formal $\mathbb{F}_q$-linear combinations of $f \cdot dg$, where f, g are in the function field $\mathbb{F}_q(E)$ of the elliptic curve.*

Almost by the above two definitions we have the following properties of Ω:

- d is a $\mathbb{F}_q$-module homomorphism from $\mathbb{F}_q(E) \to \Omega$.
- Ω is a module over $\mathbb{F}_q(E)$ and is generated by dx, dy modulo $(2ydy - (3x^2 + A)dx)$.

It turns out that there is a unique 1-dimensional subspace of Ω with *no singularities* anywhere on E. It is generated by:

$$\frac{dx}{y} = \frac{2dy}{3x^2 + A}$$

Note that $\frac{dx}{y}$ has a singularity only at $y = 0$ but at that point $3x^2 + A \neq 0$ (as E is nonsingular) and hence at $y = 0$ we can use $\frac{2dy}{3x^2+A}$ which is well defined.

How does an endomorphism ψ of E acts on $\frac{dx}{y}$? Using ψ, an $f \in \mathbb{F}_q(E)$ can be *pulled-back* to another function $\psi^*(f) := f \circ \psi \in \mathbb{F}_q(E)$. Similarly, a differential $f \cdot dg \in \Omega$ can be pulled-back to another differential $\psi^*(f \cdot dg) = \psi^*(f) \cdot d(\psi^*(g))$. Thus, an endomorphism ψ of E extends to:

- an algebra homomorphism $\psi^* : \mathbb{F}_q(E) \to \mathbb{F}_q(E)$ by $f \mapsto f \circ \psi$, and

- a $\mathbb{F}_q$-module homomorphism $\psi^* : \Omega \to \Omega$ by $f \cdot dg \mapsto (f \circ \psi) \cdot d(g \circ \psi)$.

Now any endomorphism ψ of E when applied to $\frac{dx}{y}$ gives $\frac{d(x \circ \psi)}{y \circ \psi}$ which is again nonsingular everywhere on E. By the uniqueness of the nonsingular subspace generated by $\frac{dx}{y}$ we get that:

Lemma 2. *For any endomorphism ψ of $E(\mathbb{F}_q)$ there exists a $c_\psi \in \mathbb{F}_q$ such that*

$$\psi^* \left(\frac{dx}{y} \right) = c_\psi \cdot \frac{dx}{y} \tag{6.36}$$

The above lemma shows the "usefulness" of working with the differential forms: some of these are the eigen-vectors of the endomorphisms of E.

What do these differential forms tell us about the Frobenius endomorphism ϕ_q? We could apply ϕ_q on $\frac{dx}{y}$ and get c_{ϕ_q} such that:

$$\phi_q^* \left(\frac{dx}{y} \right) = c_{\phi_q} \cdot \frac{dx}{y} \tag{6.37}$$

But then c_{ϕ_q} is an eigenvalue of ϕ_q and will satisfy the endomorphism equation of the elliptic curve:

$$c_{\phi_q}^2 - t \cdot c_{\phi_q} + q = 0 \tag{6.38}$$

and hence it seems that we can recover t from the value c_{ϕ_q} and hence compute $\#E(\mathbb{F}_q)$. Except that there is a problem: clearly $q = 0 \pmod p$, also if you do the derivation in Equation (6.37) then c_{ϕ_q} comes out to $0 \pmod p$, thus, Equation (6.38) is actually a triviality. This disaster happened because the field over which the differential forms are defined has a nonzero characteristic p. Can we generalize these ideas to a field of zero characteristic that still has a Frobenius-like endomorphism whose eigenvalues are related to $\#E(\mathbb{F}_q)$?

The idea of Satoh [Sat00] was to lift a given elliptic curve $E(\mathbb{F}_q)$ together with its Frobenius endomorphism ϕ_q to a q-adic elliptic curve $E(\mathbb{Q}_q)$ and a Frobenius endomorphism $\tilde{\phi} : E(\mathbb{Q}_q) \to E(\mathbb{Q}_q)$. Then he computed $\tilde{\phi}(dx/y)$ to get $c_{\tilde{\phi}}$. Finally, approximated t from the (now nontrivial) equation: $c_{\tilde{\phi}}^2 - t \cdot c_{\tilde{\phi}} + q = 0$ over $\mathbb{Q}_q$. Assuming a fixed p and $q = p^N$ Satoh's algorithm runs in time $O(N^2)$.

6.4 p-adic de Rham Cohomology

Satoh's algorithm is a fast p-adic algorithm for elliptic curves. Kedlaya [Ked01] used a more general cohomology and gave a p-adic algorithm that is efficient for hyperelliptic curves and potentially works for higher dimensional varieties as well.

In classical analysis de Rham cohomology is the way to associate differentials to curves (in general, manifolds) over characteristic zero (motivating case is $\mathbb{R}$). The cohomology used in Kedlaya's algorithm is a version of de Rham cohomology for curves over nonzero characteristic developed by Dwork and Monsky-Washnitzer (1960s).

Given an elliptic curve $E(\mathbb{F}_q)$ it is again lifted to $E(\mathbb{Q}_q)$. But now the Frobenius map ϕ_q is lifted to a 'strange' morphism $\tilde{\phi}$ (which is ϕ_q when restricted to $\mathbb{F}_q[x,y]$) that satisfies:

$$\tilde{\phi}^*(x) = x^q$$

$$\tilde{\phi}^*(x) = y^q \cdot \sqrt{\frac{x^{3q} + Ax^q + B}{(x^3 + Ax + B)^q}} \quad \text{written as a power series.}$$

Now the differential dx/y is no more an eigen vector of $\tilde{\phi}$ but still the action of $\tilde{\phi}$ on the differential gives some information about t. If Ω' is the module of differential forms associated to $E(\mathbb{Q}_q)$ then $\Omega'/\text{Im}(d)$ (recall that d is the derivative operator) is generated by $\frac{dx}{y}$ and $\frac{x \cdot dx}{y}$ over $\mathbb{Q}_q$. Thus, $\tilde{\phi}$ acts on $\Omega'/\text{Im}(d)$ as a 2×2 matrix which we can compute. This 2×2 matrix of $\tilde{\phi}$ still satisfies the endomorphism equation $\tilde{\phi}^2 - t \cdot \tilde{\phi} + q = 0$. Thus, we can again approximate t in $\mathbb{Q}_q$.

Lecture 7. Schoof's algorithm and some improvements

Lecturer: René Schoof Scribe: Valentina Settimi

7.1 Schoof's algorithm

In this section we present *Schoof's algorithm* which is a deterministic polynomial time algorithm to determine the number of rational points of an elliptic curve E over a finite field $\mathbb{F}_q$.

We assume $\mathrm{char}(\mathbb{F}_q) = p \neq 2, 3$ (the algorithm actually works, with slight modifications, even when $p = 2$ or 3). Let

$$Y^2 = X^3 + AX + B \qquad \text{with } A, B \in \mathbb{F}_q$$

be the *Weierstraß equation* of E and let

$$\begin{aligned} \varphi_q : E(\overline{\mathbb{F}}_q) &\longrightarrow E(\overline{\mathbb{F}}_q) \\ (x, y) &\longmapsto (x^q, y^q) \end{aligned}$$

be the q-*Frobenius*. We have $\#E(\mathbb{F}_q) = q + 1 - t$, with $t = \mathrm{trace}(\varphi_q)$ and $|t| \leq 2\sqrt{q}$ (*Hasse's Theorem*).

The main idea of Schoof's algorithm is:

- compute $t \pmod{l}$, for the first few small primes l;
- compute $t \pmod{\prod_l l}$, using *Chinese Remainder Theorem*;
- if $\prod_l l > 4\sqrt{q}$, then $t \pmod{\prod_l l} = t$, by Hasse's Theorem.

The question is: how can we control $\prod_l l$? As consequence of the *Weak Prime Number Theorem*, we have $\prod_{l \leq x, l\, prime} l \sim e^x$. We want

$$e^x \sim \prod_{l \leq x, l\, prime} l > 4\sqrt{q} \qquad \text{i.e.} \qquad x > \ln(4\sqrt{q}).$$

Since q is large, it is enough to set $x \approx \log q$ which means to take all the primes $l \leq \log q$. The number of such primes is clearly less than $\log q$.

Now we show how to compute $\#E(\mathbb{F}_q) \pmod{l}$. Below is an **example:**

$l = 2$ Compute $\#E(\mathbb{F}_q) \pmod{2}$.

$$\begin{aligned} \#E(\mathbb{F}_q) \equiv 0 \pmod{2} &\iff \#E(\mathbb{F}_q) \text{ even} \\ &\iff \exists P \in E(\mathbb{F}_q) \text{ of order } 2. \end{aligned}$$

So we want to check the existence of a point $P = (x, y) \in E(\overline{\mathbb{F}}_q)$ which satisfies the following two requirements:

1. $P \in E(\mathbb{F}_q) \Leftrightarrow \varphi_q(P) = P \Leftrightarrow (x^q, y^q) = (x, y)$.
2. P of order $2 \Leftrightarrow P + P = 0 \Leftrightarrow P = -P \Leftrightarrow (x, y) = (x, -y) \Leftrightarrow y = 0 = x^3 + Ax + B$.

Thus

$$\begin{aligned} \#E(\mathbb{F}_q) \equiv 0 \pmod 2 &\iff \exists x \in \overline{\mathbb{F}}_q \text{ s.t. } \begin{cases} x^q = x \\ x^3 + Ax + B = 0 \end{cases} \\ &\iff \gcd(X^q - X, X^3 + AX + B) \neq 1 \qquad \text{in } \mathbb{F}_q[X]. \end{aligned}$$

We cannot compute such $\gcd$ directly, because X^q is too large; but we can compute it in the following way:

- compute $h(X) \equiv X^q \pmod{X^3 + AX + B}$ in $\mathbb{F}_q[X]/(X^3 + AX + B)$;
- compute $\gcd(h(X) - X, X^3 + AX + B)$ in $\mathbb{F}_q[X]$.

$X^q \pmod{X^3 + AX + B}$ can be computed efficiently using the binary expansion of q and repeated squarings. Moreover $\#\mathbb{F}_q[X]/(X^3 + AX + B) = q^3$, so any element of the ring $\mathbb{F}_q[X]/(X^3 + AX + B)$ has size $3 \log q$. Therefore the amount of work is: $\mathcal{O}(\log q^{1+\mu})$ with $1 \leq \mu \leq 2$ (in particular $\mu = 2$ if we use standard multiplications and $\mu = 1$ if we use fast multiplications).

$l > 2$ We know that the q-Frobenius verifies

$$\varphi_q^2 - [t]\varphi_q + [q] = 0 \qquad \text{in } \mathrm{End}(E).$$

That is, $\forall P \in E(\overline{\mathbb{F}}_q)$ (and in particular $\forall P \in E[l]$):

$$[t]\varphi_q(P) = \varphi_q^2(P) + [q](P) \qquad \text{in } E.$$

Let $q_0 = q \pmod l$. Since for every $P \in E[l]$, $[n]P = [n \pmod l]P$, we can find $t \pmod l$ by checking whether

$$[i]\varphi_q = \varphi_q^2 + [q_0] \qquad \text{on } E[l]$$

for $i = 0, \ldots, l-1$. This can be done efficiently using polynomials, but to do it we need a polynomial which characterizes the l-torsion points of $E(\overline{\mathbb{F}}_q)$. We have

$$E[l] = \{P \in E(\overline{\mathbb{F}_q}) : \underbrace{P + \ldots + P}_{l \text{ times}} = 0\} \cong \mathbb{Z}/l\mathbb{Z} \times \mathbb{Z}/l\mathbb{Z}.$$

There exists polynomials, called *division polynomials*, $\Psi_l(X) \in \mathbb{F}_q[X]$ such that $\forall x \in \overline{\mathbb{F}}_q$:

$$\Psi_l(x) = 0 \iff \exists y \in \overline{\mathbb{F}}_q \text{ s.t. } (x, y) \in E[l].$$

Since $\#E[l] = l^2$, there exist $l^2 - 1$ non-zero points in $E[l]$; moreover

$$(x, y) \in E[l] \Rightarrow (x, -y) \in E[l]$$

so there exist $\frac{l^2-1}{2}$ $x \in \overline{\mathbb{F}}_q$ such that $(x, y) \in E[l]$ for some $y \in \overline{\mathbb{F}}_q$. Thus $\deg \Psi_l(X) = \frac{l^2-1}{2}$.

We can compute $\Psi_l(X)$ using recursively the formulas to add points on $E(\overline{\mathbb{F}}_q)$. For instance, let $l = 3$ and let $P = (x, y) \in E(\overline{\mathbb{F}}_q)$:

$$\begin{aligned}
P \in E[3] &\iff P + P + P = 0 \\
&\iff P + P = -P \\
&\iff (x, y) + (x, y) = (x, -y) \\
&\iff \left(-2x + \left(\frac{3x^2 + A}{2y}\right)^2, \ldots\right) = (x, \ldots) \\
&\qquad \text{(we can neglect the } Y\text{-coordinate, since each } X\text{-coordinate identifies} \\
&\qquad \text{a unique point "modulo the opposite")} \\
&\iff x = -2x + \left(\frac{3x^2 + A}{2y}\right)^2 \\
&\iff 12xy^2 = (3x^2 + A)^2 \\
&\qquad (y^2 = x^3 + Ax + B, \text{because } P \in E(\overline{\mathbb{F}}_q)) \\
&\iff 3x^4 + 6Ax^2 + 12Bx - A^2 = 0
\end{aligned}$$

that is $\Psi_3(X) = 3X^4 + 6AX^2 + 12BX - A^2$.

So we have, for $i = 0, \ldots, l - 1$:

$$\begin{array}{ll}
[i]\varphi_q = \varphi_q^2 + [q_0] & \text{in } E[l] \\
\Updownarrow & \\
[i](X^q, Y^q) \equiv (X^{q^2}, Y^{q^2}) + [q_0](X, Y) & \text{in } R := \mathbb{F}_q[X]/(\Psi_l(X), Y^2 - X^3 - AX - B)
\end{array}$$

(with $+$ the addition on E).

Since the elements of R have size $l^2 \log q$, the amount of work to check whether $[i]\varphi_q = \varphi_q^2 + [q_0]$ in $E[l]$ is:

- to compute $[i](X^q, Y^q)$: $\mathcal{O}(l(l^2 \log q)^\mu)$;
- to compute $(X^{q^2}, Y^{q^2}) + [q_0](X, Y)$: $\mathcal{O}(\log q(l^2 \log q)^\mu + l(l^2 \log q)^\mu)$.

But $l \leq \log q$, so the total amount of work to compute $\#E(\mathbb{F}_q) \pmod l$ is $\mathcal{O}(\log q^{1+3\mu})$.

We have to do it for every prime $l \leq \log q$, thus the amount of work involved in Schoof's algorithm is

$$\mathcal{O}(\log q^{2+3\mu}),$$

with $1 \leq \mu \leq 2$ (in particular it is $\mathcal{O}(\log q^8)$ if we use standard multiplications and $\mathcal{O}(\log q^5)$ if we use fast multiplications). Schoof's algorithm is therefore a deterministic polynomial time algorithm, but in practice its behavior is not so good because the size of the elements of R is too large. We conclude presenting briefly two practical improvements of the Schoof's algorithm.

7.2 Atkin's algorithms

As before, let $E/\mathbb{F}_q$ be an elliptic curve. For every prime $l \neq p = \mathrm{char}(\mathbb{F}_q)$, there exists a universal polynomial, called *modular polynomial*, $\Phi_l(S,T) \in \mathbb{Z}[S,T]$ such that for every morphism of elliptic curves $f : E_1 \to E_2$ of degree l

$$\Phi_l(j(E_1), j(E_2)) = 0.$$

Foe every l, we have:

- $\Phi_l(S,T)$ is symmetric: $\Phi_l(S,T) = \Phi_l(T,S)$;
- $\deg_S \Phi_l(S,T) = l+1$.

Naively, Atkin's idea is to reduce $\Phi_l(j(E),T) \in \mathbb{F}_q[T]$ as product of irreducible polynomials and, from their degrees, deduce partial information on $t \pmod l$.

7.3 Elkies's algorithm

Elkies's idea is to use a divisor $F(X)$ of $\Psi_l(X)$ of small degree, instead of $\Psi_l(X)$ itself.

Suppose that φ_q acts on $E[l]$ in such a way that it fixes a subgroup C of order l. Then $\exists \lambda \in \{1,\dots,l-1\}$ such that:

$$\varphi_q(P) = [\lambda]P \qquad \forall P \in C.$$

As $E[l]$ is defined by the polynomial $\Psi_l(X)$ (i.e. the zeros of $\Psi_l(X)$ are the X-coordinates of the points in $E[l]$), such eigenspace C can be defined by a polynomial $F(X) \in \mathbb{F}_q[X]$ which is such that:

- the zeros of $F(X)$ are the X-coordinates of the points in C;
- $F(X) | \Psi_l(X)$, since $C \subseteq E[l]$;
- $\deg F(X) = \frac{l-1}{2}$, since in C there are $l-1$ non-zero points and each X-coordinate corresponds to two points.

The characteristic polynomial of φ_q is $X^2 - tX + q$, so the product of its eigenvalues is equal to q and the sum is equal to t. It implies

$$t \equiv \lambda + q/\lambda \pmod l.$$

Thus, to compute $t \pmod l$, it is enough to find the eigenvalue λ of φ_q corresponding to the eigenspace C. This can be easily done by checking whether for $i = 1,\dots,l-1$

$$\varphi_q(P) = [i]P \qquad \forall P = (x,y) \in C$$

$$\Updownarrow$$

$$(X^q, Y^q) = [i](X, Y) \qquad \text{in } R' := \mathbb{F}_q[X]/(F(X), Y^2 - X^3 - AX - B).$$

Since $F(X)$ has degree $\frac{l-1}{2}$ (while $\Psi_l(X)$ has degree $\frac{l^2-1}{2}$), the element of R' have size $l \log q$. So the amount of work to compute (X^q, Y^q) in R' is $\mathcal{O}(l(l \log q)^\mu) = \mathcal{O}(\log q^{1+2\mu})$.

To conclude, we remark that Elkies's idea only works for primes l for which the q-Frobenius acting on $E[l]$ has its eigenvalues in $\mathbb{Z}/l\mathbb{Z}$, which are about 50%.

Lecture 9. The Algorithms of Lenstra and Goldwasser-Kilian-Atkin

Lecturer: René Schoof Scribe: John Voight

Today we will talk about two algorithms. The first is Lenstra's elliptic curve factoring method (ECM), and the second is the primality testing algorithm of Goldwasser-Kilian-Atkin.

9.1 Lenstra's algorithm

Recall the old $p-1$ factoring method due to Pollard. Let $n \in \mathbb{Z}_{>0}$ be the integer to be factored. First we choose a bound $B \in \mathbb{Z}_{>0}$ and precompute

$$M = \prod_{\substack{q^e < B \\ q \text{prime}}} q^e \approx \exp(B).$$

Next, we pick $x \in (\mathbb{Z}/n\mathbb{Z})^*$ at random. Then we compute $x^M \pmod{n}$, and let $d = \gcd(x^M - 1, n)$.

Then $d \mid n$, and one hopes that $d > 1$, i.e., there exists a prime p dividing d, which holds if and only if $x^M \equiv 1 \pmod{p}$. In practice, one succeeds with this approach when $p-1 \mid M$, i.e., $p-1$ is B-*smooth*, so that all primes q which divides $p-1$ are $\leq B$. (Usually, $x^M \not\equiv 1 \pmod{p}$, so when $d \neq 1$ we almost never have $d = n$.)

Here, we have $p - 1 = \#(\mathbb{Z}/p\mathbb{Z})^*$, and $x^M = 1$ in $(\mathbb{Z}/p\mathbb{Z})^*$. The computation is essentially a group-theoretic one, so it makes sense to look for other groups where this general approach may work. We replace the multiplicative group by an elliptic curve. We choose B and compute M as before.

Next, we pick an elliptic curve over $\mathbb{Z}/n\mathbb{Z}$. Note that $\mathbb{Z}/n\mathbb{Z}$ is not a field, so we have not even defined what this means! We take the lazy way out and define an elliptic curve over $\mathbb{Z}/n\mathbb{Z}$ to be defined by a Weierstrass equation $Y^2 = X^3 + AX + B$ with $A, B \in \mathbb{Z}/n\mathbb{Z}$ with $\Delta = -16(4A^3 + 27B^2)$ is invertible in $\mathbb{Z}/n\mathbb{Z}$, i.e., $\gcd(4A^3 + 27B^2, n) = 1$. In particular, if $p \mid n$ is a prime divisor, then $Y^2 = X^3 + AX + B$ considered modulo p is a genuine elliptic curve, so this is a natural generalization. The same formulas for addition on an elliptic curve hold (the subtleties here exactly lead to the factoring algorithm!); the zero element is again the point $(0 : 1 : 0)$.

[For any ring R, one can make sense of an elliptic curve over R. In particular, an elliptic curve over $\mathbb{Z}/n\mathbb{Z}$ with $n = pq$ may be thought of as a product of elliptic curves over $\mathbb{Z}/p\mathbb{Z}$ and over $\mathbb{Z}/q\mathbb{Z}$. One can also work with projective coordinates over $\mathbb{Z}/n\mathbb{Z}$; and then we define the projective plane over $\mathbb{Z}/n\mathbb{Z}$ to be the set of triples $(x : y : z)$, up to rescaling by elements of $(\mathbb{Z}/n\mathbb{Z})^*$, satisfying $\gcd(x, y, z, n) = 1$.]

Now, pick an elliptic curve $E : Y^2 = X^3 + AX + B$, pick $P \in E(\mathbb{Z}/n\mathbb{Z})$, and compute $MP = \underbrace{P + \cdots + P}_{M}$ in $E(\mathbb{Z}/n\mathbb{Z})$. Now we have to check whether for some prime p, we have the

analogue of $x^M \equiv 1 \pmod{p}$, that is, MP is the neutral element modulo p, so that $p \mid n$, and then usually MP is not the neutral element modulo the other primes dividing p. In this situation, we can also factor.

To show how this works, we will do a "Mickey mouse" example. We will factor 35. Let $E : Y^2 = X^3 - X - 2$. We have $\Delta = -16(4(-1) + 27(4))$ which has $\gcd(\Delta, 35) = 1$. We choose $P = (2, 2)$ a 'random' point, and choose $M = 3$. We compute $MP = 3P$. We first compute

$$2P = P + P = (x_3, y_3) = (-2 - 2 + (3 \cdot 2^2 - 1)^2/(2 \cdot 2)^2, y_3) = (-4 + (11/4)^2, y_3) = (-3, 3).$$

And then

$$3P = 2P + P = (-3, 3) + (2, 2) = (3 - 2 + (2 - 3)^2/(2 + 3)^2, ...)$$

which causes a disaster, since 5 is not invertible modulo 35; and computing $\gcd(5, 35) = 5 \mid 35$, and thus we have factored 35! The 'problem' is that $(-3, 3) \equiv (2, -2) = -(2, 2) \pmod{5}$, so our formulas do not apply, and by using the inappropriate formulas, we discover a factor.

To pick a point on E, if we were working over a field we would pick a random x until $x^3 + Ax + B$ is a square, and then we compute a square root. But computing a square root is notoriously difficult modulo a nonsquare (given an oracle that computes square roots, one can factor n), so we reverse the steps; first we pick a random (x, y) and a random A, then take the curve $Y^2 = X^3 + AX + B$ with $B = y^2 - x^3 - Ax$. (In fact, it is enough to choose random $(0, y)$.)

In the classical case, we had success if $\#(\mathbb{Z}/p\mathbb{Z})^* = p - 1$ is B-smooth. Now we have success if $\#E(\mathbb{Z}/p\mathbb{Z})$ is B-smooth for some prime $p \mid n$ (and not B-smooth for other primes $q \mid n$). Then, $MP \equiv \infty \pmod{p}$ and $MP \not\equiv \infty \pmod{q}$ for $p \neq q \mid n$. If $m = \#E(\mathbb{Z}/p\mathbb{Z})$, then by group theory, $mP = \infty$, and indeed $MP = \infty$ (almost in practice) if and only if $m \mid M = \prod_{q^e < B} q^e$ if and only if M is B-smooth.

Note that if we do not succeed, we can simply throw away E and choose another curve! (In the classical case, the game was over.) So we wait for a "good" curve, i.e., a curve with $\#E(\mathbb{Z}/p\mathbb{Z})$ B-smooth for some $p \mid n$. [One desperately hopes that $\#E(\mathbb{Z}/p\mathbb{Z})$ is B-smooth for some choice of E; it will almost never happen in practice that $\#E(\mathbb{Z}/q\mathbb{Z})$ will be B-smooth for other primes $q \mid n$.]

To reiterate, the algorithm runs as follows. The input is the integer $n \in \mathbb{Z}_{>0}$ to be factored. We choose B and precompute $M = \prod_{q^e < B} q^e$. We repeat: pick a random P on a random $E(\mathbb{Z}/n\mathbb{Z})$, and compute MP until one cannot invert a denominator, and then stop with the divisor produced by this failed inversion.

Now the question is: How many times do we repeat in the loop? Choose $A, B \in \mathbb{Z}/n\mathbb{Z}$ at random giving $E : Y^2 = X^3 + AX + B$, and usually $\gcd(\Delta, n) = 1$ (otherwise we are happy anyway). Let p be (the smallest) prime divisor of n. We analyze how much work it takes to find p, i.e., when does $E(\mathbb{Z}/p\mathbb{Z})$ have B-smooth order? What is essential for the success of this method is that when the elliptic curves vary, so do the group orders. Picking objects at random modulo n gives objects which are random modulo p, so we do the analysis there.

There are p^2 'choices' for an elliptic curve E modulo p, and so we ask, how are they distributed with respect to $\#E(\mathbb{Z}/p\mathbb{Z})$? Well, this order lies in the interval $(p + 1 - 2\sqrt{p}, p + 1 + 2\sqrt{p})$, and very roughly,

$$\#\{(a, b) : E : Y^2 = X^3 + AX + B \text{ has } p + 1 - t \text{ points}\} = \frac{p}{2} H(t^2 - 4p) \approx \frac{p}{2\pi} \sqrt{4p - t^2}.$$

where $H(d)$ is the class number of the order of discriminant $d < 0$. This approximation is very rough, and gives roughly 'an ellipse': there are approximately an even number around the middle, with fewer at the ends, subject to very chaotic behavior.

If we pretend that the values are equidistributed in the interval, then picking a random curve corresponds to picking a random integer in the range $(p+1-2\sqrt{p}, p+1+2\sqrt{p})$. So the key question is: what is the probability that such a random integer is B-smooth? Define $u \in \mathbb{R}_{>2}$ as $B = p^{1/u}$. Then the probability is $1/u^u$, so we need to try u^u curves, and the work for each curve is to compute MP where $M \approx \exp(B)$ so $O(B) = O(p^{1/u})$, so the total work is $O(u^u p^{1/u})$. To optimize, if B is very big one does a huge amount of work to compute MP; if B is very small, then by smoothness one must repeat many, many curves. Using calculus, we find the optimum at

$$u \approx \sqrt{\frac{2\log p}{\log\log p}}$$

so we must do the work

$$O\left(\exp(\sqrt{2\log p \log\log p})\right).$$

Lenstra's algorithm *probably* finds small prime factors p first, which is a unique feature of this algorithm. This is good for factoring numbers that you find 'in the street'; but the worst case is for RSA numbers which are $n = pq$ the product of two primes p, q; then the time is $O(\exp(\sqrt{\log n \log\log n}))$.

9.2 Goldwasser-Kilian-Atkin's algorithm

Recall Pocklington's criterion. Let n be an integer which is to be proved prime. Write $n-1 = QR$ with $Q, R \in \mathbb{Z}_{>0}$. Suppose that for all primes $q \mid Q$, there exists $a \in (\mathbb{Z}/n\mathbb{Z})^*$ satisfying

$$a^Q \equiv 1 \pmod{n} \text{ and } \gcd(a^{Q/q} - 1, n) = 1.$$

Then a has order $q^m \parallel n-1$ modulo every $p \mid n$, so for all $p \mid n$ we have $p \equiv 1 \pmod{Q}$, so in particular $p > Q$, so if $Q > \sqrt{n}$, then n is prime.

Note that one does *not* need $Q \mid (n-1)$; in practice, one needs this, but the statement does not depend on it. We do, however, need that Q is completely factored.

We now replace this by the 'elliptic version'. We look at elliptic curves modulo n; recall that after running many compositeness tests we can be almost certain that n is prime, but we would like a proof.

The translation of Pocklington's criterion reads as follows. Choose an elliptic curve E over $\mathbb{Z}/n\mathbb{Z}$. Suppose we have an integer $\mathbb{Q} \in \mathbb{Z}_{>0}$. If for all $q \mid Q$ there exists $P \in E(\mathbb{Z}/n\mathbb{Z})$ such that

$$QP = \infty \pmod{n} \text{ and } (Q/q)P \not\equiv \infty \pmod{p} \text{for any } p \mid n.$$

[One can check the latter condition by using homogeneous coordinates and computing $(Q/q)P = (x : y : z)$ and then check if $\gcd(z, n) = 1$.] Then P has order q^m in $E(\mathbb{Z}/p\mathbb{Z})$, and taking

the product we find that $Q \mid \#E(\mathbb{Z}/p\mathbb{Z})$ for all $p \mid n$, so $Q < (\sqrt{p+1})^2 \approx p$. Therefore, if $Q > (\sqrt[4]{n}+1)^2$, then we can conclude that n is prime.

We use in practice that $\#E(\mathbb{Z}/n\mathbb{Z}) = QR$; what one needs in practice the complete factorization of Q. Morally, $\#E(\mathbb{Z}/n\mathbb{Z}) \approx p$, so one will almost succeed in finding such a sufficiently large factored Q.

The idea of Goldwasser-Kilian: sometimes it will happen that R will be a probable prime. Then switch the roles of Q, R, exactly as we did with the Pocklington test. We have then proven that "if R is prime, then Q is prime". The profit is that again we can vary the curve and throw away a curve that does not work; so by the prime number theorem, we need to try approximately $\log n$ curves to have R to be a probable prime (with also $Q \geq 2$; in practice, Q may be much larger).

To summarize: Let n be the integer which is to be proved prime. First try to factor $n-1 = QR$ for Q small and R a probable prime. (This will almost never happen; so make only a small effort.) Now repeat the following loop: pick an elliptic curve E at random, compute $\#E(\mathbb{Z}/n\mathbb{Z})$, and hope that $\#E(\mathbb{Z}/n\mathbb{Z}) = QR$ with Q completely factored and R a probable prime; if not, throw away E and return. If success, then start over with R in place of n.

The important issue to discuss is computing the order $\#E(\mathbb{Z}/n\mathbb{Z})$. In the asymptotic analysis, Goldwasser-Kilian use Schoof's algorithm; in practice, this is too slow. Atkin uses CM elliptic curves and reduces them modulo n: if E has CM by $\mathbb{Z}[\sqrt{d}]$ with $d < 0$, then one can reduce over $\mathbb{Z}/n\mathbb{Z}$ with $n = x^2 - dy^2$ (which can be done very quickly using lattice reduction), then $\#E(\mathbb{Z}/n\mathbb{Z}) = (x \pm 1)^2 - dy^2$. The analysis here is shaky, but in practice it works very well.

This algorithm holds world records for primality proving (for numbers without a special form): in July 2007, $(2^{42737}+1)/3$ was proved prime.

Lecture 10. Elliptic Curves over $\mathbb{Q}$

Lecturer: Henri Darmon Scribe: Matei David

10.1 Introduction

In our lectures so far, we have considered elliptic curves over finite fields $\mathbb{F}_{p^m}$ and their applications to computing. Today, we consider elliptic curves over the field of rational numbers $\mathbb{Q}$ and the applications of computing to answering questions about such curves.

In general, an elliptic curve E over a field $\mathbf{k}$ is given by the Weierstrass equation

$$E: \ y^2 = x^3 + A \cdot x + B,$$

with $A, B \in \mathbf{k}$ (when $6 \neq 0$ in $\mathbf{k}$.) The discriminant of this curve is $\Delta = 4A^3 + 27B^2 \neq 0$. As before, we denote by $E(\mathbf{k})$ the set of points with coordinates in $\mathbf{k}$ that are on the curve E, i.e., that satisfy the equation defining E, plus the point "at infinity", (∞, ∞). We have seen before that there exists an addition operation on this set making it a group.

We will be concerned with the following two problems.

A Make a list of all elliptic curves over $\mathbb{Q}$.

B Given a fixed elliptic curve E (by its Weierstrass equation), compute $E(\mathbb{Q})$.

10.2 Basic Remarks

10.2.1 On problem A

When it comes to listing all elliptic curves over $\mathbb{Q}$, we have previously seen in lecture 4 that the notion of j-invariant gives a bijection between the set of all elliptic curves over $\mathbb{Q}$ (up to isomorphism) and the underlying field $\mathbb{Q}$. It turns out, the j-invariant is not a good measure of the "arithmetic complexity" of an elliptic curve. Instead, we could try to use its discriminant Δ.

We can assume WLOG that the coefficients A, B defining the curve are integers, otherwise we can change the equation obtaining the same curve. Then, the discriminant Δ is also an integer. (Note, if p is a prime and $p \nmid \Delta$, then $E \mod p$ is still an elliptic curve.) To make a list of all elliptic curves, we can ask questions of the form: are there elliptic curves with discriminant $\Delta = 1$? That is, are there integers A, B such that $4A^3 + 27B^2 = 1$? In this particular case, the answer is no. Continuing in this way, we would hope to list all elliptic curves by listing all curves with a given discriminant.

However, we will work with the notion of *conductor* instead, which is a better measure of the arithmetic complexity of E.

Definition 4. *The conductor N_E of an elliptic curve E over $\mathbb{Q}$ is defined to be*

$$N_E = \prod_{p \text{ prime}} p^{\delta_p},$$

where δ_p is a function of p and E, and $\delta_p \in \{0, 1, 2\}$ for $p > 3$.

When $p \nmid \Delta$, $\delta_p = 0$, so N_E is divisible by the same primes as Δ. When $p \mid \Delta$, $\delta_p \in \{1, 2\}$ depending on whether the equation defining E has a triple or a double root. For $p = 2, 3$, δ_p is computed using another recipee (Tate's algorithm), which we omit.

Thus, we can rephrase problem A as follows: given N, list all elliptic curves (up to isomorphism) with conductor N. Let $e(N)$ denote the number of such curves. We know that $e(N) = 0$ for $N < 11$, $e(11) = 3$, $e(12) = e(13) = 0$, $e(14) = 6$ and so on. There exist tables computing $e(N)$ for N up to 130000. In this lecture, we will touch upon the math involved in building these tables.

10.2.2 On problem B

Given an elliptic curve E, we want to compute $E(\mathbb{Q})$, the group of rational points on E. Unlike the case for finite fields, there is no reason for $E(\mathbb{Q})$ to be finite. However, one of the most important theorems in the study of elliptic curves over the rationals states that this group is finitely generated.

Theorem 4 (Mordell, 1923)**.** *$E(\mathbb{Q})$ is a finitely generated abelian group. That is, there exist r points $P_1, \ldots, P_r$ with rational coordinates such that every element in $E(\mathbb{Q})$ can be written as $n_1 P_1 + \cdots + n_r P_r$ with $n_1, \ldots, n_r \in \mathbb{Z}$.*

Definition 5. *The value r in the Theorem above is called* the rank of E over $\mathbb{Q}$.

Thus, problem B reduces to the following subproblems. Given an elliptic curve E,

1. find the rank r of E over $\mathbb{Q}$; and
2. find $P_1 = (x_1, y_1), \ldots, P_r = (x_r, y_r)$ that generate $E(\mathbb{Q})$.

Even for simple curves, the generators P can be very large in terms of space, so the naive approach of ranging over x while looking for points on E is not adequate.

10.3 Modularity

In what follows, we investigate the connection between elliptic curves over the rationals and *modular forms*.

Given an elliptic curve E over $\mathbb{Q}$ and a prime p not dividing N_E, E is still an elliptic curve over $\mathbb{F}_p$. Let $N_p = \#E(\mathbb{F}_p)$ be the number of points on E over the finite field $\mathbb{F}_p$. Furthermore, define $a_p = p + 1 - N_p$. This way, we associated with the curve E a sequence (a_p) for primes p not dividing N_E. In what follows, we will be interested in the structure of this sequence. As a first step in our analysis, we will extend the sequence $p \to a_p$ to a sequence over all positive integers $n \to a_n$.

step 1. for primes p dividing N_E, we define a_p as one of $\{0, 1, -1\}$ according to the nodal singularity of p.

step 2. for all primes p, define $a_{p^n} = a_p a_{p^{n-1}} - p a_{p^{n-1}}$ when $p \nmid N_E$, and $a_{p^n} = a_p^n$ when $p \mid N_E$.

step 3. in general, define $a_{mn} = a_m a_n$ when $\gcd(m, n) = 1$.

Thus, given E, we can construct the sequence $(a_1, a_2, \dots)$. A natural question to ask is, how much information about E is lost in this mapping. That is, given $(a_n)_{n\geq 1}$, can one retrieve E? The following result answers this question.

Theorem 5. *Two curves E_1, E_2 generate the same sequence $(a_n)_{n\geq 1}$ iff there exists a morphism $\phi : E_1 \to E_2$ with finite kernel.*

Proof sketch. For the "$\Leftarrow$" direction, fix a morphism ϕ between E_1 and E_2. If ϕ has finite kernel, ϕ is, in general, neither injective nor surjective. To show they generate the same sequence $(a_p)_{p\geq 1}$, we must show that for all primes p, we have $\#E_1(\mathbb{F}_p) = \#E_2(\mathbb{F}_p)$. Then, the extended sequences will be the same.

Let l be a prime not dividing $\#\mathrm{Ker}(\phi)$, and consider the induced mapping $\phi : E_1[l](\overline{\mathbb{F}_p}) \to E_2[l](\overline{\mathbb{F}_p})$. It can be shown that the Frobenius map on the left is mapped to the Frobenius map on the right, and therefore, that $\#E_1(\mathbb{F}_p) = \#E_2(\mathbb{F}_p) \mod l$. Since this holds for all l not dividing $\#\mathrm{Ker}(\phi)$ (which is a finite number), the equality holds for infinitely many l, thus we must have $\#E_1(\mathbb{F}_p) = \#E_2(\mathbb{F}_p)$.

Note: if ϕ is a map $E_1 \to E_2$, then $\phi^\vee$ is a map $E_2 \to E_1$.

The "$\Leftarrow$" direction is much harder. Faltings in 1985 showed how to construct ϕ when two elliptic curves generate the same sequence $(a_p)_{p\geq 1}$. □

Note: In the PARI programming language, the function `anell` can be used to compute the first values of the a-sequence associated with a given elliptic curve.

We have seen how to associate to each elliptic curve E an a-sequence $(a_n)_{n\geq 1}$. We can use Theorem 5 above to list all curves with the same a-sequence. Thus, to solve problem A (listing all elliptic curves over the rationals), it is enough to classify which a-sequences can be obtained from such curves. To this end, we consider several ways of packing an a-sequence into a generating series.

Definition 6. *Given an elliptic curve E over $\mathbb{Q}$, let $(a_n)_{n\geq 1}$ be its associated a-sequence. The Taylor series of E is defined to be*

$$f_E(q) = \sum_{n=1}^{\infty} a_n \cdot q^n,$$

and the Dirichelet series of E is defined to be

$$L_E(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

We also define the shifted Taylor series of E to be

$$\widetilde{f}_E(\tau) = f_E(e^{2\pi i\tau}).$$

One can show that the Taylor series converges on the open unit disk, the shifted Taylor series converges on the open halfplane defined by $\mathrm{Im}(\tau) > 0$, and the Dirichelet series converges on the open half-plane defined by $\mathrm{Re}(s) > \frac{3}{2}$ (for the latter, we need to use bounds on a_p).

Consider the special linear group of 2×2 integer matrices with determinant equal to 1

$$SL_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \ : \ a, b, c, d \in \mathbb{Z} \text{ and } a \cdot d - b \cdot c = 1 \right\}.$$

This group acts on the set of complex numbers $H = \{z : \mathrm{Im}(z) > 0\}$ by

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \tau \to \frac{a \cdot \tau + b}{c \cdot \tau + d}.$$

Let us define

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \ : \ N \mid c \right\}$$

The following theorem was the last piece in the proof of Fermat's Last Theorem.

Theorem 6 (Wiles, 1994)**.** *Take an elliptic curve E over $\mathbb{Q}$, with conductor N_E. The Taylor generating series $\widetilde{f}_E(\tau)$ is a modular form of weight 2 on the group $\Gamma_0(N_E)$, satisfying*

(a) $\widetilde{f}_E\left(\frac{a\tau+b}{c\tau+d}\right) = (c\tau + d) f_E(\tau)$ for all $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N_E)$; and

(b) a certain behaviour at the boundary, which we omit.

Note that $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma_0(N_E)$, but the fact that $\widetilde{f}_E(\tau + 1) = \widetilde{f}_E(\tau)$ is not deep because of the periodicity of $\widetilde{f}_E$. However, also note that $\begin{pmatrix} 1 & 0 \\ N_E & 1 \end{pmatrix} \in \Gamma_0(N_E)$. The proof that $\widetilde{f}_E(\frac{\tau}{N_E\tau+1}) = (N_E\tau + 1)\widetilde{f}_E(\tau)$ is over 200 pages long.

The reason we have chosen to introduce modular forms is because problems A and B are hard when dealing with elliptic curves directly, but they become much easier in the world of modular forms.

10.3.1 On problem A

By Theorems 5 and 6, the problem of listing all elliptic curves over the rationals reduces to the problem of listing all a-sequences coming from modular forms of weight 2 on $\Gamma_0(N)$, for increasing conductor N.

Let M_N be the set of all modular forms of weight 2. Then,

(a) M_N is a vector space over $\mathbb{C}$;

(b) M_N is finite dimensional (from the analogue of the Riemann Hypothesis).

(c) M_N is equipped with a natural collection of operators, called Hecke operators, indexed by integers. Initially, they are defined only on primes, but they can be extended to all integers as in the case of a-sequences. We only give two equivalent definitions for the case when p does not divide N:

1 $T_p\widetilde{f} = (T_p(\widetilde{f}))(\tau) = pf(p\tau) + \frac{1}{p}\sum_{i=0}^{p-1} f\left(\frac{\tau+i}{p}\right)$; or

2 $T_p f = (T_p(f))(q) = \sum_{p|n} a_n q^{n/p} + p\sum a_n q^{pn}$.

It can be shown that T_p preserves the space of modular forms, and that the two definitions above are equivalent.

(d) M_N has a basis consisting of eigenvectors for all the operators T_N.

It turns out that $\widetilde{f}_E$, the Taylor series associated with the elliptic curve E is in fact an eigenvector for T_N (normalized, so that $a_1 = 1$). This allows us to give a linear algebra characterization of sequences (a_p). Thus, computing M_N is equivalent to computing its eigenvectors. Moreover, if $f = \sum a_n q^n$ is an eigenfunction in M_N, then $T_N(f) = a_N f$ (seen using definitions 1 or 2 of T_N). Therefore, it is enough to compute the eigenvalues of T_N.

Theorem 7. *There exists a vector space V_N of* modular symbols *such that*

(a) V_N can be described in an explicit combinatorial way and it is equipped with an action of linear operators T_n that are described by rational matrices; and

(b) there exists an isomorphism between V_N and M_N that respects Hecke operators.

The reason for introducing V_N is that it is hard to use restrictions on infinite series from M_N, while all treatment of V_N involves finite linear algebra operations, plus the isomorphism between these vector spaces preserves Hecke operators.

The list of all elliptic curves for conductors up to $N \leq 200$ was given by Antwerp in 1972. Today, there exist lists of all curves with conductor up to 130000.

This completes our treatment of problem A.

10.3.2 On problem B

We now turn to problem B, which is, to compute $E(\mathbb{Q})$. As we have seen before, this group is finitely generated by r independent points, where r is the rank of E over $\mathbb{Q}$. Thus, our task is, given E, to find r and a set of r generators.

The work of Birch and Swinnerton-Dyer in the 60s was based on the idea that the rank r of $E(\mathbb{Q})$ should be related to the behaviour of the quantities N_p (the cardinality of $E(\mathbb{F}_p)$) as $p \to \infty$. Numerical experiments led to the following conjecture.

Conjecture 2 (BSD). $\prod_{p<x} \frac{N_p}{p} \to C_E \cdot (\log x)^r$ *as* $x \to \infty$, *where* C_E *is a constant depending only on the curve* E.

An interpretation of this conjecture is that, as we fix E and vary p, the distribution of cardinalities N_p "knows about" the rank r of E over $\mathbb{Q}$.

We can rephrase this conjecture in terms of the L-function of E. Let N be the conductor of E and recall that $a_p = p + 1 - N_p$. We can write

$$L_E(s) = \prod_{p \nmid N} (1 - a_p p^{-s} + p^{1-2s})^{-1} \prod_{p \nmid N} (1 - a_p p^{-s})^{-1}$$

Note, L_E can be rewritten as the Dirichelet series seen before $\sum_{n \geq 1} a_n / n^s$. In fact, this equivalence provides the *definition* for a_n when n is not a prime.

Evaluating the series *formally* at $s = 1$ (note that it only converges for $\mathrm{Re}(s) > 3/2$), we get $L_E(1)\text{`} = \text{`} \prod_p \frac{p}{N_p}$, which is the quantity in the BSD Conjecture 2. The existence of an analytic continuation of $L_E(s)$ was a long-standing open problem, but the following Theorem follows from the work of Wiles.

Theorem 8 (Hecke). *If* f_E *is a modular form (and by Wiles's Theorem, it is), then* $L_E(s)$ *has an analytic continuation to all* $s \in \mathbb{C}$, *and it satisfies a functional equation of the form* $\Lambda_E(s) = \pm \Lambda_E(2 - s)$, *where* $\Lambda_E(s) = (2\pi)^{-s} N^{s/2} \Gamma(s) L_E(s)$.

In light of this Theorem, the modern reformulation of the BSD Conjecture 2 is

Conjecture 3 (BSD, modern reformulation). *The order of vanishing of* $L_E(s)$ *at* $s = 1$ *equals the rank* r *of the elliptic curve* E *over* $\mathbb{Q}$.

This is Conjecture is a Clay Institute Millenium Prize problem. The work of Gross-Zagier and Kolyvagin establishes that *if* the order of vanishing of $L_E(s)$ at $s = 1$ is at most 1, *then* Conjecture 3 is true, and there exists an efficient method for calculating $E(\mathbb{Q})$.

Another Conjecture about the rank of elliptic curves is

Conjecture 4. *The sequence* $\{r_E\}_E$, *where* r_E *is the rank of the curve* E *over* $\mathbb{Q}$, *is unbounded.*

Currently, we know of curves with rank up to 28.

10.4 The Fun Stuff

Last but not least, we touch upon the proof of the famous Theorem:

Theorem 9 (Fermat's Last Theorem). *The equation* $x^n + y^n = z^n$ *has no non-zero integer solutions when* $n > 2$.

As a basic observation, one can easily show that it is enough to prove the Theorem when n is a prime, henceforth called l. We assume that there exist a, b, c a nontrivial solution to the equation, so that $a^l + b^l = c^l$. Frey had the idea to associate with this solution the elliptic curve

$$E : Y^2 = X(X - a^l)(X + b^l).$$

It can be verified that the discriminant of this curve is $\Delta = 2^{12}(abc)^{2l}$, and that the equation defining the curve might have a double root, but never a triple root. As a consequence, we have that $N = \prod_{p|\Delta} p$, that is, the conductor of the elliptic curve above is square-free. We see that N is very small relative to Δ.

From this point on, the idea is to look at the group $E[l]$ of torsion points. The a-sequence associated to $E[l]$ is simply the a-sequence of the curve E, modulo l. That is, if $(a_n)_{n\geq 1}$ is the a-sequence of the curve E, then $(a_n \mod l)_{n\geq 1}$ is the a-sequence of the curve $E[l]$. Furthermore, the conductor of the curve $E[l]$, $N_{E[l]} = 2$.

Theorem 10 (Ribet)**.** *If the a-sequence attached to E is modular of level N, then the a-sequence attached to $E[l]$ corresponds to the reduction $(\mod l)$ of an a-sequence of an element g in the space of modular forms M_2 of level $N_{E[l]} = 2$ and weight 2.*

The punchline is that it is trivial to show that there are no modular forms of weight 2 and level 2, which in turn provides the contradiction to the assumption that a non-trivial solution exists to Fermat's equation.

Bibliography

[Ked01] K. S. Kedlaya. Counting points on hyperelliptic curves using Monsky-Washnitzer cohomology. *Journal of Ramanujan Math. Soc.*, 16:323–338, 2001.

[Sat00] T. Satoh. The canonical lift of an ordinary elliptic curve over a finite field and its point counting. *Journal of Ramanujan Math. Soc.*, 15:247–270, 2000.