M4P32 Number Theory: Elliptic Curves

Lectured by Prof Toby Gee
Typed by David Kurniadi Angdinata

Autumn 2019

Syllabus

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 nonsingular, 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

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

2 The p-adic numbers

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. $|x| \geq 0$ with equality if and only if $x = 0$,
2. $|xy| = |x| \cdot |y|$, and
3. $|x + y| \leq |x| + |y|$.

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

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

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

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

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

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

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

Proof. Without loss of generality, $x, y \in \mathbb{Z}$. Also we may assume $x, y, x + y \neq 0$. 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 $x \neq 0$.*

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

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

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

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.

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 $\left|x_n + \frac{1}{3}\right|_2 = \left|\frac{10^n}{3}\right|_2 = \left|2^n \frac{5^n}{3}\right| = 2^{-n} \to 0$.

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 $y = x_N$. 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 $|x_n - y_n| < \frac{1}{n}$. 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. $\frac{1}{p} \notin \mathbb{Z}_p$, and $\left|\frac{1}{p}\right|_p = p > 1$. In fact $\mathbb{Q}_p = \mathbb{Z}_p\left[\frac{1}{p}\right]$, the field of fractions of $\mathbb{Z}_p$.

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

$$t_m - t_n = (t_m - t_{m-1}) + \cdots + (t_{n+1} - t_n),$$

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 $|x_n| \le R$ and $x_n \to 0$ then $|\sum_{n=1}^{\infty} x_n| \le R$.*

Proof. $\sum_{n=1}^{\infty} x_n$ converges if and only if $(\sum_{n=1}^{m} x_n)_{m\ge1}$ converges. Since k is complete, this is if and only if $(\sum_{n=1}^{m} x_n)_{m\ge1}$ is Cauchy. By Corollary 2.18, this is if and only if $x_{m+1} \to 0$. 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 $a_T \ne 0$, and $p \nmid a_T$, then $|\sum_{n=0}^{\infty} a_n p^n|_p = p^{-T}$.*

Proof. Since $a_n \in \mathbb{Z}$,
$$|a_n p^n|_p = |a_n|_p \cdot |p^n|_p \le |p^n|_p = p^{-n} \to 0.$$
Furthermore $\left|a_T p^T\right|_p = p^{-T}$ and $|a_n p^n|_p \le p^{-T-1}$ if $n \ge T+1$, so $\left|\sum_{n=T+1}^{\infty} a_n p^n\right|_p \le p^{-T-1}$, so
$$\left|a_T p^T + \sum_{n=T+1}^{\infty} a_n p^n\right|_p = p^{-T},$$
by Lemma 2.7. □

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 $a_T \ne b_T$, then by Lemma 2.20, $|\sum_n (a_n - b_n) p^n|_p = p^{-T}$. In particular $\sum_n (a_n - b_n) p^n \ne 0$.

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 $|\alpha|_p \le 1$, we have $|\beta|_p \le 1$, 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
$$|\alpha - a_0|_p \le \max\left(|\alpha - \beta|_p, |\beta - \gamma|_p, |\gamma - a_0|_p\right) < 1.$$
Then $|(\alpha - a_0)/p|_p \le 1$, 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 $|\alpha - (a_0 + \dots + a_n p^n)|_p \le p^{-(n+1)}$. So $\alpha = \sum_{n=0}^{\infty} a_n p^n$.

□

Corollary 2.22. *Any element α of $\mathbb{Q}_p$ can be uniquely written as*
$$\alpha = \sum_{n\ge -T} a_n p^n, \qquad a_{-T} \ne 0, \qquad a_n \in \{0, \dots, p-1\}.$$

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 $p^T \alpha$. □

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
$$|\alpha - (a_0 + \dots + a_m p^m)| \le p^{-(m+1)},$$
and $a_0 + \dots + a_m p^m \in \mathbb{Z}$. □

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 $|x|_p = |y|_p = 1$. $\square$

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 $u = \alpha p^{-n}$. $\square$

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 $f'(X), f''(X), \ldots$ 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 $t_0, t_1, \ldots$ 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 $f(t) = 0$. $\square$

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*

$$|f'(t)| = |f'(t_0)|, \qquad |f(t_0)| < |f'(t_0)|^2.$$

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. [2] $\square$

[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.

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 $\underline{x} \sim \underline{y}$ if and only if $\underline{x} = \lambda \cdot \underline{y}$ for $\lambda \in k \setminus \{\underline{0}\} = k^*$.

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** $[x_0 : \cdots : x_n]$ is an equivalence class of non-zero vectors in k^{n+1} modulo $\sim$, so

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

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

Lemma 3.5. *Let*
$$\begin{array}{rccl} \phi_i & : & \mathbb{A}^n(k) & \longrightarrow & \mathbb{P}^n(k) \\ & & (x_0, \dots, x_{n-1}) & \longmapsto & [x_0 : \dots : x_{i-1} : 1 : x_{i+1} : \dots : x_{n-1}] \end{array}.$$
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 $X_n = 0$.

Lecture 6 Tuesday 15/10/19

Let $\lambda : k^{n+1} \to k$ be a non-trivial linear function. The image of
$$\operatorname{Ker} \lambda = \left\{ \alpha_0 x_0 + \dots + \alpha_n x_n = 0 \;\middle|\; (x_0, \dots, x_n) \in k^{n+1}, \text{ not all } \alpha_i \in k \text{ are zero} \right\} \subset \mathbb{P}^n(k)$$
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
$$F(X_0, \dots, X_n) = \sum \alpha_{i_0 \dots i_n} X_0^{i_0} \dots X_n^{i_n}, \qquad i_0 + \dots + i_n = d,$$
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 $y = x^2$.

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 $\overline{k}$. $\square$

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.

Example. $x^3 = y^2$ is a **cusp**.

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 $\overline{k}$.

Lecture 7 is a problem class. Lecture 7 Thursday 17/10/19

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 Lecture 8 Monday 21/10/19

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

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.*

[3] Exercise