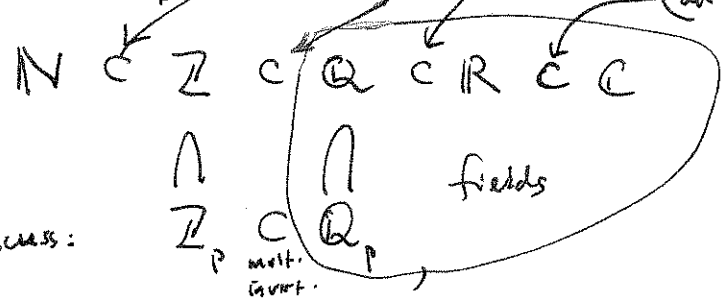
Introduction to p-adic numbers

You are already familiar with



In this talk we'll discuss: $\mathbb{Z}_p \subset \mathbb{Q}_p$ (mult. invert.) for p prime.

Why would we want to make things more complicated? One reason:

(i) Diophantine equations. = eqns. with $\mathbb{Q}$-coeffs. whose soln's (in several vars.) are sought for in $\mathbb{Q}$.

- Hilbert's 10th problem (1900): produce an algorithm for determining their solvability in a finite # of steps

  Matiyasevich (1970): none exists — $\exists$ eqns w/ no solutions but such that this essentially can't be proved (a concrete instance of Gödel incompleteness theorem)

- one case for which (apart from $(0,0,0)$) insolubility is known: the Fermat eqn.

$$x^n + y^n = z^n, \quad n \geq 3 \qquad \text{(due to Wiles (1995))}$$

- one case for which one knows all solutions is Pell's eqn.; a special case is

$$x^2 - 5y^2 = \pm 4$$

If $y_0, y_1, y_2, \ldots = 0, 1, 1, 2, 3, 5, 8, 13, \ldots$ (Fibonacci)

$x_0 = 4$, $x_n := \frac{y_{2n}}{y_n} \left(\in \mathbb{Z}\,!\right)$ the soln's are $\{(\pm x_n, \pm y_n)\}$.

- what relates this to p-adics is the Hasse–Minkowski Theorem: ($a, b, c \in \mathbb{Q}$)

If $aX^2 + bY^2 + cZ^2 = 0$ admits nonzero solutions in $\mathbb{Q}_p$ (for each p) and in $\mathbb{R}$, then it can be solved over $\mathbb{Q}$.

(easier to check)

(ii) Absolute values. functions $|\cdot| : \mathbb{Q} \to [0, \infty)$ s.t.
- $|x| = 0 \Leftrightarrow x = 0$
- $|xy| = |x||y|$
- $|x+y| \leq |x| + |y|$

There is the "usual" one $|\cdot|_\infty$ and also $|x|_p = |p^k x'|_p := p^{-k}$. "Completing" $\mathbb{Q}$ by adding all convergent sums gives $\mathbb{R}$ resp. $\mathbb{Q}_p$.

(iii) Arithmetic Geometry. Connected with modular forms, rep. thy, & Wiles proof.

Modular Arithmetic

$\mathbb{Z}/p\mathbb{Z}$: add & multiply mod p. This gives a field (can divide); its non-zero elements (p prime) give $(\mathbb{Z}/p\mathbb{Z})^*$, a cyclic group of order $(p-1)$. (Write $x \in \mathbb{Z}/p\mathbb{Z}$ as $\# \in \{0, 1, \ldots, p\}$)

- Squares. In $(\mathbb{Z}/3\mathbb{Z})^*$, $\{1\}$
  " $(\mathbb{Z}/5\mathbb{Z})^*$, $\{1,4\}$
  " $(\mathbb{Z}/7\mathbb{Z})^*$, $\{1,2,4\}$

  } looks like $\frac{1}{2}$ of elements: indeed, $(\mathbb{Z}/p\mathbb{Z})^* \to (\mathbb{Z}/p\mathbb{Z})^*$ is 2:1, since $a^2 \underset{(p)}{\equiv} b^2 \Rightarrow p \mid a^2 - b^2 = (a-b)(a+b)$
  $\Rightarrow a \underset{(p)}{\equiv} \pm b$.

- Primitive m^{th} roots of 1. When $\exists\, x \in (\mathbb{Z}/p\mathbb{Z})^*$ with $x^m \underset{(p)}{\equiv} 1$ but $x^n \underset{(p)}{\not\equiv} 1$ for $0 < n < m$?
  Since $(\mathbb{Z}/p\mathbb{Z})^*$ cyclic, $1 = x^{p-1} = x^{km+r} = x^r \Rightarrow r = 0 \Rightarrow$ (m | p-1)
  $(0 \le r < m)$
  In $\mathbb{Z}/5\mathbb{Z}$, 2 & 3 are primitive 4th roots of 1
  " $\mathbb{Z}/7\mathbb{Z}$, 2 & 4 are primitive 3rd roots of 1.

What are the p-adics?

- $\mathbb{R}$: #'s with decimal expansion

  digits

  $c_2\, c_1\, c_0 . c_{-1} c_{-2} c_{-3} c_{-4} \cdots \longrightarrow$, $0 \le c_i \le 9$

  (Terminating to left)

  $\Vert$

  $c_2 10^2 + c_1 10 + c_0 + \frac{c_{-1}}{10} + \frac{c_{-2}}{10^2} + \cdots \longrightarrow$

  (could also, in same way, expand in a base other than 10)

- What happens if we not only work in (base p, prime), but terminate to the right? $0 \le a_i \le p-1$

  (p-digits?)

  $\cdots a_3 a_2 a_1 a_0 . a_{-1} a_{-2} \mid = \frac{a_{-2}}{p^2} + \frac{a_{-1}}{p} + a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \cdots \longrightarrow$

  Multiplication & addition take place in essentially the same way, by "carrying to the left" (which now can go on forever!). That's the idea.

Definition: Let p = a prime #. $\mathbb{Z}_p$ (= p-adic integers) consists of the (sums) (infinite) series (sums all up at infinity)

$$a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \cdots$$

with each integer a_i between 0 & $p-1$ (inclusive).

- start with subset of these that have finite expansions: let's see how

$$\mathbb{N} \subset \mathbb{Z}_p.$$

Ex/ $p=5$. (Map $\mathbb{N} \to \mathbb{Z}_5$ by writing elements "in base 5".)

37 (say) $= a_0 + a_1 p + a_2 p^2 + \cdots$

mod 5: $2 \underset{(5)}{\equiv} a_0$

mod 25: $12 \underset{(25)}{\equiv} 2 + a_1 \cdot 5 \to 10 \underset{(25)}{\equiv} 5a_1 \to 2 \underset{(5)}{\equiv} a_1$

mod 125: $37 \underset{(125)}{=} 12 + a_2 \cdot 25 \to 25 \underset{(125)}{=} 25 a_2 \to 1 \underset{(5)}{\equiv} a_2$

so $37 = 2 + 2p + p^2$

Ex/ $p=7$.

$37 = 1 + p^2 + p^3$.

Operations

- Say $\alpha = a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \cdots$

α_0, α_1, α_2, α_3

$\beta = b_0 + b_1 p + b_2 p^2 + b_3 p^3 + \cdots$

Think of $\alpha_n \in \mathbb{Z}/p^{n+1}\mathbb{Z}$ as "truncations"; you know α if you know the full sequence of these.

- (since we know how to add in $\mathbb{Z}/p^{n+1}\mathbb{Z}$,) define $\alpha+\beta$ & $\alpha \cdot \beta$ by their truncations:

$$(\alpha+\beta)_n := (\alpha_n + \beta_n)_n$$
$$(\alpha \cdot \beta)_n := (\alpha_n \cdot \beta_n)_n$$

} how you're really just adding/multiplying in $\mathbb{Z}/p^{n+1}\mathbb{Z}$.

- In practice, it just looks like carrying:

Ex/ $p=5$. $\alpha = 2 + 2p + p^2$ "37"

$\beta = 4 + 3p$ "19"

$$\alpha + \beta = \underbrace{(2+4)}_{1+5} + 2p + 3p + p^2$$
$$= 1 + \underbrace{(p + 2p + 3p)}_{p + 6p} + p^2$$
$$= 1 + p + \underbrace{(p^2 + p^2)}_{2p^2}$$
$$= 1 + p + 2p^2 \quad \text{"56"}$$

$$\alpha\beta = \underbrace{2\cdot 4}_{3+5} + 2\cdot 3p + 4\cdot 2p + 2\cdot 3p^2 + 4p^2 + 3p^3$$
$$= 3 + \underbrace{(p + 6p + 8p)}_{15p} + 6p^2 + 4p^2 + 3p^3$$
$$= 3 + \underbrace{(3p^2 + 6p^2)}_{9p^2} + 4p^2 + 3p^3$$
$$= 3 + 3p^2 + \underbrace{(2p^3 + 3p^3)}_{5p^3}$$
$$= 3 + 3p^2 + p^4.$$

Ex/ $p=3$. $\alpha = 2 + 2p + 2p^2 + 2p^3 + \cdots \longrightarrow$

$\beta = 1$

$\alpha+\beta = 1 + 2 + 2p + 2p^2 + \cdots$ (have more than 1st.)

$= p + 2p + 2p^2 + \cdots$

$= p^2 + 2p^2 + 2p^3 + \cdots$

$= p^3 + 2p^3 + 2p^4 + \cdots$

$= p^4 + 2p^4 + \cdots$

$= \cdots = 0$.

$\Rightarrow \alpha = -1$!

- So :) how can we arithmetically invert? Given a rational # in $\mathbb{Z}_p$ (or more generally an arbitrary p-adic number), call it β, what is $-\beta$? This will give

$$\mathbb{Z} \subset \mathbb{Z}_p$$

Ex/ $p=3$. $\beta = 1 + p^2 + p^3$ "37" } demand $\alpha+\beta = 0$ in $\mathbb{Z}_3$.

$\alpha = a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \cdots$

mod 3: $a_0 + 1 \underset{(3)}{\equiv} 0 \Rightarrow a_0 = 2$

mod 9: $3 + 3a_1 \underset{(9)}{\equiv} 0 \Rightarrow 1 + a_1 \underset{(3)}{\equiv} 0 \Rightarrow a_1 = 2$

mod 27: $9 + 9 + 9a_2 \underset{(27)}{\equiv} 0 \Rightarrow 2 + a_2 \underset{(3)}{\equiv} 0 \Rightarrow a_2 = 1$

mod 81: $27 + 27 + 27 a_3 \underset{(81)}{\equiv} 0 \Rightarrow a_3 = 1$

and then $a_4 = a_5 = \cdots = 2$.

- Next goal: set $\mathbb{Q} \subset \mathbb{Z}_p$? FALSE. Can only multiplicatively invert those integers not divisible by p.

Ex/ $p=5$. $\alpha = 2 + 2p + p^2$ "37"

$\beta = b_0 + b_1 p + b_2 p^2 + \cdots$

$\alpha \cdot \beta = 1$

mod 5: $2b_0 \overset{(5)}{\equiv} 1 \Rightarrow b_0 = 3$

mod 25: $6 + 30 + 10b_1 \overset{(25)}{\equiv} 1 \Rightarrow 10b_1 \overset{(20)}{\equiv} -35 \rightarrow 2b_1 \equiv -7 \equiv 3 \Rightarrow b_1 = 4$

mod 125: $\cdots - - - - b_2 = 3$.

To express all rationals p-adically need p-adic rationals:

Definition: $\mathbb{Q}_p$ consists of all formal sums

$$\frac{a_{-m}}{p^m} + \frac{a_{-m+1}}{p^{m-1}} + \cdots + \frac{a_{-1}}{p} + a_0 + a_1 p + a_2 p^2 + \cdots$$

Given an integer $p^m q$, $p \nmid q$, expect $\frac{1}{q} \in \mathbb{Z}_p$ as above, then simply "shift back" by dividing by p^m formally. The same idea *extends* all elements of $\mathbb{Q}_p$. Conclude: $\mathbb{Q} \subset \mathbb{Q}_p$ and $\mathbb{Q}_p$ is a field.

Square roots

Theorem A: $\sqrt{2} \notin \mathbb{Q}$

Pf: Suppose $\sqrt{2} = \frac{a}{b}$, $a, b \in \mathbb{N}$ in lowest terms (no common prime factors)

$$\Rightarrow 2 = a^2/b^2 \Rightarrow 2b^2 = a^2$$

FTA $\Rightarrow a = p_1^{m_1} \cdots p_k^{m_k}$

$$2b^2 = a^2 = p_1^{2m_1} \cdots p_k^{2m_k}$$

(2) must appear (by uniqueness of prime fact.)

Hence $2 \mid a$, and writing $a = 2c$, have $2b^2 = (2c)^2 = 4c^2$

$$\Rightarrow b^2 = 2c^2.$$

By the same argument, $2 \mid b$, contradicting our choice of $a \nmid b$. □

Theorem B: $\sqrt{2} \in \mathbb{Q}_7$. (So $\mathbb{Q}_7$ is "bigger" than $\mathbb{Q}$. Roughly, can view $\mathbb{Q} \subset \mathbb{Q}_7$ as the "repeating sequences" just as $\mathbb{Q} \subset \mathbb{R}$ gives the repeating decimals.)

Pf: Must solve (w/ $\alpha = a_0 + a_1 7 + a_2 7^2 + \cdots$)

$$\alpha^2 = 2 \quad \text{in (effectively) } \mathbb{Z}_7.$$

Truncate: $a_0^2 \underset{(7)}{\equiv} 2 \Rightarrow a_0 = 3$ or 4, $7 \nmid a_0$.

Get $(3 + 7a_1)^2 \underset{(49)}{\equiv} 2 \Rightarrow 42 a_1 \underset{(49)}{\equiv} -7 \Rightarrow 6 a_1 \underset{(7)}{\equiv} -1$

$9 + 42a_1$ III (49)

$$\Rightarrow a_1 = 1.$$

(Can show $a_2 = 2$, etc. Problem is: we need to prove that this can be continued indefinitely.)

Suppose, then, that we have found

$$\alpha_{n-1} = a_0 + 7a_1 + 7^2 a_2 + \cdots + 7^{n-1} a_{n-1} \in [0, 7^n - 1)$$

with $\alpha_{n-1}^2 \underset{(7^n)}{\equiv} 2$. Can we find a_n s.t. $\alpha_n = \alpha_{n-1} + a_n 7^n$ has $\alpha_n^2 \underset{(7^{n+1})}{\equiv} 2$?

Write $2 \underset{(7^{n+1})}{\equiv} (a_{n-1} + 7^n a_n)^2 \underset{(7^{n+1})}{\equiv} a_{n-1}^2 + 2\cdot 7^n a_n a_{n-1} \equiv 2 + 7^n k + 2a_n a_{n-1} 7^n$ (6)

$(0 \le k \le 6)$

$\Rightarrow 0 \underset{(7^{n+1})}{\equiv} 7^n (k + 2a_n a_{n-1})$

$\Rightarrow 0 \underset{(7)}{\equiv} k + 2a_n a_{n-1} \equiv k + 2a_n a_0 = k + 6a_n \equiv k - a_n$

$\Rightarrow a_n = k$. □

- $\sqrt{2} \notin \mathbb{Q}_5$ since 2 is not a square mod 5 (so, can't get "started" with a_0). However, $\mathbb{Q}_5$ has a $\sqrt{-1}$. Try to compute some digits of this at home!

Hensel's Lemma — is the reason why solving eqns. in $\mathbb{Q}_p$ is often easier than in $\mathbb{Q}$

- Let $F(X) = A_0 + A_1 X + A_2 X^2 + \cdots + A_n X^n$ ($\mathbb{Z}$-coeffs)
  $F'(X) = A_1 + 2A_2 X + \cdots + n A_n X^{n-1}$ (formal derivative)

Theorem: If $\exists\, a_0$ s.t. $\begin{cases} F(a_0) \underset{(p)}{\equiv} 0 \\ F'(a_0) \underset{(p)}{\not\equiv} 0 \end{cases}$ then $\exists\, \alpha = a_0 + a_1 p + \cdots \in \mathbb{Z}_p$ with $F(\alpha) = 0$ (in $\mathbb{Z}_p$).

Application 1: $p \neq 2$, $m \underset{(p)}{\equiv}$ square $(\equiv a_0^2)$. Then $\sqrt{m} \in \mathbb{Q}_p$.

Pf: Apply Hensel to $X^2 - m = F(X)$, $2X = F'(X)$. We have
$a_0^2 - m \underset{(p)}{\equiv} 0$, $p \nmid 2a_0 \Rightarrow F'(a_0) \underset{(p)}{\not\equiv} 0$. Hensel $\Rightarrow \exists\, \alpha \in \mathbb{Z}_p$ s.t. $\alpha^2 - m = 0$. □

Application 2: p prime, $m > 1$, $p \nmid m$.
Show that $\exists$ primitive mth root of 1 in $\mathbb{Q}_p \iff m \mid p-1$. (Try it!)

Local-Global — not going to go into Hasse-Minkowski or its ramifications, but:

- Suppose $x \in \mathbb{Q}_{>0}$ has a $\sqrt{\ }$ in each $\mathbb{Q}_p$. Then x has a $\sqrt{\ }$ in $\mathbb{Q}$!

Pf: write (by FTA) $x = \prod_p p^{\overbrace{n_p}^{\in \mathbb{Z}}}$, and $\sqrt{x} = a_m p^m + a_{m+1} p^{m+1} + \cdots$

$x = a_m^2 p^{2m} + \cdots$.

$\Rightarrow n_p = 2m$. So each n_p is divisible by 2 $\Rightarrow \sqrt{x} = \prod_p p^{n_p/2} \in \mathbb{Q}$. □

Topology on $\mathbb{Q}_p$

- If $x = a_m p^m + a_{m+1} p^{m+1} + \cdots$, then $|x|_p = p^{-m}$. Think of p^m as small for m big.
- Unit disk (closed) in $\mathbb{Q}_p$ is $\mathbb{Z}_p$, and any two pts. in it are ≤ 1 apart.
- $|x+y|_p \le \max\{|x|_p, |y|_p\} \Rightarrow$ if $|x_k|_p \to 0$ $(k \to \infty)$, then $\sum_1^\infty x_k$ converges p-adically!!!