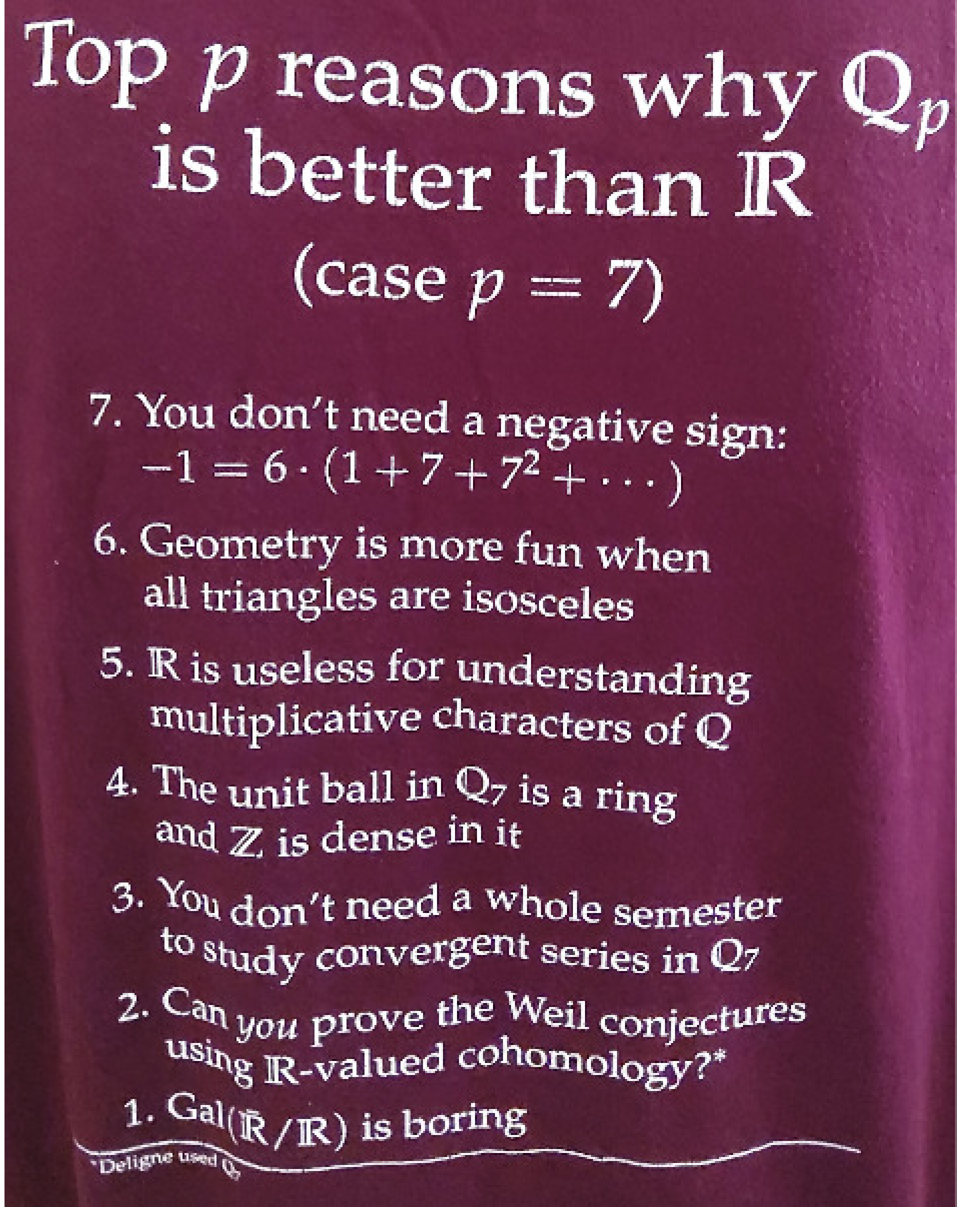
The *p*-adic numbers

Schedule this week:

Monday and Wednesday: lectures/office hours as scheduled.
Thursday: no problem set due.
Friday: no lecture.

Fun fact: Miro's autocorrect tried to change "p-adic" to "p-addict".



Warmup: rings of formal power series

k = field

$k[[x]] = \{ c_0 + c_1 x + c_2 x^2 + \cdots : c_0, c_1, c_2 \ldots \in k \}$

$\cup$

$k[x] = \{ c_0 + c_1 x + c_2 x^2 + \cdots : c_0, c_1, c_2 \ldots \in k$ all but finitely many are $0 \}$

add termwise, multiply by

$(c_0 + c_1 x + \cdots) \cdot (d_0 + d_1 x + \cdots) = e_0 + e_1 x + \cdots$

$e_k = \sum_{i+j=k} c_i d_j$

DVR, unique maximal ideal $= (x)$
$= \{$zero constant term$\}$

$k[[x]] = \varprojlim k[x]/(x^n)$

$\cdots \to \frac{k[x]}{x^3} \to \frac{k[x]}{x^2} \to \frac{k[x]}{x} \cong k$

inverse limit / projective limit / limit

Formal power series as an inverse limit

$$k[[x]] \cong \varprojlim_n k[x]/(x^n) \qquad \frac{k[x]}{(x^{n+1})} \to \frac{k[x]}{(x^n)}$$

$$= \left\{ (\alpha_n)_{n=1}^{\infty} : \alpha_n \in k[x]/(x^n), \quad \alpha_{n+1} \equiv \alpha_n \mod x^n \right\}$$

"coherent sequences"

Note:
If k is finite or countable, then $k[x]$ is countable
but $k[[x]]$ is uncountable (continuum)

p-adic "power series expansions"

Kurt Hensel (~1900)

Let p be a prime

write nonnegative integers in base p $\qquad 21_{(p)} = 2p+1$ $(p > 2)$

This amounts to writing $n = a_0 + a_1 p + a_2 p^2 + \cdots$

$\ldots a_2 a_1 a_0 (p)$ $\quad a_0, a_1, \ldots \in \{0, \ldots, p-1\}$

all but finitely many are 0

now allow infinite series expansions!

$(a_0 + a_1 p + a_2 p^2 + \ldots) \times (b_0 + b_1 p + b_2 p^2 + \ldots)$

$= c_0 + c_1 p + c_2 p^2 + \ldots$

$\{0, \ldots, p-1\}$

$\Longrightarrow \mathbb{Z}_p$ p-adic integers

Negation and fractions

$$(p-1)+(p-1)\cdot p+(p-1)p^2+(p-1)p^3+\cdots=-1.$$

$$1+p+p^2+\cdots=\frac{1}{1-p}$$

for every $\frac{r}{s}$ the $\gcd(s,p)=1$, we have $\frac{r}{s}\in\mathbb{Z}_p$

i.e. $\mathbb{Z}_{(p)}\subset\mathbb{Z}_p$

$\frac{1}{p}\notin\mathbb{Z}_p.$

$$\begin{array}{r} \cdots\ 1\ \boxed{0}\ \\ \hline \cdots\ \boxed{1}\ \end{array}$$

What if p is not prime?

if replace p with $q=p^k$

no change

$m,n>1$

If replace p with mn, $\gcd(m,n)=1$

set product of $\mathbb{Z}_m$ and $\mathbb{Z}_n$

$\Leftarrow$ (CRT)

p-adic integers as an inverse limit

$$\mathbb{Z}_p \cong \varprojlim_n \mathbb{Z}/(p^n)$$

$$a_0 + a_1 p + \cdots \mapsto \left(\text{class of } a_0 + a_1 p + \cdots a_{n-1} p^{n-1} \atop \in \mathbb{Z}/(p^n) \right)$$

$$1 + p + p^2 + \cdots = \frac{1}{1-p}$$

mod any power of p, this equality becomes a valid congruence.

The *p*-adic integers form a discrete valuation ring

Prop $\mathbb{Z}_p$ is a discrete valuation ring

= principal ideal domain &

w/ unique (nonzero) maximal ideal.

pf $\mathbb{Z}_p \to \mathbb{F}_p$ surjective homomorphism

with kernel (p).

every element of $\mathbb{Z}_p - (p)$ has a multiplicative inverse!

— every element of $\mathbb{Z} - (p)$ divides $1 - p^n$ for some n

$(1-p^n)^{-1} = 1 + p^n + p^{2n} + \cdots$

— every element of $\mathbb{Z}_p$ of form $1 - px$ has inverse $1 + px + p^2x^2 \cdots$

$\Rightarrow$ unique maximal ideal. Similar logic

$\Rightarrow$ only ideals are $(0), (p^n)$

p-adic numbers

p-adic numbers

Define $\mathbb{Q}_p = \mathbb{Z}_p\left[\frac{1}{p}\right] = \mathrm{Frac}(\mathbb{Z}_p)$

field of characteristic 0

These have base-p expansions

$$\cdots a_1 a_0 . a_{-1} \cdots a_{-m}$$

radix point

$\mathbb{Q} \subset \mathbb{Q}_p$

$\mathbb{Q}_p$ is not an inverse limit

$$\mathbb{Q}_p = \bigcup_m p^{-m}\mathbb{Z}_p$$

direct limit

injective limit

colimit

p-adic solutions of polynomial equations

Compactness

Prop $F(x_1, \ldots, x_n) \in \mathbb{Z}(x_1, \ldots, x_n)$

any polynomial!

Then $F(x_1, \ldots, x_n) = 0$ has a solution in $\mathbb{Z}_p$

clear

$\Longleftrightarrow$ $F(x_1, \ldots, x_n) \equiv 0 \bmod p^m$ has a solution in $\mathbb{Z}/p^m\mathbb{Z}$ for all m.

(not assuming existence of a convergent sequence of solutions)

Pf Assume $\exists$ solutions modulo p^m for all m.

- Reduce these solutions mod p, some solution occurs infinitely often. Pick one.
- Take the solutions that reduce to the chosen one mod p. Reduce mod p^2. Some solution occurs ∞ often, pick one.

...

Example: square roots

$c \in \mathbb{Z}_p$

$p \neq 2$ prime. $c \not\equiv 0 \mod p$

$x^2 = c$ has a solution

$\Updownarrow$

$x^2 \equiv c \mod p^n$ has a solution for all n,

$\Updownarrow$ elementary number theory

$\boxed{x^2 \equiv c \mod p.}$

example of Hensel's lemma

this is typical, except maybe for only needing mod p.