Lecture 16.1

Last time:

- The p-adic numbers are the set $\mathbb{Q}_p$ of equivalence classes of Cauchy sequences in $\mathbb{Q}$ with respect to $|\cdot|_p$.

- The p-adic integers are the subset

$$\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}.$$

- Equivalently, $\mathbb{Z}_p$ corresponds to the coherent sequences in $\mathbb{Q}$, i.e. the p-adic expansions coming from solutions to

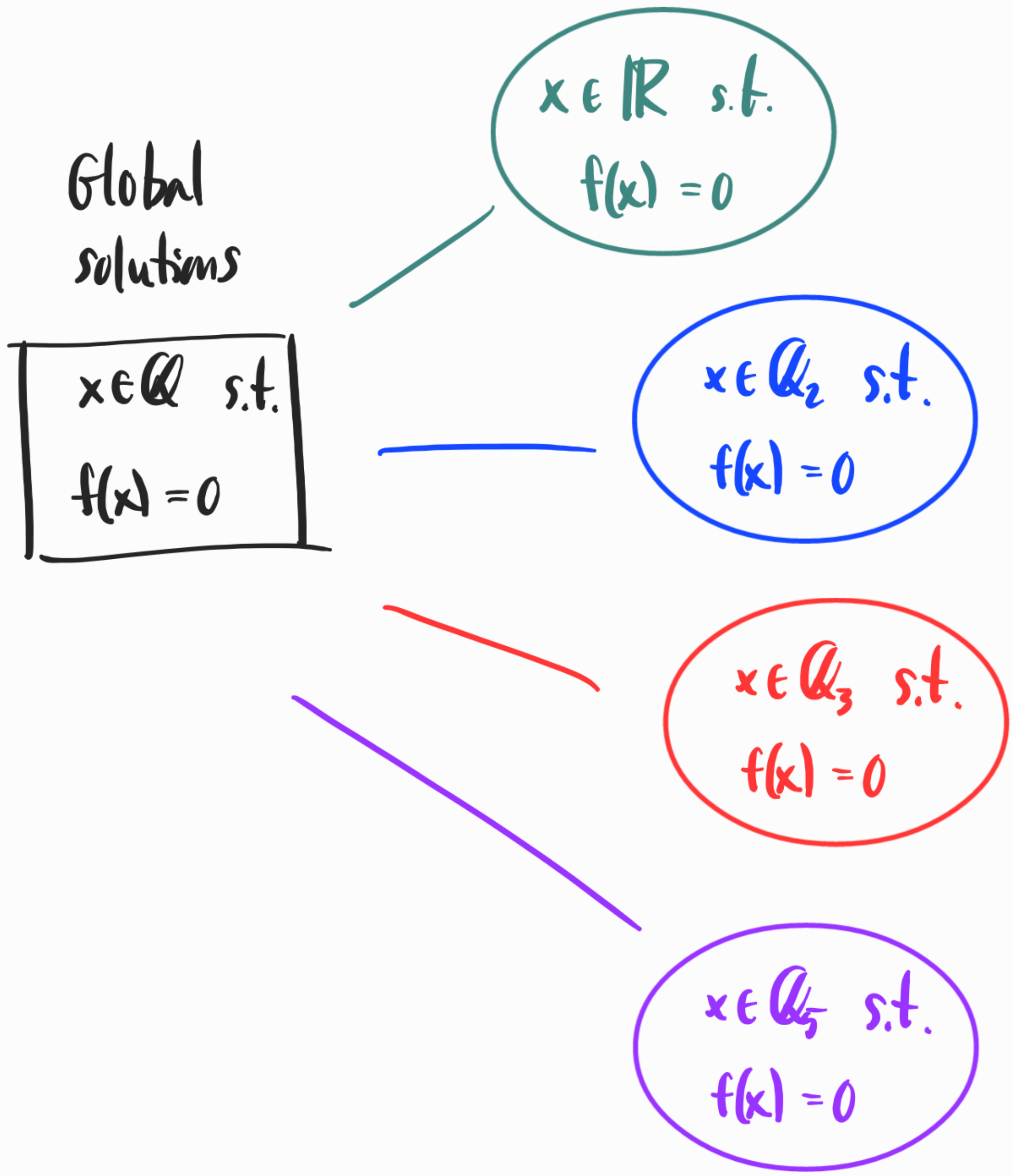
$$f(x) \equiv 0 \pmod{p^n}, \quad n \geq 1.$$

The Local-Global Principle

We have seen that some polynomial equations which do not have solutions in $\mathbb{Q}$, like $x^2+1=0$, may have solutions in some of the completions of $\mathbb{Q}$, namely $\mathbb{Q}_p$ for p prime and $\mathbb{R}$.

More generally, the local-global principle is a philosophy that says solutions to a polynomial equation $f(x)=0$ over $\mathbb{Q}$ can sometimes be understood by studying solutions to $f(x)=0$ over all completions of $\mathbb{Q}$:

Local solutions



etc.

In principle, this seems harder: there are infinitely many "local" number systems to check for solutions, plus the p-adic numbers are still new and unfamiliar to us.

In practice however, this principle — when it applies — is a powerful tool for solving polynomial equations over $\mathbb{Q}$, which is one of the main objectives in modern number theory.

$\boxed{\text{Prop}}$ Let $x \in \mathbb{Q}$. Then x is a square if and only if it's a square in $\mathbb{R}$ and $\mathbb{Q}_p$ for all primes p.

Pf: $(\Rightarrow)$ Clear, since $\mathbb{Q} \subseteq \mathbb{R}$ and $\mathbb{Q} \subseteq \mathbb{Q}_p$.

$(\Leftarrow)$ We can assume $x \neq 0$. If $x = r^2$ for some $r \in \mathbb{R}$, then $x > 0$.

On the other hand, if $x = r_p^2$ for some $r_p \in \mathbb{Q}_p$, then $v_p(x) = v_p(r_p^2) = 2v_p(r_p)$ which is an even integer.

This means that for every prime p dividing the numerator or denominator of x, p^{2k} divides the numerator or denominator, for some $k \in \mathbb{N}$.

Hence x is a rational square. $\square$

In practice, it's even easier to decide if x is a square in $\mathbb{Q}_p$ than by checking its p-adic expansion.

$xy = 1$ for some $y \in \mathbb{Z}_p$

$\boxed{\text{Theorem}}$ Let p be prime and $x \in \mathbb{Z}_p$ be invertible.

(1) If $p > 2$, then x is a square in $\mathbb{Q}_p$ if and only if its mod p reduction $\bar{x}$ is a quadratic residue mod p.

(2) If $p = 2$, then x is a square in $\mathbb{Q}_2$ if and only if $x \equiv 1 \pmod 8$.

$\boxed{\text{Ex}}$ ① For $p = 5$, $x = 14$ is not a rational square, but

$$14 \equiv 4 \equiv 2^2 \pmod 5,$$

so the Theorem implies 14 is a square in $\mathbb{Q}_5$.

Exercise 1: Find the first few terms of the 5-adic expansions of the two roots of

$$x^2 - 14 = 0$$

in $\mathbb{Q}_5$.

Exercise 2: Do the same with $x^2 - 7 = 0$ in $\mathbb{Q}_3$ and with $x^2 - 2 = 0$ in $\mathbb{Q}_7$.

Exercise 3: Show that $x = 3$ is a square mod 2 but not in $\mathbb{Q}_2$, necessitating condition (2) in the Theorem.

More generally, we can evaluate whether a polynomial $f(x)$ with coefficients in $\mathbb{Z}_p$ has roots in $\mathbb{Z}_p$ using the following:

Theorem (Hensel's Lemma) Let $f(x)$ be a polynomial with coefficients in $\mathbb{Z}_p$. If there exists

$x_0 \in \mathbb{Z}_p$ such that

$\bar{x}_0 \equiv x_0 \pmod p$

$$f(\bar{x}_0) \equiv 0 \pmod p$$

$$\text{and} \quad f'(\bar{x}_0) \not\equiv 0 \pmod p$$

these say that $\bar{x}_0$ is a simple root of f mod p

then $f(x) = 0$ has a solution in $\mathbb{Z}_p$. Moreover, there is a unique such solution $\equiv \bar{x}_0 \pmod p$.

$\boxed{\text{Ex}}$ 2 Let $p = 13$ and $f(x) = x^2 + 13x + 1$.

Then mod 13,

$$f(x) \equiv x^2 + 1 \equiv 0 \pmod{13}$$

has a solution, since $\left(\frac{-1}{13}\right) = 1$. An explicit solution is $x_0 \equiv 5 \pmod{13}$.

Meanwhile, $f'(x) = 2x + 13$ and

$$f'(5) = 10 + 13 \not\equiv 0 \pmod{13}$$

so Hensel's Lemma says that

$$x^2 + 13x + 1 = 0$$

has a solution in $\mathbb{Q}_{13}$ whose 13-adic expansions starts with

$$\ldots + a_2 13^2 + a_1 13 + 5 = \ldots a_2 a_1 5.$$

Exercise 4: Find two more terms in the 13-adic expansion of this solution.

Notice that $f(x) = x^2 + 13x + 1$ does <u>not</u> have a rational solution (use the quadratic formula).

One of the most difficult problems in modern number theory is to find all solutions to a given polynomial equation

$$f(x_1, \ldots, x_n) = 0$$

over $\mathbb{Q}$ — or over $\mathbb{Z}$, which can be even more difficult.

The local-global principle, when it applies, is one of the most useful tools at our disposal for deciding when to expect any solutions at all, i.e. if

$X_f(\mathbb{Q}) := \{(x_1, \dots, x_n) \in \mathbb{Q}^n \mid f(x_1, \dots, x_n) = 0\} \neq \emptyset.$

Local-Global Principle $X_f(\mathbb{Q}) \neq \emptyset$ if and only if $X_f(\mathbb{Q}_p) \neq \emptyset$ for all $p \leq \infty$.

One direction is always valid:

Ex 3 $f(x) = x^2 + 1 = 0$ has no solutions in $\mathbb{R}$ (use $|\cdot|_\infty$), hence

$$X_f(\mathbb{R}) = \emptyset \implies X_f(\mathbb{Q}) = \emptyset.$$

4 $f(x) = x^2 - 2 = 0$ has no solutions in

$\mathbb{Q}_2$ (check it!), so

$$X_f(\mathbb{Q}_2) = \emptyset \implies X_f(\mathbb{Q}) = \emptyset.$$

5. With a little work, one can show that $f(x,y) = x^2 - 37y^2 = 0$ has only one solution, $(x,y) = (0,0)$, in $\mathbb{Q}_5$, so this can be the only solution in $\mathbb{Q}$.

In fact, for this type of polynomial equation, the LGP holds in both directions:

$\boxed{\text{Thm (Hasse-Minkowski)}}$ Let $f(x, \ldots)$

Theorem (Hasse – Minkowski) Let $f(x_1, \dots, x_n)$

be a homogeneous quadratic form over $\mathbb{Q}$.

every term looks like

$a_{ij} x_i x_j$ or $a_{ii} x_i^2$, $a_{ij} \in \mathbb{Q}$

Then the local-global principle holds for f:

$$X_f(\mathbb{Q}) \neq \emptyset \iff X_f(\mathbb{Q}_p) \neq \emptyset \text{ for all } p \leq \infty.$$

Ex 6 Let $f(x,y) = 3x^2 - 2y^2$. First,

$X_f(\mathbb{R}) \neq \emptyset$ since, for example, $(\sqrt{\frac{2}{3}}, 1)$ is

a real solution to $f(x,y) = 0$.

On the other hand, $X_f(\mathbb{Q}_7) = \emptyset$:

- if $(x,y) \in X_f(\mathbb{Q}_7)$, we can multiply through by enough powers of 7 to make $(7^m x, 7^m y) \in X_f(\mathbb{Z}_7)$, so we can assume $(x,y) \in X_f(\mathbb{Z}_7)$ to begin with;

- reducing mod 7, we have

$$3\bar{x}^2 - 2\bar{y}^2 \equiv 0 \pmod 7$$

$$\Rightarrow \quad 3\bar{x}^2 \equiv 2\bar{y}^2 \pmod 7$$

$$\Rightarrow \quad \bar{x}^2 \equiv 3\bar{y}^2 \pmod 7 \qquad \text{(multiply by 5)}$$

$$\Rightarrow \quad 1 = \left(\frac{\bar{x}^2}{7}\right) = \left(\frac{3\bar{y}^2}{7}\right) = \left(\frac{3}{7}\right);$$

- but $\left(\frac{3}{7}\right) = -\left(\frac{7}{3}\right) = -\left(\frac{4}{3}\right) = -1$, a contradiction.

Hence $X_f(\mathbb{Q}_7) = \emptyset$ so by the Hasse-Minkowski Theorem,

$$3x^2 - 2y^2 = 0$$

has no rational solutions.

In practice, one can produce a list of finitely many primes p to check for solutions in $\mathbb{Q}_p$ (e.g. using Hensel's

Lemma).

The LGP does not hold for all higher degree polynomials:

- $x^3 - y^2 - 51 = 0$ has local solutions over $\mathbb{R}$ and each $\mathbb{Q}_p$, and happens to have a global solution:

$$(x,y) = \left(\frac{1375}{9}, \frac{50986}{27}\right).$$

- $3x^3 + 4y^3 + 5 = 0$ has solutions over $\mathbb{R}$ and all $\mathbb{Q}_p$, but it has no rational solution!

solutions?

- Same story for $x^4 - 2y^2 - 17 = 0$.

One big project in modern number theory is refining the LGP to handle higher degree polynomial equations like these.

THANKS FOR A GREAT SEMESTER!