PROFINITE FIBONACCI NUMBERS

Hendrik Lenstra

Mathematisch Instituut

Universiteit Leiden

The standard work

Hendrik Lenstra,
Profinite Fibonacci numbers,
Nieuw Archief voor Wiskunde
(5) **6** (2005), 297–300
(*with an illustration by Willem Jan Palenstijn*)

p-adic integers

$$\mathbf{Z}_p = \{(a_i)_{i=0}^{\infty} \in \prod_{i\geq 0} \mathbf{Z}/p^i\mathbf{Z} :$$
$$\forall i \leq j : a_i = (a_j \bmod p^i)\}$$
$$= \{\sum_{j\geq 0} c_j p^j : \forall j : c_j \in \{0, 1, \ldots, p-1\}\}$$

$\mathbf{Z}_2$ is homeomorphic to the Cantor set.

Profinite integers

$$\hat{\mathbf{Z}} = \{(b_n)_{n=0}^{\infty} \in \prod_{n>0} \mathbf{Z}/n\mathbf{Z} :$$
$$\forall n|m : b_n = (b_m \bmod n)\}$$

$$= \{\sum_{j\geq 1} c_j j! : \forall j : c_j \in \{0, 1, \ldots, j\}\}$$

$$\cong \mathrm{End}(\mathbf{Q}/\mathbf{Z})$$

$$(\ldots c_3 c_2 c_1)_! = \sum_{j\geq 1} c_j j!$$

Divisibility and congruence

For $s \in \hat{\mathbf{Z}}$, $b \in \mathbf{Z}_{>0}$, the following are equivalent:

- s maps to 0 in $\mathbf{Z}/b\mathbf{Z}$,
- $s \in b\hat{\mathbf{Z}}$,
- $s = bt$ for a *unique* $t \in \hat{\mathbf{Z}}$,
- the number formed by the first $b-1$ digits of s is divisible by b,
- (*notation*) $b|s$.

Write $s_1 \equiv s_2 \bmod b$ if $b|s_1 - s_2$.

Where they occur

$\mathrm{Gal}(\bar{\mathbf{F}}_p/\mathbf{F}_p) \cong \hat{\mathbf{Z}}$

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

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

The Fibonacci function

$$F_0 = 0,\ F_1 = 1,\ F_{n+2} = F_{n+1} + F_n$$

The Fibonacci function

$F_0 = 0$, $F_1 = 1$, $F_{n+2} = F_{n+1} + F_n$

There is a unique continuous function $\hat{\mathbf{Z}} \to \hat{\mathbf{Z}}$ mapping each $n \in \mathbf{Z}_{\geq 0}$ to F_n.

The Fibonacci function

$F_0 = 0,\ F_1 = 1,\ F_{n+2} = F_{n+1} + F_n$

There is a unique continuous function $\hat{\mathbf{Z}} \to \hat{\mathbf{Z}}$ mapping each $n \in \mathbf{Z}_{\geq 0}$ to F_n.

The composed function $\hat{\mathbf{Z}} \to \hat{\mathbf{Z}} \to \mathbf{Z}_p$ does *not* factor via $\hat{\mathbf{Z}} \to \mathbf{Z}_p$.

A closed principal ideal

Put

$$I = \{s \in \hat{\mathbf{Z}} : 2p|s \text{ for all primes } p\}.$$

One has

$$\hat{\mathbf{Z}}/I \cong (\mathbf{Z}/4\mathbf{Z}) \times \textstyle\prod_{p \text{ odd prime}} \mathbf{F}_p$$

and there are exact sequences

$$0 \to I \to \hat{\mathbf{Z}} \to \hat{\mathbf{Z}}/I \to 0,$$

$$1 \to 1 + I \to \hat{\mathbf{Z}}^* \to (\hat{\mathbf{Z}}/I)^* \to 1.$$

The logarithm

Theorem. *There is a unique continuous group homomorphism* $\log\colon \hat{\mathbf{Z}}^* \to I$ *such that*

$$\forall x \in I : \log(1-x) = -\textstyle\sum_{i>0} x^i/i.$$

It satisfies:

- $\log$ *restricts to an isomorphism* $1+I \to I$*,*
  with inverse $\exp\colon x \mapsto \sum_{i\geq 0} x^i/i!$*;*
- $\hat{\mathbf{Z}}^* \cong (1+I) \times (\hat{\mathbf{Z}}/I)^*$*,* $u \mapsto (\exp\log u, u+I)$*;*
- $\log u = \lim_{n\to\infty}(u^{n!}-1)/n!$ *for all* $u \in \hat{\mathbf{Z}}^*$*.*

Exponentiation

For each $u \in \hat{\mathbf{Z}}^*$, there is a unique continuous group homomorphism $\hat{\mathbf{Z}} \to \hat{\mathbf{Z}}^*$ that maps 1 to u.

It maps s to

$$u^s = \lim_{n \to s} u^n.$$

Properties:

$$(uv)^s = u^s v^s, \qquad u^{s+t} = u^s u^t,$$

$$(u^s)^t = u^{st}, \qquad u^1 = u.$$

A dangerous identity

One has

$$\text{“}u^{s+\epsilon} = u^s \cdot \exp(\epsilon \log u)\text{”}$$

in the following restricted sense.

Theorem. *For each $b \in \mathbf{Z}_{>0}$ there is an open neighborhood V of 0 in $\hat{\mathbf{Z}}$, such that for all $u \in \hat{\mathbf{Z}}^*$, $s \in \hat{\mathbf{Z}}$, $\epsilon \in V$, $k \in \mathbf{Z}_{>0}$ one has*

$$u^{s+\epsilon} \equiv u^s \cdot \exp(\epsilon \log u) \bmod b^k.$$

Put

$$\hat{\mathbf{Z}}[\vartheta] = \hat{\mathbf{Z}}[X]/(X^2 - X - 1) = \hat{\mathbf{Z}} \oplus \hat{\mathbf{Z}}\vartheta,$$

where ϑ is the residue class of X, and write $\vartheta' = 1 - \vartheta$.

Fibonacci and exponentiation

Put

$$\hat{\mathbf{Z}}[\vartheta] = \hat{\mathbf{Z}}[X]/(X^2 - X - 1) = \hat{\mathbf{Z}} \oplus \hat{\mathbf{Z}}\vartheta,$$

where ϑ is the residue class of X, and write $\vartheta' = 1 - \vartheta$.

Then $(\vartheta - \vartheta')^2 = 5$, and one has

$$F_s = (\vartheta^s - \vartheta'^s)/(\vartheta - \vartheta')$$

for all $s \in \hat{\mathbf{Z}}$.

Fibonacci fixed points

Theorem. (a) *For each* $a \in \{1, 5\}$ *and each* $b \in \{-5, -1, 0, 1, 5\}$ *there is a unique element* $z = z_{a,b} \in \hat{\mathbf{Z}}$ *with* $F_z = z$ *that for all* $k \in \mathbf{Z}_{>0}$ *satisfies*

$$z_{a,b} \equiv a \bmod 6^k, \qquad z_{a,b} \equiv b \bmod 5^k.$$

(b) *Every* odd $z \in \hat{\mathbf{Z}}$ *with* $F_z = z$ *is among the* $z_{a,b}$, *and the only* even *one is* 0.

Approximate equalities

The fixed point $z_{a,b}$ approximately inherits properties of a and b, e. g.

$$z_{a,b}^2 - (a+b)z_{a,b} + ab \approx 0.$$

A research problem

How many fixed points does the kth iterate of F have on $\hat{\mathbf{Z}}$?

Is this number *finite* for every $k > 0$?

Fibonacci and Fermat

Exercise. $\{\text{Fibonacci numbers}\}$

$$\cap \{\text{Fermat numbers}\} = \{3, 5\}.$$

Solution: go mod 48.