Math 525 Class 7 Sept 6

Why p-adic integers?

$$\sqrt{1+x} = 1 + \frac{1}{2}x - \frac{1}{8}x^2 + \frac{1}{16}x^3 - \frac{5}{128}x^4 + \cdots$$

Notice that we have only 2s in the denominator

Why is that? We could try to prove this by developing a formula, maybe doing an induction

Not much insight here — but p-adic integers can help!

First note that $\sqrt{1+x} = (1+x)^{1/2}$

$$= 1 + \binom{\frac{1}{2}}{1}x + \binom{\frac{1}{2}}{2}x^2 + \binom{\frac{1}{2}}{3}x^3 + \cdots$$

$$= \sum_{n=0}^{\infty} \binom{\frac{1}{2}}{n} x^n \quad \text{where} \quad \binom{\frac{1}{2}}{n} = \frac{\frac{1}{2}\left(\frac{1}{2}-1\right)\cdots\left(\frac{1}{2}-n+1\right)}{n!}$$

Note that $\binom{\frac{1}{2}}{n}$ is a polyn. in $\mathbb{Q}\left[\frac{1}{2}\right]$.

in fact $\binom{y}{n}$ is a polyn in $\mathbb{Q}[y]$.

This polyn. is a p-adically continuous fcn

For odd p, $\dfrac{p^k+1}{2} \in \mathbb{Z} \subset \hat{\mathbb{Z}}_p$

And. $\lim_{k\to\infty} \dfrac{p^k+1}{2} = \dfrac{1}{2}$ [p-adic limit]

$\lim_{k\to\infty} \binom{\frac{p^k+1}{2}}{n} = \binom{\frac{1}{2}}{n}$ p-adic limit.

↑ an ordinary integer: no denom..

$\mathbb{Z} \subset \hat{\mathbb{Z}}_p$ and $\hat{\mathbb{Z}}_p$ are compact.

So $\binom{\frac{1}{2}}{n}$ is an element of $\hat{\mathbb{Z}}_p$.

An element of $\hat{\mathbb{Z}}_p$ cannot have $p \in$ denom.

i.e. $\frac{1}{p} \notin \hat{\mathbb{Z}}_p$. Thus $\binom{\frac{1}{2}}{n}$ has no p in denom, true for all odd p.

Conceptual defn of p-adic integers $\hat{\mathbb{Z}}_p$.

take $\mathbb{Z}$. introduce a metric under which

$$p^k \longrightarrow 0 \quad \text{as} \quad k \longrightarrow \infty.$$

Now take the completion (the hat!) $\hat{\mathbb{Z}}_p$.

Thus: $\binom{\frac{1}{2}}{n}$ has only 2s in denom.

This application is easy to understand but not very significant.

Another example: Define a recurrence:

$$F(1) = F(2) = F(4) = 0 \qquad F(3) = 1$$

for $i \geq 5$: $F(i) = F(i-2) + F(i-4)$.

$$F(5) = F(3) + F(1) = 1$$

$$F(6) = F(4) + F(2) = 0$$

$$F(7) = F(3) + F(5) = 2$$

$F(8) = F(6) + F(4) = 0$

$F(9) = F(7) + F(5) = 3$

$F(10) = 0 \quad F(11) = 5 \quad F(12) = 0 \quad F(13) = 8.$

$F(\text{even}) = 0 \qquad F(\text{odd}) = \text{Fibonacci}?$

Notice that the set of n such that

$F(n) = 0$ is an arithmetic progression.

In general

Theorem (Skolem-Mahler-Lech).

Let $G(n)$ $n \geq 1$ be any sequence generated by an integer linear recurrence.

Then $\{n \mid G(n) = 0\}$ is a finite union of arithmetic progressions plus a finite set.

Proof uses p-adic integers — even though there is nothing in the statement about $\hat{\mathbb{Z}}_p$.

Another example:

Local - Global Principle.

⟨Fact⟩ is true over $\mathbb{Q}$ $\iff$ ⟨Fact⟩ is true over $\mathbb{R}$ and $\mathbb{Q}_p$ (for all p)

An example of a theorem in this style:

Hasse - Minkowski Theorem on classification of quadratic forms.

"Structure" — regularities that must hold for every example of ⟨math object⟩

(In a Euclidean Ring, every ideal is a principal ideal (generated by 1 elt.)

(Wedderburn's Theorem: A semisimple ring with min. cond is $\cong \prod_{i=1}^{n} M_{n_i}(D_i)$ for division rings D_i.

Group Rings over a field are an example of Semi-simple rings with min Cond.

Example 1: $\mathbb{R}[D_8] \cong \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R} \oplus M_2(\mathbb{R})$

Example 2: $\mathbb{R}[Q_8] \cong \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{R} \oplus \mathbb{H}$.

Generally if G has irred. representations of degree d_i (with mult. m_i) over $\mathbb{C}$.

then $\mathbb{C}[G] \cong \bigoplus_i M_{d_i}(\mathbb{C})^{\oplus m_i}$

In particular, any abelian group A has.

$$\mathbb{C}[A] \cong \mathbb{C}^{\oplus |A|}.$$

More complicated over $\mathbb{Q}$ or $\mathbb{Z}$.

e.g. $\mathbb{Q}[C_3] \cong \mathbb{Q} \oplus \mathbb{Q}(\omega)$ $\quad \omega^2 + \omega + 1 = 0$, $\omega \in \mathbb{C}$.

$C_3 = \{e, x, x^2\}$

$$\left(\frac{e+x+x^2}{3}\right)^2 = \frac{e+x+x^2}{3}$$

	e	x	x^2
e	e	x	x^2
x	x	x^2	e
x^2	x^2	e	x

These decompositions into direct products correspond to "orthogonal idempotents". (p. 855)

So in $\mathbb{Q}[C_3]$ we have written down

$$\frac{e+x+x^2}{3} \qquad e - \frac{e+x+x^2}{3}$$

is the other "orthogonal" idempotent.

and we have

$$\left(\frac{e+x+x^2}{3}\right)\left(e - \frac{e+x+x^2}{3}\right) = 0 .$$

$$\left(e - \frac{e+x+x^2}{3}\right)^2 = e - 2\left(\frac{e+x+x^2}{3}\right) + \frac{e+x+x^2}{3}$$

$$= e - \frac{e+x+x^2}{3}$$ it is idempotent.