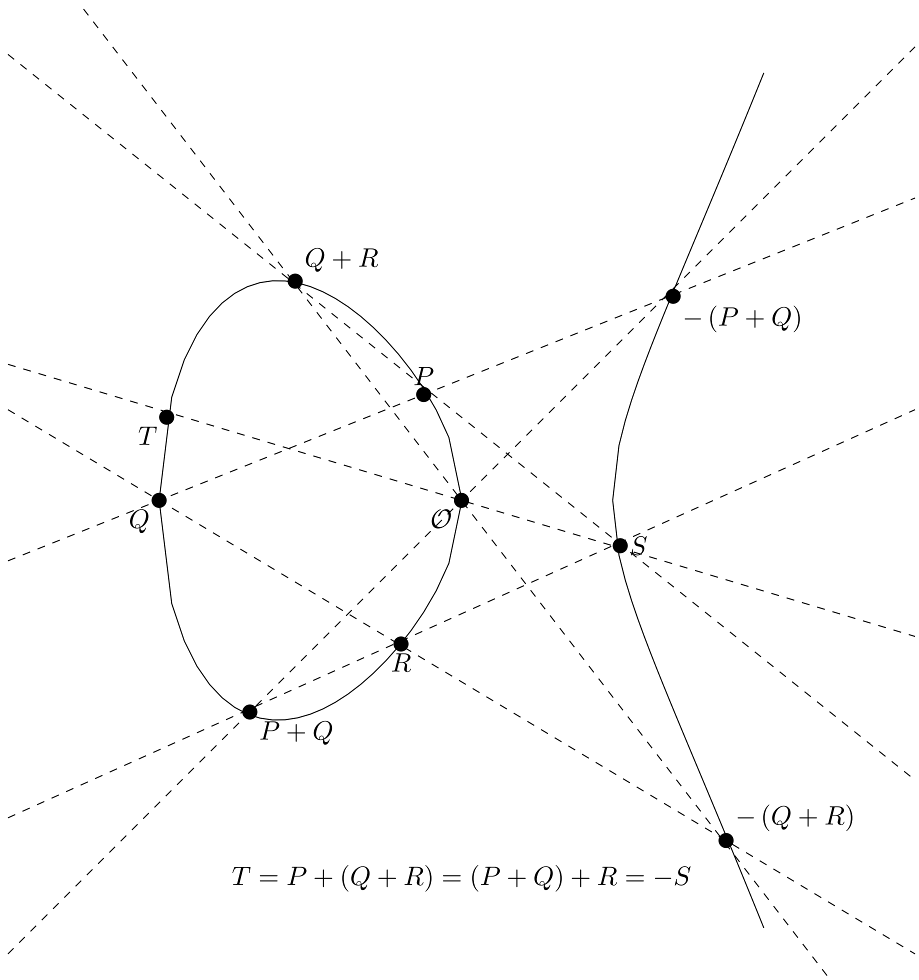
M4P32 Number Theory: Elliptic Curves

Lectured by Prof Toby Gee
Typed by David Kurniadi Angdinata

Autumn 2019



Syllabus

The p-adic numbers. Basic algebraic geometry. Plane conics. The Hasse principle. Plane cubics. The torsion subgroup of $E(\mathbb{Q})$. The torsion points in $E(\mathbb{Q}_p)$. The weak Mordell-Weil theorem for $E(\mathbb{Q})$. The full Mordell-Weil theorem for $E(\mathbb{Q})$. Counting points over $E(\mathbb{F}_p)$. Torsion subgroups and ranks of $E(\mathbb{Q})$.

Contents

1 Introduction

Lecture 1
Thursday
03/10/19

The following are books.

- J W S Cassels, Lectures on elliptic curves, 1991
- J H Silverman, The arithmetic of elliptic curves, 1986
- J H Silverman and J Tate, Rational points on elliptic curves, 1992

Note that there are a lot of books on elliptic curves out there, and a lot of them are not relevant to this course, so either different topics, or they will be too advanced. Also, about half of this course will not actually be on elliptic curves. We are going to start off by looking at conics, which are simpler but are a good place to start in order to build intuition and technique. As explained below, we will be essentially following Cassels, although there is quite a lot of material that we will not cover, and our treatment of a 2-descent, that is our method for computing the rank of an elliptic curve over $\mathbb{Q}$, will be different. The overall aim of this course is to learn more about solving polynomial equations in $\mathbb{Z}$ or $\mathbb{Q}$. For example,

$$x^2 + y^2 = 5, \qquad y^2 = x^3 - x, \qquad x^4 + y^4 = 17.$$

Let k be a field, such as $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, the field of p elements $\mathbb{F}_p$, or the p-adic numbers $\mathbb{Q}_p$, and let its polynomial ring be $k[x_0, \dots, x_n]$. A **monomial** is a term $x_0^{a_0} \dots x_n^{a_n}$, which has degree $a_0 + \dots + a_n$. The **degree** of a polynomial is the maximal degree of a monomial occuring in it.

Example. $x_1^5 + x_2 x_3 + x_{10} x_{11}^5$ has degree six.

Equations in one variable are easy to solve over $\mathbb{Q}$.

Example. Let $3x^5 - 9x^3 + x^2 + \frac{148}{81} = 0$, so $243x^5 - 729x^3 + 81x^2 + 148 = 0$. If $x = a/b$ with $(a, b) = 1$, we need $243a^5 - 729a^3b^2 + 81a^2b^3 + 148b^5 = 0$. Then $b \ne 0$, so $a \ne 0$, so $a^2 \mid 148$, so $a \mid 2$, so $a = \pm 1, \pm 2$. Similarly $b^2 \mid 243$, so $b \mid 9$, so $b = \pm 1, \pm 3, \pm 9$. Check each of these, and $x = \frac{2}{3}$.

More than two variables, over $\mathbb{Q}$, is hopeless, so let x and y be two variables.

- Degree one is very easy, since $ax + by + c = 0$ for $b \ne 0$ gives $y = -c/b - (a/b)x$.
- Degree two and three are in this course. Degree four can be reduced to degree three.

Theorem 1.1 (Mordell's conjecture and Falting's theorem)**.** *A general equation in two variables of degree greater than four has only finitely many solutions over $\mathbb{Q}$.*

General equations are non-singular, so $(x - y)\left(x^{100} + 10y + 1\right) = 0$ and $x^{73} - y^{109} = 0$ are not general.

Example 1.2. Let $x^2 + y^2 = c$ for $c \in \mathbb{Q}$.

- $x^2 + y^2 = -1$ has no solutions in $\mathbb{R}$.
- $x^2 + y^2 = 0$ has $(x, y) = (0, 0)$ in $\mathbb{R}$.
- $x^2 + y^2 = 1$ has infinitely many solutions $(x, y) = \left(\frac{3}{5}, \frac{4}{5}\right), \left(\frac{5}{13}, \frac{12}{13}\right), \dots$, since $(a/c)^2 + (b/c)^2 = 1$ gives $a^2 + b^2 = c^2$, which has infinitely many solutions $(3, 4, 5), (5, 12, 13), \dots$.
- $x^2 + y^2 = 3$ has no solutions in $\mathbb{Q}$, since $a^2 + b^2 = 3c^2$ has no solutions for $a, b, c \in \mathbb{Z}$ and $c \ne 0$. Suppose a, b, c is such a solution. Then $a^2 + b^2 \equiv 0 \mod 3$. But all squares are 0 or 1 modulo 3, so $a \equiv b \equiv 0 \mod 3$. Write $a = 3A$ and $b = 3B$ gives $3\left(A^2 + B^2\right) = c^2$, so $3 \mid c$. Write $c = 3C$ gives $A^2 + B^2 = 3C^2$, a contradiction, by induction on the biggest power of 3 dividing c. Next week $x^2 + y^2 = 3$ has no solutions in $\mathbb{Q}_3$.

Example 1.3. $x^2 + 2y^2 = 6$ has $(x, y) = (2, 1)$, which has line $y - 1 = m(x - 2)$, so

$$(2m(x - 2))^2 + x^2 - 6 = 0 \qquad \implies \qquad \left(2m^2 + 1\right)x^2 + \left(4m - 8m^2\right)x + 2(1 - 2m)^2 - 6 = 0.$$

The sum of the roots of $ax^2 + bx + c$ is $-b/a$. So the second root, other than $x = 2$ and $y = 1$, is

$$x = \frac{8m^2 - 4m}{2m^2 + 1} - 2 = \frac{4m^2 - 4m - 2}{2m^2 + 1}, \qquad y = \frac{-2m^2 - 4m + 1}{2m^2 + 1}.$$

Exercise 1.4. Do the case $xy = 0$.

2 The p-adic numbers

2.1 Norms

Lecture 2 Monday 07/10/19

Definition 2.1. A **norm** on a field k is a function $|\cdot| : k \to \mathbb{R}$ such that

1. $|x| \ge 0$ with equality if and only if $x = 0$,
2. $|xy| = |x| \cdot |y|$, and
3. $|x + y| \le |x| + |y|$.

2 implies that $|1| = |-1| = 1$. So $|x| = |-x|$.

Example. Usual absolute value on $\mathbb{R}$, that is

$$|x| = \begin{cases} x & x \ge 0 \\ -x & x < 0 \end{cases}.$$

Remark 2.2. Define

$$\begin{array}{rccc} d(\cdot,\cdot) & : & k^2 & \longrightarrow & \mathbb{R} \\ & & (x,y) & \longmapsto & |x-y| \end{array},$$

then d is a metric on k^2. Not every metric comes from a norm.

Definition 2.3. Let $k = \mathbb{Q}$. Then the **p-adic norm** is defined by

$$\begin{array}{rccc} |\cdot|_p & : & \mathbb{Q} & \longrightarrow & \mathbb{R} \\ & & x & \longmapsto & \begin{cases} 0 & x = 0 \\ p^{-n} & x = p^n \dfrac{a}{b}, \ n \in \mathbb{Z}, \ (p,a) = (p,b) = (a,b) = 1 \end{cases} \end{array}.$$

Lemma 2.4. *$|\cdot|_p$ is a norm, and in fact*

3*. $|x + y| \le \max(|x|, |y|)$.

Proof. Without loss of generality, $x, y \in \mathbb{Z}$. Also we may assume $x, y, x + y \ne 0$. Then 3* is equivalent to, if $p^n \mid x$ and $p^n \mid y$, then $p^n \mid (x + y)$. ☐

Definition 2.5. We say that 3* is the **ultrametric inequality**. If $|\cdot|$ satisfies 3*, we say that $|\cdot|$ is **non-archimedean**.

We have infinitely many norms on $\mathbb{Q}$, the one from $\mathbb{R}$, and the p-adic norm $|\cdot|_p$ for each prime p. Say that two norms $|\cdot|_1$ and $|\cdot|_2$ on k are **equivalent** if there exists $\alpha > 0$ such that $|\cdot|_1 = |\cdot|_2^\alpha$.

Exercise. Check two norms are equivalent if and only if the corresponding metrics give the same topology on k.

Theorem 2.6. *Any norm on $\mathbb{Q}$ is equivalent to exactly one of*

- *the archimedean norm coming from $\mathbb{R}$,*
- *a norm $|\cdot|_p$ for some uniquely determined p, or*
- *the discrete norm $|x| = 1$ if $x \ne 0$.*

Lemma 2.7. *If $|\cdot|$ is non-archimedean and $|x| \ne |y|$, then $|x + y| = \max(|x|, |y|)$.*

Proof. Without loss of generality $|x| > |y|$. Write $x = (x + y) + (-y)$, so that 3* gives us

$$|x| \le \max(|x + y|, |-y|) \le \max(|x|, |y|, |-y|) = |x|.$$

So $|x| = \max(|x + y|, |y|)$. But $|x| > |-y| = |y|$, so $|x| = |x + y|$. ☐

Exercise 2.8. Check Lemma 2.7 for $|\cdot|_p$ using the definition.

2.2 Completion

Recall that

- a sequence (x_n) in k is **Cauchy** if for all $\epsilon > 0$ there exists N such that $m, n \geq N$ implies that $|x_m - x_n| < \epsilon$, and
- a sequence (x_n) **converges** to $x \in k$ if for all $\epsilon > 0$ there exists M such that $n \geq M$ implies that $|x_n - x| < \epsilon$.

(x_n) converges implies that (x_n) is Cauchy, but in general (x_n) is Cauchy does not imply that (x_n) converges.

Example.

- $\mathbb{R}$ is complete.
- $\mathbb{Q}$ is not complete with respect to the usual archimedean norm. For example, $3, 3.1, \dots \to \pi \notin \mathbb{Q}$.

Example 2.9. Let $p = 2$. Then $(x_n) = 3, 33, \dots$ is Cauchy with respect to $|\cdot|_2$, and $x_n = \frac{10^n - 1}{3} \to -\frac{1}{3}$ as $n \to \infty$ because $\left|x_n + \frac{1}{3}\right|_2 = |10^n/3|_2 = |2^n (5^n/3)|_2 = 2^{-n} \to 0$.

Example 2.10. Let $x_n = 5^{2^n}$. If $p = 5$, then $x_n \to 0$, since $\left|5^{2^n}\right|_5 = 5^{-2^n} \to 0$ as $n \to \infty$. If $p = 2$, then $x_n \to 1$ as $n \to \infty$, since $(1 + y)^2 = 1 + 2y + y^2$. [1]

Example. A Cauchy sequence in $\mathbb{Q}$ for $|\cdot|_3$ which does not converge. Take a sequence converging to $\sqrt{7}$. That is, take (x_n) such that $x_n^2 - 7 \to 0$, that is $\left|x_n^2 - 7\right|_3 \to 0$ as $n \to \infty$. For example, take $x_n \in \mathbb{Z}$, chosen such that $x_n^2 \equiv 7 \mod 3^n$. For example,

$$x_1 = 1, \qquad x_2 = 4, \qquad x_3 = 13, \qquad \dots.$$

Exercise 2.11. If $p > 2$ and $t \in \mathbb{Z}$ is not a square but is a quadratic residue modulo p, that is there exists y such that $y^2 \equiv t \mod p$, then there exists a Cauchy sequence (x_n) in $\mathbb{Q}$ with $x_n^2 \to t$ as $n \to \infty$, such as $t = 1 - p$. If $p = 2$, then $t = -7$ works.

Lecture 3 Tuesday 08/10/19

$\mathbb{Q}$ is not complete with respect to any $|\cdot|_p$. Let k be a field and $|\cdot|$ be non-archimedean. Let

$$R = \{\text{Cauchy sequences in } k\},$$

where $(x_n) + (y_n) = (x_n + y_n)$ and $(x_n)(y_n) = (x_n y_n)$. Let

$$I = \{(x_n) \mid x_n \to 0 \text{ as } n \to \infty\}.$$

Exercise. Check that I is an ideal in R. If $(x_n) \notin I$, then there exists N such that $n \geq N$ implies that $x_n \neq 0$. Show that furthermore the sequence (y_n) defined by

$$y_n = \begin{cases} 0 & n < N \\ \dfrac{1}{x_n} & n \geq N \end{cases}$$

is Cauchy, and $x_n y_n = 1$ for all $n \geq N$, so $(x_n)(y_n) - 1 \in I$.

That is, I is a maximal ideal of R, so $\widehat{k} = R/I$ is a field. There is a natural map

$$\begin{array}{ccc} k & \longrightarrow & \widehat{k} \\ x & \longmapsto & (x)_{n \geq 1} \end{array}.$$

This is an injection. Call $\widehat{k}$ the **completion** of k. The norm $|\cdot|$ extends to $\widehat{k}$ by defining

$$|(x_n)| = \lim_{n \to \infty} |x_n|.$$

Exercise. Check that this is defined, and is a norm. Check that if $x_n \not\to 0$, then $|x_n|$ is eventually constant, by using Lemma 2.7.

[1] Exercise

Lemma 2.12. *k is dense in $\widehat{k}$.*

Proof. Need to show that if $x \in \widehat{k}$ and $\epsilon > 0$, then there exists $y \in k$ such that $|x - y| < \epsilon$. Write $x = (x_n)$ for $x_n \in k$, and choose N such that if $m, n \geq N$, then $|x_m - x_n| < \epsilon$. Then take $y = (x_N)_{n \geq 1}$. Then $|x - y| = \lim_{n \to \infty} |x_n - x_N| < \epsilon$. ☐

Lemma 2.13. *$\widehat{k}$ is complete.*

Proof. Let (x_n) be a Cauchy sequence in $\widehat{k}$, so x_n is itself an equivalence class of Cauchy sequences in k. By Lemma 2.12, for each $n \geq 1$ there exists $y_n \in k$ such that $|x_n - y_n| < 1/n$. Claim that $y = (y_n)$ is a Cauchy sequence, and $x_n \to y$ as $n \to \infty$. Since

$$|y_m - y_n| \leq |y_m - x_m| + |x_m - x_n| + |x_n - y_n| < \frac{1}{m} + \frac{1}{n} + |x_m - x_n|,$$

and (x_n) is Cauchy, so (y_n) is Cauchy. Then

$$|x_n - y| \leq |x_n - y_n| + |y_n - y| < \frac{1}{n} + |y_n - y|.$$

Need to check that $|y_n - y| \to 0$ as $n \to \infty$, which is what we did in the proof of Lemma 2.12. ☐

Definition 2.14. Let $k = \mathbb{Q}$ and $|\cdot| = |\cdot|_p$. Write the field of ***p*-adic numbers** $\mathbb{Q}_p$ for $\widehat{k}$, the completion of $\mathbb{Q}$ with respect to $|\cdot|_p$, and the ring of ***p*-adic integers**

$$\mathbb{Z}_p = \left\{ x \in \mathbb{Q}_p \;\middle|\; |x|_p \leq 1 \right\} \subset \mathbb{Q}_p.$$

By construction or definition, $\mathbb{Q} \subset \mathbb{Q}_p$, and $\mathbb{Z} \subset \mathbb{Z}_p$.

Exercise 2.15. Show that $\mathbb{Z}_p$ is a subring of $\mathbb{Q}_p$. More generally, if k is any non-archimedean field, then

$$\{x \in k \mid |x| \leq 1\}$$

is a subring of k.

Note. $1/p \notin \mathbb{Z}_p$, since $|1/p|_p = p > 1$. In fact $\mathbb{Q}_p = \mathbb{Z}_p[1/p]$, the field of fractions of $\mathbb{Z}_p$.

2.3 Expansion

Definition 2.16. If k is any field with a norm $|\cdot|$, then we write

$$\sum_{n=1}^{\infty} a_n = \lim_{m \to \infty} \sum_{n=1}^{m} a_n,$$

if this limit exists.

Lemma 2.17. *If k is non-archimedean, and $t_1, \dots, t_n \in k$, then*

$$\left| \sum_{i=1}^{n} t_i \right| \leq \max_{1 \leq i \leq n} t_i.$$

In particular if $|t_i| \leq R$ for all i, then $|\sum_{i=1}^{n} t_i| \leq R$.

Proof. Induction on n, where $n = 2$ is 3^*. ☐

Corollary 2.18. *A sequence (t_n) is Cauchy if and only if $|t_n - t_{n+1}| \to 0$ as $n \to \infty$.*

Proof. If $m > n$, then $t_m - t_n = (t_m - t_{m-1}) + \dots + (t_{n+1} - t_n)$, and use Lemma 2.17. ☐

Lemma 2.19. *If k is complete non-archimedean, such as $k = \mathbb{Q}_p$, then $\sum_{n=1}^{\infty} x_n$ converges if and only if $x_n \to 0$ as $n \to \infty$. If $|x_n| \leq R$ and $x_n \to 0$ then $|\sum_{n=1}^{\infty} x_n| \leq R$.*

Proof. Since k is complete, $\sum_{n=1}^{\infty} x_n$ converges if and only if $(\sum_{n=1}^{m} x_n)_{m \geq 1}$ converges, if and only if $(\sum_{n=1}^{m} x_n)_{m \geq 1}$ is Cauchy, if and only if $x_{m+1} \to 0$, by Corollary 2.18. The final statement then follows from Lemma 2.17. ☐

Lemma 2.20. *If $a_n \in \mathbb{Z}$ then $\sum_{n=0}^{\infty} a_n p^n$ converges in $\mathbb{Q}_p$. If $a_n = 0$ for $n < T$ and $a_T \neq 0$, and $p \nmid a_T$, then*

$$\left| \sum_{n=0}^{\infty} a_n p^n \right|_p = p^{-T}.$$

Proof. Since $a_n \in \mathbb{Z}$, $|a_n p^n|_p = |a_n|_p \cdot |p^n|_p \leq |p^n|_p = p^{-n} \to 0$. Furthermore $\left|a_T p^T\right|_p = p^{-T}$ and $|a_n p^n|_p \leq p^{-T-1}$ if $n \geq T+1$, so

$$\left| \sum_{n=T+1}^{\infty} a_n p^n \right|_p \leq p^{-T-1},$$

so $\left|a_T p^T + \sum_{n=T+1}^{\infty} a_n p^n\right|_p = p^{-T}$, by Lemma 2.7. $\square$

Lecture 4 Thursday 10/10/19

Proposition 2.21.

1. *If $a_n \in \{0, \dots, p-1\}$, then $\sum_n a_n p^n$ converges to an element of $\mathbb{Z}_p$. Furthermore if*

$$\sum_n a_n p^n = \sum_n b_n p^n, \qquad b_n \in \{0, \dots, p-1\},$$

then $a_n = b_n$ for all n.

2. *If $\alpha \in \mathbb{Z}_p$ then there exists (a_n) as in 1 such that $\alpha = \sum_n a_n p^n$.*

Proof.

1. Lemma 2.20 gives convergence. Suppose that T is minimal such that $a_T \neq b_T$, then by Lemma 2.20, $|\sum_n (a_n - b_n) p^n|_p = p^{-T}$. In particular $\sum_n (a_n - b_n) p^n \neq 0$.

2. By construction, $\mathbb{Q}$ is dense in $\mathbb{Q}_p$. So there exists $\beta \in \mathbb{Q}$ such that $|\alpha - \beta|_p < 1$. Since $|\alpha|_p \leq 1$, we have $|\beta|_p \leq 1$, so if $\beta = r/s$ with $(r, s) = 1$, then $p \nmid s$. So there exists $\gamma \in \mathbb{Z}$ with $|\gamma - \beta|_p < 1$, if and only if $s\gamma - r \equiv 0 \mod p$, which has solutions because $(s, p) = 1$. There exists $a_0 \in \{0, \dots, p-1\}$ such that $|\gamma - a_0|_p < 1$, so

$$|\alpha - a_0|_p \leq \max\left(|\alpha - \beta|_p, |\beta - \gamma|_p, |\gamma - a_0|_p\right) < 1.$$

Then $|(\alpha - a_0)/p|_p \leq 1$, that is $(\alpha - a_0)/p \in \mathbb{Z}_p$. Repeating the argument, there exists $a_1 \in \{0, \dots, p-1\}$ such that $|(\alpha - a_0)/p - a_1|_p < 1$, that is $(\alpha - a_0 - a_1 p)/p^2 \in \mathbb{Z}_p$. By induction, we find $a_0, a_1, \dots$ such that $|\alpha - (a_0 + \dots + a_n p^n)|_p \leq p^{-(n+1)}$. So $\alpha = \sum_{n=0}^{\infty} a_n p^n$.

$\square$

Corollary 2.22. *Any element α of $\mathbb{Q}_p$ can be uniquely written as*

$$\alpha = \sum_{n \geq -T} a_n p^n, \qquad a_{-T} \neq 0, \qquad a_n \in \{0, \dots, p-1\}.$$

Proof. If $|\alpha|_p = p^T$, then $\left|p^T \alpha\right|_p = 1$, so $p^T \alpha \in \mathbb{Z}_p$, and the claim follows from Proposition 2.21.2 applied to $p^T \alpha$. $\square$

Corollary 2.23. *$\mathbb{Z}$ is dense in $\mathbb{Z}_p$.*

Proof. If $\alpha \in \mathbb{Z}_p$, write $\alpha = \sum_n a_n p^n$. Then $|\alpha - (a_0 + \dots + a_m p^m)|_p \leq p^{-(m+1)}$, and $a_0 + \dots + a_m p^m \in \mathbb{Z}$. $\square$

For all $m \geq 1$, there is a surjective ring homomorphism

$$\begin{array}{ccc} \mathbb{Z}_p & \longrightarrow & \mathbb{Z}/p^m\mathbb{Z} \\ \sum_{n=0}^{\infty} a_n p^n & \longmapsto & \sum_{n=0}^{m-1} a_n p^n \end{array}.$$

In fact

$$\mathbb{Z}_p / p^m \mathbb{Z}_p = \mathbb{Z}/p^m\mathbb{Z}, \qquad \mathbb{Z}_p = \varprojlim_m \mathbb{Z}/p^m\mathbb{Z}.$$

Lemma 2.24.
$$\mathbb{Z}_p^\times = \left\{ x \in \mathbb{Z}_p \;\middle|\; |x|_p = 1 \right\}.$$

Proof. If $|x|_p = 1$ then $x \neq 0$, and so $x^{-1} \in \mathbb{Q}_p$, and $\left|x^{-1}\right|_p = 1/|x|_p = 1$, so $x^{-1} \in \mathbb{Z}_p$. Conversely if $x \in \mathbb{Z}_p^\times$ then there exists $y \in \mathbb{Z}_p$ such that $xy = 1$, so $|x|_p |y|_p = 1$. But $|x|_p, |y|_p \leq 1$, so $|x|_p = |y|_p = 1$. □

Now $\langle p \rangle \subset \mathbb{Z}_p$ is a maximal ideal, because $\mathbb{Z}_p / \langle p \rangle = \mathbb{Z}/p\mathbb{Z}$ is a field. Since $\mathbb{Z}_p^\times = \mathbb{Z}_p \setminus \langle p \rangle$ by Lemma 2.24, $\langle p \rangle$ is the unique maximal ideal of $\mathbb{Z}_p$, that is $\mathbb{Z}_p$ is a local ring. In fact it is a discrete valuation ring.

Notation. A unit of $\mathbb{Q}_p$ is a unit in $\mathbb{Z}_p$, that is an element of $|\cdot|_p = 1$.

Corollary 2.25. *Every element of $\mathbb{Q}_p$ other than zero is uniquely of the form $p^n u$ for $n \in \mathbb{Z}$ and u is a unit.*

Proof. If $\alpha \in \mathbb{Q}_p$ and $\alpha \neq 0$, write $|\alpha|_p = p^{-n}$ for $n \in \mathbb{Z}$, and set $u = \alpha p^{-n}$. □

2.4 Hensel's lemma

Hensel's lemma is Newton-Raphson in $\mathbb{Q}_p$. A reminder that if k is any field, and $f(X) \in k[X]$, then we can define $f'(X), f''(X), \dots$ formally by
$$\frac{\mathrm{d}}{\mathrm{d}x}(X^n) = nX^{n-1}.$$

Theorem 2.26 (Hensel's lemma)**.** *Let k be a non-archimedean field with norm $|\cdot|$ and $R = \{x \in k \mid |x| \leq 1\}$. For example, $k = \mathbb{Q}_p$, $|\cdot| = |\cdot|_p$, and $R = \mathbb{Z}_p$. Suppose $f \in R[X]$, and $t_0 \in R$ such that $|f(t_0)| < |f'(t_0)|^2$. Then there exists a unique $t \in R$ such that*
$$f(t) = 0, \qquad |t - t_0| < |f'(t_0)|.$$
Furthermore
$$|f'(t)| = |f'(t_0)|, \qquad |t - t_0| = \frac{|f(t_0)|}{|f'(t_0)|}.$$

Proof. Construct a Cauchy sequence $t_0, t_1, \dots$ by
$$t_{n+1} = t_n - \frac{f(t_n)}{f'(t_n)}.$$
It turns out that $|f'(t_n)| = |f'(t_0)|$, so
$$\left|\frac{f(t_n)}{f'(t_0)}\right| = \left|\frac{f(t_n)}{f'(t_n)}\right| = |t_{n+1} - t_n| \to 0,$$
that is $f(t_n) \to 0$, that is $f(t) = 0$. □

Lemma 2.27. *If $f(X) \in R[X]$ has a simple root $X = t \in R$, then for any $t_0 \in k$ with $|t - t_0| < |f'(t)|$, we have*
$$|f'(t)| = |f'(t_0)|, \qquad |f(t_0)| < |f'(t_0)|^2.$$

Proof. The polynomial $f'(t) - f'(t_0)$ is divisible by $t - t_0$, so $|f'(t) - f'(t_0)| \leq |t - t_0| < |f'(t)|$, and so $|f'(t)| = |f'(t_0)|$. Also using the Taylor expansion around t, $f(t_0) = (t_0 - t) f'(t) + (t_0 - t)^2 x$ for some $x \in R$, and by assumption both of these terms have norm less than $|f'(t)|^2 = |f'(t_0)|^2$. □

Exercise 2.28. The equation $X^2 = 7$ has a solution in $\mathbb{Z}_3$. Take $f(X) = X^2 - 7$. Then $f'(X) = 2X$. So $|f'(X)|_3 = |X|_3$. So we need to find t_0 such that $\left|t_0^2 - 7\right|_3 < |t_0|_3^2$. For example, choose $t_0 \in \mathbb{Z}$ such that $3 \nmid t_0$ and $t_0^2 \equiv 7 \mod 3$, for example $t_0 = 1$. Hensel's lemma implies that there exists a unique $t \in \mathbb{Z}_3$ such that $t^2 = 7$ and $|t - 1|_3 < 1$, that is $t \equiv 1 \mod 3$. In the same way, show that there exists a unique $s \in \mathbb{Z}_3$ such that $s^2 = 7$ and $s \equiv 2 \mod 3$. In fact $s = -t$, since $(-t)^2 = t^2$ and $X^2 - 7 = (X - t)(X + t)$.

Corollary 2.29. *Let $u \in \mathbb{Z}_p^\times$. If $p > 2$, then u is a square if and only if it is a square modulo p. If $p = 2$, then u is a square if and only if it is a square modulo 8, if and only if $u \equiv 1 \mod 8$.*

Proof. Exercise, using Hensel's lemma. [2] □

[2] Exercise

3 Basic algebraic geometry

Lecture 5 Monday 14/10/19

An affine **algebraic curve** over k is an equation

$$f(x, y) = 0, \qquad 0 \neq f \in k[x, y].$$

The **degree** $n = \deg f \in \mathbb{N}_{>0}$ of this curve is the total degree, so if $f(x, y) = \sum_{i,j=0}^{n} a_{ij} x^i y^j$, then

$$\deg f = \max \{i + j \mid a_{ij} \neq 0\}.$$

Algebraic curves of degree one are **lines**. Algebraic curves of degree two are **conics**. Two curves $x = 0$ and $y = f(x)$ for $f(x) \in k[x]$ have intersection points the zeroes of $f(x)$, and a non-zero polynomial of degree n has n roots, but $f(x) = x^2 + 1$ has no real zeroes, so need to work over $\mathbb{C}$ or some algebraically closed field.

Definition 3.1. A field k is **algebraically closed** if any non-zero polynomial $f(x) \in k[x]$ has a zero in k.

By induction on the degree,

$$f(x) = a_n \prod_{j=1}^{n} (x - \alpha_j), \qquad a_n, \alpha_j \in k.$$

Bézout's theorem states that two algebraic curves of degree d_1 and d_2 respectively have $d_1 d_2$ common points.

- We need to assume that k is algebraically closed. For example, the **fundamental theorem of algebra**, by Gauss, states that $\mathbb{C}$ is algebraically closed.
- We need to count multiplicities. There is a definition given for multiplicity. For example, if $\underline{0} = (0, 0)$ is the intersection point of two curves $f(x, y) = 0$ and $g(x, y) = 0$ for $f, g \in \mathbb{C}[x, y]$, so $f(\underline{0}) = g(\underline{0}) = 0$, then the **multiplicity** at $\underline{0}$ is
$$\dim_{\mathbb{C}} \mathbb{C}[[x, y]] / \langle f, g \rangle < \infty.$$
- We need to enlarge the plane to contain points at infinity. For example, the **real projective plane**
$$\mathbb{P}^2(\mathbb{R}) = \mathbb{R}^2 \cup \{\text{points at infinity}\}$$
is the equivalence classes of affine lines through $\mathbb{R}^2$ modulo parallelism, where if $l_1, l_2 \in \mathbb{R}^2$, then l_1 is parallel to l_2 if and only if $l_1 \cap l_2 = \emptyset$ or $l_1 = l_2$, which is an equivalence relation. There is an injection from points in $\{y = 1\}$ to affine lines through $\underline{0}$, and for any class of parallel affine lines on $\{y = 1\}$ there exists a unique line going through $\underline{0}$ and parallel to these lines, so
$$\mathbb{P}^2(\mathbb{R}) = \{\text{lines from } \{y = 1\}\} \cup \{\text{lines parallel to } \{y = 1\}\}.$$
This collection of subsets are called **projective lines**, which are two-dimensional subspaces in $\mathbb{R}^3$, and points are one-dimensional subspaces in $\mathbb{R}^3$. The set of points at infinity is a projective line, and any affine line $l \subset \mathbb{R}^2$ gives a projective line $l^\# = l \cup \{\text{parallelism class}\}$. Thus any two different projective lines intersect in exactly one point, and this definition makes sense for any field.

3.1 Projective space

The following is an equivalent description of $\mathbb{P}^2(k)$. Let k be any field. Then

$$\mathbb{P}^2(k) = k^3 \setminus \{\underline{0}\} / \sim$$

is the equivalence classes (x_0, x_1, x_2) such that $x_i \in k$ are not all zero modulo $\sim$, where

$$\underline{x} \sim \underline{y} \qquad \iff \qquad \underline{x} = \lambda \cdot \underline{y}, \qquad \lambda \in k \setminus \{\underline{0}\} = k^\times.$$

Definition 3.2. The **projective n-space** is

$$\mathbb{P}^n(k) = k^{n+1} \setminus \{\underline{0}\} / \sim.$$

Notation 3.3. The **homogeneous coordinates** $[x_0 : \dots : x_n]$ is an equivalence class of non-zero vectors in k^{n+1} modulo $\sim$, so

$$\mathbb{P}^n(k) = \{[x_0 : \dots : x_n] \mid x_i \in k \text{ not all zero}\}.$$

Definition 3.4. The **affine n-space** is
$$\mathbb{A}^n(k) = k^n.$$

Lemma 3.5. *Let*
$$\begin{array}{cccc} \phi_i & : & \mathbb{A}^n(k) & \longrightarrow & \mathbb{P}^n(k) \\ & & (x_0, \dots, x_{n-1}) & \longmapsto & [x_0 : \dots : x_{i-1} : 1 : x_{i+1} : \dots : x_{n-1}] \end{array}.$$
Then ϕ_i is injective, and
$$\mathbb{P}^n(k) = \bigcup_{i=0}^n \operatorname{im} \phi_i.$$

Proof. Obvious. □

Exercise 3.6. There is an isomorphism
$$\begin{array}{ccc} \mathbb{P}^{n-1}(k) & \longrightarrow & \mathbb{P}^n(k) \setminus \phi_n(\mathbb{A}^n(k)) \\ [x_0 : \dots : x_{n-1}] & \longmapsto & [x_0 : \dots : x_{n-1} : 0] \end{array}.$$

Definition 3.7. The **points at infinity** of $\mathbb{P}^n(k)$ are the ones not in $\phi_n(\mathbb{A}^n(k))$. They are recognisable as the graph of $X_n = 0$.

3.2 Homogenisation

Lecture 6 Tuesday 15/10/19

Let $\lambda : k^{n+1} \to k$ be a non-trivial linear function. The image of
$$\ker \lambda = \left\{\alpha_0 x_0 + \dots + \alpha_n x_n = 0 \;\middle|\; (x_0, \dots, x_n) \in k^{n+1}, \text{ not all } \alpha_i \in k \text{ are zero}\right\} \subset \mathbb{P}^n(k)$$
with respect to the quotient map $k^{n+1} \setminus \{\underline{0}\} \twoheadrightarrow \mathbb{P}^n(k)$ is a **linear hyperplane**. This can be generalised by taking homogeneous polynomials in general.

Definition 3.8. A polynomial $F(X_0, \dots, X_n) \in k[X_0, \dots, X_n]$ is **homogeneous** of degree $d \in \mathbb{N}$ if
$$F(X_0, \dots, X_n) = \sum_{i_0 + \dots + i_n = d} \alpha_{i_0 \dots i_n} X_0^{i_0} \dots X_n^{i_n},$$
so you only have degree d terms.

- If f is a degree d polynomial in $k[x_1, \dots, x_n]$, then here is how to **homogenise** it. Change x_i to X_i and then introduce a new variable X_0 and multiply each term with a suitable power of X_0 such that the resulting polynomial is homogeneous of the smallest possible degree.
- If F is a degree d homogeneous polynomial in $k[X_0, \dots, X_n]$, then here is how to **dehomogenise** it. Choose i with $0 \le i \le n$, set $X_i = 1$ and change all the other X_j to x_j. If we chose $i = 0$ then this recovers the initial equation.

If $f \in k[x_1, \dots, x_n]$ then the **points at infinity** of $f = 0$ are the zeroes of F, the homogenisation of f, which are in $\mathbb{P}^n(k)$ but not in $\mathbb{A}^n(k)$.

If $F \in k[X_0, \dots, X_n]$ is homogeneous of degree d, then
$$\mathrm{Z}(F) = \{[x_0 : \dots : x_n] \in \mathbb{P}^n(k) \mid F(x_0, \dots, x_n) = 0\}$$
does not depend on the representative. Homogenisation allows us to extend an algebraic subset in $\mathbb{A}^n(k)$ to $\mathbb{P}^n(k)$.

Example.

- $X^2 + YZ + Z^2 = 0$ is homogeneous of degree two and gives rise to a conic in $\mathbb{P}^2(k)$.
- $x^2 + x^3 = y^2$ and $xy = 1$ homogenises to $X^2 Z + X^3 = Y^2 Z$ and $XY = Z^2$.
- $X^2 + Y^2 = Z^2$ and $YZ = X^2$ dehomogenises to $x^2 + y^2 = 1$ and $y = x^2$.

3.3 Bézout's theorem

Theorem 3.9 (Bézout's theorem). *If $F, G \in k[X_0, X_1, X_2]$ be homogeneous non-zero polynomials of degree m and n respectively without common factors, so $\gcd(f,g) = 1$ up to associates, then*

$$|\{F = 0\} \cap \{G = 0\}| = m \cdot n,$$

counted with multiplicities, where $m \cdot n$ is always a positive integer.

Let $\overline{k}$ be the **algebraic closure** of k, the smallest algebraically closed field containing k.

Example.

- $\overline{\mathbb{Q}}$ is a subfield of $\mathbb{C}$.
- If k is algebraically closed, then $k = \overline{k}$, so $\overline{\mathbb{C}} = \mathbb{C}$, and $\overline{\mathbb{R}} = \mathbb{C}$.
- If K is a field and $\mathcal{C}$ is a collection of subfields $k \in \mathcal{C}$ such that k are algebraically closed, then $\bigcap_{k \in \mathcal{C}} k \subseteq K$ is an algebraically closed subfield.

Corollary 3.10. *If F and G are two homogeneous polynomials of degree a and b in $k[X, Y, Z]$, for k any field not necessarily algebraically closed, then either the graphs of $F = 0$ and $G = 0$ in $\mathbb{P}^2(k)$ have at most ab points in common, or F and G have a common factor.*

Proof. Immediate from Bézout applied to $\overline{k}$. ☐

3.4 Singularities

Definition 3.11. Let k be a field of $\operatorname{ch} k \nmid d$, and let $f \in k[x_1, \dots, x_n]$ be a polynomial of degree $d > 0$. Let $P \in \mathbb{A}^n(k)$ be a point on $f = 0$, that is $f(P) = 0$. Then we say that P is a **smooth point** or **non-singular point** if one of the partial derivatives of f does not vanish at P, that is if there exists some i with $1 \le i \le n$ such that $\frac{\partial f}{\partial x_i}(P) = 0$. Note that the definition of a partial derivative is formal, not a limiting process. We say that P is a **singular point** if all the partial derivatives vanish at P.

Definition 3.12. Let k be a field of $\operatorname{ch} k \nmid d > 0$, and let $F \in k[X_0, \dots, X_n]$ be a homogeneous polynomial of degree d. Let $P \in \mathbb{P}^n(k)$. Then P is a **singular point** of $F = 0$ if any of the following conditions is true.

- $\frac{\partial F}{\partial X_i}(P) = 0$ for $i = 0, \dots, n$.
- $F(P) = 0$ and $\frac{\partial F}{\partial X_i}(P) = 0$ for $i = 0, \dots, n$.
- For some of $\phi_i : \mathbb{A}^n(k) \to \mathbb{P}^n(k)$ such that $P = \phi_i(p)$ for some $p \in \mathbb{A}^n(k)$, if f is a dehomogenisation of F then $f(p) = 0$ and $\frac{\partial f}{\partial x_i}(p) = 0$ for all i.

Definition 3.13. If k is as above, then $f = 0$ or $F = 0$ is **non-singular** in $\mathbb{A}^n(k)$ or $\mathbb{P}^n(k)$ if it has no singular points over $\overline{k}$.

Example. $x^3 = y^2$ is a singular curve.

Lecture 7 Thursday 17/10/19

Lecture 7 is a problems class.

Lecture 8 Monday 21/10/19

We need to compute the multiplicity up to some precision. Let $f \in k[x, y]$, and let $P \in \mathbb{A}^2(k)$ such that $f(P) = 0$. If $P = (a_1, a_2)$ is non-singular, the **tangent line** of $f = 0$ at P is

$$\frac{\partial f}{\partial x}(P)(x - a_1) + \frac{\partial f}{\partial y}(P)(y - a_2) = 0.$$

This is a non-zero equation, by definition, so not both $\frac{\partial f}{\partial x}(P)$ and $\frac{\partial f}{\partial y}(P)$ is zero. Let $f, g \in k[x, y]$ be non-zero polynomials as above, where $f(P) = g(P) = 0$. We say that $f = 0$ and $g = 0$ **intersect transversely** at P if the tangent lines of $f = 0$ and $g = 0$ at P are different.

Theorem 3.14. *If $f(P) = g(P) = 0$ then the multiplicity at P is one if and only if the intersection is transversal at P.*

4 Plane conics

Let $X^2 + Y^2 = Z^2$. If $(a, b, c) \in \mathbb{Z}^3$ is a solution, then $(\lambda a, \lambda b, \lambda c)$ is a solution for $\lambda \in \mathbb{Z}$. A **primitive solution** has $\gcd(a, b, c) = \pm 1$. Any solution can be written as a rescaling of a primitive solution by an integer.

Algorithm 4.1 (To find out if a plane conic is singular)**.** *Say $f \in k[x, y]$ is degree two. Then $\frac{\partial f}{\partial x}$ and $\frac{\partial f}{\partial y}$ are both linear so will meet in at least one point, possibly at infinity. Just check whether this point is on $f = 0$.*

By diagonalisation of quadratic forms, if $\operatorname{ch} k \neq 2$, then for $F \in k[X_0, X_1, X_2]$ of degree two homogeneous, after rescaling by a non-zero scalar, and a permutation of variables, we can assume that

$$F(X_0, X_1, X_2) = \alpha_0 X_0^2 + \alpha_1 X_1^2 + \alpha_2 X_2^2.$$

Theorem 4.2. *The following are equivalent.*

1. *$F = 0$ is singular.*
2. *$\alpha_0 \cdot \alpha_1 \cdot \alpha_2 = 0$.*
3. *F is the product of two linear polynomials over the algebraic closure.*

Proof. $F = 0$ is non-singular if and only if the equations $2\alpha_i X_i = \frac{\partial F}{\partial X_i} = 0$ for all i has no non-zero simultaneous zeroes in k^{n+1}, if and only if not all α_i are zero, so 1 and 2 are equivalent. Let us assume 2. After permuting variables

$$F = \alpha_0 X_0^2 + \alpha_1 X_1^2 = \left(\sqrt{\alpha_0} X_0 + i\sqrt{\alpha_1} X_1\right)\left(\sqrt{\alpha_0} X_0 - i\sqrt{\alpha_1} X_1\right),$$

so 2 implies 3. Converse 3 implies 2 is an exercise. [3] ∎

Algorithm 4.3 (To find all k-points of a singular plane conic)**.** *Factor the conic into linear factors, possibly over an extension of k, and then find all the k-points on the lines.*

Lecture 9 Tuesday 22/10/19

Algorithm 4.4 (To find all k-points on a non-singular plane conic from one point)**.** *Let k be any field of $\operatorname{ch} k \neq 2$, and let $C \neq \emptyset$ be a conic $F = 0$ over k for a degree two homogeneous polynomial $F \in k[X, Y, Z]$ such that $F = 0$ is non-singular. If $O \in C$, then we can construct a bijection between points over k in C and points on a projective line over k not containing O.*

Proof. Let $\pi(P)$ be the projection of O through P onto a line l not containing O. Claim that $P \mapsto \pi(P)$ is a well-defined map. Any line can intersect C only at most two points, and it intersects C in exactly one point if and only if it is a tangent.

- If $P \neq O$, then there is a unique line $\overrightarrow{OP}$ between O and P. Then $\overrightarrow{OP}$ and l are different as l does not contain O, but $\overrightarrow{OP}$ does, so $\overrightarrow{OP} \cap l$ is one point $\pi(P)$, so $\pi(P)$ is well-defined in this case.
- The tangent line of C at O intersects C at O with multiplicity at least two, so it does not intersect C in any other point, but it still has a unique intersection point with l, so I take the latter to be $\pi(O)$.

Claim that $P \mapsto \pi(P)$ is a bijection.

- The map is injective, since if $\pi(P) = \pi(P')$, then $\overrightarrow{OP} = \overrightarrow{OP'}$, so $P, P', O \in \overrightarrow{OP} \cap C$, so $P = P'$.
- The map is surjective. If $O \neq Q \in l$, then there is another intersection point in $\overrightarrow{OQ} \cap C$ over the algebraic closure. The bad thing is that the line intersects C in two points over the algebraic closure, neither of which is a rational point. Claim that if $0 \neq h \in k[x]$ has degree two, and it has a root over k, then its other root is also defined over k. Let $h = ax^2 + bx + c$. There exists $\alpha \in k$ such that $h(\alpha) = 0$, so I can factor out $x - \alpha$, so $h = (x - \alpha) g$ for $g \in k[x]$. Then $\deg g = 1$, so $g = a(x - \beta)$ for $\beta \in k$, so β is the other root. Thus the other intersection point is another point $P \in C$.

∎

Corollary 4.5. *If k is infinite, then either C has no points, or it has infinitely many.*

[3] Exercise

5 The Hasse principle

Let C be a conic $aX^2 + bY^2 + cZ^2 = 0$ over $\mathbb{R}$. We rescale each of a, b, c by a non-zero square. Over $\mathbb{R}$ we can assume $\{a, b, c\} = \{1, -1\}$. There are two cases. Lecture 10 Thursday 24/10/19

- If $X^2 + Y^2 + Z^2 = 0$, then $C(\mathbb{R}) = \emptyset$.
- If $X^2 + Y^2 - Z^2 = 0$, then $C(\mathbb{R}) \neq \emptyset$.

Let C be a conic $aX^2 + bY^2 + cZ^2 = 0$ over $\mathbb{Q}_p$ such that p is an odd prime. After rescaling by a square I can assume that $a, b, c \in \mathbb{Z}_p$. Then $|a|_p, |b|_p, |c|_p \le 1$. By rescaling by a non-zero even power of p, I can assume the following two cases.

- If $|a|_p, |b|_p, |c|_p = 1$, then C is non-singular. As $a, b, c \in \mathbb{Z}_p$, I can reduce the equation modulo p. Pick $x \neq 0$, and let
$$A = \left\{ax^2 + by^2 \mid y \in \mathbb{F}_p\right\}.$$
Assume $A \subseteq \mathbb{F}_p^\times$, otherwise for some y, $ax^2 + by^2 + c0^2 = 0$. If $ax^2 + by^2 = ax^2 + by'^2$, then $y^2 = y'^2$, so $y = y' = 0$ or $y = -y' \neq 0$, so $|A| = (p+1)/2$. Let
$$B = \left\{-cz^2 \mid z \in \mathbb{F}_p\right\}.$$
Similarly $|B| = (p+1)/2$. If the equation has no solutions, then $A \cap B = \emptyset$, so
$$p - 1 = \left|\mathbb{F}_p^\times\right| \ge |A \cup B| = |A| + |B| = \frac{p+1}{2} + \frac{p+1}{2} = p + 1,$$
a contradiction. Then C has a point over $\mathbb{F}_p$, so it has a non-zero solution by Hensel's lemma. Thus C has a point over $\mathbb{Q}_p$.
- If $|c|_p = 1/p$ and $|a|_p, |b|_p = 1$, then C is singular, and we could still use Hensel's lemma.

Let C be a conic $aX^2 + bY^2 + cZ^2 = 0$ over $\mathbb{Q}$. I can assume that

- $a, b, c \in \mathbb{Z}$, by rescaling,
- a, b, c are relatively prime, by rescaling,
- a, b, c are square-free, since we can rescale individual variables by squares, and
- a, b, c are pairwise relatively prime, since if p is a prime number such that $p \mid a$ and $p \mid b$, then pa and pb are divisible by p^2, so I absorb the p^2 into X and Y.

Now just by looking at the signs you can tell whether C has a solution or not over the reals, and just by looking at the valuations you can tell whether C has a solution or not over the individual p-adic fields, but what can we say about the solutions of C over the rationals?

5.1 Geometry of numbers

Lemma 5.1. *Let $U \subseteq \mathbb{R}^n$ be a measurable set, for example open, and assume that it has measure $\mu(U) > m \in \mathbb{N}_{>0}$. Then there exist $c_0, \dots, c_m \in U$ such that $c_i - c_0 \in \mathbb{Z}^n \subset \mathbb{R}^n$ for all $i = 1, \dots, m$.*

Proof. Let $C = [0,1)^n \subseteq \mathbb{R}^n$. Then C is measurable and $\mu(C) = 1$, and $C + \mathbb{Z}^n = \mathbb{R}^n$. For any set $X \subseteq \mathbb{R}^n$ let
$$\chi_X(\underline{t}) = \begin{cases} 1 & \underline{t} \in X \\ 0 & \underline{t} \notin X \end{cases}$$
be the characteristic function of X. Then
$$m < \mu(U) = \int_{\mathbb{R}^n} \chi_U(\underline{t})\, \mathrm{d}\underline{t} = \sum_{\underline{x} \in \mathbb{Z}^n} \int_{\mathbb{R}^n} \chi_{(C+\underline{x}) \cap U}(\underline{t})\, \mathrm{d}\underline{t} = \int_{\mathbb{R}^n} \sum_{\underline{x} \in \mathbb{Z}^n} \chi_{(C+\underline{x}) \cap U}(\underline{t})\, \mathrm{d}\underline{t} = \int_C \sum_{\underline{x} \in \mathbb{Z}^n} \chi_U(\underline{t} + \underline{x})\, \mathrm{d}\underline{t}.$$
The function $\sum_{\underline{x} \in \mathbb{Z}^n} \chi_U(\underline{t} + \underline{x})$ is a counting function $\underline{t} \in C \mapsto |\{\underline{x} \in U \mid \underline{t} - \underline{x} \in \mathbb{Z}^n\}|$, which is an integer-valued measurable function, and if it is less than m for all points, then its integral over C is less than m, a contradiction. Thus there exists $\underline{t} \in C$ such that $|(\underline{t} + \mathbb{Z}^n) \cap U| > m$. $\square$

Definition 5.2.

- $U \subseteq \mathbb{R}^n$ is **symmetric** if for all $\underline{x} \in U$, $-\underline{x} \in U$.
- $U \subseteq \mathbb{R}^n$ is **convex** if for all $\underline{x}, \underline{y} \in U$, there exists $t \in [0,1]$ such that $t\underline{x} + (1-t)\underline{y} \in U$.

Corollary 5.3 (Minkowski's geometry of numbers)**.** *Let $\Lambda \subseteq \mathbb{Z}^n$ be a subgroup of finite index m. Let $U \subseteq \mathbb{R}^n$ be an open, convex, symmetric set of $\mu(U) > 2^n \cdot m$. Then $\Lambda \cap U \neq \{0\}$.*

Proof. Let
$$V = \frac{1}{2}U = \left\{ \frac{1}{2}\underline{x} \;\middle|\; \underline{x} \in U \right\}.$$
Then
$$\mu(V) = 2^{-n} \cdot \mu(U) > m.$$
So by the Lemma 5.1 there exist $c_0, \dots, c_m \in V$ such that $c_i - c_0 \in \mathbb{Z}^n$ for all $i = 0, \dots, m$. By the pigeonhole principle, as
$$|\{c_i - c_0 \mid i = 0, \dots, m\}| = m + 1 > [\mathbb{Z}^n : \Lambda],$$
there exist $i \neq j$ such that $c_i - c_0 \equiv c_j - c_0 \mod \Lambda$, so $c_i - c_j = (c_i - c_0) - (c_j - c_0) \in \Lambda$. Then $2c_i \in U$, and $-2c_i \in -U = U$ by symmetry of U, so $\frac{1}{2}(2c_i) + \frac{1}{2}(-2c_j) \in U$, as U is convex. ☐

Theorem 5.4. *If $n \in \mathbb{Z}_{>0}$ such that there exists t with $t^2 \equiv -1 \mod n$, then n is a sum of two squares.*

Proof. Define
$$\Lambda = \{(x,y) \mid y \equiv tx \mod n\} \subseteq \mathbb{Z}^2.$$
This has index n, because it is the kernel of
$$\begin{array}{ccc} \mathbb{Z}^2 & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ (x,y) & \longmapsto & y - tx \end{array}.$$
Let
$$V = \left\{(x,y) \in \mathbb{R}^2 \;\middle|\; x^2 + y^2 < 2n\right\}.$$
Then
$$\mu(V) = 2n \cdot \pi > 4n = 2^2 \cdot n = 2^2 \cdot \left[\mathbb{Z}^2 : \Lambda\right].$$
Corollary 5.3 implies that there exists $(x,y) \in V \cap \Lambda$ such that $(x,y) \neq (0,0)$. Then $(x,y) \in V$ implies that $x^2 + y^2 < 2n$, and $(x,y) \in \Lambda$ implies that $y \equiv tx \mod n$, so
$$x^2 + y^2 \equiv x^2 + (tx)^2 \equiv x^2\left(t^2 + 1\right) \equiv 0 \mod n.$$
So $x^2 + y^2 = n$. ☐

5.2 The Hasse-Minkowski theorem

Lecture 11 Monday 28/10/19

Theorem 5.5 (Hasse-Minkowski)**.** *Let C be*
$$f = aX^2 + bY^2 + cZ^2 = 0, \qquad a, b, c \in \mathbb{Z}, \qquad abc \neq 0, \qquad (a,b) = (b,c) = (c,a) = 1,$$
where a, b, c are square-free. Let $\Sigma = \{p \mid 2abc\}$. Then the following are equivalent.

1. *C has infinitely many solutions in $\mathbb{P}^2(\mathbb{Q})$.*
2. *C has a solution in $\mathbb{P}^2(\mathbb{Q})$.*
3. *C has a solution in $\mathbb{P}^2(\mathbb{Q}_p)$ for all p, and in $\mathbb{P}^2(\mathbb{R})$.*
4. *C has a solution in $\mathbb{P}^2(\mathbb{Q}_p)$ for all $p \in \Sigma$.*

The problem of solving conics over $\mathbb{Q}$ is algorithmically decidable, so there is a computer program which solves this problem.

Remark 5.6. Let $X \subseteq \mathbb{P}^n(\mathbb{Q})$ be a projective algebraic variety, such as hypersurfaces or plane curves. The **local-global principle** holds for X if $X(\mathbb{Q}) \neq \emptyset$ if and only if $X(\mathbb{Q}_p) \neq \emptyset$ for all p prime number and $X(\mathbb{R}) \neq \emptyset$. Hasse-Minkowski implies that conics, and all dimensions for all quadratic hypersurfaces, satisfy the local-global principle. Selmer and Chabauty proved that $3X^3 + 4Y^3 + 5Z^3 = 0$ does not.

Proof. 1 implies 2 implies 3 implies 4, and we proved 2 implies 1, so 4 implies 2 is enough. Assume 4. Claim that if $p \mid a$, then there is a solution to

$$b + cz^2 \equiv 0 \mod p.$$

By 4, there exists $(x, y, z) \in \mathbb{P}^2(\mathbb{Q}_p)$ with $ax^2 + by^2 + cz^2 = 0$. Without loss of generality $x, y, z \in \mathbb{Z}_p$, not all divisible by p. If $|y|_p < 1$ then $cz^2 = -\left(ax^2 + by^2\right) \equiv 0 \mod p$, so $|z|_p < 1$, then $\left|ax^2\right|_p \leq 1/p^2$, so $|x|_p < 1$, a contradiction. So $|y|_p = 1$, so $a\left(x/y\right)^2 + b + c\left(z/y\right)^2 = 0$, with $x/y, z/y \in \mathbb{Z}_p$. Then

$$b + c\left(\frac{z}{y}\right)^2 \equiv 0 \mod p.$$

- Now assume that p is odd and $p \mid a$. Then let $\alpha \in \mathbb{Z}/p\mathbb{Z}$ be a solution to $b + c\alpha^2 \equiv 0 \mod p$, and impose the condition
$$\alpha s + t \equiv 0 \mod p.$$
Then $ar^2 + bs^2 + ct^2 \equiv bs^2 + ct^2 \equiv bs^2 + c\left(\alpha s\right)^2 \equiv s^2\left(b + c\alpha^2\right) \equiv 0 \mod p$. If p is odd and $p \mid b$ or $p \mid c$, impose the analogous conditions.
- Now assume that $p = 2$.

  Case 1. Let $2 \mid a$, or by symmetry $2 \mid b$ or $2 \mid c$. We will write a condition to ensure that $ar^2+bs^2+ct^2 \equiv 0 \mod 8$. We saw in the proof of the claim that there exist $x, y, z \in \mathbb{Z}_2$ with $|x|_2 \leq 1$ and $|y|_2 = |z|_2 = 1$, and $ax^2 + by^2 + cz^2 = 0$. Then $ax^2 + by^2 + cz^2 \equiv ax^2 + b + c \mod 8$, that is $ax^2 + b + c \equiv 0 \mod 8$.

  - If $|x|_2 = 1$, then $a + b + c \equiv 0 \mod 8$. Impose
  $$s \equiv t \mod 4, \qquad r \equiv s \mod 2.$$
  Then either $r, s, t \equiv 1 \mod 2$, and $ar^2 + bs^2 + ct^2 \equiv a + b + c \equiv 0 \mod 8$, or $r, s, t \equiv 0 \mod 2$, and $ar^2 + bs^2 + ct^2 \equiv bs^2 + ct^2 \equiv 4\left(b + c\right) \equiv -4a \equiv 0 \mod 8$.
  - If $|x|_2 < 1$, then $ax^2 + b + c \equiv b + c \mod 8$, that is $b + c \equiv 0 \mod 8$. Impose
  $$s \equiv t \mod 4, \qquad r \equiv 0 \mod 2.$$
  Then $ar^2 + bs^2 + ct^2 \equiv bs^2 + ct^2 \equiv bs^2 + cs^2 \equiv \left(b + c\right)s^2 \equiv 0 \mod 8$.

  Case 2. Let $2 \nmid abc$. Let $(x, y, z) \in \mathbb{P}^2(\mathbb{Q}_2)$ with $ax^2 + by^2 + cz^2 = 0$. Assume $\max\left(|x|_2, |y|_2, |z|_2\right) = 1$. Then $ax^2 + by^2 + cz^2 \equiv 0 \mod 2$, that is $x^2 + y^2 + z^2 \equiv 0 \mod 2$. Then exactly one of x, y, z is even, without loss of generality $|x|_2 < 1$ and $|y|_2 = |z|_2 = 1$. Then $0 = ax^2 + by^2 + cz^2 \equiv by^2 + cz^2 \equiv b + c \mod 4$. Impose conditions
  $$r \equiv 0 \mod 2, \qquad s \equiv t \mod 2.$$
  Then $ar^2 + bs^2 + ct^2 \equiv bs^2 + ct^2 \equiv \left(b + c\right)s^2 \equiv 0 \mod 4$.

Let $\Lambda \subseteq \mathbb{Z}^3$ be the subgroup defined by all of these congruence conditions for $p \in \Sigma$. Then

$$\left[\mathbb{Z}^3 : \Lambda\right] = |4abc| = 4\prod_{p \mid abc} p,$$

using the Chinese remainder theorem. If $(r, s, t) \in \Lambda$ then $ar^2 + bs^2 + ct^2 \equiv 0 \mod 4abc$. Let

$$V = \left\{|a|X^2 + |b|Y^2 + |c|Z^2 < 4|abc|\right\}.$$

If $(r, s, t) \in \Lambda \cap V$ then $\left|ar^2 + bs^2 + ct^2\right| < 4|abc|$, so $ar^2 + bs^2 + ct^2 = 0$. So by Corollary 5.3, we just need to check that $\mu(V) > 2^3 \cdot |4abc|$, and

$$\mu(V) = \frac{\frac{4}{3}\pi\sqrt{|4abc|}^3}{\sqrt{|abc|}} = \frac{\pi}{3} \cdot 2^3 \cdot |4abc| > 2^3 \cdot |4abc|,$$

as required. $\square$

6 Plane cubics

6.1 Plane cubics

Lecture 12 Tuesday 29/10/19

Definition 6.1. A **plane cubic** is a cubic equation in two variables over a field, such as

- singular cubics over general fields, or
- non-singular cubics, particularly over $\mathbb{Q}$, and $\mathbb{Q}_p$ and $\mathbb{F}_p$.

Example.

- $3x^3 + 4y^3 = 5$ has points over $\mathbb{Q}_p$ for all p, and it also has points over $\mathbb{R}$, but it has no points over $\mathbb{Q}$.
- $x^3 + y^3 = 0$ has lots of points over $\mathbb{Q}$, but it is singular, in fact $x^3 + y^3 = (x + y)\left(x^2 - xy + y^2\right)$.
- $x^3 + y^2 = 0$ is also singular, and does not factor, even over $\mathbb{C}$.
- $x^3 + y^3 = 1$ has exactly two points over $\mathbb{Q}$, namely $(1, 0)$ and $(0, 1)$. This is a special case of Fermat's last theorem, $a^3 + b^3 = c^3$, where $a, b, c \in \mathbb{Z}$ implies that $abc = 0$. This is a non-singular cubic with finitely many points over $\mathbb{Q}$, but not empty.
- $x^3 + y^3 = 9$ has at least two points over $\mathbb{Q}$, $(2, 1)$ and $(1, 2)$. This is non-singular, since $3x^2 = 3y^2 = 0$ implies that $(x, y) = (0, 0)$, a contradiction.

Lemma 6.2. *There are non-singular plane cubics over $\mathbb{Q}$ with infinitely many points, such as $x^3 + y^3 = 9$.*

The **height** of $[x : y : z] \in \mathbb{P}^2(\mathbb{Q})$ is $|z|$ provided that $x, y, z \in \mathbb{Z}$ are coprime.

Example.

- The height of $\left[-\frac{17}{7} : \frac{20}{7} : 1\right]$ is 7.
- The height of $[1 : 2 : 1]$ is 1.

Proof. Draw tangent lines. For example, take the tangent line $(x - 1) + 4(y - 2) = 0$ at $(1, 2)$, so $4y + x = 9$. Then $y^3 + (9 - 4y)^3 = 9$, that is $-9(y - 2)^2 (7y - 20) = 0$, so $(x, y) = \left(-\frac{17}{7}, \frac{20}{7}\right)$. If $[r : s : t]$ is a point on $X^3 + Y^3 = 9Z^3$, then the third point of intersection of the tangent line at $[r : s : t]$ with this curve is

$$[R : S : T] = \left[r\left(r^3 + 2s^3\right) : -s\left(2r^3 + s^3\right) : t\left(r^3 - s^3\right)\right].$$

Claim that the height of $[R : S : T]$ is greater than the height of $[r : s : t]$. Assume that $r, s, t \in \mathbb{Z}$ are coprime, and $t > 0$, so the height of $[r : s : t]$ is t. Then $r^3 + s^3 = 9t^3$ implies that $(r, s) = (s, t) = (t, r) = 1$, by considering any common prime factor, and using that 9 is not divisible by any cube. Let d be the GCD of R, S, T. If p is a prime dividing both d and r, then $p \mid S$, so $p \mid s^4$, and $p \mid s$. But $(r, s) = 1$, so this would be a contradiction, so $(d, r) = 1$. Since $d \mid R$, we have $d \mid \left(r^3 + 2s^3\right)$. Similarly, $(d, s) = 1$ and $d \mid S$, so $d \mid \left(2r^3 + s^3\right)$. So $d \mid 3\left(r^3, s^3\right)$, that is $d \mid 3$. So $d \le 3$, and the height of $[R : S : T]$ is at least $|T/3|$. So we just have to prove that $\left|r^3 - s^3\right| > 3$. If not, then $r, s = 0, \pm 1$, which contradicts $r^3 + s^3 = 9t^3$ unless $[r : s : t] = [1 : -1 : 0]$. The only way that we could reach this point is by starting at a point of the form $[R : R : T]$, but then $2R^3 = 9T^3$, which has no solutions. ☐

Algorithm 6.3. *Suppose that C is a singular plane cubic over a field k, and that there is a singular point P with coordinates in k. Then there are infinitely many points of C over k, provided k is infinite, and we can find them all by drawing lines through P with rational slope.*

Proof. Use Bézout exactly as for conics. ☐

Remark 6.4. If C is singular then provided that either k has characteristic zero, or k is a finite field, then any singular point has coordinates in k.

Proof. By Bézout, at most one singular point, and then use Galois theory. ☐

Example 6.5. The **cusp** $y^2 = x^3$, singular at $(0, 0)$. Then $y = tx$ gives $x = t^2$ and $y = t^3$.

Example 6.6. The **node** $y^2 = x^2 (x + 1)$. Then $y = tx$ gives $x = t^2 - 1$ and $y = t^3 - t$.

Lecture 13 Thursday 31/10/19

Lecture 13 is a problems class.

6.2 Group law

Lecture 14 Monday 04/11/19

A cubic is **irreducible** if it does not have a linear factor.

Example. Any non-singular cubic will be irreducible.

Theorem 6.7. *Let f be an irreducible cubic over a field k. Assume that $f = 0$ has at least one point over k. Fix such a point $\mathcal{O}$. Let G be the set of non-singular points of $f = 0$ with coordinates in k. We can give G the structure of an abelian group with identity $\mathcal{O}$.*

Say that n points are in **general position** if no four of them lie on a line, and no seven of them lie on a conic.

Lemma 6.8. *Given eight points in general position, there exists a ninth point such that any cubic passing through the first eight points also passes through the ninth.*

Proof. Let g be a cubic, so

$$g = a_1x^3 + a_2x^2 + a_3x + a_4 + a_5y^3 + a_6y^2 + a_7y + a_8x^2y + a_9xy^2 + a_{10}xy.$$

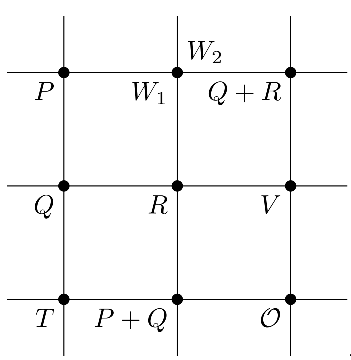
The condition that my given eight points are contained in $g = 0$ gives me eight linear equations in $a_1, \dots, a_{10}$. The condition of being in general position tells us that these equations are independent, so we have a two-dimensional space of solutions. So there exist cubics f_1 and f_2 such that every cubic containing the eight points is of the form

$$\lambda_1 f_1 + \lambda_2 f_2, \qquad \lambda_1, \lambda_2 \in k.$$

By Bézout, $\{f_1 = 0\} \cap \{f_2 = 0\}$ has nine points, and the ninth point of intersection is the point we need. $\square$

Proof of Theorem 6.7. $P + Q$ is the third point of intersection of the line $\overrightarrow{\mathcal{O}R}$, where R is the third point of intersection of the line through $\overrightarrow{PQ}$. If $P = Q$ take the tangent at P.

- To see that $P + Q \in G$, just note that given any two points in G, the third point of intersection has coordinates in k, such as by explicitly solving equations, and must be non-singular, else would have at least $2 + 1 + 1 = 4$ points of intersection with multiplicity.
- $P + Q = Q + P$ by definition.
- $P + \mathcal{O} = P$ by definition.
- Want an inverse $-P$ such that $P + (-P) = \mathcal{O}$. Let Q be the third point of intersection of the tangent line at $\mathcal{O}$. Then $-P$ is defined to be the third point of intersection of $\overrightarrow{PQ}$ with $f = 0$.
- It remains to check that $(P + Q) + R = P + (Q + R)$. Unfortunately this is not obvious. We follow Cassels' book, which almost proves it. Let



.

Associativity is the statement that $W_1 = W_2$. Apply Lemma 6.8 to

$$\mathcal{O}, \qquad P, \qquad Q, \qquad R, \qquad T, \qquad V, \qquad P+Q, \qquad Q+R.$$

Consider three cubics,

- $f = 0$,
- the three vertical lines, and
- the three horizontal lines.

There exists a unique ninth point W on all of these cubics. By Bézout, the ninth point of intersection of the first two cubics is W_1, so $W = W_1$. Similarly, $W = W_2$. So $W_1 = W_2$, and $P + (Q + R) = (P + Q) + R$.

□

Remark 6.9. This requires $\mathcal{O}, P, Q, R, T, V, P+Q, Q+R$ are in general position. This is an open condition. The equation $P + (Q + R) = (P + Q) + R$ is a closed condition. To make this a complete proof, work in the Zariski topology.

6.3 Elliptic curves

Lecture 15 Tuesday 05/11/19

Definition 6.10. An **elliptic curve** over a field k is a non-singular plane cubic together with a fixed point $\mathcal{O}$ with coordinates in k.

Definition 6.11. A **point of inflexion** is a point P such that the tangent line to the curve at P only meets the curve at P. Since we are considering cubics, these are points where the tangent line meets with multiplicity three.

Lemma 6.12. *If $\mathcal{O}$ is a point of inflexion, then $P + Q + R = \mathcal{O}$ if and only if P, Q, R are collinear.*

Proof. $P + Q + R = \mathcal{O}$ if and only if $R = -(P + Q)$, if and only if R is the third point of intersection of the line through P and Q. □

Consider cubic curves of the form $y^2 = f(x)$, where $f(x)$ is a monic cubic. In homogeneous coordinates,

$$Y^2 Z - \left(X^3 + \alpha X^2 Z + \beta X Z^2 + \gamma Z^3\right) = 0.$$

Lemma 6.13.

1. *This has a unique point at infinity, which is non-singular.*
2. *The point at infinity is a point of inflexion.*
3. *This curve is always irreducible, and if $\operatorname{ch} k \neq 2$, then it is non-singular if and only if $f(x)$ has distinct roots.*

Proof.

1. $Z = 0$ implies that $X^3 = 0$, so $X = 0$, so $[0 : 1 : 0]$ is the unique point at infinity, and $\frac{\partial}{\partial Z} = Y^2 = 1^2 = 1 \neq 0$.
2. $\frac{\partial}{\partial X} = \frac{\partial}{\partial Y} = 0$ at $[0 : 1 : 0]$, so the tangent line is just $\{Z = 0\}$. So the only point of the curve on this is $[0 : 1 : 0]$, by 1.
3. Any singular point is a point of $y^2 = f(x)$, by 1. Then $\frac{\partial}{\partial y} = 2y = 0$ and $\frac{\partial}{\partial x} = f'(x) = 0$, and $\operatorname{ch} k \neq 2$ implies that $y = 0$ and $f'(x) = 0$, so $f(x) = 0$. Thus $f(x) = f'(x) = 0$ has a solution if and only if $f(x)$ has a repeated root, since $f(x) = (x - \alpha) g(x)$.

□

If $\operatorname{ch} k \neq 2$, can always make any elliptic curve into a curve of this form. In general, need $y^2+\alpha y+\beta xy = f(x)$. If $\operatorname{ch} k \neq 2, 3$ then we can complete the cube in $f(x)$, and write

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

since $x^3 + cx^2 + \dots = \left(x + \frac{1}{3}c\right)^3 + \dots$. Let $\operatorname{ch} k \neq 2$. If $P = (x_0, y_0)$, what is $-P$? The line through P and $\mathcal{O}$ is $x = x_0$, so $-P = (x_0, -y_0)$. [4] Then

$$2P = \mathcal{O} \iff P = -P \iff y_0 = -y_0 \iff y_0 = 0 \iff P = (x_0, 0),$$

with x_0 a root of $f(x)$. The **discriminant** of $x^3 + ax + b = (x - \alpha)(x - \beta)(x - \gamma)$ is

$$\Delta = (\alpha - \beta)^2 (\beta - \gamma)^2 (\gamma - \alpha)^2 = 4a^3 + 27b^2.$$

In particular, $y^2 = x^3 + ax + b$ is an elliptic curve if and only if $\Delta \neq 0$. What changes of variable can we make that turn $y^2 = x^3 + ax + b$ into another equation $y^2 = x^3 + a'x + b'$? [5] If

$$y' = u^3 y, \qquad x' = u^2 x, \qquad u \neq 0,$$

then $u^6 y^2 = u^6 x^3 + au^6 x + bu^6$, so $y'^2 = x'^3 + au^6 x + bu^6$. This takes

$$(a, b) \leftrightarrow \left(u^4 a, u^6 b\right), \qquad \Delta \leftrightarrow u^{12} \Delta.$$

Definition 6.14. The **j-invariant** of $y^2 = x^3 + ax + b$ is

$$-\frac{1728 (4a)^3}{\Delta}.$$

This is invariant under $(x, y) \leftrightarrow \left(u^2 x, u^3 y\right)$.

Proposition 6.15. *If k is algebraically closed, then two elliptic curves are isomorphic if and only if they have the same j-invariant.*

Proof. Assume $\operatorname{ch} k \neq 2, 3$. Suppose that we have two elliptic curves $y^2 = x^3 + ax + b$ and $y^2 = x^3 + a'x + b'$. These have the same j-invariants if and only if $a^3 / \left(4a^3 + 27b^2\right) = a'^3 / \left(4a'^3 + 27b'^2\right)$, if and only if

$$\frac{b^2}{a^3} = \frac{b'^2}{a'^3}.$$

If the two curves are isomorphic, then the j-invariants are equal, as $(x, y) \leftrightarrow \left(u^2 x, u^3 y\right)$ does not change the j-invariant. Conversely, assume $b^2/a^3 = b'^2/a'^3$, that is $(a'/a)^3 = (b'/b)^2$. Since k is algebraically closed, there exists u such that $u^4 = a'/a$ and $u^6 = b'/b$. Then the transformation $(x, y) \leftrightarrow \left(u^2 x, u^3 y\right)$ takes $y^2 = x^3 + ax + b \leftrightarrow y^2 = x^3 + a'x + b'$. Implicitly assumed that $a, b, a', b' \neq 0$. More correctly, the equation is $b^2 a'^3 = b'^2 a^3$. If $a = 0$ then $b \neq 0$, as the curve is non-singular, so $a' = 0$, so $b' \neq 0$, so just choose $u^6 = b'/b$. Similarly if $b = 0$ then $a \neq 0$, so $b' = 0$ and $a' \neq 0$, and choose $u^4 = a'/a$. ☐

6.4 Examples

Lecture 16 Thursday 07/11/19

Example 6.16. Let $\operatorname{ch} k \neq 2, 3$, and let $y^2 = x^3$ with $\mathcal{O} = [0 : 1 : 0]$. The non-singular points are all points not equal to $(0, 0)$. By Lemma 6.12, $P + Q + R = \mathcal{O}$ if and only if P, Q, R are collinear. Intersect $y^2 = x^3$ with a line $ax + by = 1$. Then $x^3 = y^2 = y^2(ax + by)$, so $(x/y)^3 = a(x/y) + b$. Write $u = x/y$, so $u^3 - au - b = 0$. If the roots of this cubic are u_1, u_2, u_3, then $u_1 + u_2 + u_3 = 0$. Conversely if $u_1 + u_2 + u_3 = 0$, then u_1, u_2, u_3 are the roots of $u^3 - au - b = 0$, so $a = -(u_1 u_2 + u_2 u_3 + u_3 u_1)$ and $b = u_1 u_2 u_3$. That is, $(x_1, y_1) + (x_2, y_2) + (x_3, y_3) = 0$ if and only if $x_1/y_1 + x_2/y_2 + x_3/y_3 = 0$. We get an isomorphism

$$\begin{array}{ccc} \left\{y^2 = x^3\right\} & \longrightarrow & (k, +) \\ (x, y) & \longmapsto & \dfrac{x}{y} \end{array}.$$

[4] Exercise
[5] Exercise

Example 6.17. Let $y^2 = x^2 (x+1)$, and let $u = y + x$ and $v = y - x$. Then $x^3 = y^2 - x^2 = (y+x)(y-x)$ and $x = \frac{1}{2}(u-v)$, so $(u-v)^3 = 8uv$. Now take a line $au + bv = 1$. Then $(u-v)^3 = 8uv = 8uv(au+bv)$. Set $t = u/v$, so that $(t-1)^3 = 8t(at+b)$. The roots of this cubic are t_1, t_2, t_3 with $t_1 t_2 t_3 = 1$. So we have an isomorphism

$$\begin{array}{rcl} \left\{y^2 = x^2 (x+1)\right\} & \longrightarrow & (k^\times, \times) \\ (x,y) & \longmapsto & \dfrac{y+x}{y-x} \end{array}.$$

Example 6.18. Let $y^2 = x^3 + 1$, and let $k = \mathbb{F}_5 = \mathbb{Z}/5\mathbb{Z}$. The discriminant is $\Delta = 27 \neq 0$ in $\mathbb{F}_5$. The squares modulo five are $0, 1, 4$, and

x	0	1	2	3	4
y	± 1	$\times$	± 2	$\times$	0

Also the point $\mathcal{O}$ at infinity. So six points, so $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \cong \mathbb{Z}/6\mathbb{Z}$.

- $2P = \mathcal{O}$ if and only if $y = 0$. So $(4, 0)$ has order two.
- Claim that $(0, 1)$ is a point of order three. Then $3P = \mathcal{O}$ so we just need a line which only meets the curve at this point. Check that $Y = Z$ in projective coordinates only goes through this point. [6]
- So $(0, 1)$ has order three and $(4, 0)$ has order two. Then $y = x + 1$ passes through $(0, 1)$ and $(4, 0) = (-1, 0)$. The third point of intersection is $(2, -2) = -((0,1) + (4,0))$, so $(0,1) + (4,0) = -(2,-2) = (2, 2)$.

Exercise 6.19. Compute $n(2, -2)$ for $n = 0, \dots, 5$.

Notation 6.20. Write E for an elliptic curve, and $E(k)$ for all its points over a field k.

Example. We just computed $E(\mathbb{F}_5)$ for $E = \left\{y = x^3 + 1\right\}$.

The main goal of the course is to take an elliptic curve E over $\mathbb{Q}$, and see what we can say about $E(\mathbb{Q})$. The main theorem is the Mordell-Weil theorem, that $E(\mathbb{Q})$ is a finitely generated abelian group. That is, there exists $\mathbb{Z}^N \twoheadrightarrow E(\mathbb{Q})$, that is there exist $g_1, \dots, g_N \in E(\mathbb{Q})$ such that every element is of the form $\sum_{i=1}^N a_i g_i$ for $a_i \in \mathbb{Z}$. The group $(\mathbb{Q}, +)$ is not finitely generated. The structure theorem for finitely generated abelian groups is that any finitely generated abelian group is of the form $H \times T$, where $H \cong \mathbb{Z}^r$ for some $r \geq 0$, and T is finite. Both r and T are uniquely determined. Call r the **rank** of the group, and T the **torsion subgroup**, that is the subgroup of elements of finite order.

Remark 6.21. Page 190 of Silverman shows that if $E(L)/2E(L)$ is finite for L a finite Galois extension of $\mathbb{Q}$ then $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite. It is just a tiny bit of Galois cohomology using finiteness of 2-torsion. It is fairly straightforward to generalise the arguments we give for the finiteness of $E(\mathbb{Q})/2E(\mathbb{Q})$ to number fields, so by choosing L large enough, we could remove the assumption on E.

[6] Exercise

7 The torsion subgroup of $E(\mathbb{Q})$

Lecture 17 Monday 11/11/19

Let E be an elliptic curve over $\mathbb{Q}$. The torsion subgroup of $E(\mathbb{Q})$ is

$$T = \{P \in E(\mathbb{Q}) \mid \exists n \geq 1,\ nP = \mathcal{O}\}.$$

We will see that this is a finite abelian group, and we will see how to compute it. Write E as $y^2 = x^3+ax+b$ for $a, b \in \mathbb{Q}$. Making a change of variables $(x, y) \mapsto \left(u^2 x, u^3 y\right)$ for some $u \in \mathbb{Q}^\times$, we can send $(a, b) \mapsto \left(u^4 a, u^6 b\right)$, and we can assume $a, b \in \mathbb{Z}$ and $4a^3 + 27b^2 \neq 0$.

Theorem 7.1 (Lutz-Nagell). *Let $y^2 = x^3 + ax + b$ be an elliptic curve with $a, b \in \mathbb{Z}$. Then the torsion subgroup of $E(\mathbb{Q})$ is finite. If (x, y) is in this torsion subgroup, then $x, y \in \mathbb{Z}$. Furthermore either $y = 0$ or $y^2 \mid \left(4a^3 + 27b^2\right)$.*

To do this we need a formula for $2P = (x_d, y_d)$ in terms of $P = (x, y)$.

Algorithm 7.2 (Doubling formula). *Write $P = (x_0, y_0)$ and $2P = (x_d, y_d)$. Then $-2P = (x_d, -y_d)$ is the third point of intersection of the tangent line at P. Let this tangent line be $y = mx + c$. Differentiating $y^2 = x^3 + ax + b$, $m = \left(3x_0^2 + a\right)/2y_0$. We have to solve $(mx + c)^2 = x^3 + ax + b$. This will have roots x_0, x_0, x_d. The sum of the roots of this cubic is m^2. So $x_d = m^2 - 2x_0$, and $y_0^2 = x_0^3 + ax_0 + b$. Thus*

$$x_d = \frac{x_0^4 - 2ax_0^2 - 8bx_0 + a^2}{4\left(x_0^3 + ax_0 + b\right)}, \qquad -y_d = mx_d + c.$$

Proof of Theorem 7.1. If $(x, y) \in E(\mathbb{Q})$ is a torsion point, then by Corollary 8.12, $x, y \in \mathbb{Z}_p$ for all p. So $x, y \in \mathbb{Z}$. If (x, y) is a torsion point, then $2(x, y)$ is also a torsion point, since $nP = \mathcal{O}$ implies that $n(2P) = 2(nP) = 2\mathcal{O} = \mathcal{O}$. Then if $2(x, y) = (x_d, y_d)$, then $x_d, y_d \in \mathbb{Z}$. We will show that this implies that $y = 0$ or $y^2 \mid \left(4a^3 + 27b^2\right)$. Suppose that $y \neq 0$. Then we have that $y^2 \mid \left(3x^2 + a\right)^2$ and $y^2 = x^3 + ax + b$, and

$$\left(3x^2 + a\right)^2 \left(3x^2 + 4a\right) - \left(x^3 + ax + b\right)\left(27x^3 + 27ax - 27b\right) = 4a^3 + 27b^2.$$

So $y^2 \mid \left(4a^3 + 27b^2\right)$, as required. ◻

Algorithm 7.3 (Addition formula). *If $P = (x_1, y_1)$, $Q = (x_2, y_2)$, and $P + Q = (x_3, y_3)$, then*

$$x_3 = \frac{-2y_1y_2 + (x_1 + x_2)(x_1x_2 + a) + 2b}{(x_1 - x_2)^2}, \qquad -y_3 = mx_3 + c.$$

Example 7.4. If $y^2 = x^3 + 1$, then $4a^3 + 27b^2 = 27$, so $y = 0, \pm 1, \pm 3$, so

$$T \subseteq \{(-1, 0), (0, \pm 1), (2, \pm 3), \mathcal{O}\}.$$

Then $(0, 1)$ is a point of order three, by considering the line $y = 1$. That is, $2(0, 1) = (0, -1) = -(0, 1)$. Then we have a point of order three, and a point of order two, namely $(-1, 0)$, so the group of torsion points has order at least six, so it is exactly of order six.

Example 7.5. If $y^2 = x^3 + 17$, then $4a^3 + 27b^2 = 27(17)^2$, so $y = 0, \pm 1, \pm 3, \pm 17, \pm 51$. If $17 \mid y$ then $17 \mid x^3 = y^2 - 17$ then $17^2 \mid y^2 - x^3 = 17$, a contradiction, etc. Then $y = \pm 3$, so $x^3 = 9 - 17 = -8$. So

$$T \subseteq \{(-2, \pm 3), \mathcal{O}\}.$$

Using the doubling formula for $x_0 = -2$, $x_d = 8$. We already saw that any torsion point has $x = -2$, so this cannot be a torsion point after all. So the torsion subgroup is just $\{\mathcal{O}\}$.

Remark. This proves that there are infinitely many elements of $E(\mathbb{Q})$, that is infinitely many $x, y \in \mathbb{Q}$ such that $y^2 = x^3 + 17$. Indeed the points $n(-2, 3)$ are all distinct for $n \in \mathbb{Z}$.

8 The torsion points in $E(\mathbb{Q}_p)$

The next aim is to study elliptic curves over $\mathbb{Q}_p$ in order to show that torsion points have coordinates in $\mathbb{Z}_p$. Lecture 18 Tuesday 12/11/19

8.1 Reduction

Definition 8.1. Write $[a_1 : \dots : a_{n+1}]$ for some point, where all $a_i \in \mathbb{Z}_p$, and at least one $a_i \in \mathbb{Z}_p^\times$. There is a map

$$\begin{array}{ccc} \mathbb{P}^n(\mathbb{Q}_p) & \longrightarrow & \mathbb{P}^n(\mathbb{F}_p) \\ [a_1 : \dots : a_{n+1}] & \longmapsto & [\overline{a_1} : \dots : \overline{a_{n+1}}] \end{array}, \qquad \overline{a_i} = a_i \mod p,$$

for all n.

Can also reduce lines in $\mathbb{P}^2(\mathbb{Q}_p)$ modulo p. Write any line as $aX + bY + cZ = 0$. Rescale so that $a, b, c \in \mathbb{Z}_p$, and at least one is in $\mathbb{Z}_p^\times$. Then $\overline{a}X + \overline{b}Y + \overline{c}Z = 0$ is a well-defined line in $\mathbb{P}^2(\mathbb{F}_p)$. Let $y^2 = g(x)$, where g is a monic cubic with distinct roots. Rescaling x and y if necessary, assume $g(x) \in \mathbb{Z}_p[x]$. The **reduction modulo** p of the elliptic curve is then $y^2 = \overline{g}(x)$, where $\overline{g}(x) = g(x) \mod p$. This is an irreducible cubic, but it could be singular, if $p = 2$ or if $p \mid \Delta$.

Example 8.2. Let $p = 3$ and E be $y^2 = x^3 - 18$. Modulo three, this is $y^2 = x^3$, which has a singular point $(0, 0)$. For example, $(3, 3) \in E(\mathbb{Q}_3)$ is $[3 : 3 : 1] \mapsto [0 : 0 : 1] \mod 3$, that is to the singular point. There is a point (x, y) in $E(\mathbb{Q}_3)$ with $x = \frac{1}{9}$, since $\left(\frac{1}{9}\right)^3 - 18 = \frac{1}{27^2}\left(1 - 18 \cdot 27^2\right)$ is a square, by Hensel's lemma for $y^2 - \left(1 - 18 \cdot 27^2\right)$. Then $y = \frac{1}{27}u$ for some $u \in \mathbb{Z}_3^\times$. So

$$[x : y : 1] = [27x : 27y : 27] = [3 : u : 27] \mapsto [0 : \overline{u} : 0] = [0 : 1 : 0] = \mathcal{O} \mod 3.$$

8.2 A p-adic filtration

Lemma 8.3.

1. *If $(x_0, y_0) \in E(\mathbb{Q}_p)$ then either $x_0, y_0 \in \mathbb{Z}_p$ or there exists $n \ge 1$ such that $|x_0|_p = p^{2n}$ and $|y_0|_p = p^{3n}$.*
2. *If $g(x) = x^3 \mod p$, and $(x_0, y_0) \in E(\mathbb{Q}_p)$ with $|x_0|_p, |y_0|_p \le 1$, then either $|x_0|_p = |y_0|_p = 1$ or $|x_0|_p, |y_0|_p < 1$.*

Proof. Write

$$g(x) = x^3 + \alpha x^2 + \beta x + \gamma, \qquad \alpha, \beta, \gamma \in \mathbb{Z}_p.$$

1. If $|x_0|_p > 1$, then $\left|x_0^3\right|_p > \left|\alpha x_0^2\right|_p, |\beta x_0|_p, |\gamma|_p$. So $\left|x_0^3 + \alpha x_0^2 + \beta x_0 + \gamma\right|_p = |x_0|_p^3$. Then $|y_0|_p^2 = |x_0|_p^3$. If $|x_0|_p \le 1$, then $|y_0|_p^2 = \left|x_0^3 + \alpha x_0^2 + \beta x_0 + \gamma\right|_p \le 1$.
2. By assumption, $p \mid \alpha, \beta, \gamma$. So
$$p \mid x_0 \qquad \iff \qquad p \mid \left(x_0^3 + \alpha x_0^2 + \beta x_0 + \gamma\right) \qquad \iff \qquad p \mid y_0^2 \qquad \iff \qquad p \mid y_0.$$
That is, $|x_0|_p < 1$ if and only if $|y_0|_p < 1$.

$\square$

Definition 8.4. Write $\overline{E}$ for the cubic $y^2 = \overline{g}(x)$ in $\mathbb{P}^2(\mathbb{F}_p)$. Let

$$E(\mathbb{Q}_p)^{(0)} = \left\{P \in E(\mathbb{Q}_p) \mid \overline{P} \in \overline{E}(\mathbb{F}_p) \text{ is non-singular}\right\}.$$

Let

$$E(\mathbb{Q}_p)^{(1)} = \left\{P \in E(\mathbb{Q}_p) \mid \overline{P} = \mathcal{O} \in \overline{E}(\mathbb{F}_p)\right\}.$$

That is,

$$E(\mathbb{Q}_p)^{(1)} = \left\{(x, y) \in E(\mathbb{Q}_p) \,\middle|\, |x|_p, |y|_p > 1\right\}.$$

Lemma 8.5.

1. *$E(\mathbb{Q}_p)^{(0)}$ is a subgroup of $E(\mathbb{Q}_p)$.*

2. *Reduction modulo p is a group homomorphism from $E(\mathbb{Q}_p)^{(0)}$ to the group of non-singular points in $\overline{E}(\mathbb{F}_p)$. The kernel of this homomorphism is $E(\mathbb{Q}_p)^{(1)}$.*

Proof. The group law is $P+Q+R=\mathcal{O}$ if and only if P,Q,R are collinear.

1. Need to show that if P,Q,R are collinear, and $P,Q\in E(\mathbb{Q}_p)^{(0)}$, then $R\in E(\mathbb{Q}_p)^{(0)}$. That is, need that if $\overline{P}$ and $\overline{Q}$ are non-singular, then so is $\overline{R}$. This follows from Bézout.

2. The map is a group homomorphism because $P+Q+R=\mathcal{O}$ implies that P,Q,R are collinear, so $\overline{P},\overline{Q},\overline{R}$ are collinear, which implies that $\overline{P}+\overline{Q}+\overline{R}=\mathcal{O}$. The kernel is $E(\mathbb{Q}_p)^{(1)}$ by definition.

$\square$

Remark 8.6. The homomorphism $E(\mathbb{Q}_p)^{(0)}$ to the non-singular points in $\overline{E}(\mathbb{F}_p)$ is surjective.

Let
$$E(\mathbb{Q}_p)^{(n)}=\left\{(x,y)\in E(\mathbb{Q}_p)\ \middle|\ |x|_p\ge p^{2n}\right\},\qquad n\ge 1.$$
Say (x,y) has **level** n if $|x|_p=p^{2n}$, so $|y|_p=p^{3n}$.

Corollary 8.7. *$E(\mathbb{Q}_p)^{(n)}$ is a subgroup of $E(\mathbb{Q}_p)$ for all n.*

Proof. Let E_n be the elliptic curve obtained by the change of variables $(x,y)\mapsto\left(p^{2n}x,p^{3n}y\right)$. Then we have
$$\begin{array}{ccc} E & \longrightarrow & E_n \\ (x,y) & \longmapsto & \left(p^{2n}x,p^{3n}y\right) \end{array},$$
so $E(\mathbb{Q}_p)^{(n+1)}\xrightarrow{\sim}E_n(\mathbb{Q}_p)^{(1)}$, which is a group by Lemma 8.5. $\square$

Corollary 8.8. *For each $n\ge 1$ there is a natural injection*
$$E(\mathbb{Q}_p)^{(n)}/E(\mathbb{Q}_p)^{(n+1)}\hookrightarrow\mathbb{Z}/p\mathbb{Z}.$$

Proof. The map $E\to E_n$ takes $E(\mathbb{Q}_p)^{(n)}$ to a subgroup of $E_n(\mathbb{Q}_p)^{(0)}$, and $E(\mathbb{Q}_p)^{(n+1)}$ to $E_n(\mathbb{Q}_p)^{(1)}$. The curve E_n reduces to $y^2=x^3 \mod p$. So it suffices to show that if E' is an elliptic curve with reduction $y^2=x^3$, then we have an injection $E'(\mathbb{Q}_p)^{(0)}/E'(\mathbb{Q}_p)^{(1)}\hookrightarrow\mathbb{Z}/p\mathbb{Z}$. But reduction modulo p is a homomorphism $E'(\mathbb{Q}_p)^{(0)}/E'(\mathbb{Q}_p)^{(1)}$ to the non-singular points in $y^2=x^3 \mod p$. By Example 6.5, the right hand side is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ via $(x,y)\mapsto x/y$. $\square$

The aim is that $E(\mathbb{Q}_p)^{(1)}$ has no non-trivial torsion points, that is if $P\in E(\mathbb{Q}_p)^{(1)}$ and $mP=\mathcal{O}$ for $m\ge 1$, then $P=\mathcal{O}$. Lecture 19 Thursday 14/11/19

Remark 8.9. The idea is if P has level n, then $P=[x:y:1]=\left[p^{3n}x:p^{3n}y:p^{3n}\right]$ is close to $[0:1:0]$. We are looking at points which are close to $\mathcal{O}$, and the group law is simpler here. Near the identity in a Lie group, the group law becomes simpler. For example, in $\mathrm{GL}_n(\mathbb{C})$,
$$(1+\epsilon X)(1+\epsilon Y)=1+\epsilon(X+Y)+\mathrm{O}\left(\epsilon^2\right).$$

8.3 A formal group homomorphism

Define
$$\begin{array}{cccc} \mathrm{u} & : & E(\mathbb{Q}_p)^{(1)} & \longrightarrow & p\mathbb{Z}_p \\ & & \mathcal{O} & \longmapsto & 0 \\ & & (x,y) & \longmapsto & \dfrac{x}{y} \end{array}.$$

If $(x,y) \in E(\mathbb{Q}_p)^{(n)}$ then $|\mathrm{u}((x,y))|_p \leq p^{-n}$, with equality if (x,y) has level n. Also $-\mathrm{u}(P) = \mathrm{u}(-P)$ because $-(x,y) = (x,-y)$.

Lemma 8.10. *If $P, Q \in E(\mathbb{Q}_p)^{(1)}$, then*

$$|\mathrm{u}(P+Q) - \mathrm{u}(P) - \mathrm{u}(Q)|_p \leq \max\left(|\mathrm{u}(P)|_p^5, |\mathrm{u}(Q)|_p^5\right).$$

Proof. If $P, Q, P+Q$ equal $\mathcal{O}$, then the left hand side is zero and we are done. So assume that none of them is $\mathcal{O}$. Recall that we set E_n as $y^2 = x^3 + p^{4n}a + p^{6n}b$. Without loss of generality assume that the level of Q is at least the level of P, and take n as the level of P. Then the right hand side is p^{-5n}. Let $R = -(P+Q)$, so P, Q, R are collinear, and let P_n, Q_n, R_n be the corresponding points on E_n. Since P has level n, $P_n \in E_n(\mathbb{Q}_p)^{(0)}$ but $P_n \notin E_n(\mathbb{Q}_p)^{(1)}$ and $Q_n \in E_n(\mathbb{Q}_p)^{(0)}$, so $R_n \in E_n(\mathbb{Q}_p)^{(0)}$. Let the line through P_n, Q_n, R_n be $lx + my = 1$. Since this line, when reduced modulo p, does not pass through $(0,0)$, we have $l, m \in \mathbb{Z}_p$. Then

$$y^2(lx+my) = x^3 + p^{4n}ax(lx+my)^2 + p^{6n}b(lx+my)^3.$$

So

$$l\left(\frac{x}{y}\right) + m = \left(\frac{x}{y}\right)^3 + p^{4n}a\left(\frac{x}{y}\right)\left(l\left(\frac{x}{y}\right)+m\right)^2 + p^{6n}b\left(l\left(\frac{x}{y}\right)+m\right)^3.$$

Write $t = x/y$. This equation is a cubic in t, say $c_0t^3 + c_1t^2 + c_2t + c_3 = 0$. The sum of the roots of this cubic is $-c_1/c_0$, where

$$c_0 = 1 + p^{4n}al^2 + p^{6n}bl^3 \in \mathbb{Z}_p^\times, \qquad c_1 = 2p^{4n}alm + 3p^{6n}bl^2m \in p^{4n}\mathbb{Z}_p^\times.$$

So $|c_1/c_0|_p \leq p^{-4n}$. But

$$|\mathrm{u}(P+Q) - \mathrm{u}(P) - \mathrm{u}(Q)|_p = |\mathrm{u}(P) + \mathrm{u}(Q) + \mathrm{u}(R)|_p = p^{-n}\left|\frac{c_1}{c_0}\right|_p \leq p^{-5n} = \max\left(|\mathrm{u}(P)|_p^5, |\mathrm{u}(Q)|_p^5\right).$$

∎

A reminder that if $|x|_p \neq |y|_p$ then $|x+y|_p = \max\left(|x|_p, |y|_p\right)$. Writing $x = (x+y) + (-y)$, deduce that if $|x+y|_p < |x|_p$, then $|x|_p = |y|_p$.

Corollary 8.11.

1. *For all $n \geq 1$, $|\mathrm{u}(nP) - n\mathrm{u}(P)|_p \leq |\mathrm{u}(P)|_p^5$, and $|\mathrm{u}(nP)|_p \leq |\mathrm{u}(P)|_p$.*
2. *If $p \nmid n$, then $|\mathrm{u}(nP)|_p = |\mathrm{u}(P)|_p$.*
3. $|\mathrm{u}(pP)|_p = |p|_p |\mathrm{u}(P)|_p$.
4. *For all $n \geq 1$, $|\mathrm{u}(nP)|_p = |n|_p |\mathrm{u}(P)|_p$.*

Corollary 8.12. *If $(x,y) \in E(\mathbb{Q}_p)$ is a torsion point, then $x, y \in \mathbb{Z}_p$.*

Proof. Assume $nP = \mathcal{O}$ for $P = (x,y)$ and $n \geq 1$. If $P \in E(\mathbb{Q}_p)^{(1)}$, then we have $|n|_p |\mathrm{u}(P)|_p = |\mathrm{u}(nP)|_p = |\mathrm{u}(\mathcal{O})|_p = 0$. So $|\mathrm{u}(P)|_p = 0$, so $\mathrm{u}(P) = 0$, so $P = \mathcal{O}$. So $P \notin E(\mathbb{Q}_p)^{(1)}$, so $x, y \in \mathbb{Z}_p$. ∎

Corollary 8.13. *If $E(\mathbb{Q})$ is an elliptic curve of the form $y^2 = x^3 + ax + b$ for $a, b \in \mathbb{Z}$, and $p \nmid 2\Delta$, then the subgroup of $E(\mathbb{Q})$ of torsion points injects into $\overline{E}(\mathbb{F}_p)$.*

Proof. $p \nmid 2\Delta$ implies that $E(\mathbb{Q}_p)^{(0)} = E(\mathbb{Q}_p)$. By Corollary 8.12, the torsion subgroup of $E(\mathbb{Q})$ has trivial intersection with $E(\mathbb{Q}_p)^{(1)} = \ker\left(E(\mathbb{Q}_p) \to \overline{E}(\mathbb{F}_p)\right)$. ∎

Proof of Corollary 8.11.

1. Induction on n, where $n = 1$ is obvious. If the first statement $|\mathrm{u}(nP) - n\mathrm{u}(P)|_p \le |\mathrm{u}(P)|_p^5$ holds, then $|\mathrm{u}(nP)|_p \le |\mathrm{u}(P)|_p$, otherwise $|\mathrm{u}(nP)|_p > |\mathrm{u}(P)|_p$, and then $|\mathrm{u}(P)|_p^5 \ge |\mathrm{u}(nP) - n\mathrm{u}(P)|_p = |\mathrm{u}(nP)|_p > |\mathrm{u}(P)|_p$ but $|\mathrm{u}(P)|_p \le 1/p$, a contradiction. So we just need to assume both statements for n, and deduce the first statement for $n+1$. By Lemma 8.10,
$$\begin{aligned}|\mathrm{u}((n+1)P) - (n+1)\mathrm{u}(P)|_p &\le \max\left(|\mathrm{u}((n+1)P) - \mathrm{u}(nP) - \mathrm{u}(P)|_p, |\mathrm{u}(nP) - n\mathrm{u}(P)|_p\right) \\ &\le \max\left(|\mathrm{u}(nP)|_p^5, |\mathrm{u}(P)|_p^5\right) = |\mathrm{u}(P)|_p^5,\end{aligned}$$
by induction.
2. We have $|n\mathrm{u}(P)|_p = |\mathrm{u}(P)|_p$ and $|\mathrm{u}(nP) - n\mathrm{u}(P)|_p \le |\mathrm{u}(P)|_p^5 < |n\mathrm{u}(P)|_p$.
3. Same as 2, because $|\mathrm{u}(P)|_p^5 < |p|_p |\mathrm{u}(P)|_p$.
4. Induction on n. If $(n, p) = 1$, then 2. Otherwise $|\mathrm{u}(nP)|_p = |p|_p |\mathrm{u}((n/p)P)|_p$ by 3, and $|\mathrm{u}((n/p)P)|_p = |n/p|_p |\mathrm{u}(P)|_p$ by induction.

$\square$

Remark 8.14. Just having coefficients in $\mathbb{Z}_p$ is not enough in general, and need to actually be in the special form above. General elliptic curve is
$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$
and if we are over $\mathbb{Q}_p$ for $p \ge 5$ and all the $a_i \in \mathbb{Z}$ then completing the square and cube does not introduce any denominators. But $y^2 + xy = x^3 + 4x + 1$ is an elliptic curve over $\mathbb{Q}_2$ and $\left(-\frac{1}{4}, \frac{1}{8}\right)$ is a point of order two on this curve even though it has non-integral coefficients. Set $Y = y + x/2$ and then we get $x^2/4$ which we fix by multiplying x by four and Y by eight. More generally, for an elliptic curve over a finite extension of $\mathbb{Q}_p$ there can be torsion if there are elements u in the maximal ideal with $|u|^5 > |p|$. The argument shows that there is never any n-torsion in $E(\mathbb{Q}_p)^{(1)}$ if $p \nmid n$ but there can be p-torsion if one works over a general complete field of characteristic zero such that $|p| < 1$.

8.4 Example

Example 8.15. Let $y^2 = x^3 + 105^{10^{10}}x + 3$. Neither five nor seven divides $\Delta = 4\left(105^{10^{10}}\right)^3 + 27(3)^2$.

- Modulo five, $y^2 = x^3 + 3$. The squares modulo five are $0, 1, 4$, so

x	0	1	2	3	4
x^3+3	3	4	1	0	2
$\#y$	0	2	2	1	0

  Then $\#E(\mathbb{F}_5) = 5 + 1 = 6$, so $E(\mathbb{F}_5) \cong \mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.

- Modulo seven, $y^2 = x^3 + 3$. The squares modulo seven are $0, 1, 2, 4$, so

x	0	1	2	3	4	5	6
x^3+3	3	4	4	2	4	2	2
$\#y$	0	2	2	2	2	2	2

  Then $\#E(\mathbb{F}_7) = 12 + 1 = 13$, so $E(\mathbb{F}_7) \cong \mathbb{Z}/13\mathbb{Z}$.

So the torsion subgroup is just $\{0\}$.

Lecture 20 is a problems class. Lecture 20 Monday 18/11/19

9 The weak Mordell-Weil theorem for $E(\mathbb{Q})$

Lecture 21 Tuesday 19/11/19

The weak Mordell-Weil theorem is that $E(\mathbb{Q})/2E(\mathbb{Q})$ is a finite group. Assume that E can be written as

$$y^2 = (x - e_1)(x - e_2)(x - e_3), \qquad e_1, e_2, e_3 \in \mathbb{Q},$$

if and only if the 2-torsion subgroup of $E(\mathbb{Q})$ has order four. These are the points $\mathcal{O}, (e_1, 0), (e_2, 0), (e_3, 0)$.

9.1 Example

Example 9.1. Let $y^2 = x^3 - x = x(x-1)(x+1)$.

- Assume $y \neq 0$. Write

  $$x - 1 = au^2, \qquad x = bv^2, \qquad x + 1 = cw^2, \qquad u, v, w \in \mathbb{Q},$$

  for $a, b, c \in \mathbb{Z}$ square-free. For example, $\frac{10}{9} = 10\left(\frac{1}{3}\right)^2$, $27 = 3(3)^2$, and $-5 = -5(1)^2$.

- Claim that $a, b, c \in \{\pm 1, \pm 2\}$. Need to show that if $p > 2$ is prime, then $p \nmid abc$. Since $y^2 = x(x-1)(x+1) = abc(uvw)^2$, abc is a square. If $p \mid abc$, then p divides at least two of a, b, c. If $|x|_p > 1$, then $|x|_p = |x \pm 1|_p$. Then $|y|_p^2 = |x|_p |x-1|_p |x+1|_p = |x|_p^3$, so $|x|_p = |x \pm 1|_p = p^{2n}$ for some $n \geq 1$. Since $|b|_p = \left|x/u^2\right|_p = |x|_p / |u|_p^2 = \left(p^n / |u|_p\right)^2$ for example, $|a|_p = |b|_p = |c|_p = 1$, a contradiction. So $|x|_p \leq 1$. Then $|x \pm 1|_p \leq 1$, and if $p \mid abc$, then p divides at least two of $x, x-1, x+1$, and the difference of these two is either one or two. So $p \mid 2$.

- Since abc is a square, c is determined by a and b. For example, if $a = -1$ and $b = -2$, then $c = 2$. So there are at most sixteen possibilities for (a, b, c). Since the product of $x + 1 > x > x - 1$ is a square, either all three are positive, or $x + 1 > 0 > x > x - 1$. This leaves eight possibilities,

  $$(a, b, c) \in \{(1,1,1), (1,2,2), (2,1,2), (2,2,1), (-1,-1,1), (-1,-2,2), (-2,-1,2), (-2,-2,1)\}.$$

- Assume $y = 0$. Then $(0,0)$ and $(\pm 1, 0)$ are also solutions of $y^2 = x^3 - x$.

  - If $x = 0$, then $-1 = au^2$ and $1 = cw^2$, so $a = -1$ and $c = 1$. Then abc is a square, so $b = -1$.
  - If $x = -1$, then $-2 = au^2$ and $-1 = bv^2$, so $a = -2$ and $b = -1$. Similarly, $c = 2$.
  - If $x = 1$, then $1 = bv^2$ and $2 = cw^2$, so $b = 1$ and $c = 2$. Similarly, $a = 2$.

  Finally, $\mathcal{O}$ corresponds to $a = 1$, $b = 1$, and $c = 1$, so

  $$(a, b, c) \in \{(1,1,1), (2,1,2), (-1,-1,1), (-2,-1,2)\}.$$

- Claim that there are no solutions to $y^2 = x^3 - x$ which give $(a, b, c) = (1, 2, 2)$. Let $x - 1 = u^2$, $x = 2v^2$, and $x + 1 = 2w^2$, so $u^2 - 2v^2 = -1$ and $2w^2 - 2v^2 = 1$. Want to show that these have no solutions with $u, v, w \in \mathbb{Q}$. Writing $u = U/Z$, $v = V/Z$, and $w = W/Z$, it is enough to show that there are no non-zero solutions in $\mathbb{Z}$ to $U^2 - 2V^2 = -Z^2$ and $2W^2 - 2V^2 = Z^2$. Then $2 \mid U, V, W, Z$. Repeating, $U = V = W = Z = 0$. Similar arguments work for the other three possibilities.

We will see next time that in fact we have defined a group homomorphism

$$\begin{array}{rcccl} \delta & : & E(\mathbb{Q}) & \longrightarrow & \{\pm 1, \pm 2\}^3 \\ & & (x, y) & \longmapsto & (a, b, c) \\ & & \mathcal{O} & \longmapsto & (1, 1, 1) \end{array},$$

where $\mathbb{Q}^\times / (\mathbb{Q}^\times)^2$ is a group, and $\{\pm 1, \pm 2\} = \left\{\pm (\mathbb{Q}^\times)^2, \pm 2 (\mathbb{Q}^\times)^2\right\}$ is a subgroup under multiplication. For example, $(2)(2) = 1$, $(2)(-2) = -1$, and $(-2)(-2) = -1$. In particular, the image of δ is a subgroup of $\{\pm 1, \pm 2\}^3$, so it has order a power of two. Then $\delta(2P) = 1$ for any $P \in E(\mathbb{Q})$, because $\delta(2P) = \delta(P)^2 = 1$. In fact, we will show that the induced homomorphism $E(\mathbb{Q})/2E(\mathbb{Q}) \to \{\pm 1, \pm 2\}^3$ is injective. So the calculation we made shows that $E(\mathbb{Q})/2E(\mathbb{Q})$ has order four. In fact $E(\mathbb{Q}) = \{\mathcal{O}, (0,0), (\pm 1, 0)\}$.

9.2 The 2-descent isogeny

Lecture 22 Thursday 21/11/19

Theorem 9.2. *Let K be a field of characteristic not two, and let E be the elliptic curve*

$$y^2 = (x - e_1)(x - e_2)(x - e_3),$$

for $e_1, e_2, e_3 \in K$ distinct. Define

$$\begin{array}{rrcll} \delta & : & E(K) & \longrightarrow & \left(K^\times / (K^\times)^2\right)^3 \\ & & \mathcal{O} & \longmapsto & (1,1,1) \\ & & T_1 = (e_1, 0) & \longmapsto & ((e_1 - e_2)(e_1 - e_3), e_1 - e_2, e_1 - e_3) \\ & & T_2 = (e_2, 0) & \longmapsto & (e_2 - e_1, (e_2 - e_1)(e_2 - e_3), e_2 - e_3) \\ & & T_3 = (e_3, 0) & \longmapsto & (e_3 - e_1, e_3 - e_2, (e_3 - e_1)(e_3 - e_2)) \\ & & (x, y) & \longmapsto & (x - e_1, x - e_2, x - e_3), \qquad y \ne 0 \end{array}.$$

Then

1. *δ is a group homomorphism.*
2. $\ker \delta = 2E(K)$.

Lemma 9.3. *Let K and E as in Theorem 9.2. Let $P = (x, y) \in E(K)$. If all $x - e_i \in K^2$ for $i = 1, 2, 3$, then there exists $Q \in E(K)$ such that $P = 2Q$.*

Proof. Write $x - e_i = t_i^2$ for $i = 1, 2, 3$ for $t_i \in K$. Then $y^2 = t_1^2 t_2^2 t_3^2 = (t_1 t_2 t_3)^2$. Assume, after possibly changing the sign of some t_i, that $y = t_1 t_2 t_3$. Set

$$Q = (x_0, y_0), \qquad x_0 = x + t_1 t_2 + t_2 t_3 + t_3 t_1, \qquad y_0 = (t_1 + t_2)(t_2 + t_3)(t_3 + t_1).$$

Need to check that $Q \in E(K)$, and that $2Q = P$. Then

$$x_0 - e_1 = (x - e_1) + t_1 t_2 + t_2 t_3 + t_3 t_1 = t_1^2 + t_1 t_2 + t_2 t_3 + t_3 t_1 = (t_1 + t_2)(t_1 + t_3).$$

Similarly $x_0 - e_2 = (t_2 + t_3)(t_2 + t_1)$ and $x_0 - e_3 = (t_3 + t_1)(t_3 + t_2)$. So

$$(x_0 - e_1)(x_0 - e_2)(x_0 - e_3) = (t_1 + t_2)^2 (t_2 + t_3)^2 (t_3 + t_1)^2 = y_0^2,$$

that is $Q \in E(K)$. To compute $2Q$, we need to find the tangent line $y = mx + c$. Write $f(x) = (x - e_1)(x - e_2)(x - e_3)$, then

$$\begin{aligned} m = \frac{f'(x_0)}{2y_0} &= \frac{(x_0 - e_2)(x_0 - e_3) + (x_0 - e_3)(x_0 - e_1) + (x_0 - e_1)(x_0 - e_2)}{2y_0} \\ &= \frac{(t_1 + t_2)(t_2 + t_3)(t_3 + t_1)((t_1 + t_2) + (t_2 + t_3) + (t_3 + t_1))}{2y_0} = t_1 + t_2 + t_3. \end{aligned}$$

Then

$$m(x_0 - x) = (t_1 + t_2 + t_3)(t_1 t_2 + t_2 t_3 + t_3 t_1) = (t_1 + t_2)(t_2 + t_3)(t_3 + t_1) + t_1 t_2 t_3 = y_0 + y.$$

So the point $(x, -y)$ also lies on the tangent line to E at (x_0, y_0). So $-2Q = (x, -y)$, that is $2Q = (x, y) = P$. ☐

Proof of Theorem 9.2. Once we know that δ is a group homomorphism, then $2E(K) \subset \ker \delta$, because $\delta(2P) = \delta(P)^2 = 1$. Lemma 9.3 implies that $\ker \delta \subset 2E(K)$. So we have 2. Need to prove that if $P_1 + P_2 + P_3 = \mathcal{O}$, then $\delta(P_1)\delta(P_2)\delta(P_3) = 1$. Note that by definition, $\delta(P) = \delta(-P)$. Note that by definition, $\delta(P) = \delta(-P)$. If $P_1 = P_2 = P_3 = \mathcal{O}$, then obvious. If $P_1 = \mathcal{O}$ and $P_2 \ne \mathcal{O}$, then $P_2 + P_3 = \mathcal{O}$, and

$$\delta(P_1)\delta(P_2)\delta(P_3) = \delta(P_2)\delta(P_3) = \delta(P_2)\delta(-P_2) = \delta(P_2)^2 = 1.$$

By symmetry assume none of P_1, P_2, P_3 is $\mathcal{O}$. Otherwise P_1, P_2, P_3 all lie on some line $Y = mX + c$. Write $P_i = (x_i, y_i)$.

- Assume firstly that $2P_i \ne \mathcal{O}$ for $i = 1, 2, 3$, that is $x_i \ne e_1, e_2, e_3$. Then
$$(x - x_1)(x - x_2)(x - x_3) = (x - e_1)(x - e_2)(x - e_3) - (mx + c)^2.$$
Substituting $x = e_1$, $(e_1 - x_1)(e_1 - x_2)(e_1 - x_3) = -(me_1 + c)^2$, that is
$$(x_1 - e_1)(x_2 - e_1)(x_3 - e_1) = (me_1 + c)^2 \in \left(K^\times\right)^2.$$
Similarly $(x_1 - e_2)(x_2 - e_2)(x_3 - e_2) \in (K^\times)^2$ and $(x_1 - e_3)(x_2 - e_3)(x_3 - e_3) \in (K^\times)^2$. That is, $\delta(P_1)\delta(P_2)\delta(P_3) = 1$.

- Now assume that one of $2P_1, 2P_2, 2P_3$ is $\mathcal{O}$. Without loss of generality $P_1 = T_1 = (e_1, 0)$. Assume that $2P_2, 2P_3 \ne \mathcal{O}$. The calculation above shows that $\delta(P_1)\delta(P_2)\delta(P_3) \in K^\times/(K^\times)^2 \times 1 \times 1$. By definition, $\operatorname{im}\delta \subset \{(a, b, c) \mid abc = 1\}$. So $\delta(P_1)\delta(P_2)\delta(P_3) = 1$ in this case.

- Now assume that at least two of P_1, P_2, P_3 are equal to T_1, T_2, T_3. The only possibility with $P_1 + P_2 + P_3 = \mathcal{O}$ but $P_i \ne \mathcal{O}$ is $\{P_1, P_2, P_3\} = \{T_1, T_2, T_3\}$. Then $\delta(P_1)\delta(P_2)\delta(P_3) = \delta(T_1)\delta(T_2)\delta(T_3) = 1$.

$\square$

Remark 9.4. We have
$$\delta : E(K)/2E(K) \xrightarrow{\sim} \operatorname{im}\delta \subset \left\{(a, b, c) \in \left(K^\times/\left(K^\times\right)^2\right)^3 \;\middle|\; abc = 1\right\} \subset \left(K^\times/\left(K^\times\right)^2\right)^3.$$

Example. $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ is not a finite group, since for each prime p, $p \in \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$, and these are linearly independent, as elements of $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$, which is an $\mathbb{F}_2$-vector space.

9.3 The weak Mordell-Weil theorem

Lecture 23 Monday 25/11/19

Let
$$y^2 = (x - e_1)(x - e_2)(x - e_3), \qquad e_1, e_2, e_3 \in \mathbb{Z}.$$

Proposition 9.5. $\operatorname{im}\delta$ *is finite, and more precisely,*
$$\operatorname{im}\delta \subset \mathbb{Q}(S, 2)^3, \qquad S = \{p \text{ prime} \mid p \mid (e_1 - e_2)(e_2 - e_3)(e_3 - e_1)\},$$
where $\mathbb{Q}(S, 2) \subset \mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ is the subgroup generated by the elements of S, that is the coset representatives generated by square-free integers only divisible by primes in S.

Proof. Let p be prime, and consider a point $(x, y) \in E(\mathbb{Q})$. Then $y^2 = (x - e_1)(x - e_2)(x - e_3)$, so $|y|_p^2 = |x - e_1|_p |x - e_2|_p |x - e_3|_p$. Either

1. $|x - e_1|_p, |x - e_2|_p, |x - e_3|_p \in p^{2\mathbb{Z}}$, or
2. exactly one of $|x - e_1|_p, |x - e_2|_p, |x - e_3|_p \in p^{2\mathbb{Z}}$.

We need to show in case 2 we have $p \in S$. So suppose that 2 holds. If $|x|_p > 1$, then $|x - e_i|_p = |x|_p$ for $i = 1, 2, 3$, because $|e_i|_p \le 1 < |x|_p$, a contradiction. So $|x|_p \le 1$, and $|x - e_i|_p \le 1$ for $i = 1, 2, 3$. Suppose that $|x - e_1|_p, |x - e_2|_p \notin p^{2\mathbb{Z}}$. Then $|x - e_1|_p, |x - e_2|_p < 1$, so $|e_1 - e_2|_p \le \max\left(|x - e_1|_p, |x - e_2|_p\right) < 1$, that is $p \mid (e_1 - e_2)$. We are done by symmetry. $\square$

Theorem 9.6 (Weak Mordell-Weil theorem)**.** $E(\mathbb{Q})/2E(\mathbb{Q})$ *is finite.*

Proof. $\delta : E(\mathbb{Q})/2E(\mathbb{Q}) \hookrightarrow \mathbb{Q}(S, 2)^3$, and $\mathbb{Q}(S, 2)$ is finite. $\square$

In fact $\#\operatorname{im}\delta \ge 4$ for any E, because we have four points coming from $\mathcal{O}$ and $(e_i, 0)$ for $i = 1, 2, 3$. If $s = \#S$, so $s \ge 1$, because $2 \in S$, then $\#\mathbb{Q}(S, 2) = 2^{s+1}$. So $\#\operatorname{im}\delta \le \left(2^{s+1}\right)^3 = 8^{s+1}$. By definition, if $\delta(P) = (a, b, c)$, then $abc = 1$. So $\#\operatorname{im}\delta \le \left(2^{s+1}\right)^2 = 4^{s+1}$. Considering the signs of $x - e_1, x - e_2, x - e_3$, and the condition that their product is a square, get $\#\operatorname{im}\delta \le 2^{2s+1}$.

Corollary 9.7. $\#\operatorname{im}\delta \le 2^{1+2\#S}$.

Example 9.8. Let $y^2 = x^3 - x$. We saw that $\operatorname{im}\delta$ has order four.

9.4 The rank of $E(\mathbb{Q})$

Now assume that we know the Mordell-Weil theorem, so that $E(\mathbb{Q}) \cong T \times \mathbb{Z}^r$, where T is the finite torsion subgroup. Then $E(\mathbb{Q})/2E(\mathbb{Q}) \cong T/2T \times (\mathbb{Z}/2\mathbb{Z})^r$. Then $\#\operatorname{im}\delta = \#(E(\mathbb{Q})/2E(\mathbb{Q})) = \#(T/2T) \times 2^r$.

Lemma 9.9. *For any finite abelian group T, $\#T/2T = \#T[2]$, where $T[2] = \{x \in T \mid 2x = 0\}$.*

Proof. Consider the map

$$\begin{array}{rcrcl} 2 & : & T & \longrightarrow & T \\ & & x & \longmapsto & 2x \end{array}.$$

This is a group homomorphism with kernel $T[2]$ and image $2T$. So by the first isomorphism theorem, $T/T[2] \cong 2T$. Now computing orders, $\#T/\#T[2] = \#2T$, that is $\#T/\#2T = \#T[2]$. ☐

Thus

$$0 \to T[2] \to T \xrightarrow{2} T \to T/2T \to 0$$

is exact. Going back to E, if $y^2 = (x-e_1)(x-e_2)(x-e_3)$, and T is the torsion subgroup, we have

$$\#T/2T = \#T[2] = \#\{P \in E(\mathbb{Q}) \mid 2P = \mathcal{O}\} = \#\{\mathcal{O}, (e_1,0), (e_2,0), (e_3,0)\} = 4.$$

So $2^r = \#\operatorname{im}\delta/4$.

Example. If E is $y^2 = x^3 - x$, then $2^r = 4/4 = 1$ so $r = 0$. So $E(\mathbb{Q})$ is finite.

Lecture 24 Tuesday 26/11/19

Example 9.10. Let E be $y^2 = (x-5)(x-6)(x+11)$. Then $\Delta = (-5-(-6))^2(-5-11)^2(11-(-6))^2 = 2^8 17^2$. Compute $E(\mathbb{Q})_{\text{tors}}$ and $E(\mathbb{Q})/2E(\mathbb{Q})$.

- The only primes dividing Δ are two and seventeen. Modulo three, $y^2 = x(x+1)(x-1) = x^3 - x$. This has solutions $(0,0), (1,0), (-1,0)$ in $\mathbb{F}_3$, so $E(\mathbb{F}_3)$ has four points, and $E(\mathbb{F}_3) \cong (\mathbb{Z}/2\mathbb{Z})^2$. Then $E(\mathbb{Q})_{\text{tors}} \hookrightarrow E(\mathbb{F}_3) \cong (\mathbb{Z}/2\mathbb{Z})^2$. So

$$E(\mathbb{Q})_{\text{tors}} = \{\mathcal{O}, (5,0), (6,0), (-11,0)\}.$$

- Let

$$\begin{array}{rcrcll} \delta & : & E(\mathbb{Q})/2E(\mathbb{Q}) & \longrightarrow & \left(\mathbb{Q}^\times/(\mathbb{Q}^\times)^2\right)^2 & \\ & & (x,y) & \longmapsto & (x-5, x-6, x+11), & y \neq 0 \end{array}.$$

Then $\operatorname{im}\delta \subset \left\{(a,b,c) \in \{\pm1, \pm2, \pm17, \pm34\}^3 \,\middle|\, abc = 1\right\}$. From now on, regard δ as

$$\begin{array}{rcrcl} \delta & : & E(\mathbb{Q})/2E(\mathbb{Q}) & \longrightarrow & \left(\mathbb{Q}^\times/(\mathbb{Q}^\times)^2\right)^2 \\ & & (x,y) & \longmapsto & (x-5, x-6) \\ & & \mathcal{O} & \longmapsto & (1,1) \\ & & (5,0) & \longmapsto & (-1,-1) \\ & & (6,0) & \longmapsto & (1,17) \\ & & (-11,0) & \longmapsto & (-1,-17) \end{array}.$$

To find $\operatorname{im}\delta$, we need to solve the equations

$$x - 5 = b_1 u^2, \qquad x - 6 = b_2 v^2, \qquad x + 11 = b_3 w^2, \qquad u, v, w \in \mathbb{Q}^\times,$$

where $b_1, b_2, b_3 \in \{\pm1, \pm2, \pm17, \pm34\}$ such that $b_1 b_2 b_3 = 1$, so

$$b_1 u^2 - b_2 v^2 = 1, \qquad b_1 b_2 w^2 - b_1 u^2 = 16.$$

For these to have solutions in $\mathbb{R}$, need $b_1 b_2 > 0$. Also, $\delta((5,0)) = (-1,-1)$, so if $(b_1, b_2) \in \operatorname{im}\delta$, then $(-b_1, -b_2) \in \operatorname{im}\delta$. So it suffices to determine which $(b_1, b_2) \in \operatorname{im}\delta$ for $b_1, b_2 > 0$.

Let ✓ be $(b_1, b_2) \in \operatorname{im} \delta$ and × be $(b_1, b_2) \notin \operatorname{im} \delta$.

- $\delta(\mathcal{O}) = (1,1)$ and $\delta((6,0)) = (1,17)$, so $(1,1), (1,17) \in \operatorname{im}\delta$. Then

$b_1 \backslash b_2$	1	2	17	34
1	✓		✓	
2				
17				
34				

.

- If $(b_1, b_2) = (1,2)$, then $u^2 - 2v^2 = 1$ and $2w^2 - u^2 = 16$, so $U^2 - 2V^2 = Z^2$ and $2W^2 - U^2 = 16Z^2$, so $2 \mid U, V, W, Z$, so $U = V = W = Z = 0$, a contradiction, so $(1,2) \notin \operatorname{im}\delta$, so $(1,34) = (1,2)(1,17) \notin \operatorname{im}\delta$. Then

$b_1 \backslash b_2$	1	2	17	34
1	✓	×	✓	×
2				
17				
34				

.

- This argument only used $2 \mid b_2$ and $2 \nmid b_1$, so $(17,2), (17,34) \notin \operatorname{im}\delta$. Then

$b_1 \backslash b_2$	1	2	17	34
1	✓	×	✓	×
2				
17		×		×
34				

.

- If $(b_1, b_2) = (2,1)$, then $2u^2 - v^2 = 1$ and $w^2 - u^2 = 8$ has a solution $u = v = 1$ and $w = 3$, so $(2,1) \in \operatorname{im}\delta$, so $x - 5 = 2u^2 = 2$ and $y^2 = 36 = 6^2$, so $(x,y) = (7, \pm 6)$, so $(2,17) = (2,1)(1,17) \in \operatorname{im}\delta$ and $(2,2), (2,34), (34,2), (34,34) \notin \operatorname{im}\delta$. Then

$b_1 \backslash b_2$	1	2	17	34
1	✓	×	✓	×
2	✓	×	✓	×
17		×		×
34		×		×

.

- If $(b_1, b_2) = (17,1)$, then $17u^2 - v^2 = 1$ and $17w^2 - 17u^2 = 16$, so $17U^2 - V^2 = Z^2$ and $17W^2 - 17U^2 = 16Z^2$, so $17 \mid U, V, W, Z$, so $U = V = W = Z = 0$, a contradiction, so $(17,1) \notin \operatorname{im}\delta$, so $(17,17) = (1,17)(17,1) \notin \operatorname{im}\delta$. Then

$b_1 \backslash b_2$	1	2	17	34
1	✓	×	✓	×
2	✓	×	✓	×
17	×	×	×	×
34		×		×

.

- This argument only used $17 \mid b_1$ and $17 \nmid b_2$, so $(34,1), (34,17) \notin \operatorname{im}\delta$. Then

$b_1 \backslash b_2$	1	2	17	34
1	✓	×	✓	×
2	✓	×	✓	×
17	×	×	×	×
34	×	×	×	×

.

Thus $\# \operatorname{im}\delta = 8$ and E has rank one, since $2^{2+r} = 8$, and $(7, \pm 6) \in E(\mathbb{Q})$ is not torsion.

Lecture 25 is a problems class. Lecture 25 Thursday 28/11/19

10 The full Mordell-Weil theorem for $E(\mathbb{Q})$

Lecture 26 Monday 02/12/19

The Mordell-Weil theorem is that if $E(\mathbb{Q})$ is an elliptic curve, then $E(\mathbb{Q})$ is a finitely generated abelian group. So far, if all the 2-torsion points of E are defined over $\mathbb{Q}$, that is we can write E as $y^2 = (x-e_1)(x-e_2)(x-e_3)$ for $e_1, e_2, e_3 \in \mathbb{Q}$, then $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite, by the weak Mordell-Weil theorem. We do not need the assumption that $y^2 = (x-e_1)(x-e_2)(x-e_3)$ for $e_i \in \mathbb{Q}$ for the rest of the argument. From now, assume that

$$y^2 = x^3 + Ax + B, \qquad A, B \in \mathbb{Z}$$

is E, and $E(\mathbb{Q})/2E(\mathbb{Q})$ is finite.

Note. There are many abelian groups G with $G/2G$ finite but G not finitely generated.

Example. $G = (\mathbb{Q}, +)$ and $G/2G = \{0\}$.

What we need to show, morally, is that if $P \in E(\mathbb{Q})$, then there is a bound on the biggest power of two such that there exists $Q \in E(\mathbb{Q})$ with $2^n Q = P$. However, if P is a 3-torsion point, then $4P = P$, so $16P = 4(4P) = 4P = P$, etc. The idea is to follow what we did for $x^3 + y^3 = 9$, and show that usually $2P$ is more complicated than P.

Definition 10.1. Let $q \in \mathbb{Q}$, and write $q = l/m$ for $l, m \in \mathbb{Z}$ such that $(l,m) = 1$. The **height** of q is

$$\mathrm{H}(q) = \max(|l|, |m|).$$

Example. $\mathrm{H}\left(-\frac{3}{5}\right) = 5$.

Definition 10.2. If $(x,y) \in E(\mathbb{Q})$, set

$$\mathrm{H}((x,y)) = \mathrm{H}(x).$$

Set

$$\mathrm{h}(P) = \begin{cases} \log \mathrm{H}((x,y)) & P = (x,y) \\ 0 & P = \mathcal{O} \end{cases}.$$

10.1 The three key lemmas

Lemma 10.3. *For any $Q \in E(\mathbb{Q})$, there exists $C = C(Q) \in \mathbb{R}$ such that for all $P \in E(\mathbb{Q})$,*

$$\mathrm{h}(P+Q) \le 2\mathrm{h}(P) + C.$$

Proof. Without loss of generality $P \ne \mathcal{O}, \pm Q$. If $Q = \mathcal{O}$, then we need to find C such that $\mathrm{h}(P) \ge -C$ for all P, but $\mathrm{h}(P) = \log \mathrm{H}(P) \ge \log 1 = 0$. So $C = 0$ works. So we may assume that $P, Q \ne \mathcal{O}$ and $P \ne \pm Q$. That is, P and Q are distinct, and $-(P+Q) \ne \mathcal{O}$. We showed that if $(x,y) \in E(\mathbb{Q})$ and $|x|_p > 1$ for some p, then there exists $n \ge 1$ such that $|x|_p = p^{2n}$ and $|y|_p = p^{3n}$. Then $p^{2n}x, p^{3n}y \in \mathbb{Z}$, and $p \nmid p^{2n}x, p^{3n}y$. Thus we can write $(x,y) = (e/g^2, f/g^2)$ for $e, f, g \in \mathbb{Z}$ such that $(g, ef) = 1$, by setting $g = \prod_{|x|_p > 1} p^n$. So we can write

$$P = \left(\frac{a}{d^2}, \frac{b}{d^3}\right), \qquad Q = \left(\frac{e}{g^2}, \frac{f}{g^3}\right), \qquad a, b, d, e, f, g \in \mathbb{Z}, \qquad (d, ab) = (g, ef) = 1.$$

So $\mathrm{H}(P) = \max(|a|, d^2)$. Let the line through P and Q be $y = mx + c$. If $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$, then $m = (y_Q - y_P)/(x_Q - x_P)$, and if $P + Q = (x_3, y_3)$, then x_P, x_Q, x_3 are the three roots of $(mx+c)^2 = x^3 + Ax + B$. So

$$x_P + x_Q + x_3 = -m^2 = -\left(\frac{y_Q - y_P}{x_Q - x_P}\right)^2 = \frac{\left(x_Q^3 + Ax_Q + B\right) + \left(x_P^3 + Ax_P + B\right) - 2y_P y_Q}{(x_Q - x_P)^2},$$

so

$$x_3 = \frac{\left(A + x_P^2\right) x_Q + \left(A + x_Q^2\right) x_P - 2y_P y_Q + 2B}{(x_Q - x_P)^2}.$$

Substituting $x_P = a/d^2$ and $y_P = b/d^3$, and $x_Q = e/g^2$ and $y_Q = f/g^3$, and clearing powers of d and g, get $x_3 = N/D$, where

$$N = \left(2Bd^4 + Aad^2\right) g^4 + \left(Aed^4 + ea^2\right) g^2 - 2bfdg + e^2ad^2, \qquad D = a^2g^4 - 2ead^2g^2 + e^2g^4,$$

so $\mathrm{H}(P+Q) = \mathrm{H}(x_3) \le \max(|N|, |D|)$. Since $Q = \left(e/g^2, f/g^3\right)$ is fixed, so are e, f, g, as are A and B. Want $\mathrm{h}(P+Q) \le 2\mathrm{h}(P) + C$, that is $\mathrm{H}(P+Q) \le \mathrm{H}(P)^2 e^C$. That is, it suffices to prove

$$\max(|N|, |D|) \le K \max\left(a^2, d^4\right),$$

for some $K > 0$ independent of a, b, d. Every term in N or D can be bounded by $K' \max\left(a^2, d^4\right)$, except $-2bfdg$. To deal with this term, since $\left(a/d^2, b/d^3\right) \in E(\mathbb{Q})$, we have $\left(b/d^3\right)^2 = \left(a/d^2\right)^3 + A\left(a/d^2\right) + B$, that is $b^2 = a^3 + Aad^4 + Bd^6$. That is, $b^2d^2 = a^3d^2 + Aad^6 + Bd^8 \le K''^2 \max\left(a^2, d^4\right)^2$, that is $bd \le K'' \max\left(a^2, d^4\right)$, as required. ☐

Lecture 27 Tuesday 03/12/19

Lemma 10.4. *There exists $D \in \mathbb{R}$, depending only on E, such that for all $P \in E(\mathbb{Q})$,*

$$\mathrm{h}(2P) \ge 4\mathrm{h}(P) - D.$$

Proof. If $P = (x_0, y_0)$, then the tangent at P is $y = mx + c$, where $m = \left(3x_0^2 + A\right)/2y_0$. If $2P = (x_d, y_d)$, then

$$x_d = m^2 - 2x_0 = \frac{x_0^4 - 2Ax_0^2 - 8Bx_0 + A^2}{4\left(x_0^3 + Ax_0 + B\right)},$$

since $y_0^2 = x_0^3 + Ax_0 + B$. Write $x_0 = s/t$ such that $(s, t) = 1$, so $\mathrm{H}(P) = \max(|s|, |t|)$ and $x_d = f/g$, where

$$f = s^4 - 2As^2t^2 - 8Bst^3 + A^2t^4, \qquad g = 4\left(s^3t + Ast^3 + Bt^4\right).$$

Then

$$Cf + Dg = \left(16A^3 + 108B^2\right) t^7 = 4\Delta t^7,$$

where

$$C = 12s^2t + 16At^3 \in \mathbb{Z}[s, t], \qquad D = -3s^3 + 5Ast^2 + 27Bt^3 \in \mathbb{Z}[s, t]$$

are homogeneous of degree three, and

$$Ef + Fg = \left(16A^3 + 108B^2\right) s^7 = 4\Delta s^7,$$

where

$$E = 4\left(4A^3 + 27B^2\right) s^3 - 4A^2Bs^2t + 4A\left(3A^3 + 22B^2\right) st^2 + 12B\left(A^3 + 8B^2\right) t^3 \in \mathbb{Z}[s, t],$$

$$F = A^2Bs^3 + A\left(5A^3 + 32B^2\right) s^2t + 2B\left(13A^3 + 96B^2\right) st^2 - 3A^2\left(A^3 + 8B^2\right) t^3 \in \mathbb{Z}[s, t]$$

are homogeneous of degree three. In particular, $(f, g) \mid \left(4\Delta s^7, 4\Delta t^7\right) = 4\Delta$, which only depends on E. So $\mathrm{H}(2P) \ge \max(|f|, |g|)/4\Delta$. Want $\mathrm{h}(2P) \ge 4\mathrm{h}(P) - D$, that is $\mathrm{H}(2P) \ge \mathrm{H}(P)^4 e^{-D}$. That is,

$$\mathrm{H}(P)^4 \le K\mathrm{H}(2P),$$

for some K. Then

$$|t|^7 = \frac{1}{4\Delta}|Cf + Dg| \le \frac{1}{4\Delta}(|C||f| + |D||g|) \le K' \max(|s|, |t|)^3 \max(|f|, |g|),$$

for K' some constant. Similarly $|s|^7 \le K'' \max(|s|, |t|)^3 \max(|f|, |g|)$ for K'' some constant. So $\max(|s|, |t|)^7 \le K''' \max(|s|, |t|)^3 \max(|f|, |g|)$ for some K''', that is $\max(|s|, |t|)^4 \le K''' \max(|f|, |g|)$, that is $\mathrm{H}(P)^4 \le K\mathrm{H}(2P)$ for some K. ☐

Lemma 10.5. *If $K \in \mathbb{R}$ then there are only finitely many $P \in E(\mathbb{Q})$ with $\mathrm{h}(P) \le K$.*

Proof. $\mathrm{h}(P) \le K$ if and only if $\mathrm{H}(P) \le e^K$, if and only if $P = (x, y)$ with $x = l/m$ such that $|l|, |m| \le e^K$. So only finitely many l and m, that is finitely many x, that is finitely many P. ☐

10.2 The height machine

Proposition 10.6. *Let A be an abelian group and $h : A \to \mathbb{R}$. Assume that*

1. *for all $Q \in A$, there exists $C(Q) \in \mathbb{R}$ such that for all $P \in A$,*
$$h(P+Q) \le 2h(P) + C(Q),$$
2. *there exists $D \in \mathbb{R}$ such that for all $P \in A$,*
$$h(2P) \ge 4h(P) - D,$$
3. *if $K \in \mathbb{R}$, then $\{a \in A \mid h(a) \le K\}$ is finite, and*
4. *$A/2A$ is finite.*

Then A is finitely generated.

Proof. Write $Q_1, \dots, Q_r \in A$ for a set of representatives of $A/2A$, that is
$$A/2A = \left\{\overline{Q_1}, \dots, \overline{Q_r}\right\}, \qquad \overline{Q_i} = Q_i + 2A,$$
by 4. Let $C_1 = \max C(Q_i)$. Let $C_2 = (C_1 + D)/2$. Let
$$S = \{a \in A \mid h(a) \le C_2\} \cup \{Q_1, \dots, Q_r\}.$$
Then S is finite, by 3. We will prove that S generates A. Let B be the subgroup of A generated by S. Take $P_0 \in A$ arbitrary. By the definition of the Q_i, we can write
$$P_0 = 2P_1 - Q_{i_1}, \qquad P_1 = 2P_2 - Q_{i_2}, \qquad \dots,$$
for some $1 \le i_1, i_2, \dots \le r$. For each j,
$$\begin{aligned} h(P_j) &\le \frac{h(2P_j) + D}{4} = \frac{h\left(P_{j-1} + Q_{i_j}\right) + D}{4} && \text{by 2} \\ &\le \frac{2h(P_{j-1}) + C_1 + D}{4} = \frac{h(P_{j-1}) + C_2}{2} && \text{by 1.} \end{aligned}$$
In particular if $h(P_{j-1}) > C_2$, then $h(P_j) < h(P_{j-1})$. If $h(P_j) > C_2$ for all j, then we would have $h(P_0) > h(P_1) > \dots$. This contradicts the finiteness of $\{a \in A \mid h(a) \le h(P_0)\}$. So there exists j such that $h(P_j) \le C_2$, that is $P_j \in S$. Then
$$P_{j-1} = 2P_j - Q_{i_j} \in B, \qquad P_{j-2} = 2P_{j-1} - Q_{i_{j-1}} \in B, \qquad \dots.$$
Then by descending induction on j, $P_0 \in B$, so $A = B$, as required. □

Corollary 10.7 (Mordell-Weil)**.** *If $E(\mathbb{Q})$ is an elliptic curve, such that all points of order two are in $E(\mathbb{Q})$, then $E(\mathbb{Q})$ is a finitely generated abelian group, that is*
$$E(\mathbb{Q}) \cong T \times \mathbb{Z}^r,$$
where T is finite and $r \ge 0$.

Remark 10.8. The formulas for H and h look a bit ad hoc, but a modification works more cleanly. Define
$$\widehat{\mathrm{h}}(P) = \lim_{n \to \infty} \frac{\mathrm{h}(2^n P)}{4^n}.$$
Then $\mathrm{h}(2P) \ge 4\mathrm{h}(P) - D$, and a similar argument gives $\mathrm{h}(2P) \le 4\mathrm{h}(P) + D'$, so $\widehat{\mathrm{h}}(2P) = 4\widehat{\mathrm{h}}(P)$. In fact $\widehat{\mathrm{h}}$ determines a quadratic form on $E(\mathbb{Q}) \otimes_{\mathbb{Z}} \mathbb{Q}$.

11 Counting points over $E(\mathbb{F}_p)$

Lecture 28 Thursday 05/12/19

Let E be $y^2 = x^3 - x$. Then $E(\mathbb{Q}) = \{\mathcal{O}, (0,0), (\pm 1, 0)\}$ and $\Delta = -4$. If $p > 2$, then E defines an elliptic curve over $\mathbb{F}_p$.

Theorem 11.1 (Hasse 1933)**.** $|\#E(\mathbb{F}_p) - (p+1)| < 2\sqrt{p}$.

What more can we say about $\#E(\mathbb{F}_p)$?

$p = 3$

x	0	1	2
$\#(x,y)$	1	1	1

$\#E(\mathbb{F}_3) = 4$

$p = 5$

x	0	1	2	3	4
$\#(x,y)$	1	1	2	2	1

$\#E(\mathbb{F}_5) = 8$

$p = 7$

x	0	1	2	3	4	5	6
$\#(x,y)$	1	1	0	0	2	2	1

$\#E(\mathbb{F}_7) = 8$

Let $\mathrm{a}_p = p + 1 - \#E(\mathbb{F}_p)$, so $\mathrm{a}_p / 2\sqrt{p} \in (-1, 1)$. Then

p	3	5	7	11	13	17
a_p	0	-2	0	0	6	2

If $p \equiv 3 \mod 4$, then -1 is not a quadratic residue modulo p, that is not a square modulo p. So if $x^3 - x \ne 0$, then exactly one of $x^3 - x$ and $(-x)^3 - (-x) = -\left(x^3 - x\right)$ is a square.

Proposition 11.2. *If $p \equiv 3 \mod 4$, then the number of points $x = \pm x_0$ is exactly two for any $x_0 \ne 0$.*

If $p \equiv 1 \mod 4$, then we can write $p = a^2 + b^2$ for some a and b. Fix a and b by demanding $a + ib \equiv 1 \mod (1+i)^3$. For example, if $p = 5 = 2^2 + 1^2$, then $\{a, b\} = \{\pm 1, \pm 2\}$, so $a = -1$ and $b = 2$.

Proposition 11.3. *If $p \equiv 1 \mod 4$, then $\mathrm{a}_p = 2a$.*

E is a **CM (complex multiplication)** elliptic curve. Let

$$\mathrm{P}(x) = \lim_{N \to \infty} \frac{\#\left\{p \le N \;\middle|\; \mathrm{a}_p / 2\sqrt{p} = x\right\}}{\#\{p \le N\}}.$$

Theorem 11.4 (Hecke 1920)**.** *Over all CM elliptic curves,* $\mathrm{P}(0) = \frac{1}{2}$*, and if $x \ne 0$, then*

$$\mathrm{P}(x) = \frac{1}{2\pi\sqrt{1 - x^2}}.$$

Theorem 11.5 (Sato-Tate conjecture 1960, Clozel-Harris-Shepherd-Barron-Taylor 2008)**.** *Over all non-CM elliptic curves,*

$$\mathrm{P}(x) = \frac{2}{\pi}\sqrt{1 - x^2}.$$

Let E be $y^2 + y = x^3 - x^2$, the **first elliptic curve in nature**. Then $E(\mathbb{Q}) = \mathbb{Z}/5\mathbb{Z} = \langle (0,0) \rangle$ and $\Delta = -11$. If $p \ne 11$, then E defines an elliptic curve over $\mathbb{F}_p$. Computing a_p,

p	2	3	5	7	13	17
a_p	-2	-1	1	-2	4	-2

Let $z \in \mathbb{C}$ such that $\operatorname{Im} z > 0$. Set $q = e^{2\pi i z}$. Consider the infinite product

$$f(z) = q \prod_{n=1}^{\infty} (1 - q^n)^2 \left(1 - q^{11n}\right)^2 = q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 - 2q^{10} + q^{11} - 2q^{12} + 4q^{13} + 4q^{14} - q^{15} - 4q^{16} - 2q^{17} + \dots.$$

which converges, so $f(z)$ is a holomorphic function. Then $f(z+1) = f(z)$, and $f(-1/11z) = (11z)^2 f(z)$, so f is a **modular form of level $\Gamma_0(11)$ and weight two**.

Theorem 11.6 (Modularity of elliptic curves 1957, Wiles 1995 and Breuil-Conrad-Diamond-Taylor 2001)**.** *For each elliptic curve E over $\mathbb{Q}$, there exists a corresponding weight two modular form $f_E = q + b_2 q^2 + b_3 q^2 + \dots$, such that $b_p = \mathrm{a}_p$.*

Lecture 29 Monday 09/12/19

Lecture 29 is a problems class.

12 Torsion subgroups and ranks of $E(\mathbb{Q})$

Lecture 30 Tuesday 10/12/19

How large is the torsion subgroup on average? Let E be $y^2 = x^3 + ax + b$. If we chose $a, b \in \mathbb{Z}$ at random, what is the probability that E has any points of order two? That is, what is the probability that $x^3 + ax + b$ has a rational root?

Proposition 12.1. 0% *of elliptic curves over* $\mathbb{Q}$ *has any points of order two. In fact, it can be shown that* 100% *of elliptic curves over* $\mathbb{Q}$ *have trivial torsion subgroup.*

How large can the torsion subgroup be? Is there any bound on the order of the torsion subgroup of $E(\mathbb{Q})$?

Theorem 12.2 (Mazur 1977)**.** *For any* $E(\mathbb{Q})$*, the torsion subgroup is of the form*

$$\mathbb{Z}/N\mathbb{Z}, \qquad 1 \le N \le 10, \qquad \mathbb{Z}/12\mathbb{Z},$$
$$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2N\mathbb{Z}, \qquad 1 \le N \le 4.$$

Is the same true for the rank? Heuristically, if the rank of $E(\mathbb{Q})$ is large, then $\#E(\mathbb{F}_p)$ is also large.

Example 12.3. Let E be $y^2 = x^3 - Dx$. If $p \equiv 3 \mod 4$, then $\#E(\mathbb{F}_p) = p + 1$. But these curves can have rank $0, 1, 2, \dots$.

Definition 12.4. The **Riemann zeta function** is

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} \sum_{m=0}^{\infty} \frac{1}{p^{ms}} = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}.$$

Then $\zeta(s)$ has a meromorphic continuation to $\mathbb{C}$ and a simple pole at $s = 1$, and converges for $\operatorname{Re} s > 1$.

Definition 12.5. The **L-function** of $E(\mathbb{Q})$ is

$$\mathrm{L}(E, s) = \sum_{n=1}^{\infty} \frac{\mathrm{a}_n}{n^s} = \prod_{p \nmid \Delta \text{ prime}} \frac{1}{1 - \mathrm{a}_p p^{-s} + p^{1-2s}} \prod_{p \mid \Delta \text{ prime}} \frac{1}{1 - \mathrm{a}_p p^{-s}},$$

where a_p are as above, and $\mathrm{a}_{p^n} = 1 + p^n - \#E(\mathbb{F}_{p^n})$.

Then $\mathrm{L}(E, s)$ converges for $\operatorname{Re} s > \frac{3}{2}$, which follows from $|\mathrm{a}_p| < 2\sqrt{p}$.

Theorem 12.6 (Hasse-Weil conjecture)**.** $\mathrm{L}(E, s)$ *has an analytic continuation to all of* $\mathbb{C}$*, and no poles.*

This was conjectured in the 1940s and follows from modularity, which was known for CM elliptic curves $y^2 = x^3 - Dx$ in the 1960s, which were the ones that Birch and Swinnerton-Dyer looked at.

Conjecture 12.7 (Birch-Swinnerton-Dyer 1965)**.** *The order of vanishing of* $\mathrm{L}(E, s)$ *at* $s = 1$ *is the rank of* $E(\mathbb{Q})$.

Theorem 12.8 (Gross-Zagier 1986 and Kolyvagin 1989)**.** *The conjecture holds if* $E(\mathbb{Q})$ *has rank at most one.*

Nothing is known if the rank is greater than one. How large is the rank on average?

Conjecture 12.9. 100% *of elliptic curves over* $\mathbb{Q}$ *have rank at most one. In fact* 50% *have rank zero and* 50% *have rank one.*

Computing the rank of E basically comes down to computing $E(\mathbb{Q})/2E(\mathbb{Q})$, and that comes down to computing $\operatorname{im} \delta$ for $\delta : E(\mathbb{Q})/2E(\mathbb{Q}) \hookrightarrow \left(\mathbb{Q}^\times / (\mathbb{Q}^\times)^2\right)^3$. Define the **2-Selmer group** $\mathcal{S}_2$ to be the same as $\operatorname{im} \delta$, except that you only demand that the equations you write have solutions in $\mathbb{Q}_p$ for all p, and not necessarily in $\mathbb{Q}$. Then compute $\operatorname{im} \delta$ for $\delta : E(\mathbb{Q})/2E(\mathbb{Q}) \hookrightarrow \mathcal{S}_2$. The following is the best known result.

Theorem 12.10 (Bhargava-Shankar 2011)**.** *The average rank is less than one.*

How large can the rank of E be?

Theorem 12.11 (Elkies 2006)**.** *There exists* $E(\mathbb{Q})$ *with rank at least* 28.

Conjecture 12.12. *There are only finitely many* $E(\mathbb{Q})$ *of rank greater than* 21.

A Diagonalisation of quadratic forms

Definition A.1. Let k be any field, and let V be a k-linear vector space. A **symmetric bilinear pairing** on V is a map $\langle \cdot, \cdot \rangle : V \times V \to k$ such that for all $\alpha_1, \alpha_2 \in k$ and $\underline{v_1}, \underline{v_2}, \underline{v_3} \in V$,

- $\langle \alpha_1 \underline{v_1} + \alpha_2 \underline{v_2}, \underline{v_3} \rangle = \alpha_1 \langle \underline{v_1}, \underline{v_3} \rangle + \alpha_2 \langle \underline{v_2}, \underline{v_3} \rangle$,
- $\langle \underline{v_3}, \alpha_1 \underline{v_1} + \alpha_2 \underline{v_2} \rangle = \alpha_1 \langle \underline{v_3}, \underline{v_1} \rangle + \alpha_2 \langle \underline{v_3}, \underline{v_2} \rangle$, and
- $\langle \underline{v_1}, \underline{v_2} \rangle = \langle \underline{v_2}, \underline{v_1} \rangle$.

Example A.2. Dot product in $\mathbb{R}^n$ over $\mathbb{R}$.

Definition A.3. If $\operatorname{ch} k \neq 2$, then the associated **quadratic form** to a symmetric bilinear pairing is

$$\begin{array}{cccc} \mathrm{B} & : & V & \longrightarrow & k \\ & & \underline{v} & \longmapsto & \langle \underline{v}, \underline{v} \rangle \end{array}.$$

Remark A.4. Then B is uniquely determined by $\langle \cdot, \cdot \rangle$, but the converse is also true, since

$$\mathrm{B}(\underline{v_1} + \underline{v_2}) = \langle \underline{v_1} + \underline{v_2}, \underline{v_1} + \underline{v_2} \rangle = \langle \underline{v_1}, \underline{v_1} \rangle + \langle \underline{v_1}, \underline{v_2} \rangle + \langle \underline{v_2}, \underline{v_1} \rangle + \langle \underline{v_2}, \underline{v_2} \rangle = \mathrm{B}(\underline{v_1}) + \mathrm{B}(\underline{v_2}) + 2 \langle \underline{v_1}, \underline{v_2} \rangle,$$

by bilinearity and symmetry, so

$$\langle \underline{v_1}, \underline{v_2} \rangle = \frac{1}{2} \left(\mathrm{B}(\underline{v_1} + \underline{v_2}) - \mathrm{B}(\underline{v_1}) - \mathrm{B}(\underline{v_2}) \right).$$

Example A.5. Let $V = k^n$, and let A be a symmetric $n \times n$ matrix over k. Then

$$\langle \underline{v_1}, \underline{v_2} \rangle = \underline{v_1}^{\intercal} A \underline{v_2} \in k, \qquad \underline{v_1}, \underline{v_2} \in V$$

is a symmetric bilinear pairing. More generally, let V be any finite-dimensional vector space, so $V = \langle \underline{e_1}, \dots, \underline{e_n} \rangle_k$ for $\{\underline{e_i}\}$ a k-basis, and let the (i,j)-th entry of A be $\left(\underline{e_i}, \underline{e_j}\right)$. Under the unique isomorphism

$$\begin{array}{ccccc} \phi & : & V & \longrightarrow & k^n \\ & & \underline{e_i} & \longmapsto & \begin{pmatrix} 0 \dots 0 & 1 & 0 \dots 0 \end{pmatrix} \end{array},$$

we get a symmetric bilinear pairing

$$\langle \underline{v}, \underline{w} \rangle = \phi(\underline{v})^{\intercal} A \phi(\underline{w}) \in k, \qquad \underline{v}, \underline{w} \in V.$$

Definition A.6. A **quadratic space** over k is an ordered pair $(V, \langle \cdot, \cdot \rangle)$ for V a finite-dimensional k-linear vector space, and $\langle \cdot, \cdot \rangle : V \times V \to k$ a symmetric bilinear pairing. Two quadratic spaces $(V, \langle \cdot, \cdot \rangle)$ and $(W, \langle\langle \cdot, \cdot \rangle\rangle)$ are **isometric** if there exists $\phi : V \to W$ an isomorphism such that $\langle \underline{v}, \underline{w} \rangle = \langle\langle \phi(\underline{v}), \phi(\underline{w}) \rangle\rangle$ for all $\underline{v}, \underline{w} \in V$, so any quadratic space is isometric to a specimen from the example.

Remark A.7. Change of basis has the following effect. Let A be the matrix of the symmetric bilinear pairing $\langle \cdot, \cdot \rangle$ in the basis $\underline{e_1}, \dots, \underline{e_n}$. If the matrix of the change of basis is B, in the basis the matrix of the symmetric bilinear pairing is $B^{\intercal} A B$, since $(B\underline{v})^{\intercal} A (B\underline{w}) = \underline{v}^{\intercal} (B^{\intercal} A B) \underline{w}$.

Theorem A.8 (Gram-Schmidt orthogonalisation process)**.** *If $(V, \langle \cdot, \cdot \rangle)$ is a quadratic space, then V has a basis $\underline{e_1}, \dots, \underline{e_n}$ in which the matrix of $\langle \cdot, \cdot \rangle$ is diagonal.*

Proof. Two cases. If $\mathrm{B} \equiv 0$, then $\langle \cdot, \cdot \rangle \equiv 0$. Otherwise there exists $\underline{v} \in V$ such that $\mathrm{B}(\underline{v}) \neq 0$. Let $\underline{e_1} = \underline{v}$, and

$$\underline{v}^{\perp} = \{ \underline{w} \in V \mid \langle \underline{v}, \underline{w} \rangle = 0 \}.$$

This is an k-linear subspace. This is trivial as $\underline{w} \mapsto \langle \underline{v}, \underline{w} \rangle$ is k-linear. Then $\underline{v} \notin \ker \langle \underline{v}, \cdot \rangle$, so $\dim \underline{v}^{\perp} = \dim V - 1$. We apply the process to $\left(\underline{v}^{\perp}, \langle \cdot, \cdot \rangle|_{\underline{v}^{\perp}} \right)$, by using induction on the dimension. $\square$

Remark A.9. The **general linear group**

$$\mathrm{GL}_{n+1}(k) = \mathrm{Aut}_k\, k^{n+1}$$

acts on $\mathbb{P}^n(k)$, and maps scalar multiples to scalar multiples, so maps equivalence classes under rescaling to equivalence classes, so have an induced action on $\mathbb{P}^n(k)$. The centre $\mathrm{Z}_{n+1}(k)$ of $\mathrm{GL}_{n+1}(k)$ is the scalar matrices $\{\lambda \mathrm{I}_3 \mid \lambda \in k^\times\}$, which acts trivially on $\mathbb{P}^n(k)$. This is a normal subgroup, so I can form the quotient group

$$\mathrm{PGL}_{n+1}(k) = \mathrm{GL}_{n+1}(k) / \mathrm{Z}_{n+1}(k),$$

the **projective linear group** of rank $n+1$. Projective algebraic geometry is invariant under projective linear transformations. If $F = 0$ is non-singular, then its image under $\mathrm{PGL}_{n+1}(k)$ is also non-singular, and multiplicities in Bézout's theorem does not change under $\mathrm{PGL}_{n+1}(k)$, etc.

Theorem A.10. *If $\mathrm{ch}\, k \neq 2$, then for $F \in k[X_0, \dots, X_n]$ of degree two homogeneous, there exists a linear transformation, such that after the change of variables, F is of the form*

$$\alpha_0 X_0^2 + \dots + \alpha_n X_n^2, \qquad \alpha_0, \alpha_1, \alpha_2 \in k.$$

Proof. Let $F(X_0, \dots, X_n) = \sum_{i<j} a_{ij} X_i X_j$ for $a_{ij} \in k$. It is the quadratic form on k^{n+1} associated to the bilinear pairing in the standard basis with matrix $A = (b_{ij})$, where

$$b_{ij} = \begin{cases} \frac{1}{2} a_{ij} & i \leq j \\ \frac{1}{2} a_{ji} & i > j \end{cases}.$$

Now apply the Gram-Schmidt theorem. $\square$