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:

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

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: $c_1 \equiv n \bmod 2$.

Conversion

Given n, one finds all c_i by

$$c_1 = (\text{remainder of } n_1 = n \text{ upon division by } 2),$$

$$c_i = \left(\text{remainder of } n_i = \frac{n_{i-1} - c_{i-1}}{i} \text{ upon division by } i+1\right),$$

until $n_i = 0$.

Conversion

Given n, one finds all c_i by

$$c_1 = (\text{remainder of } n_1 = n \text{ upon division by } 2),$$

$$c_i = (\text{remainder of } n_i = \frac{n_{i-1} - c_{i-1}}{i} \text{ upon division by } i+1),$$

until $n_i = 0$.

Knowing $c_1, c_2, \ldots, c_{k-1}$ is equivalent to knowing n modulo $k!$.

Profinite numbers

If one starts with $n = -1$, one finds $c_i = i$ for all i:

$$-1 = (\dots 54321)_!.$$

In general, for a negative integer n one finds $c_i = i$ for almost all i.

Profinite numbers

If one starts with $n = -1$, one finds $c_i = i$ for all i:

$$-1 = (\ldots 54321)_!.$$

In general, for a negative integer n one finds $c_i = i$ for almost all i.

A *profinite integer* is an infinite string $(\ldots c_3 c_2 c_1)_!$ with each $c_i \in \mathbf{Z}$, $0 \leq c_i \leq i$.

Notation: $\hat{\mathbf{Z}} = \{\text{profinite integers}\}$.

A citizen of the world

Features of $\hat{\mathbf{Z}}$:

- it has an *algebraic structure*,
- it comes with a *topology*,
- it occurs in *Galois theory*,
- it shows up in *arithmetic geometry*,
- it connects to *ultrafilters*,
- it carries *"analytic" functions*,
- and it knows *Fibonacci numbers*!

Addition and multiplication

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

Likewise for $n \cdot m$.

Addition and multiplication

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 profinite integers, and $\hat{\mathbf{Z}}$ is a *commutative ring*.

Ring homomorphisms

Call a profinite integer $(\ldots c_3 c_2 c_1)_!$ *even* if $c_1 = 0$ and *odd* if $c_1 = 1$.

The map $\hat{\mathbf{Z}} \to \mathbf{Z}/2\mathbf{Z}$, $(\ldots c_3 c_2 c_1)_! \mapsto (c_1 \bmod 2)$, is a ring homomorphism. Its kernel is $2\hat{\mathbf{Z}}$.

Ring homomorphisms

Call a profinite integer $(\ldots c_3c_2c_1)_!$ *even* if $c_1 = 0$ and *odd* if $c_1 = 1$.

The map $\hat{\mathbf{Z}} \to \mathbf{Z}/2\mathbf{Z}$, $(\ldots c_3c_2c_1)_! \mapsto (c_1 \bmod 2)$, is a ring homomorphism. Its kernel is $2\hat{\mathbf{Z}}$.

More generally, for any $k \in \mathbf{Z}_{>0}$, one has a ring homomorphism $\hat{\mathbf{Z}} \to \mathbf{Z}/k!\mathbf{Z}$ sending $(\ldots c_3c_2c_1)_!$ to $(\sum_{i<k} c_i i! \bmod k!)$, and it has kernel $k!\hat{\mathbf{Z}}$.

Visualising profinite numbers

Define $\mathrm{v}\colon \hat{\mathbf{Z}} \to [0,1]$ by

$$\mathrm{v}((\ldots c_3 c_2 c_1)_!) = \sum_{i\geq 1} \frac{c_i}{(i+1)!}.$$

Then $\mathrm{v}(2\hat{\mathbf{Z}}) = [0, \frac{1}{2}]$, $\mathrm{v}(1+2\hat{\mathbf{Z}}) = [\frac{1}{2}, 1]$, $\mathrm{v}(1+6\hat{\mathbf{Z}}) = [\frac{1}{2}, \frac{2}{3}]$.

Visualising profinite numbers

Define $\mathrm{v}\colon \hat{\mathbf{Z}} \to [0,1]$ by

$$\mathrm{v}((\ldots c_3 c_2 c_1)_!) = \sum_{i\geq 1} \frac{c_i}{(i+1)!}.$$

Then $\mathrm{v}(2\hat{\mathbf{Z}}) = [0, \frac{1}{2}]$, $\mathrm{v}(1+2\hat{\mathbf{Z}}) = [\frac{1}{2}, 1]$, $\mathrm{v}(1+6\hat{\mathbf{Z}}) = [\frac{1}{2}, \frac{2}{3}]$.

One has

$$\#\mathrm{v}^{-1}r = 2 \text{ for } r \in \mathbf{Q} \cap (0,1),$$
$$\#\mathrm{v}^{-1}r = 1 \text{ for all other } r \in [0,1].$$

Examples:

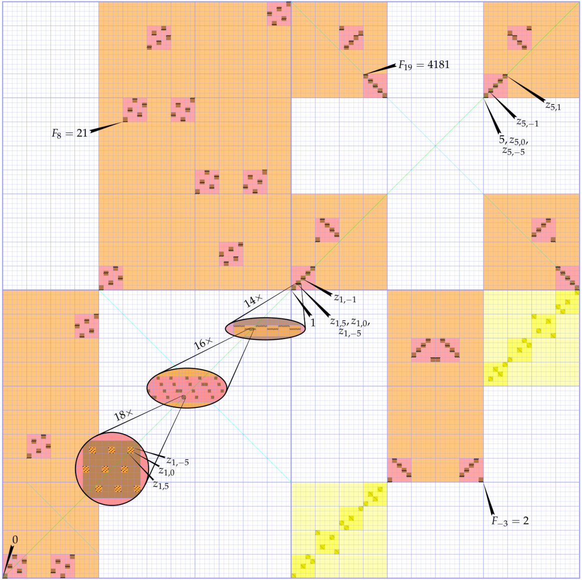
$$\mathrm{v}^{-1}\tfrac{1}{2} = \{-2, 1\}, \quad \mathrm{v}^{-1}\tfrac{2}{3} = \{-5, 3\}, \quad \mathrm{v}^{-1}1 = \{-1\}.$$

Graphs

For graphical purposes, we represent $a \in \hat{\mathbf{Z}}$ by $\mathrm{v}(a) \in [0, 1]$.

We visualise a function $f : \hat{\mathbf{Z}} \to \hat{\mathbf{Z}}$ by representing its graph $\{(a, f(a)) : a \in \hat{\mathbf{Z}}\}$ in $[0, 1] \times [0, 1]$.

Illustration by Willem Jan Palenstijn



Four functions

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 $a \mapsto F(a)$, the "a-th Fibonacci number".

A formal definition

A more satisfactory definition is

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

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

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

A formal definition

A more satisfactory definition is

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

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

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

Alternative definition: $\hat{\mathbf{Z}} = \mathrm{End}(\mathbf{Q}/\mathbf{Z})$, the *endomorphism ring* of the abelian group $\mathbf{Q}/\mathbf{Z}$. Then $\hat{\mathbf{Z}}^* = \mathrm{Aut}(\mathbf{Q}/\mathbf{Z})$.

Basic facts

The ring $\hat{\mathbf{Z}}$ is *uncountable*, it is *commutative*, and it has $\mathbf{Z}$ as a subring. It has lots of zero-divisors.

Basic facts

The ring $\hat{\mathbf{Z}}$ is *uncountable*, it is *commutative*, and it has $\mathbf{Z}$ as a subring. It has lots of zero-divisors.

For each $m \in \mathbf{Z}_{>0}$, there is a ring homomorphism

$$\hat{\mathbf{Z}} \to \mathbf{Z}/m\mathbf{Z}, \quad a = (a_n)_{n=1}^{\infty} \mapsto a_m,$$

which together with the group homomorphism $\hat{\mathbf{Z}} \to \hat{\mathbf{Z}}$, $a \mapsto ma$, fits into a short exact sequence

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

Profinite rationals

Write

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

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

Profinite rationals

Write

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

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

It is a commutative ring, with $\mathbf{Q}$ 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).

Topology

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 $\prod_{n=1}^{\infty}(\mathbf{Z}/n\mathbf{Z})$.

Topology

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 $\prod_{n=1}^{\infty}(\mathbf{Z}/n\mathbf{Z})$.

One can define the topology on $\hat{\mathbf{Z}}$ by the metric

$$\mathrm{d}(x,y) = \frac{1}{\min\{k \in \mathbf{Z}_{>0} : x \not\equiv y \bmod (k+1)!\}} = \frac{1}{\min\{k \in \mathbf{Z}_{>0} : c_k \neq d_k\}}$$

if $x = (\ldots c_3 c_2 c_1)_!$, $y = (\ldots d_3 d_2 d_1)_!$, $x \neq y$.

More topology

Fact: $\hat{\mathbf{Z}}$ is a compact Hausdorff totally disconnected topological ring.

One can make the map $\mathrm{v}\colon \hat{\mathbf{Z}} \to [0,1]$ into a homeomorphism by "cutting" $[0,1]$ at every $r \in \mathbf{Q} \cap (0,1)$.

More topology

Fact: $\hat{\mathbf{Z}}$ is a compact Hausdorff totally disconnected topological ring.

One can make the map $\mathrm{v}\colon \hat{\mathbf{Z}} \to [0,1]$ into a homeomorphism by "cutting" $[0,1]$ at every $r \in \mathbf{Q} \cap (0,1)$.

A neighborhood base of 0 in $\hat{\mathbf{Z}}$ is $\{m\hat{\mathbf{Z}} : m \in \mathbf{Z}_{>0}\}$.

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

Amusements for algebraists

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

Theorem. *One has* $\mathrm{A}/\hat{\mathbf{Z}} \cong \mathrm{A}$ *as additive topological groups.*

Proof (Carlo Pagano): write down a surjective continuous group homomorphism $\epsilon\colon A \to A$ with $\ker \epsilon = \hat{\mathbf{Z}}$.

Amusements for algebraists

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

Theorem. *One has* $\mathrm{A}/\hat{\mathbf{Z}} \cong \mathrm{A}$ *as additive topological groups.*

Proof (Carlo Pagano): write down a surjective continuous group homomorphism $\epsilon\colon A \to A$ with $\ker \epsilon = \hat{\mathbf{Z}}$.

Theorem. *One has* $\mathrm{A} \cong \mathrm{A} \times \hat{\mathbf{Z}}$ *as groups but not as topological groups.*

Here the axiom of choice comes in.

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 $\alpha \in \bar{\mathbf{F}}_p$.

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

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

Arithmetic geometry

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

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

Just as $\hat{\mathbf{Z}}$, it is a compact Hausdorff totally disconnected topological ring.

p-adic numbers

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

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

Just as $\hat{\mathbf{Z}}$, it is a compact Hausdorff totally disconnected topological ring.

It is also a *principal ideal domain*, with $p\mathbf{Z}_p$ as its only non-zero prime ideal. Its field of fractions is written $\mathbf{Q}_p$.

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

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

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:

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

For each p, the projection map $\hat{\mathbf{Z}} \to \mathbf{Z}_p$ induces a ring homomorphism $\pi_p \colon \hat{\mathbf{Q}} \to \mathbf{Q}_p$.

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. Many of these are caused by the set $\mathcal{P}$ of primes being *infinite*.

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 and ultrafilters

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

The spectrum and ultrafilters

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

With each $\mathbf{p} \in \operatorname{Spec} \hat{\mathbf{Z}}$ one associates the *ultrafilter*

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

on the set $\mathcal{P}$ of primes, where $e_S \in \prod_{p \in \mathcal{P}} \mathbf{Z}_p = \hat{\mathbf{Z}}$ has coordinate 0 at $p \in S$ and 1 at $p \notin S$.

Then $\mathbf{p}$ is closed if and only if $\Upsilon(\mathbf{p})$ is principal, and

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

The logarithm

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

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.

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

$$\begin{array}{ccccccccc}
1 & \longrightarrow & \hat{\mathbf{Z}}^*_{\mathrm{tor}} & \longrightarrow & \hat{\mathbf{Z}}^* & \xrightarrow{\log} & 2\mathrm{J} & \longrightarrow & 0 \\
 & & \downarrow \wr & & \| & & \wr \uparrow & & \\
1 & \longleftarrow & (\hat{\mathbf{Z}}/2\mathrm{J})^* & \longleftarrow & \hat{\mathbf{Z}}^* & \longleftarrow & 1+2\mathrm{J} & \longleftarrow & 1
\end{array}$$

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

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

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 for each prime p there is a neighborhood U of x_0 in D such that for all $x \in U$ the equality

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

is valid in the topological field $\mathbf{Q}_p$.

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

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

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.

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

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

Up to eleven

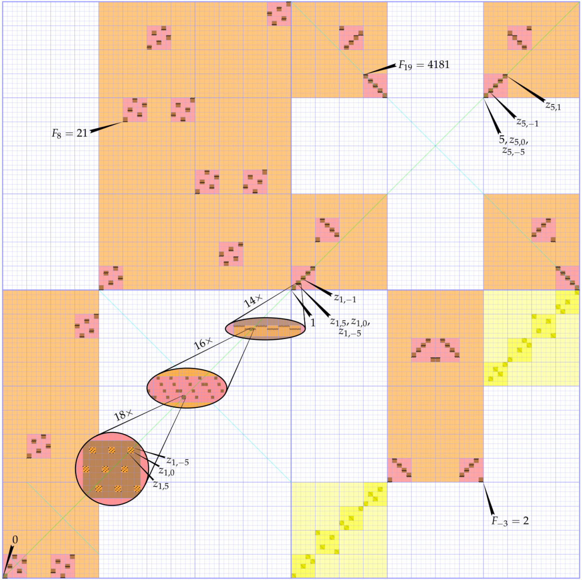
One has $\#\{x \in \hat{\mathbf{Z}} : F(x) = x\} = 11$.

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

Illustration by Willem Jan Palenstijn



Graphing the fixed points

The graph of $a \mapsto F(a)$ is shown in orange/red/brown.

Intersecting the graph with the diagonal one obtains the fixed points 0 and $z_{a,b}$, for $a = 1, 5$, $b = -5, -1, 0, 1, 5$.

Graphing the fixed points

The graph of $a \mapsto F(a)$ is shown in orange/red/brown.

Intersecting the graph with the diagonal one obtains the fixed points 0 and $z_{a,b}$, for $a = 1, 5$, $b = -5, -1, 0, 1, 5$.

Surprise: one has $z_{5,-5}^2 - 25 = \sum_{i=1}^{\infty} c_i i!$ with $c_i = 0$ for $i \leq 200$ and $c_{201} \neq 0$.

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.*

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 $n \in \mathbf{Z}_{>0}$.