Elliptic Curves*

Yankı Lekili

■ Statement of a convention used throughout the text.
► Little facts that can be checked but we don't bother to check explicitly. If you don't find what's stated intuitive, you should stop and think about how to prove it. If you can't, then consult a book and if that doesn't help either, please come ask me. I will assume that you know how to prove these.
◁ Exercise. Try it!
□ Marks the end of a proof.

When something is defined for the first time, I make it **bold** and when I want to emphasize something I underline it.

```
Code snippets in PARI/GP are inserted with this font.
I won't ask you any coding problems in the exam but you should install PARI/GP
in your computer and have fun with it as you learn Elliptic curves.
PARI/GP is freely available at
```

https://pari.math.u-bordeaux.fr/

ƨ These are fresh notes that I typed up recently. I expect that there are lots of typos. If you detect them, please send me an email and then come to the office hour to collect your triple chocolate cookie.

$:=$ denotes a definition. $\simeq$ denotes an isomorphism. I very often make a mistake and use $=$ where I really meant to use $:=$ or $\simeq$. No cookies for that!

1 Prelude

The overall aim of this course is to learn about solving polynomial equations over the rational numbers $\mathbb{Q}$, and sometimes, over the integers $\mathbb{Z}$.

The letter k will almost invariably denote a field, and generally be one of $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p$ or $\mathbb{Q}_p$. Don't worry if you don't know the last one, we'll cover it in detail. We may occasionally venture into algebraic number theory and let $k = \mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{3})$, but nothing more complicated than those.

*A more accurate title of this course would be "Conics and Cubics on the plane"

The polynomial equations will generally be given by polynomials in $k[x, y]$ or $k[x, y, z]$. Moreover, the highest degree monomial will generally be 2 or 3, with some exceptions.

To begin, we will consider **conics**. These are equations of degree 2 such as

$$x^2 + y^2 = 17$$

or more generally,

$$ax^2 + bxy + cy^2 + dx + ey + f = 0, \quad a, b, c, d, e, f \in k$$

These form a good place to start in order to build intuition and technique.

Later on, we will study elliptic curves in detail, these are equations of the form

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_1, a_2, a_3, a_4, a_6 \in k$$

If the characteristic of the field k is not equal to 2 or 3, we can apply a change of variables to bring the equation to the form

$$y^2 = x^3 + ax + b \quad , a, b \in k$$

When the discriminant $\Delta = 4a^3 + 27b^2 \neq 0$, a fundamental result of Mordell says the set of rational solutions ($k = \mathbb{Q}$ or any number field, really),

$$E(\mathbb{Q}) := \{(x, y) \in \mathbb{Q} \times \mathbb{Q} : y^2 = x^3 + ax + b\},$$

is a finitely generated abelian group. By the basic structural result on finitely generated abelian groups, we must have

$$E(\mathbb{Q}) = \mathbb{Z}^r \times E(\mathbb{Q})_{tors}$$

It is our main goal in these lectures to prove this result and learn techniques for computing $E(\mathbb{Q})$.

There are three main ideas that will be prevalent. We will give elementary examples of these ideas in this first lecture with the hope that the student will recognize these ideas in more complicated scenarios that will appear later in the course.

Geometric method of constructing solutions.

The idea here is to use geometric constructions to find rational solutions. Often it turns out that complicated algebraic formulae have simple and beautiful geometric interpretations. Let's work through some examples.

Consider the equation of "the circle"

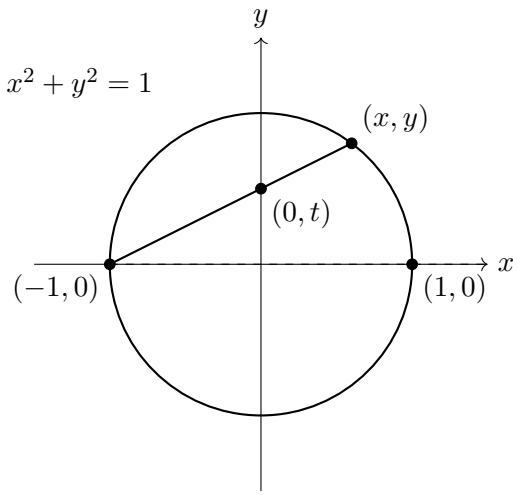
$$x^2 + y^2 = 1$$

We all are familiar with the solution set over $\mathbb{R}$, but how about solutions over $\mathbb{Q}$?

We will be brief, as this is all too well covered in the textbooks: All rational solutions are given by

$$x = \frac{1 - t^2}{1 + t^2} \quad , \quad y = \frac{2t}{1 + t^2} \text{ for } t \in \mathbb{Q} \cup \{\infty\}.$$

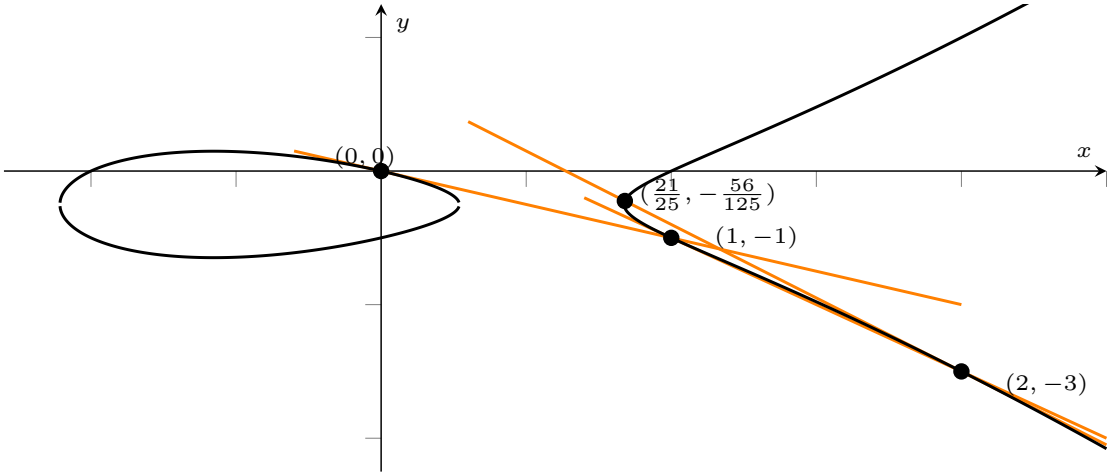
and this can be deduced from the following picture.



So, let us look another example. Consider the elliptic curve given by

$$E : y^2 + y = x^3 - x$$

whose set of $\mathbb{R}$ solutions is pictured in the below figure. We notice an obvious solution, namely $P = (0, 0)$.



To produce other solutions, we consider the line ℓ_P which is the tangent line to E at the point P. We have[1]

$$\ell_P : y = -x$$

Intersecting ℓ_p with E, we get another point $Q = (1, -1)$ on E. Now, we repeat this. The tangent line at Q is given by

$$\ell_Q : y = -2x + 1$$

[1]Recall that if $F(x, y) = 0$ is a plane curve, then the tangent line at a smooth point (a, b) is given by the formula $\frac{\partial F}{\partial x}(a, b)(x - a) + \frac{\partial F}{\partial y}(a, b)(y - b) = 0$.

and intersecting this with E gives us the point $R = (2, -3)$, and the tangent line at R is given by

$$\ell_R : y = (-11/5)x + 7/5$$

and the intersecting this with E, we get $S = (21/25, -56/125)$.

Can we continue this procedure ad infinitum? Do we get all rational solutions? The answers to these will be revealed throughout the course.

By the way, here is how we can do this on the computer. Launch GP and use the following commands (leaving out the commments)

```
E = ellinit([0,0,1,-1,0])  // Defines the elliptic curve
P = [0,0]                  // Defines the point P
Q = ellmul(E,P,-2)         // The intersection of the tangent line at P with E
R = ellmul(E,Q,-2)
S = ellmul(E,R,-2)
...
```

$\lhd$ Given an arbitrary $P = (x, y)$ on the curve E, find a general formula that expresses intersection of the tangent line at P with E. *End of lec. 1*

Descent.

This is the idea that if you have a way to measure the size of a solution, perhaps it is possible to start from a solution and go to a smaller size solution. Finally, a classification of "small" solutions leads to a procedure to obtain all solutions. The simplest applications of this idea is used in proving non-existence results. Let's see an example.

Consider a right angled triangle with rational side lengths a, b, c. These satisfy the Pythagoras theorem $a^2 + b^2 = c^2$ and the area of the triangle is given by $ab/2$.

Theorem 1.1. *(Fermat) There is no right angled triangle with rational side lengths whose area is a square.*

Proof. We can always scale a given triangle $(a, b, c) \to (\lambda a, \lambda b, \lambda c)$, and this changes the area by λ^2. So, it suffices to show that there is no right angled triangle with integer side lengths $(a, b, c) \in \mathbb{N}^3$ whose sides maybe assumed to be mutually prime and $ab/2$ is a square. Then, we can write

$$a = p^2 - q^2, b = 2pq, c = p^2 + q^2$$

where p, q are mutually prime, $p > q$ and $p - q$ is odd. The area is then given by $pq(p-q)(p+q)$. Suppose that this is a square. Then, we have

$$p = x^2, q = y^2, p + q = u^2, p - q = v^2$$

where u, v must be odd and mutually prime. Consider now the right-angled triangle with sides $(\frac{u+v}{2}, \frac{u-v}{2}, x)$. The side lengths of this triangle are mutually prime and the area is $\frac{u^2-v^2}{8} = \frac{q}{4} = (\frac{y}{2})^2$ which is a square. Note that, as u and v are odd, it follows that $8|u^2 - v^2$, hence $\frac{y}{2}$ is an

integer. But, $4(\frac{y}{2})^2 = q < pq(p-q)(p+q)$. Hence, we obtained a new right-angled triangle with integer side lengths whose area is strictly smaller. Repeating the argument, by "infinite descent", we arrive at a contradiction. □

◁ Let $p, q \in k[t]$ be relatively prime polynomials (k a field of characteristic $\neq 2$). Suppose that there exist linearly independent vectors $(a_i, b_i) \in k^2$ for $i = 1, 2, 3, 4$ such that $a_i p + b_i q$ is a square in $k[t]$ for all i. Show by "infinite descent" that $p, q \in k$, that is, they must be constant polynomials. (Hint: Apply Möbius transformations to assume without loss of generality that the four vectors are $(1, 0), (0, 1), (1, -1), (1, -\mu)$ with $\mu \neq 0, 1$.)

Local to Global.

Suppose we are given an equation over $\mathbb{Q}$, we can of course multiply the coefficients with a common denominator and then write the equation over $\mathbb{Z}$, and then reduce the equation modulo p to an equation over $\mathbb{F}_p$. So, now, it is clear that if the original equation had a solution over $\mathbb{Q}$, then this reduced equation will have a solution modulo p for every p. More generally, we can reduce to any field $\mathbb{F}_q$ with $q = p^k$ for some k. Sometimes, we also let $p = \infty$ to mean that we consider the equation over $\mathbb{R}$.

The Hasse principle is concerned with the converse direction. Suppose that we have a solution to an equation modulo $q = p^k$ for all k and all p (or simply we have a solution in $\mathbb{Q}_p$), and over $\mathbb{R}$, then can we conclude that there is a solution over $\mathbb{Q}$? If so, we say that Hasse principle is satisfied for this equation.

Let's give an example where existence of a solution over $\mathbb{Q}$ is prohibited, because there are no solutions in $\mathbb{Q}_2$.

Consider the equation

$$x^2 + y^2 = 2(x + y)z + z^2$$

We claim that there are no non-trivial rational solutions to this equation. Indeed, putting $t = x + y + z$, we can rewrite this equation as

$$2x^2 + 2xy + 2y^2 = t^2$$

Since the equation is homogeneous, it suffices to prove that there are no integer solutions (otherwise, scale $(x, y, z) \to (dx, dy, dz)$ for an appropriate d to get integer solutions). Similarly, we may assume that $\gcd(x, y, t) = 1$.

Now, since the left hand side is divisible by 2, it follows that t is divisible by 2, then it follows that $x^2 + xy + y^2$ is divisible by 2. Now, note that $x^2 + xy + y^2 = 0(2)$ if and only if $x = y = 0(2)$, but then we see that $2|\gcd(x, y, t)$, a contradiction. Indeed, it follows that the equation does not have any solution modulo 4, hence not in $\mathbb{Q}_2$, and so in $\mathbb{Q}$.

Hasse principle is the statement that, quadratic equations such as the one above have a solution over $\mathbb{Q}$, if and only if they can be solved modulo p-powers for any p. Giving a proof of this result for plane conics is our first goal in this course.

On the other hand, a famous example of Selmer given by

$$E : 3x^3 + 4y^3 + 5z^3 = 0$$

shows that Hasse principle fails for cubics. (If time permits, we will prove this.)

2 The p-adic numbers

Here is a quick and easy way of defining p-adic numbers. A **p-adic integer** $x \in \mathbb{Z}_p$ is a formal solution of the system of consistent congruences

$$x \equiv x_n \pmod{p^n}, \quad n = 1, 2, \ldots$$

The consistency condition is that $x_n \equiv x_{n+1} \pmod{p^n}$. Two sequences of integers (x_n) and (y_n) define the same p-adic integer if and only if $x_n \equiv y_n \pmod{p^n}$. The p-adic rationals can be defined just the same way where the numbers x_n might be arbitrary rationals. If $x_n = r/s$, then we think of $x \equiv x_n \pmod{p^n}$ as a solution to the congruence relation $sx \equiv r \pmod{p^n}$.

Let us now develop this in a bit more depth.

A **norm** on a field k is a function $|\cdot| : k \to \mathbb{R}_{\geq 0}$ such that

$$\begin{aligned} |x| = 0 &\iff x = 0 \\ |xy| &= |x||y| \\ |x + y| &\leq |x| + |y| \end{aligned}$$

▶ It follows immediately that $|-x| = |x|$ for all x.

▶ Given a norm on a field, we can define a metric by setting

$$d(x, y) = |x - y|, x, y \in k$$

The notion of a norm is an abstraction of the usual absolute value on $\mathbb{R}$ or $\mathbb{C}$. When we equip $\mathbb{Q}$ with the norm associated with the usual absolute value, we write the norm function as $|\cdot|_\infty$. Suppose now that p is a prime number. We define the **p-adic norm** $|\cdot|_p : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ as follows. Given any rational $r \neq 0$, we can write

$$r = p^\rho a/b, \rho \in \mathbb{Z}, a, b \in \mathbb{Z}, p \nmid a, b$$

then we let

$$|r|_p = p^{-\rho}$$

Thus, something is p-adically small if it is divisible by a high power of p.

Proposition 2.1. *$|.|_p : \mathbb{Q} \to \mathbb{R}_{\geq 0}$ is a norm.*

Proof. The first two properties of the norm is pretty clear. To see the last one, let $r = p^\rho a/b$ and $s = p^\sigma c/d$ for $\rho, \sigma, a, b, c, d \in \mathbb{Z}, p \nmid a, b, c, d$. So, $|r|_p = p^{-\rho}$ and $|s|_p = p^{-\sigma}$, where without loss of generality, $\sigma \geq \rho$. Then

$$r + s = p^\rho(ad + p^{\sigma-\rho}cb)/bd$$

and $p \nmid bd$. The numerator is an integer but for $\sigma = \rho$ it maybe divisible by p. Hence,

$$|r + s|_p \leq p^{-\rho}$$

that is

$$|r + s|_p \leq \max\{|r|_p, |s|_p\}$$

□

This last inequality is called **ultrametric inequality** and it clearly implies the triangle inequality. A norm which satisfies the ultrametric inequality is said to be **non-archimedean**.

End of lec. 2

The metric properties of a non-archmedean norm can be counter-intuitive at first. As an example, we show that in non-archimedean geometry every triangle is isosceles!

Lemma 2.2. *Let $|.| : k \to \mathbb{R}_{\geq 0}$ be a non-archimedean norm. If $|x| < |y|$ then $|x - y| = |y|$.*

Proof. We have $|x-y| \leq \max\{|x|, |y|\} = |y|$ since $|x| < |y|$. On the other hand, $y = (y-x)+x$, hence $|y| \leq \max\{|x-y|, |x|\} = |x-y|$ since $|x| < |y|$. □

◁ Let $(k, |.|)$ be a field with a non-archimedean norm. Let $a \in k$, and consider the unit disk $D = \{x : |x-a| < 1\}$ with center a. Let $b \in D$ any point, then show that $D = \{x : |x-b| < 1\}$, that is, every point of the disk can be taken to be the center of the disk!

◁ Let $n \in \mathbb{Z}$ be a composite number (not a prime number). For $r \in \mathbb{Q}$ write $r = n^\rho a/b, n \in \mathbb{Z}, a, b \in \mathbb{Z}, n \nmid a, b$ and define $|r|_n = n^{-\rho}$. Is $|\cdot|_n$ a norm on $\mathbb{Q}$?

Next, we adapt the notions from basic analysis defined using the absolute value to the non-archimedean case. Given a field k with a norm $|.|$. We say that a sequence $(x_n)_{n\geq 1}$ with $x_i \in k$ is a **Cauchy sequence** if $\forall \epsilon > 0, \exists n_0 \geq 1$ such that $|x_n - x_m| < \epsilon$ for all $n, m \geq n_0$.

We say that a sequence $(x_n)_{n\geq 1}$ converges to a **limit** x if $\forall \epsilon > 0$, $\exists n_0 \geq 0$ such that $|x_n - x| < \epsilon$ for all $n \geq n_0$.

▶ Let $p = 5$ and consider the sequence $x_1 = 4$, $x_2 = 34$, $x_3 = 334$, ..., $x_n = 33\ldots34, \ldots$ of integers. Then $(x_n)_{n\geq 1}$ is a Cauchy sequence for $|.|_5$. Moreover, it converges to $2/3$ as can be seen by showing that $|3x_n - 2|_5 \to 0$ as $n \to \infty$.

A field k is called **complete** with respect to a norm if every Cauchy sequence has a limit.

It is easy to see that the field $\mathbb{Q}$ equipped with $|.|_p$ is not complete for any p. For example, we can construct a sequence $\{x_n\}$ of integers such that

$$x_n^2 + 1 \equiv 0 \quad (5^n)$$
$$x_{n+1} \equiv x_n \quad (5^n)$$

Start with $x_1 = 2$. Suppose that we have already constructed x_n. Write $x_n^2 + 1 = 5^n c$. We are aiming to construct $x_{n+1} = x_n + b5^n$ such that $(x_n + b5^n)^2 + 1 \equiv 0(5^{n+1})$. Thus, we need $2x_n b + c \equiv 0 \quad (5)$ but this can be solved since x_n is not divisible by 5.

We have just constructed a 5-adic Cauchy sequenece as $|x_n - x_m|_5 \leq 5^{-n}$ for $m \geq n$. Suppose now that x_n converges to x, then x_n^2+1 converges to x^2+1. But, by our construction, $x_n^2+1 \to 0$, hence it must be that $x^2 + 1 = 0$. No such x exists in $\mathbb{Q}$.

Here is how you can construct the sequence (x_n) for the equation up to specified precision in GP:

```
polrootspadic(x^2 + 1, 5, 31)
```

◁ For any prime p, find a $t \in \mathbb{Z}$ that is not a square and a Cauchy sequence $(x_n)_{n\geq 1}$ such that $x_n^2 \to t$ as $n \to \infty$.

Just like the field $\mathbb{R}$ can be constructed by completing the rationals with respect to the ordinary absolute value, we can construct completions of rationals with respect to $|.|_p$, the resulting field $\mathbb{Q}_p$ is called the **p-adic numbers**.

We now give the construction of completion of a normed field $(k, |.|)$. We assume that the norm is non-archimedean but that changes very little.

The idea is very simple, we simply construct a bigger field by adding in the limit points of Cauchy sequences. However, we have to be a bit more careful since a limit point can arise as a limit of many sequences.

Let

$$\mathcal{C} \coloneqq \{(x_n)_{n\geq 1} : x_n \in k, (x_n) \text{ a Cauchy sequence } \},$$

be the set of Cauchy sequences in k. We call two Cauchy sequences (x_n) and (y_n) equivalent if $|x_n - y_n| \to 0$ as $n \to \infty$. We define $\hat{k}$ the set of equivalence classes of Cauchy sequences. Said differently, let

$$\mathcal{I} \coloneqq \{(x_n)_{n\geq 1} \in \mathcal{C} : \lim_{n\to\infty} x_n = 0\}.$$

and define $\hat{k} \coloneqq \mathcal{C}/\mathcal{I}$.

Here are some properties of this construction, that shows that $\hat{k}$ is a normed field and $k \to \hat{k}$ is a dense embedding. All of these are elementary; we give proofs of some of these and leave the rest as exercises.

▶ $\mathcal{C}$ is a commutative ring with $(x_n) \pm (y_n) = (x_n \pm y_n)$, $(x_n) \cdot (y_n) = (x_n y_n)$, $0 = (0)_{n\geq 1}$ and $1 = (1)_{n\geq 1}$.

The fact that $\mathcal{I}$ is an ideal is immediate from the defining properties of the norm. To see that it is maximal, we use the following observation.

Lemma 2.3. *Suppose $(x_n)_{n\geq 1} \in \mathcal{C} \setminus \mathcal{I}$. There exists an $n_0 \geq 1$ such that $|x_n| = |x_{n_0}|$ for all $n \geq n_0$.*

Proof. Since $(x_n) \notin \mathcal{I}$, for all $\epsilon > 0$ and for all $N \geq 1$, there exists $n(N) > N$ with $|x_{n(N)}| > \epsilon$. On the other hand, (x_n) is a Cauchy sequence, therefore, there exists $M \geq 1$ such that $|x_n - x_m| < \epsilon$ for all $n, m \geq M$. Fix some $\epsilon > 0$, find M and let $n_0 = n(M) > M$. Then, for all $n \geq n_0$,

$$|x_{n_0}| > \epsilon > |x_n - x_{n_0}|.$$

It follows from the isosceles property of triangles (Lem. 2.2) that $|x_{n_0}| = |x_n|$ for all $n \geq n_0$. □

It follows that $x_n \neq 0$ for all $n > n_0$. Hence, we can define a new sequence (y_n) with $y_n = 1/x_n$ for $n \geq n_0$, and 0 otherwise. Then, $x_n y_n = 1$ for $n \geq n_0$, hence $(x_n)(y_n) - 1 \in \mathcal{I}$. Hence, $\mathcal{I}$ is maximal.

Moreover, the map $|.| : \hat{k} \to \mathbb{R}_{\geq 0}$ by letting $|(x_n)| = \lim_{n\to\infty} |x_n| = |x_{n_0}|$ is a norm on $\hat{k}$.

▶ When completing $\mathbb{Q}$ to $\mathbb{R}$, the possible values of $|.|$ is enlarged. When we complete $\mathbb{Q}$ to $\mathbb{Q}_p$ the possible values remain the same: $\{p^n\}_{n\in\mathbb{Z}} \cup \{0\}$.

Lemma 2.4. *The field embedding $k \to \hat{k}$ given by $x \to (x)_{n\geq 1}$ is dense.*

Proof. Let $(x_n) \in \widehat{k}$ and $\epsilon > 0$. Choose N such that if $m, n \geq N$, then $|x_m - x_n| < \epsilon$. Consider $y = (x_N)_{n\geq 1} \in k$. Then $|x - y| = \lim_{n\to\infty} |x_n - x_N| < \epsilon$. □

Henceforth, we identify elements of k with the constant sequences in $\hat{k}$.

Lemma 2.5. *$\widehat{k}$ 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 2.4, 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

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

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

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

Now, $|y_n - y| \to 0$ as $n \to \infty$ by how we defined $|y|$, hence $x_n \to y$ as $n \to \infty$. □

End of lec. 3

The rational numbers $\mathbb{Q}$ has a subring $\mathbb{Z}$ such that $\mathbb{Q}$ is the field of fractions. We define **p-adic integers** $\mathbb{Z}_p := \{x \in \mathbb{Q}_p : |x|_p \leq 1\} \subset \mathbb{Q}_p$.

▶ $\mathbb{Z}_p$ is indeed a ring:

$$|\alpha|_p, |\beta|_p \leq \implies |\alpha\beta|_p \leq 1, |\alpha + \beta|_p \leq 1$$

Note that this uses the ultrametric property. ▶ A rational number b is in $\mathbb{Z}_p$ precisely when it has the form $b = u/v$ where $u, v \in \mathbb{Z}$ and $p \nmid v$. In other words, $\mathbb{Z}_p \cap \mathbb{Q} = \mathbb{Z}_{(p)}$ is the localisation of $\mathbb{Z}$ at the prime ideal (p), and $\mathbb{Z}_{(p)} = \{u/v \in \mathbb{Q} : p \nmid v\}$.

▶ The number $\epsilon \in \mathbb{Z}_p$ with $|\epsilon|_p = 1$ are the **p-adic units**. Every $\beta \neq 0$ in $\mathbb{Q}_p$ is of the form $\beta = p^n\epsilon$ for some $n \in \mathbb{Z}$ and ϵ is a unit. Note that for any non-zero $x \in \mathbb{Q}_p$ either $x \in \mathbb{Z}_p$ or $x^{-1} \in \mathbb{Z}_p$. The units are precisely the elements x of $\mathbb{Q}_p$ such that both $x \in \mathbb{Z}_p$ and $x^{-1} \in \mathbb{Z}_p$.

► The ring $\mathbb{Z}_p$ has a unique maximal ideal $(p) = \{x \in \mathbb{Z}_p : |x|_p < 1\}$. It is maximal because $\mathbb{Z}_p/(p) = \mathbb{F}_p$ is a field.

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

In $\mathbb{Q}_p$ we define a series $\sum_{n=0}^{\infty} \beta_n$ in the usual way as the limit of partial sums $\sum_{n=0}^{N} \beta_n$. The convergence test is much easier in non-archimedean analysis.

Lemma 2.6. *The series $\sum_{n=0}^{\infty} \beta_n$ converges if and only if $\beta_n \to 0$.*

Proof. One direction is clear and same as in usual analysis. Suppose $\beta_n \to 0$, then we observe that

$$|\sum_{0}^{N} \beta_n - \sum_{0}^{M} \beta_n|_p = |\sum_{M+1}^{N} \beta_n|_p \leq \max_{M<n\leq N} |\beta_n|_p$$

hence $\sum_0^N \beta_n$ is a Cauchy sequence, and thus converges by completeness of $\mathbb{Q}_p$. □

Thus, there is no analogue of the harmonic series $1 + \frac{1}{2} + \frac{1}{3} + \ldots$ of real numbers, whose terms approach to zero and yet the sum diverges.

Lemma 2.7. *The elements of $\mathbb{Z}_p$ are precisely the sums*

$$\alpha = \sum_{0}^{\infty} a_n p^n$$

where $a_n \in \{0, 1, \ldots, p-1\}$ for all n.

Proof. By the previous lemma, the sum converges to an element of $\mathbb{Z}_p$. Conversely, suppose $\alpha \in \mathbb{Z}_p$. By construction $\mathbb{Q}$ is dense in $\mathbb{Q}_p$, therefore there is a $b \in \mathbb{Q}$ such that $|\alpha - b|_p < 1$. Since $|\alpha|_p \leq 1$, we have $|b|_p \leq 1$. Hence, we if we write $b = r/s$ with $(r, s) = 1$, then $p \nmid s$. Therefore, there is a unique solution $a_0 \in \{0, \ldots, p-1\}$ to the congruence $sa_0 - r \equiv 0 \pmod{p}$. In other words, $|b - a_0|_p < 1$. Then, since $|b - a_0|_p, |\alpha - b|_p < 1$, we have $|\alpha - a_0|_p < 1$. We can write

$$\alpha = a_0 + p\alpha_1$$

where $|\alpha_1|_p \leq 1$, that is, $\alpha_1 \in \mathbb{Z}_p$. We can now proceed inductively to get

$$\alpha = a_0 + a_1 p + \ldots a_n p^N + \alpha_N p^{N+1}$$

with $\alpha_N \in \mathbb{Z}_p$. So, $\alpha = \sum_{n=0}^{\infty} a_n p^n$. □

Corollary 2.8. *Any $\alpha \in \mathbb{Q}_p$ can be uniquely written as*

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

Proof. This follows immediately from the observation that if $|\alpha|_p = p^T$, then $|p^T\alpha|_p = 1$, hence $p^T\alpha \in \mathbb{Z}_p$. □

This motivates the idea that we may think of $\mathbb{Z}_p$ as being analogous to $k[[x]]$ and $\mathbb{Q}_p$ as being analogous to $k((x))$, the rings of power series and Laurent series over some field k.

If we truncate the expansions above, we see that we can approximate any element of $\mathbb{Z}_p$ with integers. Hence:

Corollary 2.9. *$\mathbb{Z}$ is dense in $\mathbb{Z}_p$*

▶ We have a ring map $\mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ for any n, by taking the series expansion and reducing modulo p^n. One can show that these rings maps can be assembled together to show an isomorphism between $\mathbb{Z}_p$ and $\varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})$.

You can type in a p-adic number (up to specified precision) and do basic arithmetic in GP as follows.

```
x  = 3^-1 + 2 + 2*3 + 3^2 + 3^3 + 3^4 + O(3^5)
y  = 1/4 + O(3^5)
x*y
x+y
```

◁ Prove that a p-adic number $\alpha \in \mathbb{Q}_p$ has a finite expansion (that is, $a_i = 0$ for $i > N$ for some N) if and only if α is a positive rational number whose denominator is a positive power of p.

◁ Prove that a p-adic number $\alpha \in \mathbb{Q}_p$ is in $\mathbb{Q}$ if and only if it has an eventually periodic expansion, that is, there exists some N and s such that $a_i = a_{i+s}$ for all $i > N$. *End of lec. 4*

What about solutions to polynomial equations in $\mathbb{Q}_p$? Do all numbers in $\mathbb{Q}_p$ have square roots? There is a general method collectively known as "Hensel's lemma" that allows one to lift solutions over $\mathbb{F}_p$ to $\mathbb{Q}_p$. Let us first consider the following special cases to exercise our understanding.

◁ Let $\epsilon \in \mathbb{Z}_p$ be a unit. For $p \neq 2$, a necessary and sufficient condition for $\epsilon = \alpha^2$ for some $\alpha \in \mathbb{Q}_p$ is that ϵ is a square mod p.

Suppose $p \neq 2$, Let $x \in \mathbb{F}_p$ such that $x^2 = \epsilon(p)$. Then we construct inductively $\alpha_1 = x, \alpha_2, \ldots,$ such that

$$|\alpha_n^2 - \epsilon| \leq p^{-n}$$
$$|\alpha_{n+1} - \alpha_n| \leq p^{-n}$$

Indeed, if we have already constructed α_n, we set $\alpha_{n+1} = \alpha_n + p^n\beta$. As we have $\alpha_{n+1}^2 \equiv \alpha_n^2 + 2p^n\alpha_n\beta \pmod{p^{n+1}}$ and $p^n|\alpha_n^2 - \epsilon$, what we need to arrange is that $2\alpha_n\beta \equiv \frac{\epsilon - \alpha_n^2}{p^n} \pmod{p}$. We can arrange this since $p \nmid 2$ and $p \nmid \epsilon$.

◁ Let $p > 0$ be a prime, $p \equiv 2(3)$. For any integer $a, p \nmid a$, show that there is an $x \in \mathbb{Z}_p$ with $x^3 = a$.

Consider the group homomorphism $x \to x^3$ from $\mathbb{F}_p^\times$ to itself. Since $3 \nmid p-1$, there are no order 3 elements in $\mathbb{F}_p^\times$. Therefore, this map is injective, hence also surjective. This means that we can find x_1 with $x_1^3 \equiv a(p)$. Next, suppose that we have $x_n^3 \equiv a(p^n)$ and pose $x_{n+1} = x_n + p^n y$ and we seek to solve $x_{n+1}^3 \equiv a(p^{n+1})$. We compute $x_{n+1}^3 = (x_n + p^n y)^3 \equiv x_n^3 + 3p^n x_n^2 y (p^{n+1})$. As by assumption $p^n \mid x_n^3 - a$, if we let y such that $3x_n^2 y = \frac{a-x_n^3}{p^n}(p)$ (which we can do since $p \nmid 3x_n^2$, as $p \nmid a$ and $p \neq 3$), then $p^{n+1} \mid x_{n+1}^3 - a$ as required.

◁ Show that there is no 7-adic number $x = 2 + y$ with $|y|_7 \leq 7^{-1}$ such that $x^3 + x^2 - 2x - 1 = 0$.

Lemma 2.10. *(Hensel's lemma) Let $f = \sum_{i=0}^n a_i X^i \in \mathbb{Z}_p[x]$. Suppose that there exists $x_0 \in \mathbb{Z}_p$ such that*

$$|f(x_0)| < |f'(x_0)|^2 \tag{1}$$

where $f'(X) = \sum_{i=1}^n i a_i X^{i-1}$ is the (formal) derivative. Then, there exists a unique root x of f in $\mathbb{Z}_p$ satisfying $|x - x_0| < |f'(x_0)|$.

Furthermore, $|x - x_0| = |f(x_0)|/|f'(x_0)| < |f'(x_0)|$ and $|f'(x)| = |f'(x_0)|$.

Let $\overline{\ } : \mathbb{Z}_p \to \mathbb{Z}_p/(p) = \mathbb{F}_p$ be the reduction homomorphism to the residue field, and $\overline{f} = \sum_{i=0}^n \overline{a}_i X^i \in \mathbb{F}_p[X]$. Instead of (1), you may see that some authors state this result by assuming the existence of a simple root of $\overline{f}$ over $\mathbb{F}_p$ (which is an easier to check but a stronger assumption). Indeed, assume that there exists $\bar{x}_0 \in \mathbb{F}_p$ such that

$$\overline{f}(\overline{x}_0) = 0 \quad \text{and} \quad \overline{f}'(\overline{x}_0) \neq 0, \tag{2}$$

This implies the assumption (1). Indeed, let $x_0 \in \mathbb{Z}_p$ be any lift of $\overline{x}_0 \in \mathbb{F}_p$. We have $p | f(x_0)$ but $p \nmid f'(x_0)$ so $|f(x_0)|_p < 1$ and $|f'(x_0)| = 1$.

Proof. Since $|\frac{f(x_0)}{f'(x_0)}| < |f'(x_0)| \leq 1$, there exists y_0 with $|y_0|_p < 1$ such that $f(x_0) + y_0 f'(x_0) = 0$.

Let us define (finitely many) polynomials $f_1, f_2, \ldots \in \mathbb{Z}_p[X]$ via the identity

$$f(X + Y) = f(X) + f_1(X)Y + f_2(X)Y^2 + \ldots$$

Then $f_1(X) = f'(X)$.

We have

$$|f(x_0 + y_0)| \leq \max_{j \geq 2} |f_j(x_0) y_0^j|$$

Here, $|f_j(x_0)| \leq 1$ since $f_j(X) \in \mathbb{Z}_p[X]$ and $x_0 \in \mathbb{Z}_p$. Hence,

$$|f(x_0 + y_0)| \leq |y_0|^2 = \frac{|f(x_0)|^2}{|f'(x_0)|^2} < |f(x_0)|$$

Similarly,

$$|f'(x_0 + y_0) - f'(x_0)| \leq |y_0| < |f'(x_0)|$$

and so $|f'(x_0+y_0)| = |f'(x_0)|$ by the the isosceles triangle property (Lemma 2.2).

We now put $x_1 = x_0 + y_0$ and note that $|f(x_1)| < |f'(x_1)|^2$, so we can repeat this process.

In this way, we obtain a sequence $(x_n)_{n\geq 0}$ using Newton's formula $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$ with the properties

(i) $|x_n| \leq 1$ hence $x_n \in \mathbb{Z}_p$.

(ii) $|f'(x_n)| = |f'(x_0)|$

(iii) $|f(x_{n+1})| \leq \frac{|f(x_n)|^2}{|f'(x_n)|^2} = \frac{|f(x_n)|^2}{|f'(x_0)|^2} < |f(x_n)|$ and so $f(x_n) \to 0$ as $n \to \infty$.

(iv) $|x_{n+1} - x_n| = |y_n| = \frac{|f(x_n)|}{|f'(x_n)|} = \frac{|f(x_n)|}{|f'(x_0)|} \to 0$ as $n \to \infty$.

It follows that $(x_n)_{n\geq 0}$ is a Cauchy sequence. Then, the element $x \coloneqq \lim_{n\to\infty} x_n \in \mathbb{Z}_p$ exists and $f(x) = 0$.

To see that $|x - x_0| = |f(x_0)|/|f'(x_0)|$, let us observe that

$$|x_{n+1} - x_n| = \frac{|f(x_n)|}{|f'(x_n)|} < \frac{|f(x_0)|}{|f'(x_0)|}$$

for all $n \geq 1$. Now, note that $|x_1 - x_0| = |f(x_0)|/|f'(x_0)|$ and if $|x_n - x_0| = |f(x_0)|/|f'(x_0)|$ for some n, then it follows that $|x_{n+1} - x_0| = |f(x_0)|/|f'(x_0)|$ since we have $|x_{n+1} - x_0| = |x_n - x_0|$ by the isosceles triangle property (Lemma 2.2).

Finally to see the uniqueness, suppose $\tilde{x}$ is another solution with $|\tilde{x} - x_0| < |f'(x_0)|$ and $x \neq \tilde{x}$. Then, let $\tilde{x} = x + \tilde{y}$. We have

$$0 = f(x+\tilde{y}) - f(x) = f'(x)\tilde{y} + f_2(x)\tilde{y}^2 + \dots$$

But, $|\tilde{y}| = |x - x_0 + x_0 - \tilde{x}| \leq \max\{|x - x_0|, |\tilde{x} - x_0|\} < |f'(x_0)| = |f'(x)|$ and $|f_i(x)| \leq 1$, the first term on the right side of the above equation has strictly greater norm than the others, hence the sum cannot be 0, which is a contradiction. □

Let us work out an explicit example that uses the method of proof of Hensel's lemma. Consider $f(x) = x^2 - 11 \in \mathbb{Z}_7[x]$. Let $x_0 = 2$. We have $f(x_0) = -7$ so this gives a solution over $\mathbb{F}_7 = \mathbb{Z}_7/(7)$. Moreover, $f'(x) = 4 \neq 0 \in \mathbb{F}_7$. Then we let $x_1 = x_0 - \frac{f(x_0)}{f'(x_0)} = 2 + (7/4) = 15/4$. We have $f(x_1) = 225/16 - 11 = 7^2/2^4$, hence this gives a solution over $\mathbb{Z}_7/(7^2)$. Moreover, $f'(x_1) = 15/2 \neq 0 \in \mathbb{F}_7$ as it should. So, we can continue to define $x_2 = x_1 - \frac{f(x_1)}{f'(x_1)} = \frac{401}{2^3.3.5}$. We can see that $f(x_2) = 7^4/2^6 3^2 5^2$, hence we get a solution over $\mathbb{Z}_7/(7^4)$. We were looking to obtain a solution modulo 7^3, but we got lucky and in fact got a solution modulo 7^4. As we proved above, the process can be continued to obtain a solution in $\mathbb{Q}_7$.

We can also find the 7-adic expansion as follows: First, we observe the identities

$$\begin{aligned}
401 &= 2 + 1.7 + 1.7^2 + 1.7^3 \\
1/2 &= 4 + 3.7 + 3.7^2 + 3.7^3 + O(7^4) + \dots \\
1/3 &= 5 + 4.7 + 4.7^2 + 4.7^3 + O(7^4) + \dots \\
1/5 &= 3 + 1.7 + 4.7^2 + 5.7^3 + O(7^4) + \dots
\end{aligned}$$

Then, a solution in $\mathbb{Z}_7/(7^4)$ is given by

$$(2+1.7+1.7^2+1.7^3)(4+3.7+3.7^2+3.7^3)^3(5+4.7+4.7^2+4.7^3)(3+1.7+4.7^2+5.7^3)$$
$$= 2+2.7+4.7^2+4.7^3+O(7^4)$$

While it is possible to do these computations by hand, I cheated and used GP with the following commands:

```
x = 401 + O(7^4)
y = 1/2 + O(7^4)
z = 1/3 + O(7^4)
w = 1/5 + O(7^4)
x*y^3*z*w
```

End of lec. 5

▶ The method used in Hensel's lemma is the adaptation of Newton's method of approximations to the roots of a real polynoominal, where successive approximations are defined by the formula $x_n = x_{n-1} - \frac{f(x_{n-1})}{f'(x_{n-1})}$. However, in the non-archimedean setting it's guaranteed that the sequence converges, whereas in the real case, it usually converges but not always. For example, if you take $f(x) = x^3 - x$ and choose $x_0 = \frac{1}{\sqrt{5}}$, then we get $x_i = \frac{(-1)^i}{\sqrt{5}}$ for all $i \geq 0$.

Corollary 2.11. *Consider $f(x) = x^{p-1} - 1 \in \mathbb{Z}_p[x]$. Then, for every $a \in \mathbb{F}_p^\times$ there exists a unique $\alpha \in \mathbb{Z}_p$ such that $f(\alpha) = 0$ and $\alpha = a \in \mathbb{Z}_p/(p) = \mathbb{F}_p$.*

Proof. We have $f'(\alpha) = (p-1)\alpha^{p-2} \neq 0 \in \mathbb{F}_p$. $\overline{f}(x) = x^{p-1} - 1 = \prod_{0 \neq a \in \mathbb{F}_p}(x-a)$. Hence, by Hensel, f has a root in $\mathbb{Z}_p$ lifting a. □

As an example, take $p = 5$. Here are the four solutions of the equation $x^4 = 1$ over $\mathbb{Z}_5$ (up to $O(5^{11})$):

$$[1] = 1$$
$$[2] = 2 + 1.5 + 2.5^2 + 1.5^3 + 3.5^4 + 4.5^5 + 2.5^6 + 3.5^7 + 3.5^9 + 2.5^{10} + O(5^{11})$$
$$[3] = 3 + 3.5 + 2.5^2 + 3.5^3 + 1.5^4 + 2.5^6 + 1.5^7 + 4.5^8 + 1.5^9 + 2.5^{10} + O(5^{11})$$
$$[4] = 4 + 4.5 + 4.5^2 + 4.5^3 + 4.5^4 + 4.5^5 + 4.5^6 + 4.5^7 + 4.5^8 + 4.5^9 + 4.5^{10} \ldots$$

◁ Let $\epsilon \in \mathbb{Z}_2$ be a unit. Then $\epsilon = \alpha^2$ for some $\alpha \in \mathbb{Q}_2$ if and only if $\epsilon \equiv 1(8)$.

Let's apply Hensel's lemma. If $\epsilon = \alpha^2$, then $|\alpha|^2 = 1$, hence α is a unit. In $\mathbb{Z}_2/8\mathbb{Z}_2 = \mathbb{Z}/8\mathbb{Z}$, the units are $1, 3, 5$ and 7 which square to $1 \pmod 8$. Conversely, suppose $\epsilon \equiv 1 \pmod 8$. Let $f(X) = X^2 - \epsilon \in \mathbb{Z}_2[X]$. We have $|f(1)|_2 = |1-\epsilon|_2 \leq 1/8$ and $|f'(1)|_2 = |2|_2 = 1/2$, hence $|f(1)|_2 < |f'(1)|_2^2$. Thus, by Hensel's lemma, $f(X)$ has a root in $\mathbb{Z}_2$.

3 Crash course on Algebraic Curves

We will quickly cover some basic notions from algebraic geometry of curves. More details on this are covered in the Algebraic Curves module. Alternatively, you can read up on the topic in Appendix A of [3] which is more than sufficient.

Let $0 \neq f \in k[x, y]$ and $k \subset K$ be a field extension (we usually will either take $K = k$ or $K = \overline{k}$ that is an algebraic closure of k).

Recall that a field k is **algebraically closed** if any non-constant polynomial $f \in k[x]$ has a root. It follows that f can factored as:

$$f(x) = c \prod (x - r_i)^{e_i}, \quad , c, r_i \in k$$

where r_i are distinct roots of f. A polynomial of degree d has d roots counted with multiplicity. Some examples of algebraically closed fields are complex numbers $\mathbb{C}$ and $\overline{\mathbb{Q}}$, the algebraic closure of $\mathbb{Q}$.

An **affine algebraic curve** over K is the subset of K^2 of the form

$$C_f(K) = \{(x, y) : K^2 : f(x, y) = 0\}.$$

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

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

Algebraic curves of degree one, two and three are **lines**, **conics** and **cubics**, respectively.

Nearly everything that we do is independent under an **affine linear** change of co-ordinates, that is, we will consider two curves equivalent if they are related by a change of co-ordinates:

$$\tilde{x} = px + qy + u$$
$$\tilde{y} = rx + sy + v$$

with $p, q, r, s, u, v \in K$ and $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ invertible over K,

Let C be an algebraic curve defined by a polynomial $f(x, y) \in k[x, y]$. A point (a, b) is called **singular point** of C if

$$f(a, b) = \frac{\partial f}{\partial x}(a, b) = \frac{\partial f}{\partial y}(a, b) = 0.$$

We say that C is **non-singular** or **smooth** if C has no singular points over $K = \overline{k}$.

$\lhd$ Show that the curve $f(x, y) = y^2 + yx - x^3$ is not smooth. This singularity is called a **node**.

$\lhd$ The algebraic curve defined by $f(x, y) = y^2 - p(x)$ where $p \in k[x]$ a polynomial, is smooth if and only if $p(x)$ has no multiple roots.

▶ Note that in order to see the singular points of a polynomial, one might need to look for them in an algebraic extension of k. For example, consider $f(x,y) = y^2 - (x^4 - 4x^2 + 4) \in \mathbb{Q}[x,y]$. Then, partial derivatives give $x^3 - 2x = 0$ and $2y = 0$. We see that $(x,y) = (\pm\sqrt{2}, 0)$ give singular points but these are not defined over $\mathbb{Q}$.

A polynomial $f(x,y) \in k[x,y]$ which has no nonconstant polynomial factors other than scalar multiples of itself is called **irreducible**. Recall that $k[x,y]$ is a UFD, so every polynomial can be factored into irreducible factors. We say that a curve defined by f is irreducible, if f is irreducible over $\overline{k}[x,y]$.

▶ The notion of irreducibility of a polynomial depends on the coefficient field k. For example, $x^2 + y^2$ is irreducible in $\mathbb{Q}[x,y]$ but is reducible in $\mathbb{C}[x,y]$.

The **tangent line** to an algebraic curve C_f at a smooth point (a,b) is given by

$$\frac{\partial F}{\partial x}(a,b)(x-a) + \frac{\partial F}{\partial y}(a,b)(y-b) = 0.$$

Of main interest to us is the intersection $C \cap D$ of two algebraic curves. In particular, given two such curves, we would like to understand how many points of intersection there are? By trial and error, one might get to the conclusion that the equality

$$\#(C \cap D) = \deg C \cdot \deg D$$

should be true, but there are some annoying technical issues. Let us point these out now.

Field of definition. Intersections might not be defined over the field K. Two curves $y = f(x)$ and $y = 0$ for $f(x) \in k[x]$ intersect at the zeroes of $f(x)$. We'd expect that there are $\deg(f)$ zeroes, but that's only guaranteed if k is algebraically closed. For example, $x^2 - 1$ has 2 zeroes, but $x^2 + 1$ has no zeroes over $\mathbb{Q}$. The solution to this is to work over algebraic closure of k or we could be more conservative and work in a finite algebraic extension (that depends on the curves) that guarantees that the intersection points are defined over k.

Intersections at infinity.

If we take our polynomials f and g sufficiently generically, we can ensure that all the intersections of C_f and C_g lie in k^2, and then we will get $\deg f \cdot \deg g$ intersections. However, it is possible that C_f and C_g are in a special position with respect to each other, which pushes some of the intersection points to "infinity". For instance, let's consider the lines $y = x$ and $y = tx + 1$ for some $t \in k$. For almost all values of t, these two lines intersect at one point, namely at $(x,y) = (1/(1-t), 1/1-t)$. However, we see at as $t \to 1$, the point of intersection goes to "infinity", and as a matter of fact, $y = x$ and $y = x + 1$ do not intersect.

To address this issue, one introduces a compactification of the affine space k^2, namely the projective space $\mathbb{P}^2(k)$. The idea is to identify $(x,y) \in k^2$ with the one dimensional k-linear subspace of k^3 spanned by $(x,y,1)$. Every one-dimensional linear space in k^3 which is not on the plane $\{(x,y,z) \in k^3 : z = 0\}$ contains a unique point of the form $(x,y,1)$. Thus the one dimensional subspaces of $\{(x,y,z) \in k^3 : z = 0\}$ can be thought as "points at infinity". We

will study the projective space and how to go between an affine curve and its projectivization in more detail below.

Multiplicities. 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 $f, g \in k[x,y]$, so $f(\underline{0}) = g(\underline{0}) = 0$, then the **intersection number** of f and g at $\underline{0}$ is

$$\dim_k k[[x,y]]/(f,g) < \infty.$$

For $p \in C_f \cap C_g$, we write $(C_f \cdot C_g)_p$ for the **intersection number** at p.

In the special case when g is linear, here is a straightforward way to compute the intersection multiplicity of a curve C_f and a line $C_g = L$. By a suitable change of co-ordinates, we can assume that C_f and L intersects at the origin in k^2 and so we can parametrize points of L as:

$$x = at, y = bt, \text{ for some } a, b \in k^\times$$

Substituting this into f gives:

$$p(t) = f_1(a,b)t + f_2(a,b)t^2 + \ldots + f_d(a,b)t^d \tag{3}$$

where $f_i(x,y)$ are homogeneous polynomials of degree i such that $f(x,y) = \sum_{i=1}^{d} f_i(x,y)$. Then the multiplicity of the intersection is the order of vanishing of $p(t)$ at $t = 0$, and is equal to

$$\max_i \{f_1(a,b) = f_2(a,b) = \ldots = f_i(a,b) = 0\}$$

▶ Let C_f be a smooth curve, and L be a tangent line on a point (x,y) to C_f. Show that the multiplicity of the intersection of L with C_f at the point (x,y) is greater than 1. (Generally, it will be 2 but it can be higher.)

A non-singular point P of a curve C_f is called a **flex** or an **inflection point** if the intersection multiplicity of the tangent line at P to C_f with C_f is ≥ 3.

Common factors. For example, $x^2 - y^2 = 0$ and $x^3 - y^3 = 0$ have more than 6 points in common. This is because they share a common factor $x - y$. The solution in this situation is to simply remove the common factors.

With these precautions in mind, we get that if f and g are polynomials in $k[x,y]$ with k algebraically closed, C_f and C_g intersect at $\deg(f) \cdot \deg(g)$ points. To be more precise about intersections at infinity, we will now study the projective space and projectivizations in a bit more detail. *End of lec. 6*

Projective space.

Let k be any field. Then

$$\mathbb{P}^2_k = k^3 \setminus \{\mathbf{0}\} / \sim$$

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

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

More generally, we define the **projective n-space** as

$$\mathbb{P}^n_k = k^{n+1} \setminus \{\mathbf{0}\} / \sim .$$

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

$$\mathbb{P}^n_k = \{[x_0 : \cdots : x_n] \text{ such that } x_i \in k \text{ not all zero}\}.$$

The **affine n-space** is

$$\mathbb{A}^n_k = k^n.$$

We have an embedding $\phi : \mathbb{A}^n_k \to \mathbb{P}^n_k$ given by $(x_0, x_1, \ldots, x_n) \to [1 : x_1 : x_2 : \ldots : x_{n-1} : x_n]$. The points of $\mathbb{P}^n_k$ in the complement of the image of ϕ are called **points at infinity**. They are given by the equivalence classes of non-zero vectors of the form $[0 : x_1 : \ldots : x_{n-1} : x_n]$, which can in turn be identified with the projective space of one lower dimension, which leads to the decomposition

$$\mathbb{P}^n_k = \mathbb{A}^n_k \cup \mathbb{P}^{n-1}_k$$

In particular, we see that $\mathbb{P}^2_k$ is obtained by compatifying $\mathbb{A}^2_k$ by adding a line $\mathbb{P}^1_k$ at infinity.

▶ Clearly, there is nothing special about the first co-ordinate x_0; we may construct embeddings $\phi_i : \mathbb{A}^n_k \to \mathbb{P}^n_k$ by $(x_0, x_1, \ldots, x_n) \to [x_0 : \ldots : x_{i-1} : 1 : x_{i+1} : \ldots, x_n]$.

Let $\ell : k^{n+1} \to k$ be a non-trivial linear function. The image of

$$\ker \ell = \{\alpha_0 x_0 + \cdots + \alpha_n x_n = 0 : (x_0, \ldots, x_n) \in k^{n+1}, \text{ not all } \alpha_i \in k \text{ are zero}\} \subset \mathbb{P}^n_k$$

with respect to the quotient map $k^{n+1} \setminus \{\mathbf{0}\} \twoheadrightarrow \mathbb{P}^n_k$ is a **linear hyperplane**. This can be generalised by taking homogeneous polynomials in general.

A polynomial $F(X_0, \ldots, X_n) \in k[X_0, \ldots, X_n]$ is **homogeneous** of degree $d \in \mathbb{N}$ if

$$F(X_0, \ldots, X_n) = \sum_{i_0 + \cdots + i_n = d} \alpha_{i_0 \ldots i_n} X_0^{i_0} \ldots X_n^{i_n},$$

so you only have degree d terms.

If f is a degree d polynomial in $k[x_1, \ldots, x_n]$, 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 $k[X_0, \ldots, X_n]$, then here is how to **dehomogenise** it. Choose i with $0 \leq i \leq n$, 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 $f \in k[x_1, \ldots, x_n]$ 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 $F \in k[X_0, \ldots, X_n]$ is homogeneous of degree d and $k \subset K$ a field extension, then

$$C_F(K) = \{[x_0 : \cdots : x_n] \in \mathbb{P}^n_K : F(x_0, \ldots, x_n) = 0\}$$

is well-defined. Homogenisation allows us to extend an algebraic subset in $\mathbb{A}^n_K$ to $\mathbb{P}^n_K$.

For $F \in k[X, Y, Z]$, we call this subset $C_F \subset \mathbb{P}^2_K$ the **projective curve** over K defined by F.

▶ $X^2 + YZ + Z^2 = 0$ 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 $X^2Z + X^3 = Y^2Z$ and $XY = Z^2$.

▶ $X^2 + Y^2 = Z^2$ and $YZ = X^2$ dehomogenises to $x^2 + y^2 = 1$ and $y = x^2$.

Nearly everything that we do is independent under a **projective linear** change of co-ordinates, that is, we will consider two curves equivalent i they are related by a change of co-ordinates:

$$\begin{aligned}\tilde{X} &= c_{11}X + c_{12}Y + c_{13}Z \\ \tilde{Y} &= c_{21}X + c_{22}Y + c_{23}Z \\ \tilde{Z} &= c_{31}X + c_{32}Y + c_{33}Z\end{aligned}$$

where $c_{ij} \in K$ and the matrix (c_{ij}) is invertible over K.

We can now state the main theorem on intersections of algebraic curves.

Theorem 3.1 (Bézout's theorem)**.** *Let $K = \overline{k}$ be an algebraic closure of k. If $F, G \in k[X_0, X_1, X_2]$ be homogeneous non-zero polynomials without common factors, then*

$$\sum_{p \in C_F(K) \cap C_G(K)} (C_F \cdot C_G)_p = \deg F \cdot \deg G.$$

We will not prove this result as it is a topic covered in Algebraic Curves module but an elementary proof can be read from Appendix A of [3].

Corollary 3.2. *If F and G are two homogeneous polynomials in $k[X, Y, Z]$, for k any field not necessarily algebraically closed, then either the curves C_F and C_G in $\mathbb{P}^2_k$ have at most $\deg F \cdot \deg G$ points in common, or F and G have a common factor.*

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

We say that a point $P \in \mathbb{P}^n_k$ is **singular point** of $F = 0$ if $F(P) = 0$ and $(\partial F/\partial X_i)(P) = 0$ for all $i = 0, \ldots, n$. We say that $C_F = \{F = 0\}$ is **non-singular** or **smooth** if all of its points over $K = \overline{k}$ are non-singular, that is, for all points $P \in C_F$, there exists at least one i such that $\partial F/\partial X_i(P) \neq 0$.

$\lhd$ A point P is singular if and only if there exists some dehomogenisation f of F, obtained by setting some $X_i = 1$, such that $f(P) = 0$ and $\partial f/\partial X_i = 0$ for all $i = 1, \ldots, n$.

Let $f, g \in k[x, y]$ be non-zero polynomials with $f(P) = g(P) = 0$. We say that $f = 0$ and $g = 0$ **intersect transversely** at P if P is smooth for both f and g and the tangent lines of $f = 0$ and $g = 0$ at P are different.

$\lhd$ If $f(P) = g(P) = 0$, then the multiplicity of intersection of C_f and C_g at P is one if and only if the intersection is transversal at P.

$\lhd$ Let $f(x, y) = y^2 - x^3$ and $g(x, y) = y^2 - x^3 - x^2$. Show that $(C_f \cdot C_g)_{(0,0)} = 4$.

Any conic in $\mathbb{P}^2_k$ is given by a quadratic form

$$Q(X_1, X_2, X_3) = \sum q_{ij} X_i X_j$$

where $q_{ij} = q_{ji} \in k$. Thus Q is completely described by a symmetric 3×3 matrix. We assume char$k \neq 2$ when dealing with conics[2]. The conic is nonsingular if and only if

$$\det(q_{ij}) \neq 0$$

Indeed, we can easily compute that Q is singular if and only if there exist a non-trivial solution to the system of linear equations:

$$\begin{aligned}
\partial_{X_1} Q &= 2(q_{11}X_1 + q_{12}X_2 + q_{13}X_3) = 0 \\
\partial_{X_2} Q &= 2(q_{21}X_1 + q_{22}X_2 + q_{23}X_3) = 0 \\
\partial_{X_3} Q &= 2(q_{31}X_1 + q_{32}X_2 + q_{33}X_3) = 0
\end{aligned}$$

and this is equivalent $\det(q_{ij}) \neq 0$.

Lemma 3.3. *Let k be a field with* char $\neq 2$. *Let $C_Q \subset \mathbb{P}^2_k$ be a conic defined by $Q \in k[X_1, X_2, X_3]$. Then C_Q is singular if and only if Q is a product of two linear polynomial over the algebraic closure.*

Proof. By diagonalisation of quadratic forms[3] for $Q \in k[X_1, X_2, X_3]$ of homogeneous of degree 2, after rescaling by a non-zero scalar, and a permutation of variables, we can assume that

$$Q(X_1, X_2, X_3) = a_1 X_1^2 + a_2 X_2^2 + a_3 X_3^2.$$

Then, by the above discussion, we see that C_Q is singular if and only if $a_1 a_2 a_3 = 0$.

Now, say $a_3 = 0$, then, we have

$$Q(X_1, X_2, X_3) = (\sqrt{a_1}X_1 + \sqrt{a_2}X_2)(\sqrt{a_1}X_1 - \sqrt{a_2}X_2).$$

[2]There are additional complications with quadratic forms over characteristic 2 fields. We will not concern ourselves with these in this module.

[3]This is not true in characteristic 2

Conversely, suppose $Q = L_1 L_2$ where $L_i \in \overline{k}[X_1, X_2, X_3]$ are linear forms. If $L_1 = L_2$, then every point on Q is singular (we can arrange by a projective linear tranfromation that $L_1 = L_2 = X_1$). Suppose that L_1 and L_2 are distinct, then by Bézout's theorem, they intersect at point P. Now, observe that

$$\partial Q_{X_i} = (\partial_{X_i} L_1)(P) L_2(P) + L_1(P)(\partial_{X_i} L_2)(P) = 0$$

Hence, Q is singular at $P \in L_1 \cap L_2$. □

Proposition 3.4. *Let $C \subset \mathbb{P}^2_k$ be a smooth curve defined by a degree d homogeneous polynomial $F \in k[X_1, X_2, X_3]$. Assume*[4] $\mathrm{char} k \nmid 2(d-1)$. *Then a point $P \in C$ is a flex if and only $H(P) = 0$, where $H(X, Y, Z) = \det\left(\partial^2 F / \partial X_i \partial X_j\right)_{1 \le i,j \le 3}$ is the Hessian.*

Proof. As $F(P) = 0$, the Taylor expansion of F at $P = (P_1, P_2, P_3)$ is of the form

$$F(P_1 + X_1, P_2 + X_2, P_3 + X_3) = \sum_{i=1}^{3} \frac{\partial F}{\partial X_i}(P) X_i + \frac{1}{2} \sum_{i,j=1}^{3} \frac{\partial^2 F}{\partial X_i \partial X_j}(P) X_i X_j + \dots$$

Let $L = \sum_{i=1}^{3} \frac{\partial F}{\partial X_i}(P) X_i$ be the tangent line at P, and $Q = \sum_{i,j=1}^{3} \frac{\partial^2 F}{\partial X_i \partial X_j}(P) X_i X_j$ be the osculating conic.

Since F is homogeneous, we have $F(\lambda X_1, \lambda X_2, \lambda X_3) = \lambda^d F(X_1, X_2, X_3)$. Differentiating with respect to λ gives the Euler relation:

$$\sum_i X_i \frac{\partial F}{\partial X_i} = dF$$

and differentiating again, we arrive at

$$\sum_{i,j} X_i X_j \frac{\partial^2 F}{\partial X_i \partial X_j} = d(d-1)F$$

Hence, we see that $P \in Q$. Moreover, the tangent line to Q at P is given by

$$2 \sum_i \left(\sum_j \frac{\partial^2 F}{\partial X_i \partial X_j}(P) P_j \right) X_i = 2(d-1) \sum_i \frac{\partial F}{\partial X_i}(P) X_i = 0$$

Hence, when $2(d-1) \neq 0$, it coincides with L. Therefore, we conclude that Q is smooth at P.

One can check directly from the definition that the point P is an inflection point if and only if $L \subset Q$ (we leave this as an exercise). This implies Q is singular, hence $H(P) = 0$. Conversely, if Q is singular, it is reducibe (product of lines), but is smooth at P, then $L \subset Q$. Hence P is an inflection point. □

[4] Prove that this assumption is necessary!

$\lhd$ Check that a smooth point $P \subset C$ is an inflection point if and only the tangent line L to C at P is contained in the osculating conic Q.

$\lhd$ Consider the cubic curve $C : \{X^3 + Y^3 + Z^3 + 3XYZ = 0\}$ over k of characteristic not equal to 2 or 3, and $P = [0 : -1 : 1]$ on this curve. Show that the tangent line at P is $X - Y - Z = 0$ and the oscullating conic is $(X - Y - Z)(Y - Z) = 0$. Hence, conclude that P is an inflection point (but observe that it is a smooth point of both C and Q).

Corollary 3.5. *Let $C \subset \mathbb{P}^2$ be smooth projective cubic over a field k that is algebrically closed and characteristic $\neq 2$, then there exists a projective change of co-ordinates on $\mathbb{P}^2$ such that the equation of the C takes the form (called the* **Weierstrass form***):*

$$Y^2Z = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

and the roots of the polynomial $f(X) = X^3 + a_2X^2 + a_4X + a_6 \in k[X]$ are distinct.

Proof. Let $C = \{F(X, Y, Z) = 0\} \subset \mathbb{P}^2$. By the previous theorem, the inflection points on C are given by the intersection of C and the cubic curve $H_F = 0$. By Bézout's theorem, there are 9 inflection points (here use k is algebraically closed and char$k \neq 2$). Let $P \in C$ be an inflection point. Choose co-ordinates such that $P = [0 : 1 : 0]$ and the tangent line at P is given by $Z = 0$. As P is an inflection point, we see that $F(t, 1, 0) = ct^3$ for some $c \in k$, so F has no X^2Y, XY^2 or Y^3 terms. Therefore, we can write it as

$$\alpha Y^2Z + a_1XYZ + a_3YZ^2 = \beta X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

Moreover, as P is a smooth point, it is easy to check that $\alpha, \beta \neq 0$, hence by rescaling ($X \to \alpha\beta X, Y \to \alpha\beta^2 Y$), we can reduce to

$$\alpha Y^2Z + a_1XYZ + a_3YZ^2 = \beta X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3$$

Finally, replacing Y by $Y - \frac{1}{2}a_1X - \frac{1}{2}a_3Z$, we arrive at the desired form. The fact that the resulting $f(X)$ has distinct roots follows by the smoothness assumption. $\square$

$\blacktriangleright$ Over a field of characteristic 2, we can't do the last step, so the general Weierstrass form of an elliptic curve is given by

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \quad a_1, a_2, a_3, a_4, a_6 \in k$$

The notation is absolutely standard, and one records these coefficients as a vector $[a_1, a_2, a_3, a_4, a_6]$. Here is how you can create an elliptic curve in GP:

```
E = ellinit([0,0,-1,1,0])
```

This creates the curve $y^2 - y = x^3 + x$. You can also use the short form.

```
E = ellinit([-432,8208])
```

This creates the curve $y^2 = x^3 - 432x + 8208$. An additional argument has to be entered to specify the field over which the curve is defined if this cannot be inferred from the coefficients. For example,

`E = ellinit([0,0,1,0,1],2)`

defines the curve $y^2 + y = x^3 + 1$ over $\mathbb{F}_2$ and

`E = ellinit([-3,1], O(5^10))`

defines the curve $y^2 = x^3 - 3x + 1$ over $\mathbb{Q}_5$ (up to 10^{th} power of 5).

I used the following references when preparing these lecture notes. This subject is a classical topic. Nothing I wrote is original.

References

[1] K. Buzzard - Lecture notes, inspired by a course given by Cassels.

[2] J.W.S. Cassels - Lectures on Elliptic Curves

[3] J. H. Silverman, J. T. Tate - Rational points on Elliptic Curves