Last time:

$$\mathbb{Q}_p^\times \cong \mathbb{Z}_p^\times \times \mathbb{Z}$$

units $\quad \pi^n$

$$\mathbb{Z}_p^\times \cong 1+p\mathbb{Z}_p \times \mathbb{F}_p^\times \cong \mathbb{Z}_p \times \mathbb{F}_p^\times \quad p \text{ odd}$$

$x \mapsto \exp(px)$

$$\mathbb{Z}_2^\times \cong \{\pm 1\} \times (1+4\mathbb{Z}_2) \cong \{\pm 1\} \times \mathbb{Z}_2$$

$x \mapsto \exp(4x)$

§ Quadratic extensions of $\mathbb{Q}_p$

K any field of char. $\neq 2$

quadratic extensions of K $\longleftrightarrow$ (1:1) non-trivial classes in $K^\times/K^{\times 2}$

$K(\sqrt{d}) \longleftarrow d$

F any quad. ext. of K $\longrightarrow a^2-4b$

$F = K(\alpha)$, $\alpha^2 + a\alpha + b = 0$

some $a, b \in K$, then

$$F = K\left(\frac{-a+\sqrt{a^2-4b}}{2}\right) = K\left(\sqrt{a^2-4b}\right)$$

Ex $K = \mathbb{C}$

$\mathbb{C}^\times = \mathbb{C}^{\times 2}$ $\Rightarrow$ no quad. exts.

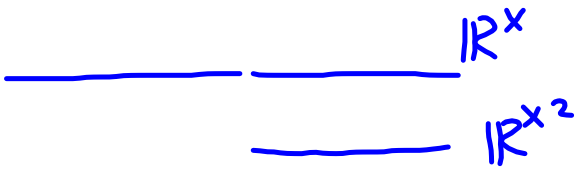
Ex $K = \mathbb{R}$

$\mathbb{R}^\times = \mathbb{R} \setminus \{0\}$

$\mathbb{R}^{\times 2} = \mathbb{R}_{>0}$

$\mathbb{R}^\times / \mathbb{R}^{\times 2} \cong \mathbb{Z}/2\mathbb{Z}$ $\Rightarrow$ the unique quad. ext. of $\mathbb{R}$ is $\mathbb{R}(\sqrt{-1}) = \mathbb{C}$.

$\{1, -1\}$



Ex $K = \mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}$ $(p > 2)$

$\mathbb{F}_p^\times$ cyclic of order $p-1$

$\mathbb{F}_p^{\times 2}$ cyclic of order $\frac{p-1}{2}$

{quadratic residues}

$\mathbb{F}_p^\times / \mathbb{F}_p^{\times 2} \cong \mathbb{Z}/2\mathbb{Z}$ $\Rightarrow$ $\mathbb{F}_p$ has a unique quad. ext., namely $\mathbb{F}_p(\sqrt{\eta}) \cong \mathbb{F}_{p^2}$

$\{1, \eta\}$ — η: any quadratic non-residue

Ex $K = \mathbb{Q}$

$$\mathbb{Q}^\times / \mathbb{Q}^{\times 2} \overset{1:1}{=} \{\text{square-free integers } d\}$$

$\Rightarrow \infty$ quad. exts of $\mathbb{Q}$, e.g.

$$\mathbb{Q}(\sqrt{-1}),\ \mathbb{Q}(\sqrt{2}),\ \mathbb{Q}(\sqrt{3}),\ \mathbb{Q}(\sqrt{-2}),\ \ldots$$

Ex $K = \mathbb{Q}_p$; p odd

$$\mathbb{Q}_p^\times \cong \mathbb{Z}_p^\times \times \mathbb{Z} \cong (1+p\mathbb{Z}_p) \times \mathbb{F}_p^\times \times \mathbb{Z}$$

from residue field cyclic of order $p-1$

$1+p\mathbb{Z}_p$: all $(\mathbb{Z}_p, +)$ by log, exp

$\mathbb{Z}$: gen. by p

$$\mathbb{Q}_p^{\times 2} = (1+p\mathbb{Z}_p) \times \mathbb{F}_p^{\times 2} \times 2\mathbb{Z}$$

same group because $\mathbb{Z}_p \xrightarrow{\times 2} \mathbb{Z}_p$ is an isomorphism ($p \neq 2$)

$$\mathbb{Q}_p^\times / \mathbb{Q}_p^{\times 2} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

with classes $\{1, \eta, p, \eta p\}$ for any $\eta \in \mathbb{Z}_p^\times$ that reduces to a non-residue mod p

$\Rightarrow \mathbb{Q}_p$ has 3 quadratic extensions,

$$\mathbb{Q}_p(\sqrt{\eta}),\ \mathbb{Q}_p(\sqrt{p}),\ \mathbb{Q}_p(\sqrt{\eta p}).$$

anything $\equiv 1 \bmod 4$, $\not\equiv 1 \bmod 8$

Ex $K = \mathbb{Q}_2$

$$\mathbb{Q}_2^\times \cong (1+4\mathbb{Z}_2) \times \{\pm 1\} \times \mathbb{Z}$$

$1+4\mathbb{Z}_2 \xrightarrow{\log} 4\mathbb{Z}_2$, $\exp$ in the other direction

$$\mathbb{Q}_2^{\times 2} = (1+8\mathbb{Z}_2) \times \{1\} \times 2\mathbb{Z}$$

$$\mathbb{Q}_2^\times / \mathbb{Q}_2^{\times 2} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$

5 $\quad$ -1 $\quad$ 2

So $\mathbb{Q}_2$ has 7 quadratic extensions, namely

$$\mathbb{Q}_2(\sqrt{d}) \qquad d \in \{-1, 2, 5, -2, -5, 10, -10\}$$

<u>Cor</u> p odd.

$a \in \mathbb{Z}_p^\times$ is a square $\iff$ $a \bmod p \in \mathbb{F}_p^\times$ is a quad. residue.

$p = 2$

$a \in \mathbb{Z}_2^\times$ is a square $\iff$ $a \equiv 1 \bmod 8$.

Cor p odd

$$(\mathbb{Z}/p^n\mathbb{Z})^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/p^{n-1}\mathbb{Z})$$

cyclic

cyclic order $p-1$

cyclic order p^{n-1}

← classical results in number theory.

$p=2$

$$(\mathbb{Z}/2^n\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{n-3}\mathbb{Z}$$

± 1 gen. by 5

§ Diophantine equations in $\mathbb{Z}_p$

These are special cases of a very general framework.
E.g. we proved that the following are equivalent:

For $a \in \mathbb{Z}_2^\times$

(1) a is a square in $\mathbb{Z}_2$

(2) a is a square mod 2^n for all $n \geq 1$.

(3) a is a square mod 2^3

$x^2 - a \equiv 0$ has solutions

(1) in $\mathbb{Z}_2$

(2) in $\mathbb{Z}/2^n\mathbb{Z}$

(3) in $\mathbb{Z}/8\mathbb{Z}$

Rmk This is why p-adics are useful in number theory:
to study eqns $/\mathbb{Z}$, $/\mathbb{Q}$ first understand
them $/\mathbb{R}$, $/\mathbb{Z}/p^n\mathbb{Z}$, equivalently $/\mathbb{R}$, $/\mathbb{Q}_p$.

bad rings: zero divisors, finite characteristic

great. These are
1) fields
2) characteristic 0
3) complete.

Thm Suppose

$$V: \begin{cases} f_1(x_1, \dots, x_k) = 0 \\ \\ f_r(x_1, \dots, x_k) = 0 \end{cases}$$

system of poly. eqns with $\mathbb{Z}$- (or $\mathbb{Z}_p$-) coefficients. Then

V has a p-adic solution $(a_1, \dots, a_k) \in \mathbb{Z}_p^k$

$\Leftrightarrow$

V has a solution in $\mathbb{Z}/p^n\mathbb{Z}$ for every $n \geq 1$.

Proof $\Rightarrow$ clear: Take a solution $(a_1, \ldots, a_k) \in \mathbb{Z}_p^k$ and reduce it mod p^n.

$\Leftarrow$ Let $a^{(n)} = (a_1^{(n)}, \ldots, a_k^{(n)}) \in \mathbb{Z}_p^k$ be a solution mod p^n, lifted to $\mathbb{Z}_p^k$, i.e. $f_i(a_1^{(n)}, \ldots, a_k^{(n)}) \equiv 0 \mod p^n$ for all i.

$\mathbb{Z}_p^k$ compact $\Rightarrow$ $(a^{(n)})_{n \geq 1}$ has a convergent subsequence, $a^{(n_j)} \to a \in \mathbb{Z}_p^k$ (exc.)

By continuity, all $f_i(a) = 0$ ∎

§ Hensel's lemma

K non-Archimedean, complete w.r.to $|.|$ $\quad \mathbb{Q}_p$

$\mathcal{O}$ ring of integers $\{x \mid |x| \leq 1\}$ $\quad \mathbb{Z}_p$

$\mathfrak{m}$ maximal ideal $\{x \mid |x| < 1\}$ $\quad (p)$

$\mathcal{O}/\mathfrak{m} \cong k$ residue field $\quad \mathbb{F}_p$

$a \longmapsto \bar{a}$

Thm (Hensel's lemma v1) $f(x) \in \mathcal{O}[x]$ monic,

suppose $x_1 \in \mathcal{O}$ s.t.

$$|f(x_1)| < 1 \,, \quad |f'(x_1)| = 1$$

$[\Leftrightarrow f(x_1) \equiv 0 \bmod m$
$f'(x_1) \not\equiv 0 \bmod m]$
$\Leftrightarrow \overline{f}(x)$ has a simple zero $\overline{x_1}$ in k]

Then $\exists!\ x \in \mathcal{O}$ s.t. $f(x) = 0$ and $|x - x_1| \le |f(x_1)|$

$[\Leftrightarrow x \equiv x_1 \bmod m]$

Proof Pick any $\pi \in m \setminus \{0\}$ s.t. $\pi \mid f(x_1)$ (e.g. uniformizer if $|\cdot|$ is discrete).

Proceed by induction:

Given $x_n \in \mathcal{O}$ s.t. $|x_n - x_1| \leq |f(x_1)|$ and $f(x_n) \equiv 0 \mod \pi^n$

want (unique mod π^{n+1})

$x_{n+1} \in \mathcal{O}$ s.t. $|x_{n+1} - x_1| \leq |f(x_1)|$, and $f(x_{n+1}) \equiv 0 \mod \pi^{n+1}$

$x_{n+1} \equiv x_n \mod \pi^n$

Then (x_n) is a Cauchy sequence $\Rightarrow$ $x_n \to x \in \mathcal{O}$ and $f(x) = 0$ by continuity.

Consider $\mathcal{O}[T] \ni f(x_n + \pi^n T) \equiv f(x_n) + f'(x_n)\pi^n T \mod \pi^{n+1}$.

$\equiv 0 \mod \pi^n$

($f'(x_1)$ unit $\Rightarrow$ $f'(x_n)$ is a unit)

To force this to be $\equiv 0 \mod \pi^{n+1}$ set

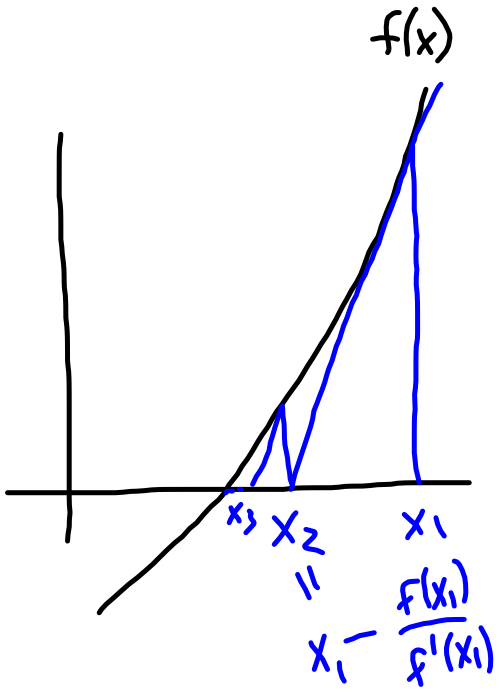
$$T = -\frac{f(x_n)}{f'(x_n)\pi^n} \in \mathcal{O} \leftarrow \text{unique choice mod } \pi$$

In other words, if we let

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

then this sequence is Cauchy and $f(x_n) \to 0$.

Rmk This is exactly like Newton-Raphson's method over $\mathbb{R}$



Ex $f(x) = x^2 + 1$ in $\mathbb{Q}_5$.

$\overline{f}(x) = x^2+1 = (x-2)(x-3)$

$\overline{f}(x)$: $f(x)$ mod 5 in $\mathbb{F}_5[x]$

$(x-2)(x-3)$: two roots of x^2+1 in $\mathbb{F}_5$, both simple (i.e. $\overline{f}'(2) \neq 0$, $\overline{f}'(3) \neq 0$)

Hensel's lemma $\Rightarrow \exists! i \in \mathbb{Z}_5$, $i \equiv 2 \mod 5$ s.t. $i^2 + 1 = 0$.

(and it can be constructed from $x_1 = 2$ (say) by

$$x_{n+1} := x_n - \frac{f(x_n)}{f'(x_n)} = x_n - \frac{x_n^2+1}{2x_n}$$

$x_1 = 2, \quad x_2 = 2 - \frac{5}{4} = \frac{3}{4}, \ldots$

Variants (proof: similar)

$\left(\frac{3}{4}\right)^2 + 1 = \frac{9}{16} + 1 = \frac{25}{16} \equiv 0 \bmod 5^2$

Thm (Hensel's lemma v2: non-singular points on varieties)

$f_1, \ldots, f_r \in \mathcal{O}[X_1, \ldots, X_d]$; $r \leq d$

Suppose $\exists a_1 \in \mathcal{O}^d$ s.t. 1) $f_i(a_1) \equiv 0 \bmod m$ $\forall i$

2) $\left(\frac{\partial f_i}{\partial x_j}\right)(a_1) \bmod m$ has rank r.

Then $\exists\, a \in \mathcal{O}^\times$ s.t. $a \equiv a_1 \bmod \mathfrak{m}$ and

$$a \text{ ll } f_i(a) = 0.$$

Thm (Hensel's Lemma v3 : factorisation)

$f \in \mathcal{O}[x]$ monic s.t. $\overline{f} = g \cdot h \in k[x]$

with g, h monic and coprime.

Then $\exists!$ factorisation $f = G \cdot H$, $G, H \in \mathcal{O}[x]$ monic

lifting it.

Thm (Hensel's lemma v4: deeper roots)

$f \in \mathcal{O}[x]$ monic, $x_1 \in \mathcal{O}$ s.t. $|f(x_1)| < |f'(x_1)|^2$.

Then $\exists!\ x \in \mathcal{O}$ s.t. $f(x) = 0$ and $|x - x_1| \leq \dfrac{|f(x_1)|}{|f'(x_1)|}$

Ex Another proof that $a \in \mathbb{Z}_2^\times$ is a square

$\iff a \equiv 1 \bmod 8$.

Let $a \in \mathbb{Z}_2$, $a \equiv 1 \bmod 8$, $f(x) = x^2 - a$.

Take $x_1 = 1 \Rightarrow f(x) = 1^2 - a \equiv 0 \bmod 8$

$f'(x_1) = 2x_1 = 2$

$|f(x_1)| \leq \frac{1}{8}$

$|f'(x_1)| = \frac{1}{2}$

Hensel's condition satisfied $\Rightarrow$ $\exists$ root of $x^2 = a$ in $\mathbb{Z}_2$.

Rmk In general this gives an explicit condition for which n to test whether $f(x) \equiv 0 \bmod p^n$ to guarantee the existence of a p-adic solution.

§ Inverse limit

Alternative construction of the p-adics :

Instead of

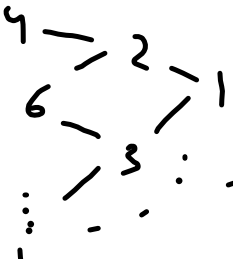
$\mathbb{Q}$ —completion→ $\mathbb{Q}_p$ —ring of integers→ $\mathbb{Z}_p$ "topological way"

$(\mathbb{Z}/p^n\mathbb{Z})_{n\geq 1}$ —inverse limit→ $\mathbb{Z}_p$ —field of fractions→ $\mathbb{Q}_p$

Def $(I, \leq)$ partially ordered index set

[e.g. $\mathbb{N}, \leq$ $\cdots - 4 - 3 - 2 - 1$

or $\mathbb{N}, |$



$(A_i)_{i \in I}$ groups [rings, sets, top. spaces, ...]

$f_{ij} : A_j \longrightarrow A_i$ homomorphisms for all $i \leq j$

s.t. $f_{ij} \circ f_{jk} = f_{ik}$ and $f_{ii} = id$.

The <u>inverse limit</u> (or <u>projective limit</u>)

$$\varprojlim_{i \in I} A_i = \left\{ (a_i)_{i \in I} \mid a_i \in A_i,\ f_{ij}(a_j) = a_i \text{ for all } i \leq j \right\}.$$

(again a group (ring, top. space, ...) for top. spaces topology induced from the product topology $\varprojlim A_i \subseteq \prod A_i$, called the inverse limit topology.