Profinite number theory

Hendrik Lenstra

Mathematisch Instituut
Universiteit Leiden

The factorial number system

Each $n \in \mathbf{Z}_{\geq 0}$ has a unique representation

$$n = \sum_{i=1}^{\infty} c_i i! \quad \text{with } c_i \in \mathbf{Z},$$

$$0 \leq c_i \leq i, \quad \#\{i : c_i \neq 0\} < \infty.$$

In factorial notation:

$$n = (\ldots c_3 c_2 c_1)_!.$$

Examples: $25 = (1001)_!$, $1001 = (121221)_!$.

Note: $c_1 \equiv n \bmod 2$.

Arithmetic

For any k, the k last digits of $n + m$ depend only on the k last digits of n and of m.

Likewise for $n \cdot m$.

Hence one can also define the sum and the product of *any* two infinite sequences $(\ldots c_3 c_2 c_1)_!$ with each $c_i \in \mathbf{Z}$, $0 \leq c_i \leq i$.

Profinite numbers

Example: $(\ldots 4321)_! + (\ldots 0001)_! = (\ldots 0000)_! = 0$,
so $(\ldots 4321)_! = -1$.

The set of such sequences $(\ldots c_3 c_2 c_1)_!$ is a *ring* with these operations, the *ring of profinite integers*.

Notation: $\hat{\mathbf{Z}}$.

A formal definition

Better:

$$\hat{\mathbf{Z}} = \{(a_n)_{n=1}^{\infty} \in \prod_{n=1}^{\infty} (\mathbf{Z}/n\mathbf{Z}) : n|m \Rightarrow a_m \equiv a_n \bmod n\}.$$

This is a subring of $\prod_{n=1}^{\infty} (\mathbf{Z}/n\mathbf{Z})$.

Its unit group $\hat{\mathbf{Z}}^*$ is a subgroup of $\prod_{n=1}^{\infty} (\mathbf{Z}/n\mathbf{Z})^*$.

Equivalent definition:

$$\hat{\mathbf{Z}} = \mathrm{End}(\mathbf{Q}/\mathbf{Z}),$$
$$\hat{\mathbf{Z}}^* = \mathrm{Aut}(\mathbf{Q}/\mathbf{Z}).$$

Three exercises

Exercise 1. The ring homomorphism $\mathbf{Z} \to \hat{\mathbf{Z}}$ is injective but not surjective.

Exercise 2: $\hat{\mathbf{Z}}$ is uncountable.

Exercise 3. For each $m \in \mathbf{Z}_{>0}$, the maps $\hat{\mathbf{Z}} \to \hat{\mathbf{Z}}$, $a \mapsto ma$ and $\hat{\mathbf{Z}} \to \mathbf{Z}/m\mathbf{Z}$, $a = (a_n)_{n=1}^{\infty} \mapsto a_m$ fit into a short exact sequence

$$0 \to \hat{\mathbf{Z}} \to \hat{\mathbf{Z}} \to \mathbf{Z}/m\mathbf{Z} \to 0.$$

Profinite rationals

Define

$$\hat{\mathbf{Q}} = \{(a_n)_{n=1}^{\infty} \in \prod_{n=1}^{\infty} (\mathbf{Q}/n\mathbf{Z}) : n|m \Rightarrow a_m \equiv a_n \bmod n\mathbf{Z}\}.$$

Exercise 4. The additive group $\hat{\mathbf{Q}}$ has exactly one ring multiplication extending the ring multiplication on $\hat{\mathbf{Z}}$.

Exercise 5. The ring $\hat{\mathbf{Q}}$ is commutative, it has $\mathbf{Q}$ and $\hat{\mathbf{Z}}$ as subrings, and

$$\hat{\mathbf{Q}} = \mathbf{Q} + \hat{\mathbf{Z}} = \mathbf{Q} \cdot \hat{\mathbf{Z}} \cong \mathbf{Q} \otimes_{\mathbf{Z}} \hat{\mathbf{Z}}$$

(as rings).

Topological structure

If each $\mathbf{Z}/n\mathbf{Z}$ has the discrete topology and $\prod_{n=1}^{\infty}(\mathbf{Z}/n\mathbf{Z})$ the product topology, then $\hat{\mathbf{Z}}$ is *closed* in $\prod_{n=1}^{\infty}(\mathbf{Z}/n\mathbf{Z})$.

It is a compact Hausdorff totally disconnected topological ring. A neighborhood base of 0 is $\mathcal{B} = \{m\hat{\mathbf{Z}} : m \in \mathbf{Z}_{>0}\}$.

With the same neighborhood base, $\hat{\mathbf{Q}}$ is also a topological ring. It is locally compact, Hausdorff, and totally disconnected.

Amusing isomorphisms

We have $\hat{\mathbf{Z}} \subset \mathrm{A} = \prod_{n=1}^{\infty}(\mathbf{Z}/n\mathbf{Z})$.

Exercise 7: $\mathrm{A}/\hat{\mathbf{Z}} \cong \mathrm{A}$ as additive topological groups.

Exercise 8: $\mathrm{A} \cong \mathrm{A} \times \hat{\mathbf{Z}}$ as groups but not as topological groups.

Profinite groups

In infinite Galois theory, the Galois groups that one encounters are *profinite groups*.

A profinite group is a topological group that is isomorphic to a closed subgroup of a product of finite discrete groups.

Equivalent definition: it is a compact Hausdorff totally disconnected topological group.

Examples: the additive group of $\hat{\mathbf{Z}}$ and its unit group $\hat{\mathbf{Z}}^*$ are profinite groups.

$\hat{\mathbf{Z}}$ as the analogue of $\mathbf{Z}$

Familiar fact. For each group G and each $\gamma \in G$ there is a unique group homomorphism $\mathbf{Z} \to G$ with $1 \mapsto \gamma$, namely $n \mapsto \gamma^n$.

Analogue for $\hat{\mathbf{Z}}$. For each profinite group G and each $\gamma \in G$ there is a unique group homomorphism $\hat{\mathbf{Z}} \to G$ with $1 \mapsto \gamma$, and it is continuous. Notation: $a \mapsto \gamma^a$.

Examples of infinite Galois groups

For a field k, denote by $\bar{k}$ an algebraic closure.

Example 1: with p prime and $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ one has

$$\hat{\mathbf{Z}} \cong \mathrm{Gal}(\bar{\mathbf{F}}_p/\mathbf{F}_p), \quad a \mapsto \mathrm{Frob}^a,$$

where $\mathrm{Frob}(\alpha) = \alpha^p$ for all $\alpha \in \bar{\mathbf{F}}_p$.

Example 2: with

$$\mu = \{\text{roots of unity in } \bar{\mathbf{Q}}^*\} \cong \mathbf{Q}/\mathbf{Z}$$

one has

$$\mathrm{Gal}(\mathbf{Q}(\mu)/\mathbf{Q}) \cong \mathrm{Aut}\,\mu \cong \hat{\mathbf{Z}}^*$$

as topological groups.

Radical Galois groups

Example 3. For $r \in \mathbf{Q}$, $r \notin \{-1, 0, 1\}$, put

$$\sqrt[\infty]{r} = \{\alpha \in \bar{\mathbf{Q}} : \exists n \in \mathbf{Z}_{>0} : \alpha^n = r\}.$$

Theorem (Abtien Javanpeykar)**.** *Let G be a profinite group. Then there exists $r \in \mathbf{Q} \backslash \{-1, 0, 1\}$ with $G \cong \mathrm{Gal}(\mathbf{Q}(\sqrt[\infty]{r})/\mathbf{Q})$ (as topological groups) if and only if there is a non-split exact sequence*

$$0 \to \hat{\mathbf{Z}} \xrightarrow{\iota} G \xrightarrow{\pi} \hat{\mathbf{Z}}^* \to 1$$

of profinite groups such that

$$\forall a \in \hat{\mathbf{Z}}, \gamma \in G : \gamma \cdot \iota(a) \cdot \gamma^{-1} = \iota(\pi(\gamma) \cdot a).$$

Diophantine equations

Given $f_1, \ldots, f_k \in \mathbf{Z}[X_1, \ldots, X_n]$, one wants to solve the system $f_1(x) = \ldots = f_k(x) = 0$ in $x = (x_1, \ldots, x_n) \in \mathbf{Z}^n$.

Theorem. (a) *There is a solution* $x \in \mathbf{Z}^n \Rightarrow$ *for each* $m \in \mathbf{Z}_{>0}$ *there is a solution modulo* $m \Leftrightarrow$ *there is a solution* $x \in \hat{\mathbf{Z}}^n$.

(b) *It is decidable whether a given system has a solution* $x \in \hat{\mathbf{Z}}^n$.

p-adic numbers

Let p be prime. The *ring of p-adic integers* is

$$\mathbf{Z}_p = \{(b_i)_{i=0}^{\infty} \in \prod_{i=0}^{\infty} (\mathbf{Z}/p^i\mathbf{Z}) : i \le j \Rightarrow b_j \equiv b_i \bmod p^i\}.$$

It is a compact Hausdorff totally disconnected topological ring.

$\mathbf{Z}_p$ is a *principal ideal domain*, with $p\mathbf{Z}_p$ as its only non-zero prime ideal.

All ideals of $\mathbf{Z}_p$ are *closed*, and of the form $p^h\mathbf{Z}_p$ with $h \in \mathbf{Z}_{\ge 0} \cup \{\infty\}$, where $p^\infty \mathbf{Z}_p = \{0\}$.

The Chinese remainder theorem

For $n = \prod_{p \text{ prime}} p^{i(p)}$ one has

$$\mathbf{Z}/n\mathbf{Z} \cong \prod_{p \text{ prime}} (\mathbf{Z}/p^{i(p)}\mathbf{Z}) \qquad \text{(as rings)}.$$

In the limit:

$$\hat{\mathbf{Z}} \cong \prod_{p \text{ prime}} \mathbf{Z}_p \qquad \text{(as topological rings)}.$$

Profinite number theory

The isomorphism $\hat{\mathbf{Z}} \cong \prod_p \mathbf{Z}_p$ reduces most questions that one may ask about $\hat{\mathbf{Z}}$ to similar questions about the much better behaved rings $\mathbf{Z}_p$.

Profinite number theory studies the exceptions.

Ideals of $\hat{\mathbf{Z}}$

For an ideal $\mathbf{a} \subset \hat{\mathbf{Z}} = \prod_p \mathbf{Z}_p$, one has:

$$\mathbf{a} \text{ is closed} \Leftrightarrow \mathbf{a} \text{ is finitely generated} \Leftrightarrow \mathbf{a} \text{ is principal}$$

$$\Leftrightarrow \ \mathbf{a} = \prod_p \mathbf{a}_p \text{ where each } \mathbf{a}_p \subset \mathbf{Z}_p \text{ an ideal.}$$

The set of closed ideals of $\hat{\mathbf{Z}}$ is in bijection with the set $\{\prod_p p^{h(p)} : h(p) \in \mathbf{Z}_{\geq 0} \cup \{\infty\}\}$ of *Steinitz numbers*.

Most ideals of $\hat{\mathbf{Z}}$ are not closed.

The spectrum of $\hat{\mathbf{Z}}$

The *spectrum* $\operatorname{Spec} R$ of a commutative ring R is its set of prime ideals. *Example*: $\operatorname{Spec} \mathbf{Z}_p = \{\{0\}, p\mathbf{Z}_p\}$.

One studies $\operatorname{Spec} \hat{\mathbf{Z}}$ through the set of *ultrafilters* on the set $\mathcal{P}$ of prime numbers.

For $S \subset \mathcal{P}$, let $e_S \in \prod_{p \in \mathcal{P}} \mathbf{Z}_p = \hat{\mathbf{Z}}$ have coordinate 0 at $p \in S$ and 1 at $p \notin S$.

There is a map $\Upsilon \colon \operatorname{Spec} \hat{\mathbf{Z}} \to \{\text{ultrafilters on } \mathcal{P}\}$ defined by

$$\Upsilon(\mathbf{p}) = \{S \subset \mathcal{P} : e_S \in \mathbf{p}\}.$$

The spectrum and ultrafilters

Example: If $\mathbf{p} = \ker(\hat{\mathbf{Z}} \to \mathbf{Z}_p \text{ or } \mathbf{F}_p)$ for some $p \in \mathcal{P}$, then $\Upsilon(\mathbf{p})$ is principal: $S \in \Upsilon(\mathbf{p}) \Leftrightarrow p \in S$.

Theorem. (a) $\mathbf{p}$ *is closed in* $\hat{\mathbf{Z}} \Leftrightarrow \Upsilon(\mathbf{p})$ *is principal.*

(b) $\Upsilon(\mathbf{p}) = \Upsilon(\mathbf{q}) \Leftrightarrow \mathbf{p} \subset \mathbf{q}$ *or* $\mathbf{q} \subset \mathbf{p}$.

(c) *The fibre* $\Upsilon^{-1}U = \{\mathbf{p} \in \operatorname{Spec} \hat{\mathbf{Z}} : \Upsilon(\mathbf{p}) = U\}$ *over an ultrafilter* U *on* $\mathcal{P}$ *has size* 2 *if* U *is principal and is infinite if* U *is free.*

Question: how does the order type of the totally ordered set $\Upsilon^{-1}U$ vary as U ranges over all ultrafilters on $\mathcal{P}$?

The logarithm

$u \in \mathbf{R}_{>0} \Rightarrow \log u = (\frac{\mathrm{d}}{\mathrm{d}x} u^x)_{x=0} = \lim_{\epsilon \to 0} \frac{u^\epsilon - 1}{\epsilon}$.

Analogously, define $\log\colon \hat{\mathbf{Z}}^* \to \hat{\mathbf{Z}}$ by

$$\log u = \lim_{n \to \infty} \frac{u^{n!} - 1}{n!}.$$

This is a well-defined continuous group homomorphism.

Its kernel is $\hat{\mathbf{Z}}^*_{\mathrm{tor}}$, which is the closure of the set of elements of finite order in $\hat{\mathbf{Z}}^*$.

Its image is $2\mathrm{J} = \{2x : x \in \mathrm{J}\}$, where $\mathrm{J} = \bigcap_p p\hat{\mathbf{Z}}$ is the *Jacobson radical* of $\hat{\mathbf{Z}}$.

Structure of $\hat{\mathbf{Z}}^*$

The logarithm fits in a commutative diagram

$$\begin{tikzcd}
1 \arrow[r] & \hat{\mathbf{Z}}^*_{\mathrm{tor}} \arrow[r] \arrow[d, "\wr"] & \hat{\mathbf{Z}}^* \arrow[r, "\log"] \arrow[d, equal] & 2\mathrm{J} \arrow[r] & 0 \\
1 & (\hat{\mathbf{Z}}/2\mathrm{J})^* \arrow[l] & \hat{\mathbf{Z}}^* \arrow[l] & 1+2\mathrm{J} \arrow[l] \arrow[u, "\wr"'] & 1 \arrow[l]
\end{tikzcd}$$

of profinite groups, where the other horizontal maps are the natural ones, the rows are exact, and the vertical maps are *isomorphisms*.

Corollary: $\hat{\mathbf{Z}}^* \cong (\hat{\mathbf{Z}}/2\mathrm{J})^* \times 2\mathrm{J}$ *(as topological groups).*

More on $\hat{\mathbf{Z}}^*$

Less canonically, with $\mathrm{A} = \prod_{n \geq 1} (\mathbf{Z}/n\mathbf{Z})$:

$$2\mathrm{J} \cong \hat{\mathbf{Z}},$$

$$(\hat{\mathbf{Z}}/2\mathrm{J})^* \cong (\mathbf{Z}/2\mathbf{Z}) \times \prod_p (\mathbf{Z}/(p-1)\mathbf{Z}) \cong \mathrm{A},$$

$$\hat{\mathbf{Z}}^* \cong \mathrm{A} \times \hat{\mathbf{Z}},$$

as topological groups, and

$$\hat{\mathbf{Z}}^* \cong \mathrm{A}$$

as groups.

Power series expansions

The inverse isomorphisms

$$\log\colon 1+2\mathrm{J} \xrightarrow{\sim} 2\mathrm{J}$$
$$\exp\colon 2\mathrm{J} \xrightarrow{\sim} 1+2\mathrm{J}$$

are given by power series expansions

$$\log(1-x) = -\sum_{n=1}^{\infty} \frac{x^n}{n}, \qquad \exp x = \sum_{n=0}^{\infty} \frac{x^n}{n!}$$

that converge for all $x \in 2\mathrm{J}$.

The logarithm is analytic on all of $\hat{\mathbf{Z}}^*$ in a weaker sense.

Two topologies on $\hat{\mathbf{Q}}$

Reminder: $\hat{\mathbf{Q}}$ is a topological ring, the set

$$\mathcal{B} = \{m\hat{\mathbf{Z}} : m \in \mathbf{Z}_{>0}\}$$

of $\hat{\mathbf{Z}}$-ideals being a neighborhood base of 0.

The set of closed maximal ideals of $\hat{\mathbf{Q}}$ is a subbase for the neighborhoods of 0 in a second ring topology on $\hat{\mathbf{Q}}$ that we need. A neighborhood base for 0 in that topology is given by the set

$$\mathcal{C} = \{\mathbf{Q} \cdot \bigcap_{n=0}^{\infty} m^n\hat{\mathbf{Z}} : m \in \mathbf{Z}_{>0}\},$$

which consists of $\hat{\mathbf{Q}}$-ideals.

Analyticity

Let $x_0 \in D \subset \hat{\mathbf{Q}}$. We call $f \colon D \to \hat{\mathbf{Q}}$ *analytic in* x_0 if there is a sequence $(a_n)_{n=0}^{\infty} \in \hat{\mathbf{Q}}^{\infty}$ such that one has

$$f(x) = \sum_{n=0}^{\infty} a_n \cdot (x - x_0)^n$$

in the sense that

$$\forall U \in \mathcal{C} : \exists V \in \mathcal{B} : \forall x \in (x_0 + V) \cap D : \forall W \in \mathcal{B} :$$

$$\exists N_0 \in \mathbf{Z}_{\geq 0} : \forall N \geq N_0 : \sum_{n=0}^{N} a_n \cdot (x - x_0)^n \in f(x) + U + W.$$

To understand this formula, first omit all U's.

Examples of analytic functions

The map $\log\colon \hat{\mathbf{Z}}^* \to \hat{\mathbf{Z}} \subset \hat{\mathbf{Q}}$ is analytic in each $x_0 \in \hat{\mathbf{Z}}^*$, with expansion

$$\log x = \log x_0 - \sum_{n=1}^{\infty} \frac{(x_0 - x)^n}{n \cdot x_0^n}.$$

For each $u \in \hat{\mathbf{Z}}^*$, the map

$$\hat{\mathbf{Z}} \to \hat{\mathbf{Z}}^* \subset \hat{\mathbf{Q}}, \qquad x \mapsto u^x$$

is analytic in each $x_0 \in \hat{\mathbf{Z}}$, with expansion

$$u^x = \sum_{n=0}^{\infty} \frac{(\log u)^n \cdot u^{x_0} \cdot (x - x_0)^n}{n!}.$$

A Fibonacci example

Define $F\colon \mathbf{Z}_{\geq 0} \to \mathbf{Z}_{\geq 0}$ by

$$F(0) = 0, \quad F(1) = 1, \quad F(n+2) = F(n+1) + F(n).$$

Theorem. *The function F has a unique continuous extension $\hat{\mathbf{Z}} \to \hat{\mathbf{Z}}$, and it is analytic in each $x_0 \in \hat{\mathbf{Z}}$.*

Notation: F.

For $n \in \mathbf{Z}$, one has

$$F(n) = n \Leftrightarrow n \in \{0, 1, 5\}.$$

Fibonacci fixed points

One has $\#\{x \in \hat{\mathbf{Z}} : F(x) = x\} = 11$.

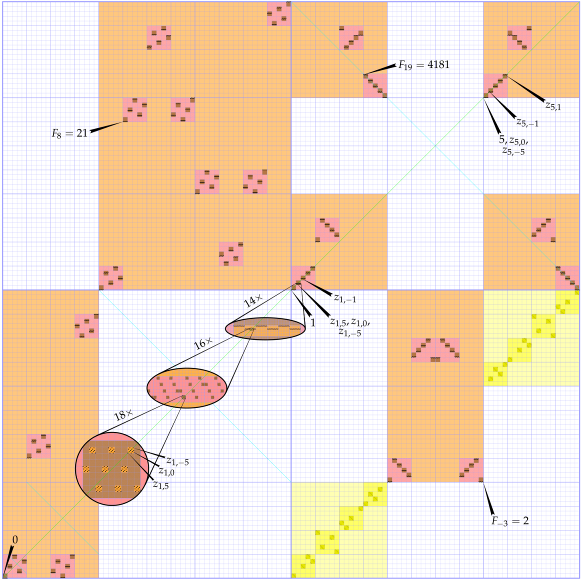
The only *even* fixed point of F is 0, and for each $a \in \{1, 5\}$, $b \in \{-5, -1, 0, 1, 5\}$ there is a unique fixed point $z_{a,b}$ with

$$z_{a,b} \equiv a \bmod \bigcap_{n=0}^{\infty} 6^n \hat{\mathbf{Z}}, \quad z_{a,b} \equiv b \bmod \bigcap_{n=0}^{\infty} 5^n \hat{\mathbf{Z}}.$$

Examples: $z_{1,1} = 1$, $z_{5,5} = 5$.

The number $z_{5,-5}^2$ is exceedingly close to 25 without being equal to it.

Illustration by Willem Jan Palenstijn



Explanation of the picture

$(\ldots c_3c_2c_1)_! = \sum_{i\geq 1} c_i i! \in \hat{\mathbf{Z}}$ is represented by $\sum_{i\geq 1} c_i/(i+1)! \in [0,1]$.

In green: the graph of $a \mapsto a$.
In blue: the graph of $a \mapsto -a$.
In yellow: the graph of $a \mapsto a^{-1} - 1$ $(a \in \hat{\mathbf{Z}}^*)$.
In orange/red/brown: the graph of $a \mapsto F(a)$.

Intersection of the latter graph with the diagonal:

$$\{0\} \cup \{z_{a,b} : a \in \{1,5\}, b \in \{-5,-1,0,1,5\}\}.$$

Larger cycles

I believe:

$$\#\{x \in \hat{\mathbf{Z}} : F(F(x)) = x\} = 21,$$
$$\#\{x \in \hat{\mathbf{Z}} : F^n(x) = x\} < \infty \quad \text{for each } n \in \mathbf{Z}_{>0}.$$

Question: does F have cycles of length greater than 2?

Other linear recurrences

If $E\colon \mathbf{Z}_{\geq 0} \to \mathbf{Z}$, $t \in \mathbf{Z}_{>0}$, $d_0, \ldots, d_{t-1} \in \mathbf{Z}$ satisfy

$$\forall n \in \mathbf{Z}_{\geq 0} : E(n+t) = \sum_{i=0}^{t-1} d_i \cdot E(n+i),$$

$$d_0 \in \{1, -1\},$$

then E has a unique continuous extension $\hat{\mathbf{Z}} \to \hat{\mathbf{Z}}$. It is analytic in each $x_0 \in \hat{\mathbf{Z}}$.

Finite cycles

Suppose also $X^t - \sum_{i=0}^{t-1} d_i X^i = \prod_{i=1}^{t} (X - \alpha_i)$, where

$$\alpha_1, \ldots, \alpha_t \in \mathbf{Q}(\sqrt{\mathbf{Q}}),$$
$$\alpha_j^{24} \neq \alpha_k^{24} \qquad (1 \leq j < k \leq t).$$

Tentative theorem. *If $n \in \mathbf{Z}_{>0}$ is such that the set*

$$S_n = \{x \in \hat{\mathbf{Z}} : E^n(x) = x\}$$

is infinite, then $S_n \cap \mathbf{Z}_{\geq 0}$ contains an infinite arithmetic progression.

This would imply that $\{x \in \hat{\mathbf{Z}} : F^n(x) = x\}$ is finite for each $n \in \mathbf{Z}_{>0}$.

Envoi

And that's the end.
Now carp at me. I don't intend
to justify this tale to you.
Why tell it? Well, I wanted to!

Alexander Pushkin
(*translation*: Ranjit Bolt)