M4P32 Number Theory: Elliptic Curves

Lectured by Prof Toby Gee
Typeset by David Kurniadi Angdinata

Autumn 2018

Contents

Lecture 1 Thursday 04/10/18

0 Introduction

0.1 Outline

1. Introduction
2. Conics
   (a) The p-adic numbers
   (b) Basic algebraic geometry
   (c) Plane curves
   (d) The Hasse principle
3. Cubics
   (a) Definitions
   (b) Elliptic curves over $\mathbb{Q}_p$
   (c) Elliptic curves over $\mathbb{Q}$
   (d) The Mordell-Weil theorem

The theme of the course will be studying polynomial equations over $\mathbb{Z}$ or $\mathbb{Q}$.

Example. For $x^7+y^7+z^7=1$, what are the solutions with $x, y, z \in \mathbb{Q}$? Answer is hard. However $x^2-1=0$ is easy. In fact any equation in one variable is easy to solve over $\mathbb{Q}$. For example, $3x^5-9x^3+x^2+148/81=0$ iff $243x^5-729x^3+81x^2+148=0$. Letting $x=r/s$ for $(r,s)=1$ and $s \geq 1$, such as $r=-2$ and $s=5$ in $-2/5$, gives $243r^5-729r^3s^2+81r^2s^3+148s^5=0$. So $r^2 \mid 148s^5$, but $(r,s)=1$, so $r^2 \mid 148$. Similarly $s^2 \mid 243$. Now check the finitely many possibilities to get $x=2/3$ as the only solution in $\mathbb{Q}$.

If k is a field, such as $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$, $\mathbb{Q}_p$, we write $k[x_1, \dots, x_n]$ for the polynomial ring in n variables $x_1, \dots, x_n$. A **monomial** is an expression $x_1^{\alpha_1}, \dots, x_n^{\alpha_n}$ for $a_i \in \mathbb{Z}_{>0}$. The **degree** of $x_1^{\alpha_1}, \dots, x_n^{\alpha_n}$ is $a_1+\dots+a_n$. An element of $k[x_1, \dots, x_n]$ is just a finite sum of multiples of monomials with coefficients in k. Its degree is the largest degree of any monomial occurring in it. For example, $5x_{10}^3+x_2x_3^{10}-(2/3)\,x_1^7$ has degree 11. Typically we will be looking at the case of two variables x_1, x_2, which we will usually call x, y.

Theorem 0.1 (Falting's theorem)**.** The general equation in two variables of degree greater than four over $\mathbb{Q}$ is known to only have finitely many solutions in $\mathbb{Q}$.

Example. $x^4+y^4=17$ only has $(\pm 1, \pm 2)$ and $(\pm 2, \pm 1)$ as solutions, which is proved only in 2001. $\left(x^{100}+5y^{100}-7\right)(x-y)=0$ is not a general equation and has infinitely many solutions.

Example. $x^2+y^2=-1$ has no solutions in $\mathbb{Q}$. $x^2+y^2=0$ has finitely many solutions in $\mathbb{Q}$ $(x=y=0)$. $x^2+y^2=1$ has infinitely many solutions in $\mathbb{Q}$. Let $x=a/c$ and $y=b/c$ for $a, b, c \in \mathbb{Z}$ gives Pythagorean triples $a^2+b^2=c^2$, such as $3^2+4^2=5^2$, $5^2+12^2=13^2$, etc.

Example. $x^2+y^2=3$ has solutions in $\mathbb{R}$ but no solutions in $\mathbb{Q}$. Equivalently, $a^2+b^2=3c^2$ has no solutions with $a, b, c \in \mathbb{Z}$ except $a=b=c=0$. Suppose we have a solution. Then $a^2+b^2 \equiv 0 \mod 3$. A fact is that if $n \in \mathbb{Z}$, then $n^2 \equiv 0 \mod 3$ if $3 \mid n$, or $n^2 \equiv 1 \mod 3$ if $3 \nmid n$. So $a \equiv b \equiv 0 \mod 3$, or $3 \mid a, b$. Write $a=2A$ and $b=3B$. Then $(3A)^2+(3B)^2=3c^2$ iff $9\left(A^2+B^2\right)=3c^2$, iff $3\left(A^2+B^2\right)=c^2$. So $3 \mid c^2$ and $3 \mid c$. Write $c=3C$. Then $3\left(A^2+B^2\right)=(3C)^2$ iff $3\left(A^2+B^2\right)=9C^2$, iff $A^2+B^2=3C^2$. Thus $a=b=c=0$.

$x^2+y^2=-1$ has an obstruction in $\mathbb{R}$. $x^2+y^2=3$ has an obstruction in $\mathbb{Q}_3$. Hasse principle will tell us that for general equations of degree two in x, y, there are either infinitely many solutions in $\mathbb{Q}$ or no solutions, and furthermore either no solutions in $\mathbb{R}$ or no solutions in $\mathbb{Q}_p$ for some prime p.

Lecture 2 Friday 05/10/18

We study plane conics and plane cubics. Plane refers to 2 variables x, y. Conic refers to degree two while cubic refers to degree three.

Example. $x^2 + 2y^2 = 6$ has a rational solution $(2, 1)$. Drawing lines at $(2, 1)$ with rational slope $y - 1 = m(x - 2)$ will get all rational solutions by intersecting with $x^2 + 2y^2 = 6$. Then $x^2 + 2(m(x - 2) + 1)^2 = 6$ gives $\left(2m^2 + 1\right) x^2 + 4m(1 - 2m)x + 2\left(2m^2 - 1\right)^2 = 0$. The sum of the roots of this equation is $4m(2m - 1) / \left(2m^2 + 1\right)$. Since $x = 2$ is a root, the other root is

$$x_0 = \frac{4m(2m-1)}{2m^2+1} - 2 = \frac{4m^2-4m-2}{2m^2+1}, \qquad y_0 = m(x_0 - 2) + 1 = m\left(\frac{-4m-4}{2m^2+1}\right) + 1 = \frac{-2m^2-4m+1}{2m^2+1}.$$

If $m \in \mathbb{Q}$, $(x_0, y_0) \in \mathbb{Q}^2$ and conversely, which is easy. For example, $m = 1$ gives $(x_0, y_0) = (-2/3, -5/3)$ and $m \to \infty$ gives $(x_0, y_0) \to (2, -1)$. Exercises for $x^2 + y^2 = 1$, $x^2 + y^2 = 0$, $xy = 0$, $x^2 - y^2 = 0$.

0.2 References

1. J W S Cassels, Lectures on elliptic curves, 1991

2. J H Silverman, The arithmetic of elliptic curves, 1986

3. J H Silverman and J Tate, 1992

1 The p-adic numbers

Definition 1.1. A **norm** on a field k is a function $|\cdot| : k \to \mathbb{R}$ such that:

1. $|x| \geq 0$ with equality iff $x = 0$,
2. $|xy| = |x|\,|y|$, and
3. $|x + y| \leq |x| + |y|$.

Note. $|1| = |-1| = 1$ and $|-x| = |-1|\,|x| = |x|$.

Example. Let $k = \mathbb{Q}$ or $\mathbb{R}$ and $|x|$ is the absolute value of x, that is $|x| = x$ if $x \geq 0$ and $|x| = -x$ if $x < 0$.

Example. Discrete norm $|x| = 0$ if $x = 0$ and $|x| = 1$ if $x \neq 0$.

Remark 1.2. Any norm on k defines a metric by $d(x, y) = |x - y|$. In particular, a norm determines a topology.

Example. The discrete norm determines the discrete topology.

Definition 1.3. Let p be a prime number. Let $a/b \in \mathbb{Q}$ with $(a, b) = 1$. Let p^n be the biggest power of p dividing a/b, so $a/b = p^n (c/d)$ with $(c, p) = (d, p) = 1$. Then the **p-adic norm** is $|a/b|_p = p^{-n}$.

Example. $|1/6|_5 = 1$, $|1/6|_3 = 3$. $p^n \to 0$ into the p-adic topology as $n \to \infty$.

Lemma 1.4. $|\cdot|_p$ is a norm on $\mathbb{Q}$.

Proof.

1. Trivial.
2. Unique factorisation.
3. Prove $3'$: $|x + y|_p \leq \max\left(|x|_p, |y|_p\right)$. Without loss of generality, $x, y, x + y \neq 0$. Multiplying x, y by any power of p does not affect the truth of $3'$, so without loss of generality $x, y \in \mathbb{Z}$. Then we have to show that $p^r \mid x$ and $p^r \mid x + y$, which is obvious.

$\square$

$3'$ is the **ultrametric inequality**.

Definition 1.5. If $|\cdot|$ satisfies $3'$, we say that $|\cdot|$ is **nonarchimedean**. Otherwise $|\cdot|_p$ is **archimedean**.

Say that two norms $|\cdot|_1$, $|\cdot|_2$ on a field k are equivalent if $|\cdot|_1 = |\cdot|_2^\alpha$ for some $\alpha > 0$. If two norms are equivalent, they define the same topology. **Ostrowski's theorem** states that up to equivalence, the only norms on $\mathbb{Q}$ are the usual archimedean norm, the discrete norm, and the p-adic norms.

Lecture 3 Tuesday 09/10/18

Lemma 1.6. If $|\cdot|$ is nonarchimedean and $|x| \neq |y|$, then $|x + y| = \max(|x|, |y|)$.

Proof. Without loss of generality, $|x| > |y|$. Write $x = (x + y) + (-y)$, so $|x| \leq \max(|x + y|, |-y|)$. So equality holds in all inequalities, so $|x| = |x + y|$. $\square$

Example. Think about $D(a, r) = \{x \mid |x - a| < r\}$ and $D(b, r) = \{x \mid |x - b| < r\}$. What are the possibilities for $D(a, r) \cap D(b, r)$?

Example. TODO Exercise: directly prove Lemma 1.6 from the definition.

Let k be a field, let $|\cdot|$ be any norm on k. $d(x, y) = |x - y|$ is a metric, so k is a metric space with metric d. We have the usual definitions for sequences (x_n). Say that x_n **converges** to x if for all $\epsilon > 0$, there exists N such that $n \geq N$ gives $|x_n - x| < \epsilon$. Say that (x_n) is **Cauchy** if $\epsilon > 0$, there exists N such that $m, n \geq N$ gives $|x_n - x_m| < \epsilon$. Say that (x_n) is **convergent** if x_n converges to x for some $x \in k$. Write $x_n \to x$. If (x_n) is convergent, then (x_n) is Cauchy. Say that k is **complete** with respect to $|\cdot|$ if all Cauchy sequences converge.

Example. Let $k = \mathbb{Q}$ with the usual archimedean norm $|\cdot|$. $1, 1.4, 1.41, 1.414, \dots \to \sqrt{2} \notin \mathbb{Q}$.

Example. Let $k = \mathbb{Q}$ with $|\cdot|_2$. $3, 33, 333, 3333, \dots$ is a Cauchy sequence. In fact, if $m > n$, $|x_m - x_n|_2 = 2^{-n}$. So if $m, n \geq N$, $|x_m - x_n| \leq 2^{-N}$. $x_n = (10^n - 1)/3$ so $x_n + 1/3 = 10^n/3 = 2^n(5^n/3)$. $|x_n + 1/3|_2 = 2^{-n}$, so $x_n + 1/3 \to 0$.

Example. Let $k = \mathbb{Q}$ with $|\cdot|_5$. $\left|5^{2^n}\right|_5 = 5^{-2^n} \to 0$ as $n \to \infty$.

Example. Let $k = \mathbb{Q}$ with $|\cdot|_2$. $\left(5^{2^n}\right)$ is $5, 25, 625, \dots \to 1$. Want to show that $5^{2^n} - 1 \to 0$, so that bigger and bigger powers of two divide $5^{2^n} - 1$. Use the lemma that $t \equiv 1 \mod 2^k$ gives $t^2 \equiv 1 \mod 2^{k+1}$.

Example. Let $k = \mathbb{Q}$ with $|\cdot|_7$. 5^{2^n} is not Cauchy. In fact $\mod 7$ it looks like $5, 4, 2, 4, 2, \dots$, so $|x_n - x_{n+1}|_7 = 1$.

Example. An example of a Cauchy sequence in $\mathbb{Q}$ for some $|\cdot|_p$ which does not converge. Want to find a Cauchy sequence (x_n) with $x_n^2 \to 7$, so write down a sequence (x_n) such that $\left|x_n^2 - 7\right|_3 \to 0$. If $x_1 = 1$, then $x_1^2 \equiv 7 \mod 3$. If $x_2 = 4$, then $x_2^2 \equiv 7 \mod 9$. Find some $n \in \mathbb{N}$ such that $x_3 = 4 + 9n$ and $x_3^2 \equiv 7 \mod 27$. $x_3^2 = \left(4 + 9n^2\right) = 16 + 8(9n) + (9n)^2 \equiv 16 + 8(9n) \mod 27$. So want $9 + 8(9n) \equiv 0 \mod 27$, so $1 + 8n \equiv 0 \mod 3$, such as $n = 1$. So $x_3 = 13$. Similar $x_4 = 13 + 27n$ and find some $n \in \mathbb{N}$.

Example. Show that for all primes p there is a Cauchy sequence (x_n) in $\mathbb{Q}$ for $|\cdot|_p$ with the property that $x_n^2 \to t$ for some integer t which is not a perfect square, such as $t = 1 - p$ if $p > 2$ and $t = -7$ if $p = 2$. (TODO Exercise)

There is a general notion of completing a field with respect to a norm. The result is a field K containing k, for which all Cauchy sequences in k converge, and such that K is minimal with this property.

Example. Let $k = \mathbb{Q}$ with the archimedean norm $|\cdot|$, then $K = \mathbb{R}$.

Lecture 4 Thursday 11/10/18

Let k be a field and $|\cdot|$ be a norm on k. Let R be the ring of Cauchy sequences in k, so elements of R are (x_n) for $x_n \in k$, where $(x_n) + (y_n) = (x_n + y_n)$ and $(x_n)(y_n) = (x_n y_n)$.

Let $I = \{(x_n) \in R \mid x_n \to 0 \text{ as } n \to \infty\}$. Claim that I is an ideal in R. $(x_n), (y_n) \in I$ then $(x_n + y_n) \in I$ because $x_n \to 0$ and $y_n \to 0$ gives $x_n + y_n \to 0$. If $(x_n) \in R$, $(y_n) \in I$ then (x_n) is bounded, so $x_n y_n \to 0$.

Define the completion of k to be $\hat{k} = R/I$. Claim that $\hat{k}$ is a field, so I is a maximal ideal of R. Need to show that if $(x_n) \in R$ with $x_n \not\to 0$, then there exists $(y_n) \in R$ such that $(x_n y_n) \in 1 + I$. $x_n \not\to 0$ gives ϵ, N such that $n \geq N$ gives $|x_n| \geq \epsilon > 0$. Set $y_n = 0$ if $n < N$ and $y_n = 1/x_n$ if $n \geq N$. Show that $(y_n) \in R$ (TODO Exercise). Then $(x_n y_n) = 0$ if $n < N$ and $(x_n y_n) = 1$ if $n \geq N$, so $x_n y_n \to 1$ as $n \to \infty$, as required.

k is a subfield of $\hat{k}$ by $x \mapsto (x)$. Check that $\hat{k}$ has a natural norm extending $|\cdot|$ on k, and $\hat{k}$ is complete with respect to this norm, so $|(x_n)| = \lim_{n \to \infty} |x_n|$. (TODO Exercise)

Prove that if $|\cdot|$ on k is a nonarchimedean norm, then so is the induced norm on $\hat{k}$. (TODO Exercise) Furthermore, the sequence $|x_n|$ is eventually constant for any Cauchy sequence $|x_n| \in R \setminus I$. (TODO Exercise)

Note. For $|\cdot|_p$ on $\mathbb{Q}$ this means that $|\cdot|$ is taking values in $p^{\mathbb{Z}}$.

Definition 1.7. The ***p*-adic numbers** $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to the p-adic norm. The ***p*-adic integers** $\mathbb{Z}_p$ is the closed unit disc in $\mathbb{Q}_p$, so $\mathbb{Z}_p = \left\{x \in \mathbb{Q}_p \mid |x|_p = 1\right\}$.

Prove that $\mathbb{Z}_p$ is a subring of $\mathbb{Q}_p$. Use that $|\cdot|_p$ is nonarchimedean. (TODO Exercise) Also $\mathbb{Q} \cap \mathbb{Z}_p = \{r/s \mid (r, s) = 1,\ p \nmid s\}$. In particular $\mathbb{Z} \subset \mathbb{Z}_p$. (TODO Exercise)

Prove that $\mathbb{Q}$ is dense in $\mathbb{Q}_p$. Indeed k is dense in $\hat{k}$. (TODO Exercise) A less obvious fact is that $\mathbb{Z}$ is dense in $\mathbb{Z}_p$.

Definition 1.8. Let k be a field with a norm $|\cdot|$, and (x_n) be any sequence. Then $\sum_{n=1}^{\infty} = \lim_{N \to \infty} \sum_{n=1}^{N} x_n$, if this limit exists.

Lemma 1.9. If k is nonarchimedean and $x_1, \dots, x_r$ satisfy $|x_i| \leq R$ for some R, then $|\sum_{n=1}^{r} x_i| \leq R$.

Proof. Induction with ultrametric inequality. $\square$

Corollary 1.10. If k is nonarchimedean then (x_n) is Cauchy iff $x_n - x_{n+1} \to 0$ as $n \to \infty$.

Proof. Forward direction is obvious. Conversely, $m > n$ gives $x_m - x_n = (x_m - x_{m-1}) + \dots + (x_{n+1} - x_n)$. If $|x_{i+1} - x_i| \leq \epsilon$ for all $i \geq N$ then $|x_m - x_n| \leq \epsilon$ for all $m, n \geq N$ by Lemma 1.9. □

Lemma 1.11. If k is complete and nonarchimedean then $\sum_{n=1}^{\infty} x_n$ converges iff $x_n \to 0$ as $n \to \infty$. If $|x_n|^{n-1} \leq R$ for all n and $x_n \to 0$ then $|\sum_{n=1}^{\infty} x_n| \leq R$.

Proof. Apply Lemma 1.9 and Corollary 1.10 to the sequence $(\sum_{i=1}^{n} x_i)$. □

Lemma 1.12. If $a_n \in \mathbb{Z}$ for all $n \geq 0$, then $\sum_{n=0}^{\infty} a_n p^n$ converges in $\mathbb{Q}_p$. If $a_n = 0$ for $n < T$ and $p \nmid a_T$ then $|\sum_{n=0}^{\infty} a_n p^n| = p^{-T}$.

Proof. $|a_n p^n|_p \leq |p^n|_p = p^{-n} \to 0$ as $n \to \infty$, so $\sum_{n=o}^{N} a_n p^n$ converges by Lemma 1.11. If $N \geq T$ then $\left|\sum_{n=o}^{N} a_n p^n\right| = p^{-T}$. (TODO Exercise: use lemma 1.6) □

Proposition 1.13.

1. If $a_n \in \{0, \dots p-1\}$, then $\sum_{n=0}^{\infty} a_n p^n \in \mathbb{Z}_p$. Further more if $a_n, b_n \in \{0, \dots, p-1\}$ and $\sum_{n=0}^{\infty} a_n p^n = \sum_{n=0}^{\infty} b_n p^n$ then $a_n = b_n$ for all n.
2. If $x \in \mathbb{Z}_p$ then there is a unique sequence (a_n) as in 1 with $x = \sum_{n=0}^{\infty} a_n p^n$.

Proof.

1. Convergence is Lemma 1.12. If $(a_n) \neq (b_n)$ let T be minimal such that $a_T \neq b_T$. Then
$$\left|\sum_{n=0}^{\infty} a_n p^n - \sum_{n=0}^{\infty} a_n p^n\right| = \left|\sum_{n=0}^{\infty} (a_n - b_n) p^n\right| = p^{-T}$$
by Lemma 1.12, so $\sum_{n=0}^{\infty} a_n p^n \neq \sum_{n=0}^{\infty} a_n p^n$.
2. Let $x \in \mathbb{Z}_p$. Since $\mathbb{Q}$ is dense in $\mathbb{Q}_p$ by construction, there exists $r/s \in \mathbb{Q}$, $(r, s) = 1$ with $|x - r/s|_p < 1$. Since $|x|_p \leq 1$, $|r/s|_p \leq 1$, so $p \nmid s$. So there exists $\gamma \in \mathbb{Z}$ with $|\gamma - r/s|_p < 1$, so $s\gamma \equiv r \mod p$. Then $|\gamma - x|_p < 1$. Now choose $a_0 \in \{0, \dots, p-1\}$ with $\gamma \equiv a_0 \mod p$. Then $|a_0 - x|_p < 1$. So $|(a_0 - x)/p|_p \leq 1$, and repeating the process, there exists $a_1 \in \{0, \dots, p-1\}$ with $|(a_0 - x)/p - a_1|_p < 1$, and so on. $|x - a_0 - a_1 p|_p \leq 1/p^2$, etc.

□

Lecture 5 Friday 12/10/18

Corollary 1.14. Every element of $\mathbb{Q}_p$ has a unique expression as $a = \sum_{n \geq -T} a_n p^n$ for $a_n \in \{0, \dots, p-1\}$, $a_{-T} \neq 0$, and $|a|_p = p^T$.

Proof. Given $a \in \mathbb{Q}_p$, let T be such that $|a|_p = p^T$. Apply Proposition 1.13 to $p^T a$. □

Corollary 1.15. $\mathbb{Z}$ is dense in $\mathbb{Z}_p$.

Proof. If $a \in \mathbb{Z}_p$, write $a = \sum_{n=0}^{\infty} a_n p^n$. Then $\sum_{n=0}^{N} a_n p^n$ is a sequence in $\mathbb{Z}$ which converges to a. □

For each $n \geq 1$ there is a ring homomorphism $\mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ that sends $\sum_{i=0}^{\infty} a_i p^i \mapsto \sum_{i=0}^{n} a_i p^i$. The kernel of this map is $p^n\mathbb{Z}_p$, so $\mathbb{Z}_p/p^n\mathbb{Z}_p \cong \mathbb{Z}/p^n\mathbb{Z}$.

Note. In fact, $\mathbb{Z}_p \cong \lim_{\leftarrow n} \mathbb{Z}/p^n\mathbb{Z}$.

$p\mathbb{Z}_p$ is a maximal ideal of $\mathbb{Z}_p$ because $\mathbb{Z}_p/p\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$ is a field. If $a \in \mathbb{Z}_p$, $a \notin p\mathbb{Z}_p$, then $a \in \mathbb{Z}_p^*$. Write $a = a_0 + pa_1 + \dots$ for $a_0 \in \{1, \dots, p-1\}$.

Example. $a = a_0 + pA$. Show that a has an inverse using the formula for the sum of a geometric progression. (TODO Exercise) For example $(1-p)^{-1} = 1 + p + \dots$.

Alternatively, $a \in \mathbb{Z}_p$ is in $p\mathbb{Z}_p$ iff $|a|_p < 1$. So if $a \in \mathbb{Z}_p \setminus p\mathbb{Z}_p$, then $|a|_p = 1$. Then $|1/a|_p = 1/|a|_p = 1$, so $1/a \in \mathbb{Z}_p$. $1/a$ exists because $\mathbb{Q}_p$ is a field. So $p\mathbb{Z}_p$ is the unique maximal ideal of $\mathbb{Z}_p$, so $\mathbb{Z}_p$ is a local ring. $\mathbb{Z}_p^* = \mathbb{Z}_p \setminus p\mathbb{Z}_p$ is the group of units. Terminology: $a \in \mathbb{Q}_p$ is a **unit** iff $a \in \mathbb{Z}_p^*$, so iff $|a|_p = 1$.

Lemma 1.16. $a \in \mathbb{Z}_p^*$ iff $|a|_p = 1$.

Proof. TODO - bring above paragraph down here. ☐

Corollary 1.17. Every element of $\mathbb{Q}_p^* = \mathbb{Q}_p \setminus \{0\}$ is uniquely of the form $p^n u$ for $n \in \mathbb{Z}$ and $u \in \mathbb{Z}_p^*$.

Proof. Set $|a|_p = p^{-n}$, then $|p^{-n}a|_p = 1$, so $u = p^{-n}a$, so $a = up^n$. ☐

Aim is to solve the equation $x^2 - 7 = 0$ in $\mathbb{Z}_3$ starting with a solution to $x^2 \equiv 7 \mod 3$. We did this by solving $x^2 \equiv 7 \mod 3^n$ for $n = 1, 2, \dots$. Write $f(x) = x^2 - 7$. Then $|f(1)|_3 = 1/3$, $|f(4)|_3 = 1/9$, $|f(13)|_3 = 1/27$, etc. So starting with $x_0 = 1$, we construct a sequence (x_n) with $|x_{n+1} - x_n| \le 1/3^{n+1}$ and $|f(x_{n+1})|_3 \le 1/3^n$. So in particular (x_n) is Cauchy, and so converges to some $x \in \mathbb{Q}_3$ with $f(x) = 0$. Newton-Raphson method over $\mathbb{R}$ works over $\mathbb{Q}_p$, and this is called **Hensel's Lemma**.

Definition 1.18. If R is a ring and $f(X) \in R[X]$ is a polynomial, say $f(x) = \sum_{n=0}^m a_n x^n$, then $f'(x) = \sum_{n=0}^m n a_n x^{n-1}$.

In addition, for any x, h we have $f(x+h) = f(x) + hf'(x) + \frac{1}{2}h^2 f''(x) + \dots$. Why is $\frac{1}{2}f''(x)$ defined? If $f(x) = \sum_{n=0}^\infty a_n x^n$, $\frac{1}{2}f''(x) = \sum_{n=2}^\infty \frac{1}{2}n(n-1)a_n x^{n-2}$, where $n(n-1)$ is even.

Theorem 1.19 (Hensel's Lemma)**.** Let k be a field which is complete with respect to a nonarchimedean norm $|\cdot|$. Let $R = \{x \in k \mid |x| \le 1\}$, such as $k = \mathbb{Q}_p$, $R = \mathbb{Z}_p$, $|\cdot| = |\cdot|_p$. Let $f(x) \in R[x]$, and $t_0 \in R$ with $|f(t_0)| > |f'(t_0)|^2$. Then there is a unique $t \in R$ with $f(t) = 0$ and $|t - t_0| < |f'(t_0)|$. Moreover, $|f'(t_0)| = |f'(t_0)|$, and $|t_- t_0| = |f(t_0)| / |f'(t_0)| < 1$.

Example. Let $k = \mathbb{Q}_3$ and $f(x) = x^2 - 7$. Then $f'(x) = 2x$. $t_0 = 1$, so $|f(t_0)|_3 = |-6|_3 = 1/3$. $|f'(t_0)|_3 = |2|_3 = 1$. So there is a unique $t \in \mathbb{Z}_3$ with $t^2 = 7$ and $|t-1|_3 < 1$, so $t \equiv 1 \mod 3$.

Harder part of the proof of Hensel's Lemma is existence, which is done by constructing a sequence $t_0, t_1, \dots$ as above. For uniqueness, suppose $s \ne t$ and $f(s) = f(t) = 0$, and $|s - t_0| < |f'(t_0)|$ and $|t - t_0| < |f'(t_0)|$, so $|s - t| \le \max(|s - t_0|, |t - t_0|) < |f'(t_0)|$. Taylor expansion gives $f(s) = f(t) + (s-t)f'(t) + \dots$. So there exists $x \in R$ with $(s-t)f'(t) = (s-t)^2 = x$. So $f'(t) = (s-t)x$. $|f'(t)| = |s-t||x| \le |s-t| < |f'(t_0)|$. So $|f'(t)| < |f'(t_0)|$. On the other hand it is easy to show that $|f'(t)| = |f'(t_0)|$, a contradiction. See handout for the full proof of Hensel's Lemma and some remarks about in what sense it is best possible. Lecture 6 Tuesday 16/10/18

What are the squares in $\mathbb{Q}_p^*$? We know that we can write any element of $\mathbb{Q}_p^*$ uniquely as $p^n u$ for u a unit, that is $|u|_p = 1$. Suppose that $p^n u = (p^r v)^2$ for $r \in \mathbb{Z}$ and v a unit. Then $p^n = p^{2r}$ and $u = v^2$, that is $n = 2r$ and $u = v^2$, that is the squares in $\mathbb{Q}_p^*$ are exactly the $p^{2r}u$, where $u \in \mathbb{Z}_p^*$ is a square. If $p > 2$, we claim that u is a square iff u is a square modulo p, that is u is a quadratic residue. If $u = t^2$, then $u \equiv t^2 \mod p$. Conversely, suppose that $u \equiv t_0^2 \mod p$. Now use Hensel's lemma with $f(X) = X^2 - u$ and t_0 as above. $|f(t_0)|_p = |t_0^2 - u|_p \le |p|_p = 1/p$. $|f'(t_0)|_p = |2t_0|_p = |t_0|_p = 1$. If $p \mid t_0$ then $p \mid u$ because $u \equiv t_0^2 \mod p$. Hensel's lemma gives a unique $t \in \mathbb{Z}_p$ such that $t^2 = u$ and $|t - t_0| < 1$, that is $t \equiv t_0 \mod p$. In this case, the equation $X^2 = u$ has exactly two solutions, namely t and $-t$. In any field, a polynomial of degree d has at most d roots. For $p = 2$, $u \in \mathbb{Z}_2^*$ is a square iff there exists t_0 such that $u \equiv t_0^2 \mod 8$, that is $u \equiv 1 \mod 8$, since $(2m+1)^2 = 4m(m+1) + 1 \equiv 1 \mod 8$.

(TODO missing)

2 Basic algebraic geometry

We want to consider curves in the plane given by the equations $f(x, y) = 0$. We want to understand the points of intersection of two such curves.

Example. If C has degree two and g has degree one, we expect to get in general two points of intersection.

More generally, if f has degree a and g has degree b, can hope to get ab points of intersection. This can fail to be true in several different ways.

1. $y = x^2$ and $y = 0$, that is $f = y - x^2$, $g = y$, meet only at $(0,0)$. Solution is to count this point with multiplicity two. In this course, we will explain exactly when the multiplicity is one.
2. For $x^2 - y^2 = 0$ and $x^3 - y^3 = 0$, any point with $x = y$ is on the intersection. Solution is to demand that f and g are coprime, that is they have no common factor, unlike $x^2 - y^2 = (x-y)(x+y)$ and $x^3 - y^3 = (x-y)\left(x^2 + xy + y^2\right)$.
3. $y = x^2$ and $y = 2$ intersect at $\left(\pm\sqrt{2}, \sqrt{2}\right)$. But if for example we are working over $\mathbb{Q}$, these points do not exist. Solution is to only work over fields which are algebraically closed, such as $\mathbb{C}$.
4. $y = x + 1$ and $y = x$ meet at infinity in projective space.

Definition 2.1. A field K is **algebraically closed** if every polynomial over K of degree at least one factors as a product of linear factors.

Example. $K = \mathbb{C}$ is algebraically closed. $K = \mathbb{Q}, \mathbb{R}$ is not algebraically closed. Any finite field is not algebraically closed.

A basic fact is if k is an field, there exists an algebraically closed field K with $k \subset K$, and in fact there exists a smallest possible choice, the **algebraic closure** of k.

Lecture 7 Thursday 18/10/18

Definition 2.2. If $f \in k[x_1, \dots, x_n]$ of degree d, then the **homogenisation** of f is the polynomial $F \in k[X_1, \dots, X_{n+1}]$ obtained as follows. If

$$f = \sum_{\underline{i}=(i_1,\dots,i_n)\in\mathbb{Z}_{\geq 0}^n} a_{\underline{i}} x_1^{i_1} \dots x_n^{i_n} \qquad \implies \qquad F = \sum_{\underline{i}} a_{\underline{i}} X_1^{i_1} \dots X_n^{i_n} X_{n+1}^{d-(i_1+\dots+i_n)}.$$

Given $G \in k[X_1, \dots, X_{n+1}]$ homogeneous of degree d, that is every monomial in G has degree exactly d, then for each $1 \leq i \leq n+1$, the i-th **dehomogenisation** is given by setting $X_i = 1$ and writing x_j for X_j.

Example. Let $G = X_1^2 X_2^2 + X_3^4 + X_2 X_3^2$, so $n = 2$. First dehomogenisation is $x_2^2 + x_3^4 + x_2 x_3^3$. Second dehomogenisation is $x_1^2 + x_3^4 + x_3^3$. Third dehomogenisation is $x_1^2 x_2^2 + 1 + x_2$.

If $n = 2$, usually write x, y and X, Y, Z for our variables.

Example. If $f = y^2 + x^3 + x + 1$, $F = Y^2 Z + X^3 + XZ^2 + Z^3$. Dehomogenisations of F are $y^2 z + 1 + z^2 + z^3$, $z + x^3 + xz^2 + z^3$, and $y^2 + x^3 + x + 1$.

Let k be a field, and define an equivalence relation on k^{n+1} by $(a_1, \dots, a_{n+1}) \sim (b_1, \dots, b_{n+1})$ iff there exists $\lambda \in k^*$ such that $b_i = \lambda a_i$ for $1 \leq i \leq n+1$.

Definition 2.3. For each $n \geq 0$, $\mathbb{P}^n(k)$, **the n-dimensional projective space over** k, is defined to be

$$k^{n+1} \setminus \{(0, \dots, 0)\} / \sim .$$

Write $[a_1 : \dots : a_{n+1}]$ for the equivalence class of $(a_1, \dots, a_{n+1})$ in $\mathbb{P}^n(k)$. This makes sense as long as some $a_i \neq 0$.

Let us see why we can think of $\mathbb{P}^n(k)$ as being k^n together with some points at infinity.

Example. $\mathbb{P}^1(k)$ should be k together with a point infinity. Any point of $\mathbb{P}^1(k)$ is of the form $[a_1 : a_2]$ with a_1, a_2 not both zero. If $a_2 \neq 0$, then $[a_1 : a_2] = [a_1/a_2 : 1]$. On the other hand, if $[a : 1] = [b : 1]$, then there exists $\lambda \in k^*$ such that $(a, 1) = \lambda(b, 1) = (b\lambda, \lambda)$, so $\lambda = 1$ and $a = b$. So there is a bijection between k and the points $[a_1 : a_2]$ with $a_2 \neq 0$, given by $k \to \mathbb{P}^1(k)$ by $a \mapsto [a : 1]$. The remaining points of $\mathbb{P}^1(k)$ are those with $a_2 = 0$. Then $[a_1 : 0] = [1 : 0]$, so we have exactly one point in $\mathbb{P}^1(k) \setminus k$, the point at infinity.

For each $1 \leq i \leq n+1$, let $\phi_i : k^n \to \mathbb{P}^n(k)$ be the map putting one in the i-th coordinate, that is $(a_1, \dots, a_n) \mapsto [a_1 : \dots : a_{i-1} : 1 : a_i : \dots : a_n]$.

Example. $\phi_{n+1}((a_1, \dots, a_n)) = [a_1 : \dots : a_n : 1]$.

Lemma 2.4. Each map ϕ_i is injective.

Proof. If $[a_i : \dots : a_{i-1} : 1 : a_i : \dots a_n] = [b_1 : \dots : b_{i-1} : 1 : b_i : \dots : b_n]$ then $(a_1, \dots, a_{i-1}, 1, a_i, \dots, a_n) = \lambda(b_1, \dots, b_{i-1}, 1, b_i, \dots, b_n)$. Looking at i-th coordinate, $\lambda = 1$, so $a_j = b_j$ for all j. □

Usually think of k^n as lining inside $\mathbb{P}^n(k)$ via ϕ_{n+1}. Think of the complement as the points at infinity, that is the points $[x_1 : \dots : x_n : 0]$. Given a polynomial $F \in k[X_1, \dots, X_{n+1}]$, it never makes sense to ask what the value of F at $[a_1 : \dots : a_{n+1}] \in \mathbb{P}^n(k)$ is, because $[a_1 : \dots : a_{n+1}] = [\lambda a_1 : \dots : \lambda a_{n+1}]$. On the other hand, if F is homogeneous of degree d, then $F(\lambda a_1, \dots, \lambda a_{n+1}) = \lambda^d F(a_1, \dots, a_{n+1})$, so it does makes sense to ask whether or not $F([a_1 : \dots : a_{n+1}]) = 0$. The **graph** of $F(X, Y, Z)$ homogeneous are the points P of $\mathbb{P}^2(k)$ where $F(P) = 0$. If F is the homogenisation of f, then the graph of F is the graph of f together with points at infinity. (TODO Exercise: $f(a, b) = 0$ iff $F(a, b, 1) = 0$)

Example. f is a line, say $f = y - mx - c$, so $F = Y - mX - cZ$. What are the points at infinity? If $Z = 0$ and $Y = mX$, that is $[1 : m : 0]$, the line $y = mx + c$ has one point at infinity, namely $[1 : m : 0]$. If $X = 0$, points at infinity are $Z = 0$, $[0 : Y : 0] = [0 : 1 : 0]$. So two lines meet at infinity iff they are parallel.

Lecture 8 Friday 19/10/18

Proof of the following theorem is in Fulton's Algebraic Curves.

Theorem 2.5 (Bézout's theorem)**.** Let F, G be homogeneous polynomials in $k[X, Y, Z]$ of degrees a, b respectively. If F and G have no common factors, and k is algebraically closed, then the graphs of $F = 0$ and $G = 0$ meet at ab points in $\mathbb{P}^2(k)$, counted with multiplicities.

Corollary 2.6. If F, G are as in Theorem 2.5, and for some k, $F = 0$ and $G = 0$ meet at more than ab points with multiplicity, then F and G have a common factor.

Definition 2.7. If $f \in k[x_1, \dots, x_n]$ is a polynomial, and let $P = (a_1, \dots, a_n) \in k^n$ with $f(P) = 0$. Then P is a **smooth** point of the graph of f, or a **nonsingular** point, if for some i, $(\partial f / \partial x)(P) \neq 0$. A singular point is one for which all $(\partial f / \partial x_i)(P) = 0$ for $1 \le i \le n$.

Example. $(\partial / \partial x_2)(x_1 x_2^5) = 5 x_1 x_2^4$.

Example. If $f = x^2 - y^5$, $\partial f / \partial x = 2x$ and $\partial f / \partial y = -5y^4$. $(0, 0)$ is singular and $(1, 1)$ is nonsingular.

Motivation is that tangent space to $f = 0$ at P should be $\sum_{i=1}^{n} (\partial f / \partial x_i)(P)(x_i - a_i) = 0$. Generalising to projective space, consider $F \in k[X_1, \dots, X_{n+1}]$ homogeneous. Consider P with $F(P) = 0$. Say that P is nonsingular if at least one $(\partial F / \partial X_i)(P) \neq 0$ for $1 \le i \le n + 1$, singular if all $(\partial F / \partial X_i)(P) = 0$.

A fact is $Im(P) \in Im(\phi_i)$ for $\phi_i : k^n \to \mathbb{P}^n(k)$ insert 1 at i-th coordinate. Then P is nonsingular as a point of $F = 0$ iff the corresponding point $\phi_i^{-1}(P)$ is nonsingular for the i-th dehomogenisation of F. A key fact is if F is homogeneous of degree d, then $dF = \sum_{i=0}^{n+1} X_i (\partial F / \partial X_i)$.

Definition 2.8. Say the graph of f or F is nonsingular, or smooth, if it is nonsingular at every point of k^n or $\mathbb{P}^n(k)$ respectively.

Example. Any polynomial of degree one has a nonsingular graph. If $f = \sum_{i=1}^{n} a_i x_i$, then $\partial f / \partial x_i = a_i$.

Example. Let $k = \mathbb{Q}$.

1. $y^2 = x^2(x + 1) = x^3 + x^2$. If $f = y^2 - x^3 - x^2$, then $\partial f / \partial x = -3x^2 - 2x$ and $\partial f / \partial y = 2y$. So if f is singular, $y = 0$, so $x = 0$ or $x = -1$, so $x = 0$. So $(0, 0)$ is the only singular point.
2. If $f = y^2$, then $\partial f / \partial x = 0$ and $\partial f / \partial y = 2y$. So any point $(x, 0)$ is singular.
3. $y^2 = (x^2 - 2)^2$ has singular points $(\pm\sqrt{2}, 0)$. Still say that this is singular, even though the singular points are not defined over $\mathbb{Q}$.

Example. If $y = x + 1$, then $F = Y - X - Z$. $\partial F / \partial X = -1$, $\partial F / \partial Y = 1$, $\partial F / \partial Z = -1$. This is non singular.

Example. If $y = x^3$, then $F = YZ^2 - X^3$. $\partial F / \partial X = -3X^2$, $\partial F / \partial Y = Z^2$, $\partial F / \partial Z = 2YZ$. So $X = Z = 0$, that is $[0 : 1 : 0]$ is a singular point. Homogenise with respect to Y gives $z^2 - x^3 = 0$ singular at $(x, z) = (0, 0)$.

Theorem 2.9. If $f, g \in k[x, y]$ then a point P on $f = 0$ and $g = 0$ has multiplicity one iff

1. P is a nonsingular point for both $f = 0$ and $g = 0$, and
2. the tangent lines to $f = 0$ and $g = 0$ at P are distinct.

Tangent line at P is
$$(\partial f / \partial x)(P)(x - x(P)) + (\partial f / \partial y)(P)(x - y(P)) = 0.$$

3 Plane conics

Let k be a field. $k[X]$ is a PID, so a UFD. $k[X_1, \dots, X_n]$ is a UFD, but not a PID.

Example. (X_1, X_2) in $k[X_1, X_2]$ is not principal.

If k is algebraically closed, then the prime ideals of $k[X]$ are just (0) and $(X - \alpha)$ for $\alpha \in K$. If k is not algebraically closed, you have more.

Example. $\left(X^2 - 2\right)$ is a prime ideal of $\mathbb{Q}[X]$.

Even if k is algebraically closed, there are many prime ideals in $k[X, Y]$ than in $k[X]$.

Example. $X^2 - Y^2 - 1$ does not factor in $\mathbb{C}[X, Y]$.

Lecture 9 Tuesday 23/10/18

A **plane conic** is just the graph of some $f \in k[x, y]$ where f has degree two. Same terminology also covers $F = 0$ for $F \in k[X, Y, Z]$ homogeneous of degree two. The next steps are

1. to understand when this is singular,
2. to understand how to find all solutions to $f = 0$ or $F = 0$ if it is singular, and
3. to understand how to find all solutions to $f = 0$ in the nonsingular case given one solution.

Then in the next section we will specialise to $k = \mathbb{Q}$ and see how to find solutions, or prove there are not any.

Example. $x^2 - y^2$ is singular, because $(0, 0)$ is a singular point.

Algorithm 3.1 (Checking if $f = 0$ is singular)**.** Suppose $f \in k[x, y]$ degree two. Then any singular points are given by solving $\partial f / \partial x = 0$, $\partial f / \partial y = 0$. These are linear, so solve them and substitute back into $f = 0$.

Example. Let $f = x^2 - y^2 - 1$. $\partial f / \partial x = 2x$ and $\partial f / \partial y = -2y$ gives $x = y = 0$, so $f(0, 0) \neq 0$. So f is nonsingular.

Example. Let $f = x^2 - 2xy + y^2 = (x - y)^2$. $\partial f / \partial x = 2x - 2y$ and $\partial f / \partial y = 2y - 2x$. If characteristic of $k \neq 2$, solutions are $x = y$, and any such point is a solution. So every point is singular.

Theorem 3.2. Let k be algebraically closed, and let $f \in k[X, Y, Z]$ be homogeneous of degree two. Then f has a singular point in $\mathbb{P}^2(k)$ iff F is a product of two linear factors.

Proof. If F factors, then any point of intersection of the two lines is a singular point. (TODO Exercise) The lines do meet, by Bézout. Suppose conversely that P is a singular point of $F = 0$. Let Q be any other point of $F = 0$, and let L be the line joining P and Q, so L is given by some equation $G = 0$, where G has degree one. If $F = GH$ for some H, then we are done. Otherwise, F and G are coprime because G has degree one, so has no proper factors. So by Bézout's theorem, $F = 0$ and $G = 0$ meet in exactly two points, counted with multiplicity. Since P is a singular point of $F = 0$, it follows from Theorem 2.9 that the multiplicity of P is at least $2 + 1 = 3$, a contradiction. So G is a factor of F, as required. $\square$

Algorithm 3.3 (Finding all rational points on a singular conic)**.**

1. Find the singular point.
2. Write down another point.
3. Factor the conic as a product of linear factors.
4. Solve the two linear equations.

Example. Let $F = X^2 - 2Y^2$. Singular point is $2X = -4Y = 0$, so $X = Y = 0$. Any other point is $Y = 1$ and $X = \sqrt{2}$. $X = \sqrt{2}Y$ is the line through these two points. So $X - 2Y$ is a factor of $X^2 - 2Y^2$, and indeed $X^2 - 2Y^2 = \left(X + \sqrt{2}Y\right)\left(X - \sqrt{2}Y\right)$. So if $k = \mathbb{C}$, then the solutions are $\left(\pm\sqrt{2}t, t\right)$ for $t \in \mathbb{C}$. If $k = \mathbb{Q}$, the only solution is $(0, 0)$.

Example. Now for a nonsingular case, let $x^2 + 2y^2 = 6$. Start with one solution, such as $(2, 1)$. Find all solutions by drawing lines through this point.

Algorithm 3.4. Let F be a nonsingular conic over some field k, and suppose that we are given a point with coordinates in k where $F = 0$. Then we can find all points by drawing lines with rational slope through this point, and finding the second point of intersection with $F = 0$.

Note. If k is algebraically closed, then Bézout tells us that we have exactly two points of intersection, when counted with multiplicity. Since f is nonsingular, and any line is nonsingular, the only way you can have a multiplicity is if the line you draw is the tangent line at that point. If k is not algebraically closed, just need to check that the other point of intersection has coordinates in k iff the slope of the line joining the points is in k. (TODO Exercise)

Lecture 10 is a problem class. Lecture 10 Thursday 25/10/18

4 The Hasse principle

Lecture 11 Friday 26/10/18

We have seen that for any field k, and any plane conic, there are algorithms to

1. check if the conic is singular or not,
2. if it is singular, write it as a product of two linear factors, and so find all the points over k, and
3. if it is nonsingular, or smooth, find all points over k given one such point, by drawing lines through this point.

What is missing is given a nonsingular curve, determine if it has any points over k, and find such a point if there is one. For $k = \mathbb{Q}$, we will do this by using the cases $k = \mathbb{Q}_p$ for all primes p. Over $\mathbb{Q}_p$, it is not so hard to check if there are points. Use Hensel's lemma to reduce modulo p, use quadratic reciprocity. Very easy over $\mathbb{R}$. Hasse's principle says a nonsingular plane conic over $\mathbb{Q}$ has points over $\mathbb{Q}$ if and only if it does over $\mathbb{Q}_p$ and $\mathbb{R}$ for all p. Forward direction is trivial, converse direction is harder. Crucially, this holds for conics, that is polynomials of degree two, but not true for degree three or higher.

Example. $3X^3 + 4Y^3 + 5Z^3$.

Example. $X^2 + Y^2 = 6$ has no solution in $\mathbb{Q}_3$ gives none in $\mathbb{Q}$. $X^2 + Y^2 = -1$ has no solution in $\mathbb{R}$ gives none in $\mathbb{Q}$.

Basic idea is if we have solutions to some equation in every $\mathbb{Q}_p$, we have solutions modulo N for all $N \in \mathbb{Z}$. Use Chinese remainder theorem to reduce to $N = p^k$, Hensel's Lemma says that equations have solutions in $\mathbb{Z}_p$ iff modulo p^k for all k. We would like a technique for upgrading solutions to congruences to solutions to equations in $\mathbb{Q}$ or in $\mathbb{Z}$. Aim is to prove that if $p \equiv 1 \mod 4$ then $p = x^2 + y^2$ for some $x, y \in \mathbb{Z}$. Input is n such that $n^2 \equiv -1 \mod p$.

Lemma 4.1. If $U \subset \mathbb{R}^n$ is measurable, or just open, and its measure, or volume, is bigger than m, then we can find distinct points $c_0, \dots, c_m$ such that for all i, $c_0 - c_i \in \mathbb{Z}^n$.

Proof. Let C be the unit cube, $C = \{(x_1, \dots, x_n) \in \mathbb{R}^n \mid \forall i,\ 0 \le x_i < 1\}$. By assumption $\int_{\mathbb{R}^n} 1_U(x)\, dx > m$ where

$$1_U(x) = \begin{cases} 1 & x \in U \\ 0 & x \notin U \end{cases}.$$

$\int_{\mathbb{R}^n} 1_U(x)\, dx = \int_C \sum_{t \in \mathbb{Z}^n} 1_U(x+t)\, dx > m$. The measure of C is 1, so there exists $x \in C$ such that $\sum_{t \in \mathbb{Z}^n} 1_U(x+t) > m$. So there exists $t_0, \dots, t_m \in \mathbb{Z}^n$, $x \in C$ such that $x + t_i \in U$ for all i. Set $c_i = x + t_i$. ☐

Definition 4.2. Say U is **convex** if $x, y \in U$ and $\lambda \in [0,1]$ gives $\lambda x + (1-\lambda) y \in U$. Say that U is **symmetric** if $x \in U$ gives $-x \in U$.

Corollary 4.3 (Minkowski)**.** If $\Lambda \in \mathbb{Z}^n$ is a finite index subgroup, and if V is convex and symmetric, with measure greater than $2^n [\mathbb{Z}^n : \Lambda]$, then $V \cap \Lambda \neq \{0\}$.

Remark 4.4. $0 \in V$, because given $x \in V$, $-x \in V$, so $\frac{1}{2}(x + (-x)) \in V$.

A **lattice** is a finite index subgroup of $\mathbb{Z}^n$.

Proof. Set $U = \frac{1}{2} V = \left\{ \frac{1}{2} x \mid x \in V \right\}$. So measure of U is greater than $[\mathbb{Z}^n : \Lambda] = m$. By Lemma 4.1, there exists $c_0, \dots, c_m \in U$ such that $c_i - c_0 \in \mathbb{Z}^n$ for all i. Consider $c_0 - c_0, \dots, c_m - c_0 \in \mathbb{Z}^n$. We have $m+1$ differences, so there exists $i \neq j$ such that $(c_i - c_0) - (c_j - c_0) \in \Lambda$, that is $c_i - c_j \in \Lambda$, $c_i - c_j \neq 0$. Since $c_i - c_j = \frac{1}{2}(2c_i - 2c_j)$, $2c_i, 2c_j \in V$ by definition, and $-2c_j \in V$ by symmetry, so $\frac{1}{2}(2c_i - 2c_j) \in V$ by convexity. ☐

How do you use this to prove that $p = x^2 + y^2$?

Lecture 12 Tuesday 30/10/18

Theorem 4.5. If $n \in \mathbb{Z}$ and there exists t such that $t^2 \equiv -1 \mod n$, then there exists $x, y \in \mathbb{Z}$ such that $x^2 + y^2 = n$.

Proof. $\Lambda = \{(x,y) \mid y \equiv tx \mod n\} \subseteq \mathbb{Z}^2$. $\Lambda = Ker\left(\mathbb{Z}^2 \to \mathbb{Z}/n\mathbb{Z}\right)$ by $(x,y) \mapsto y - tx$. This is surjective, so by the first isomorphism theorem, $\mathbb{Z}^2/\Lambda \cong \mathbb{Z}/n\mathbb{Z}$. So $\left[\mathbb{Z}^2 : \Lambda\right] = \#(\mathbb{Z}/n\mathbb{Z}) = n$. Let $V = \left\{(x,y) \mid x^2 + y^2 < 2n\right\}$. Measure of V is $\pi\left(\sqrt{n}\right)^2 = 2\pi n = 2^2\left[\mathbb{Z}^2 : \Lambda\right] = 4n$ because $\pi > 2$. So by Corollary 4.3, there exists $(x,y) \in \Lambda \cap V$ such that $(x,y) \neq (0,0)$. $(x,y) \in V$ gives $0 < x^2 + y^2 < 2n$. $(x,y) \in \Lambda$ gives $x^2 + y^2 \equiv x^2\left(t^2 + 1\right) \equiv 0 \mod n$. So $x^2 + y^2 = n$, as required. ☐

Want to consider plane conics over $\mathbb{Q}$, that is homogeneous equations of degree two in X, Y, Z . Completing the square, that is existence of orthogonal basis, can write this in the form $aX^2 + bY^2 + cZ^2$. If this is nonsingular, $abc \neq 0$. Conversely if $abc \neq 0$, this is nonsingular. Rescaling X, Y, Z, we can change a, b, c by squares of elements of $\mathbb{Q}^*$. So without loss of generality, a, b, c are all in $\mathbb{Z}$. We can then furthermore arrange by rescaling again that each of a, b, c is squarefree, that is not divisible by the square of any prime. If a, b, c share a common factor, we can divide by it, so we can assume that $(a,b,c) = 1$. If $p \mid a$, $p \mid b$, so $p \mid c$, we can replace (a,b,c) by $(a/p, b/p, pc)$ since $aX^2 + bY^2 + cZ^2 = p\left((a/p)X^2 + (b/p)Y^2 + pc(Z/p)^2\right)$. Repeating this, we can assume that $(a,b) = 1$, $(b,c) = 1$, $(c,a) = 1$. So without loss of generality $aX^2 + bY^2 + cZ^2$, a, b, c nonzero squarefree integers, pairwise coprime. Let $\Sigma = \{p \mid 2abc\}$ for p prime.

Lemma 4.6. Write $F = aX^2 + bY^2 + cZ^2$ as above. Then the following are equivalent.

1. $F = 0$ has infinitely many solutions in $\mathbb{P}^2(\mathbb{Q})$.
2. $F = 0$ has a solution in $\mathbb{P}^2(\mathbb{Q})$.
3. $F = 0$ has solutions in $\mathbb{P}^2(\mathbb{Q}_p)$ for all p and in $\mathbb{P}^2(\mathbb{R})$.
4. $F = 0$ has solutions in $\mathbb{P}^2(\mathbb{Q}_p)$ for all $p \in \Sigma$.

Proof. $1 \implies 2 \implies 3 \implies 4$. $2 \implies 1$ by drawing lines through a point. So we need to do $4 \implies 2$. Use Corollary 4.3 in $\mathbb{Z}^3$. Want to find V, Λ with measure of V greater than $2^3 \left[\mathbb{Z}^3 : \Lambda\right]$, so that $V \cap \Lambda = \{0\}$. Want to know that we will have $ax^2 + by^2 + cz^2 = 0$ if $(x, y, z) \in V \cap \Lambda$. Choose $V = \left\{|a| x^2 + |b| y^2 + |c| z^2 < 4 |abc|\right\}$. This has measure $\frac{\pi}{3} \cdot 2^3 \cdot 4 |abc|$. So to prove the theorem, it is enough to find Λ with $\left[\mathbb{Z}^3 : \Lambda\right] = 4 |abc|$, and satisfying $(x, y, z) \in \Lambda$ gives $ax^2 + by^2 + cz^2 \equiv 0 \mod 4 |abc|$. So if $(x, y, z) \in V \cap \Lambda$ then $0 \le \left|ax^2 + by^2 + cz^2\right| < |a| x^2 + |b| y^2 + |c| z^2 < 4 |abc|$, so $ax^2 + by^2 + cz^2 = 0$. ☐

Lecture 13 Thursday 01/11/18

Lemma 4.7. If $p \mid a$ then there is a solution to $b + cz^2 \equiv 0 \mod p$.

Proof. $p \mid a$ gives $p \in \Sigma$ so there exists $x, y, z \in \mathbb{Q}_p$ not all zero such that $ax^2 + by^2 + cz^2 = 0$. By multiplying by an appropriate power of p, we can assume that $\max\left(|x|_p, \langle y\rangle_p, |z|_p\right) = 1$. $p \mid a$ and $(a, b) = (a, c) = 1$ gives $p \nmid b$, $p \nmid c$, that is $|a|_p < 1$ and $|b|_p = |c|_p = 1$. If $|y|_p < 1$ then $\left|by^2\right|_p < 1$, $\left|ax^2\right|_p \le |a|_p < 1$, so $\left|cz^2\right|_p = \left|ax^2 + by^2\right| < 1$, so $|z|_p < 1$. Then $|x|_p = 1$, so $\left|ax^2\right|_p = |a|_p$ but $\left|ax^2\right|_p = \left|by^2 + cz^2\right|_p \le \max\left(\left|y^2\right|_p, \left|z^2\right|_p\right) \le 1/p^2$. So $p^2 \mid a$, a contradiction, as a is squarefree. So $|y|_p = 1$. Now divide by y, $a (x/y)^2 + b + c (z/y)^2 = 0$ and $x/y, z/y \in \mathbb{Z}_p$. Reduce modulo p gives $b + c (z/y)^2 \equiv 0 \mod p$, as claimed. ☐

If $p \in \Sigma$ and $p > 2$, then by symmetry without loss of generality $p \mid a$. Then the lemma applies, so there exists α with $b + c\alpha^2 \equiv 0 \mod p$. So we impose the condition that $z \equiv \alpha y \mod p$. Then if $x, y, z \in \mathbb{Z}$ satisfying $z \equiv \alpha y \mod p$, then $ax^2 + by^2 + c \equiv by^2 + cz^2 \equiv by^2 + c\alpha^2 y^2 \equiv y^2 \left(b + c\alpha^2\right) \equiv 0 \mod p$. Now have to deal with $p = 2$. Suppose $2 \mid a$. Lemma gives a solution to $b + cz^2 \equiv 0 \mod 2$, and a solution to $ax^2 + by^2 + cz^2 = 0$ in $\mathbb{Q}_2$ with $|y|_2 = 1$, so $y^2 \equiv 1 \mod 8$. $(2m + 1)^2 = 4m (m + 1) + 1 \equiv 1 \mod 8$. In fact, squares modulo 8 are 0, 1, 4. Similarly, $|z|_2 = 1$ gives $z^2 \equiv 1 \mod 8$. Since $ax^2 + by^2 + cz^2 = 0$, $ax^2 + by^2 + cz^2 = 0$, $ax^2 + by^2 + cz^2 \equiv 0 \mod 8$, that is $ax^2 + b + c \equiv 0 \mod 8$. If $|x|_2 = 1$ then $x^2 \equiv 1 \mod 8$, so $a + b + c \equiv 0 \mod 8$. Impose

$$y \equiv z \mod 4, \qquad x \equiv y \mod 2.$$

If $(x, y, z) \in \mathbb{Z}^3$ satisfies this condition, then either x, y, z all odd, and $ax^2 + by^2 + cz^2 \equiv a + b + c \equiv 0 \mod 8$, or x, y, z all even, and $ax^2 + by^2 + cz^2 \equiv by^2 + cz^2 \mod 8$. $y \equiv z \mod 4$ gives either $4 \mid y$, $4 \mid z$, which is fine, or $y \equiv z \equiv 2 \mod 4$, and $by^2 + cz^2 \equiv 4 (b + c) \equiv -4a \equiv 0 \mod 8$. If $|x|_2 < 1$, then $ax^2 \equiv 0 \mod 8$, so $b + c \equiv 0 \mod 8$. Impose

$$y \equiv z \mod 4, \qquad x \equiv 0 \mod 2.$$

Then if these conditions hold, $ax^2 + by^2 + cz^2 \equiv by^2 + cz^2 \equiv (b + c) y^2 \equiv 0 \mod 8$. The cases $2 \mid b$, $2 \mid c$ are dealt with by symmetry. Now suppose that $2 \nmid abc$. Again $2 \in \Sigma$ gives by assumption $x, y, z \in \mathbb{Q}_2$ not all zero with $ax^2 + by^2 + cz^2 = 0$. Again, without loss of generality $\max(|x|_2, |y|_2, |z|_2) = 1$ or without loss of generality $|z|_2 = 1$, so $\left|cz^2\right|_2 = 1$, so at least one of $|x|_2, |y|_2$ is 1. Without loss of generality $|y|_2 = 1$. If $|x|_2 = 1$ then $ax^2 + by^2 + cz^2 \equiv 1 + 1 + 1 \mod 2$, a contradiction. So $|x|_2 < 1$. So $ax^2 + by^2 + cz^2 \equiv b + c \mod 4$, that is $b + c \equiv 0 \mod 4$. Impose

$$x \equiv 0 \mod 2, \qquad y \equiv z \mod 2.$$

If these hold, $ax^2 + by^2 + cz^2 \equiv by^2 + cz^2 \equiv (b + c) y^2 \equiv 0 \mod 4$. What have we done? If $p > 2$ and $p \in \Sigma$, we found a congruence modulo p which guaranteed that $ax^2 + by^2 + cz^2 \equiv 0 \mod p$. If $2 \mid abc$, found conditions guaranteeing that $ax^2 + by^2 + cz^2 \equiv 0 \mod 8$. If $2 \nmid abc$, $ax^2 + by^2 + cz^2 \equiv 0 \mod 4$. Define Λ as the subgroup of $\mathbb{Z}^3$ satisfying all of these congruence conditions. Since abc is squarefree, if $(x, y, z) \in \Lambda$ then $ax^2 + by^2 + cz^2 \equiv 0 \mod 4abc$. It remains to check that $\left[\mathbb{Z}^3 : \Lambda\right] = |4abc|$. To see this, write Λ as the kernel of a map from $\mathbb{Z}^3$ to a product of a group of order four or eight and $\prod_{p > 2,\ p \mid abc} \mathbb{Z}/p\mathbb{Z}$ and use the Chinese remainder theorem.

Lecture 14 Friday 02/11/18

Lecture 14 is a problem class.

Lecture 15 Tuesday 06/11/18

5 Plane cubics

Definition 5.1. A **plane cubic** is a polynomial $f(x, y)$ of degree three, or a homogeneous $F(X, Y, Z)$ of degree three.

Call f nonsingular if all its points are nonsingular.

Example. $y^2 - x^3$ is singular because $(0, 0)$ is a singular point but it does not factor.

Main aim of the rest of the course is to try to find all the points where $f(x, y) = 0$, particularly in the case that we are working over $\mathbb{Q}$. We will also think a bit about points over $\mathbb{Q}_p$.

Example. $3x^3 + 4y^3 = 5$ has solutions in $\mathbb{Q}_p$ for all p and in $\mathbb{R}$, but no solution in $\mathbb{Q}$, so we do not have a version of the Hasse principle. $x^3 + y^3 = 0$ has infinitely many rational points, and it is singular. $x^3 + y^3 = 1$ has finitely many points over $\mathbb{Q}$, in fact just $(1, 0)$ and $(0, 1)$, and is nonsingular. For $x^3 + y^3 = 9$, $(2, 1)$ and $(1, 2)$ are rational points. $x + y = 3$ is the line through these two points. $x^3 + (3 - x)^3 = 9$ is quadratic, so $x = 1$ or $x = 2$. (TODO Exercise: do this in projective coordinates and find a point at infinity) Instead, try tangent lines. (TODO Exercise: try this with $x^3 + y^3 = 1$ and see what happens) Tangent line at $(1, 2)$ is $x + 4y = 9$. Substitute in $y^3 + (9 - 4y)^3 = 9$, that is $-9(y - 2)^2(7y - 20) = 0$, to give $(-17/7, 20/7)$.

Lemma 5.2. $x^3 + y^3 = 9$ is nonsingular and has infinitely many points over $\mathbb{Q}$.

Idea to see that there are infinitely many solutions is to show that the z coordinate is getting bigger. If $[x : y : z] \in \mathbb{P}^2(\mathbb{Q})$, we will say for now that the height of $[x : y : z]$ is $|z|$, provided that $x, y, z \in \mathbb{Z}$, and have no common factor.

Example. $[1 : 2 : 1]$ had height 1. $[-17 : 22 : 7]$ had height 7.

Proof. Firstly check for singular points. $F = X^3 + Y^3 - 9Z^3$, $\partial F/\partial X = 3X^2$ gives $X = Y = Z = 0$, which is a contradiction. To prove there are infinitely many points over $\mathbb{Q}$, we draw tangent lines. Claim that if $[r : s : t]$ is on $F = 0$, then the third point of intersection of the tangent line at $[r : s : t]$ with $F = 0$ is $\left[r\left(r^3 + 2s^3\right) : -s\left(2r^3 + s^3\right) : t\left(r^3 - s^3\right)\right]$. (TODO Exercise: check this in two ways. First way do this as we did for $(1, 2)$. Second way use that I told you the answer.) If $[r : s : t]$ is on $X^3 + Y^3 = 9Z^3$, and if $r, s, t \in \mathbb{Z}$ and have no common factor, then since 9 is cubefree, in fact have $(r, s) = (s, t) = (r, t) = 1$. Suppose that some prime p divides all three factors of $\left[r\left(r^3 + 2s^3\right) : -s\left(2r^3 + s^3\right) : t\left(r^3 - s^3\right)\right]$. Suppose that some prime p divides all three factors. If $p \mid r$ then $p \mid -s\left(2r^3 + s^3\right)$, so $p \mid -s^4$, so $p \mid s$, but $(r, s) = 1$. So $p \nmid r$. Similarly if $p \mid s$ then $p \mid r^4$ gives $p \mid r$, a contradiction. So $p \nmid s$. Since $p \mid r\left(r^3 + 2s^3\right)$ and $p \nmid r$, we have $p \mid \left(r^3 + 2s^3\right)$. Similarly $p \mid \left(2r^3 + s^3\right)$. So $p \mid \left(2\left(2r^3 + s^3\right) - r^3 + 2s^3\right)$, so $p \mid 3r^3$. Again $p \nmid r$, so $p \mid 3$, so $p = 3$. (TODO Exercise: in fact, the same analysis shows that the only power of three which could divide all three terms is three itself) So the height of our new point is at least $\frac{1}{3}|t|\left|r^3 - s^3\right|$. So we will be unless $\left|r^3 - s^3\right| \le 3$. But this inequality is only satisfied if $r, s \in \{-1, 0, 1\}$. But then $r^3 + s^3 = 9t^3$ has no solutions other than $[-1 : 1 : 0]$. So as long as we start with any other point, such as $[1 : 2 : 1]$, we get infinitely many points. ☐

Algorithm 5.3 (Finding all points for a singular cubic)**.** First find the singular point. Remark that using Galois theory, you can show that if you are working over a field of characteristic zero, then the singular point will have coordinates in this same field. Then draw lines through this point.