Profinite number theory

Hendrik Lenstra

Mathematisch Instituut
Universiteit Leiden
The factorial number system

Each \( n \in \mathbb{Z}_{\geq 0} \) has a unique representation

\[
n = \sum_{i=1}^{\infty} c_i i! \quad \text{with } c_i \in \mathbb{Z},
\]

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

In factorial notation:

\[
n = (\ldots c_3 c_2 c_1)!.
\]

**Examples:** \( 25 = (1001)! \), \( 1001 = (121221)! \).

Note: \( c_1 \equiv n \mod 2 \).
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 $(\ldots c_3c_2c_1)_i$ with each $c_i \in \mathbb{Z}$, $0 \leq c_i \leq i$. 
Profinite numbers

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

The set of such sequences \((\ldots c_3c_2c_1)!\) is a ring with these operations, the ring of profinite integers.

Notation: \(\hat{\mathbb{Z}}\).
A formal definition

Better:

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

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

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

Equivalent definition:

$$\hat{\mathbb{Z}} = \text{End}(\mathbb{Q}/\mathbb{Z}),$$
$$\hat{\mathbb{Z}}^* = \text{Aut}(\mathbb{Q}/\mathbb{Z}).$$
Three exercises

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

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

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

$$0 \to \hat{\mathbb{Z}} \to \hat{\mathbb{Z}} \to \mathbb{Z}/m\mathbb{Z} \to 0.$$
Profinite rationals

Define

\[ \hat{\mathbb{Q}} = \left\{ (a_n)_{n=1}^{\infty} \in \prod_{n=1}^{\infty} (\mathbb{Q}/n\mathbb{Z}) : n|m \Rightarrow a_m \equiv a_n \mod n\mathbb{Z} \right\}. \]

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

Exercise 5. The ring \( \hat{\mathbb{Q}} \) is commutative, it has \( \mathbb{Q} \) and \( \hat{\mathbb{Z}} \) as subrings, and

\[ \hat{\mathbb{Q}} = \mathbb{Q} + \hat{\mathbb{Z}} = \mathbb{Q} \cdot \hat{\mathbb{Z}} \cong \mathbb{Q} \otimes_{\mathbb{Z}} \hat{\mathbb{Z}} \]

(as rings).
Topological structure

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

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

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

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

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

Exercise 8: $A \cong A \times \hat{\mathbb{Z}}$ 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 $\hat{\mathbb{Z}}$ and its unit group $\hat{\mathbb{Z}}^*$ are profinite groups.
\( \hat{\mathbb{Z}} \) as the analogue of \( \mathbb{Z} \)

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

*Analogue for \( \hat{\mathbb{Z}} \).* For each profinite group \( G \) and each \( \gamma \in G \) there is a unique group homomorphism \( \hat{\mathbb{Z}} \to G \) 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 $\mathbf{F}_p = \mathbb{Z}/p\mathbb{Z}$ one has

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

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

*Example 2*: with

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

one has

$$\text{Gal}(\mathbb{Q}(\mu)/\mathbb{Q}) \cong \text{Aut } \mu \cong \hat{\mathbb{Z}}^*$$

as topological groups.
Radical Galois groups

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

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

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

$$0 \to \widehat{\mathbb{Z}} \xrightarrow{\iota} G \xrightarrow{\pi} \widehat{\mathbb{Z}}^* \to 1$$

of profinite groups such that

$$\forall a \in \widehat{\mathbb{Z}}, \gamma \in G : \gamma \cdot \iota(a) \cdot \gamma^{-1} = \iota(\pi(\gamma) \cdot a).$$
Diophantine equations

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

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

(b) It is decidable whether a given system has a solution \( x \in \hat{\mathbb{Z}}^n \).
**p-adic numbers**

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

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

It is a compact Hausdorff totally disconnected topological ring.

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

All ideals of $\mathbb{Z}_p$ are *closed*, and of the form $p^h\mathbb{Z}_p$ with $h \in \mathbb{Z}_{\geq 0} \cup \{\infty\}$, where $p^\infty\mathbb{Z}_p = \{0\}$.
The Chinese remainder theorem

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

\[
\mathbb{Z}/n\mathbb{Z} \cong \prod_{p \text{ prime}} (\mathbb{Z}/p^{i(p)}\mathbb{Z}) \quad \text{(as rings)}.
\]

In the limit:

\[
\hat{\mathbb{Z}} \cong \prod_{p \text{ prime}} \mathbb{Z}_p \quad \text{(as topological rings)}.
\]
Profinite number theory

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

*Profinite number theory* studies the exceptions.
Ideals of $\hat{\mathbb{Z}}$

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

$a$ is closed $\iff$ $a$ is finitely generated $\iff$ $a$ is principal

$\iff a = \prod_p a_p$ where each $a_p \subset \mathbb{Z}_p$ an ideal.

The set of closed ideals of $\hat{\mathbb{Z}}$ is in bijection with the set

$\{\prod_p p^{h(p)} : h(p) \in \mathbb{Z}_{\geq 0} \cup \{\infty\}\}$ of Steinitz numbers.

Most ideals of $\hat{\mathbb{Z}}$ are not closed.
The spectrum of $\hat{\mathbb{Z}}$

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

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

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

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

$$\Upsilon(p) = \{S \subset \mathcal{P} : e_S \in p\}.$$
The spectrum and ultrafilters

*Example:* If $p = \ker(\hat{\mathbb{Z}} \to \mathbb{Z}_p$ or $F_p)$ for some $p \in \mathcal{P}$, then $\Upsilon(p)$ is principal: $S \in \Upsilon(p) \iff p \in S$.

**Theorem.** (a) $p$ is closed in $\hat{\mathbb{Z}} \iff \Upsilon(p)$ is principal.
   (b) $\Upsilon(p) = \Upsilon(q) \iff p \subset q$ or $q \subset p$.
   (c) The fibre $\Upsilon^{-1}U = \{p \in \text{Spec} \hat{\mathbb{Z}} : \Upsilon(p) = U\}$ 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

\[ u \in \mathbb{R}_{>0} \Rightarrow \log u = \left( \frac{d}{dx} u^x \right)_{x=0} = \lim_{\epsilon \to 0} \frac{u^\epsilon - 1}{\epsilon}. \]

Analogously, define \( \log : \hat{\mathbb{Z}}^* \to \hat{\mathbb{Z}} \) by

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

This is a well-defined continuous group homomorphism.

Its kernel is \( \hat{\mathbb{Z}}_{\text{tor}}^* \), which is the closure of the set of elements of finite order in \( \hat{\mathbb{Z}}^* \).

Its image is \( 2J = \{ 2x : x \in J \} \), where \( J = \bigcap_p p\hat{\mathbb{Z}} \) is the Jacobson radical of \( \hat{\mathbb{Z}} \).
Structure of $\hat{\mathbb{Z}}^*$

The logarithm fits in a commutative diagram

\[
\begin{array}{cccccc}
1 & \rightarrow & \hat{\mathbb{Z}}_{tor}^* & \rightarrow & \hat{\mathbb{Z}}^* & \rightarrow & 2J & \rightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
1 & \leftarrow & (\hat{\mathbb{Z}}/2J)^* & \leftarrow & \hat{\mathbb{Z}}^* & \leftarrow & 1 + 2J & \leftarrow & 1
\end{array}
\]

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

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

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

$$2J \cong \hat{\mathbb{Z}},$$

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

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

as topological groups, and

$$\hat{\mathbb{Z}}^* \cong A$$

as groups.
Power series expansions

The inverse isomorphisms

\[ \log: 1 + 2J \sim 2J \]
\[ \exp: 2J \sim 1 + 2J \]

are given by power series expansions

\[ \log(1 - x) = - \sum_{n=1}^{\infty} \frac{x^n}{n}, \quad \exp x = \sum_{n=0}^{\infty} \frac{x^n}{n!} \]

that converge for all \( x \in 2J \).

The logarithm is analytic on all of \( \hat{\mathbb{Z}}^* \) in a weaker sense.
Two topologies on $\hat{\mathbb{Q}}$

 Reminder: $\hat{\mathbb{Q}}$ is a topological ring, the set
$$ \mathcal{B} = \{ m\hat{\mathbb{Z}} : m \in \mathbb{Z}_{>0} \} $$
of $\hat{\mathbb{Z}}$-ideals being a neighborhood base of 0.

The set of closed maximal ideals of $\hat{\mathbb{Q}}$ is a subbase for the neighborhoods of 0 in a second ring topology on $\hat{\mathbb{Q}}$ that we need. A neighborhood base for 0 in that topology is given by the set
$$ \mathcal{C} = \{ \mathbb{Q} \cdot \bigcap_{n=0}^{\infty} m^n\hat{\mathbb{Z}} : m \in \mathbb{Z}_{>0} \}, $$which consists of $\hat{\mathbb{Q}}$-ideals.
Analyticity

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

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

in the sense that

\[
\forall U \in \mathcal{C} : \exists V \in \mathcal{B} : \forall x \in (x_0 + V) \cap D : \forall W \in \mathcal{B} : \\
\exists N_0 \in \mathbb{Z}_{\geq 0} : \forall N \geq N_0 : \sum_{n=0}^N a_n \cdot (x - x_0)^n \in f(x) + U + W.
\]

To understand this formula, first omit all \( U \)'s.
Examples of analytic functions

The map \( \hat{\mathbb{Z}}^* \to \hat{\mathbb{Z}} \subset \hat{\mathbb{Q}} \) is analytic in each \( x_0 \in \hat{\mathbb{Z}}^* \), with expansion

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

For each \( u \in \hat{\mathbb{Z}}^* \), the map

\[
\hat{\mathbb{Z}} \to \hat{\mathbb{Z}}^* \subset \hat{\mathbb{Q}}, \quad x \mapsto u^x
\]

is analytic in each \( x_0 \in \hat{\mathbb{Z}} \), 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 $F : \mathbb{Z}_{\geq 0} \rightarrow \mathbb{Z}_{\geq 0}$ 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 $\hat{F} : \hat{\mathbb{Z}} \rightarrow \hat{\mathbb{Z}}$, and it is analytic in each $x_0 \in \hat{\mathbb{Z}}$.

**Notation:** $F$.

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

$$F(n) = n \iff n \in \{0, 1, 5\}.$$
Fibonacci fixed points

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

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

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

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

Profinite number theory

Hendrik Lenstra
Explanation of the picture

\[(\ldots c_3 c_2 c_1)! = \sum_{i \geq 1} c_i i! \in \hat{\mathbb{Z}} \text{ is represented by} \]
\[\sum_{i \geq 1} c_i / (i + 1)! \in [0, 1].\]

In green: the graph of \(a \mapsto a\).
In blue: the graph of \(a \mapsto -a\).
In yellow: the graph of \(a \mapsto a^{-1} - 1 \ (a \in \hat{\mathbb{Z}}^*)\).
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:

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

**Question:** does $F$ have cycles of length greater than 2?
Other linear recurrences

If \( E: \mathbb{Z}_{\geq 0} \rightarrow \mathbb{Z}, \ t \in \mathbb{Z}_{>0}, \ d_0, \ldots, d_{t-1} \in \mathbb{Z} \) satisfy

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

\[d_0 \in \{1, -1\},\]

then \( E \) has a unique continuous extension \( \hat{\mathbb{Z}} \rightarrow \hat{\mathbb{Z}} \). It is analytic in each \( x_0 \in \hat{\mathbb{Z}} \).
Finite cycles

Suppose also \( X^t - \sum_{i=0}^{t-1} d_i X^i = \prod_{i=1}^{t} (X - \alpha_i) \), where
\[
\alpha_1, \ldots, \alpha_t \in \mathbb{Q}(\sqrt{Q}),
\]
\[
\alpha_j^{24} \neq \alpha_k^{24} \quad (1 \leq j < k \leq t).
\]

**Tentative theorem.** *If \( n \in \mathbb{Z}_{>0} \) is such that the set
\[
S_n = \{ x \in \hat{\mathbb{Z}} : E^n(x) = x \}
\]
is infinite, then \( S_n \cap \mathbb{Z}_{\geq 0} \) contains an infinite arithmetic progression.*

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