Arithmetical Congruence Preserving Functions

on
- integers $\mathbb{N}$, $\mathbb{Z}$
- integers modulo n $\mathbb{Z}/n\mathbb{Z}$
- p-adic / profinite integers $\mathbb{Z}_p$, $\widehat{\mathbb{Z}}$

A journey in number theory

Serge Grigorieff

LIAFA, CNRS & Université Denis Diderot-Paris 7

Joint work with

Patrick Cégielski & Irène Guessarian

(Université Paris 12) (Université Paris 6)

Yurifest, Berlin, 11/09/2015

The issue : Capture the following notion

Definition

$f : \mathbb{N} \to \mathbb{Z}$ is congruence preserving if

$$\boxed{\forall a, b \in \mathbb{N} \qquad a - b \quad \text{divides} \quad f(a) - f(b)}$$

or equivalently (justifying the denomination),

$$\forall n \geq 1 \;\; \forall a, b \in \mathbb{N} \;\; (\; a \equiv b \bmod n \quad \Longrightarrow \quad f(a) \equiv f(b) \bmod n \;)$$

- Obvious example : Polynomials in $\mathbb{Z}[x]$
- **What about non polynomial functions ?**
- Idem with functions
  - $\mathbb{Z} \to \mathbb{Z}$
  - on p-adic/profinite integers
  - on integers modulo n

Congruence preserving (or compatible) functions

Definition (Grätzer, 1964 — A notion from universal algebra)

Let A be an algebra and $\mathcal{C}$ a family of congruences.

$f : A^n \to A$ is $\mathcal{C}$-congruence preserving if,

$$\forall \theta \in \mathcal{C} \quad \forall x_1, \ldots, x_n, y_1, \ldots, y_n \in A$$

$$\bigwedge_{i=1}^{i=n} x_i \, \theta \, y_i \quad \Longrightarrow \quad f(x_1, \ldots, x_n) \, \theta \, f(x_1, \ldots, x_n)$$

- $\mathcal{C}$ = modular congruences on $\mathbb{N}$ $\rightsquigarrow$ our notion on $\mathbb{N}$
  $\mathcal{C}$ = modular congr. on $\mathbb{Z}$ = all congr. $\rightsquigarrow$ our notion on $\mathbb{Z}$
- Example : "Polynomial functions"
  = expressible by terms with constants in A
- Mostly studied :

- Lattices/Boolean algebras (Grätzer 1960's, Haviar, Ploščica, Farley 2000's . . .)
- Finite groups/expanded groups (Bhargava, 1997 ; Aichinger, 2006)

- - Much studied question (Grätzer, Kaarli, Pixley) :

Are "polynomials" the sole congruence preserving functions ?

A topological motivation

$\mathcal{V}$ variety of finite monoids (à la Eilenberg)

Profinite pseudo-metric $d_{\mathcal{V}}(x,y) = 2^{-r_{\mathcal{V}}(x,y)}$ on a monoid M

(pseudo-metric : $d(x,x) = 0$ but $d(x,y) = 0$ does not imply $x = y$)

$$r_{\mathcal{V}}(x,y) = \begin{cases} \text{size of smallest } F \in \mathcal{V} \text{ separating } x, y \\ +\infty \quad \text{if there no such } F \end{cases}$$

F separates $x, y \iff \exists$ morphism $\varphi : M \twoheadrightarrow F \quad \varphi(x) \neq \varphi(y)$

Theorem with $M = (\mathbb{N}, +)$ and $M = (\mathbb{Z}, +)$ (Pin & Silva, 2011)

$\forall\mathcal{V}$ variety of finite monoids $f : \mathbb{N} \to \mathbb{N}$ is $d_{\mathcal{V}}$-uniformly continuous
$\iff f$ is constant or congruence preserving & $f(x) \geq x$.

$\forall\mathcal{V}$ variety of finite groups $f : \mathbb{Z} \to \mathbb{Z}$ is $d_{\mathcal{V}}$-uniformly continuous
$\iff f$ is constant or congruence preserving

Proof. Case $\mathbb{Z} \to \mathbb{Z}$ | $\mathcal{V}_u$ = variety generated by $\{\mathbb{Z}/p^n\mathbb{Z} \mid n \leq k\}$ p prime
$\mathcal{V}_u$ separates integers x, y if $x \not\equiv y \bmod p^n$

Another motivation

Question (asked to us by Jean-Éric Pin) :

Which functions $f : \mathbb{N} \to \mathbb{N}$ are such that

$$\begin{array}{l} \forall \mathcal{L} \text{ lattice of finite subsets of } \mathbb{N} \\ \forall L \in \mathcal{L} \;\; Succ^{-1}(L) \in \mathcal{L} \implies \forall L \in \mathcal{L} \;\; f^{-1}(L) \in \mathcal{L} \end{array} \qquad (*)$$

$Succ$ = successor function on $\mathbb{N}$

Theorem (CGG 2014)

$f : \mathbb{N} \to \mathbb{N}$ satisfies (*) $\iff$

f is <u>congruence preserving</u> & non-decreasing & $f(x) \geq x$.

Idem for lattices of regular subsets of $\mathbb{N}$

Idem with $\mathbb{Z}$ in place of $\mathbb{N}$

Congruence preserving functions $\mathbb{N} \to \mathbb{Z}$

Tool 1 : Newton representation of functions $\mathbb{N} \to \mathbb{Z}$

We represent functions $\mathbb{N} \to \mathbb{Z}$ by

series of polynomials in $\mathbb{Q}[x]$ mapping $\mathbb{N}$ into $\mathbb{Z}$

Binomial polynomial function $\mathbb{N} \to \mathbb{N}$ in $\mathbb{Q}[x]$

$$\binom{x}{0} = 1 \qquad \binom{x}{n} = \frac{x(x-1)\cdots(x-n+1)}{n!}$$

Proposition (Pólya, 1915)

finite $\mathbb{Z}$-linear combinations of the binomial polynomials

$\overset{1\text{-}1}{\equiv}$ *polynomials in $\mathbb{R}[x]$ mapping $\mathbb{N}$ into $\mathbb{Z}$*

Proposition (Newton, 1687)

infinite $\mathbb{Z}$-linear combinations of the binomial polynomials

$\overset{1\text{-}1}{\equiv}$ *functions $\mathbb{N} \to \mathbb{Z}$*

NO CONVERGENCE PROBLEM : For every $x \in \mathbb{N}$

the infinite sum $\sum_{n \in \mathbb{N}} a_n \binom{x}{n}$ reduces to the finite sum $\sum_{n \leq x} a_n \binom{x}{n}$

Tool 2 : Unary least common multiple function (Tchebychev, 1852)

$$\boxed{\begin{array}{rcl} lcm(k) & = & lcm(1,2,\ldots,k) \\ \psi(x) & = & \log(lcm(x)) \end{array}} \qquad lcm(0) = 1$$

Neperian logarithm

(Nair, 1982) (Hanson, 1972)

$$2^{k-1} \leq lcm(k) < 3^k \qquad \text{for } k \geq 1$$

$$\lim_{x\to+\infty} \frac{\psi(x)}{x} = 1$$

(consequence of the prime number theorem)

P. L. Tchebichef, *Mémoire sur les nombres premiers*
J. Math. Pures et Appliquées. 17 (1852), 366-390.

D. Hanson, *On the product of primes.* Canadian Math. Bull. 15(1) :33-37, 1972

M. Nair, *On Chebyshev-type inequalities for primes*,
Amer. Math. Monthly 89 (1982), 126-129

Newton representation of congruence preserving functions $\mathbb{N} \to \mathbb{Z}$

$f : \mathbb{N} \to \mathbb{Z}$ congruence preserving $\iff \forall x, y$ $\boxed{x - y \text{ divides } f(x) - f(y)}$

$lcm(k) = lcm(1, 2, \ldots, k) \qquad lcm(0) = 1$

Theorem (CGG, Int. J. Number Theory, 2015)

Let $f : \mathbb{N} \to \mathbb{Z}$, $\qquad f = \sum_{n \in \mathbb{N}} a_n \binom{x}{n} \qquad$ with $a_n \in \mathbb{Z}$

f is congruence preserving $\iff \forall n \in \mathbb{N}$ $lcm(n)$ divides a_n

Snapshot of the proof : combinatorics of binomial coefficients

Lemma. $\quad 0 \leq n - k < p \leq k \implies p$ divides $lcm(k) \binom{n}{k}$

Lemma. $\quad k \leq b \implies n$ divides $lcm(k) \left(\binom{b+n}{k} - \binom{b}{k} \right)$

Examples of congruence preserving functions

$2^{\aleph_0}$ *nonpolynomial* congruence preserving functions

Examples of congruence preserving functions $\mathbb{N} \to \mathbb{Z}$ (CGG)

$$\forall x \in \mathbb{N} \ \sum_{n\in\mathbb{N}} n! \binom{x}{n} = \begin{cases} \lfloor e\, x! \rfloor & \text{if } x \geq 1 \quad e \text{ Euler number } 2.718\ldots \\ 1 & \text{if } x = 0 \end{cases}$$

$$\sum_{n\in\mathbb{N}} a^n \ n! \binom{x}{n} = \begin{vmatrix} \lfloor e^{1/a}\, a^x\, x! \rfloor & \text{for } a \in \mathbb{N},\ a \geq 2 \\ \lfloor e^{1/a}\, a^x\, x! \rfloor + 1 & \text{for } a \in \mathbb{Z},\ a \leq -1 \end{vmatrix}$$

$$\sum_{n\in 2\mathbb{N}} 2^n \ n! \binom{x}{n} = \begin{cases} \lfloor \cosh(1/2)\ 2^x\ x! \rfloor & \text{if } x \in 2\mathbb{N} \\ \lfloor \sinh(1/2)\ 2^x\ x! \rfloor & \text{if } x \in 2\mathbb{N}+1 \end{cases}$$

$$\sum_{n\in\mathbb{N}} lcm(n) \binom{x}{n} = \ ???$$

Similar with $\lceil \cdots \rceil$ *in place of* $\lfloor \cdots \rfloor$

Thus,

if $x \in \mathbb{N} \setminus \{0\}$	x	divides	$\lfloor e\, x! \rfloor - 1$
if $x, y \in \mathbb{N} \setminus \{0\}$	$x - y$	divides	$\lfloor e\, x! \rfloor - \lfloor e\, y! \rfloor$
if $a \in \mathbb{Z} \setminus \{0,1\}$, $x, y \in \mathbb{N}$	$x - y$	divides	$\lfloor e^{1/a}\, a^x\, x! \rfloor - \lfloor e^{1/a}\, a^y\, y! \rfloor$

Not very intuitive properties...

A bit of robustness in our examples

Trivial : If f is congruence preserving so is $k\,f$ for $k \in \mathbb{Z}$

In our examples, k can go inside the $\lfloor \cdots \rfloor$

A bit of robustness (CGG)

For every $k \in \mathbb{Z}$, for $a \in \mathbb{Z} \setminus \{0\}$,

$$x \mapsto \lfloor k\, e\, x! \rfloor \qquad x \mapsto \lfloor k\, e^{1/a}\, a^x\, x! \rfloor$$

duly modified for $x \in \{0, \ldots, |se| - 1\}$

are congruence preserving.

The finite modification is no accident

Let α be a nonnull real.

The function $\lfloor \alpha\, x! \rfloor$ is NOT congruence preserving.

Idem with $\lceil \cdots \rceil$

Badly failing congruence preservation

$f, g : \mathbb{N} \to \mathbb{R}$

f uniformly close to g if $\sup\{|f(n) - g(n)| \mid n \in \mathbb{N}\}$ is finite

Not surprisingly, the explicit examples are exceptions (CGG)

1. *If $a_i \in \mathbb{R} \setminus \mathbb{Z}$ for some $i \geq 1$ then $x \mapsto a_n x^n + \cdots + a_1 x + a_0$ is uniformly close to NO congruence preserving function*
2. *$\forall k \in \mathbb{N} \setminus \{0\}$ $\forall \alpha \in \mathbb{R} \setminus \{0\}$ $x \mapsto \alpha\, k^x$ is uniformly close to NO congruence preserving function*
3. *$\forall a \in \mathbb{Z} \setminus \{0\}$ $\forall \alpha \in \mathbb{Q} \setminus \{0\}$ $x \mapsto \alpha\, e!$ and $x \mapsto \alpha\, a^x\, x!$ are uniformly close to NO congruence preserving function*
4. *$\forall a \in \mathbb{R} \setminus \{0\}$ for almost all $\alpha \in \mathbb{R}$ $x \mapsto \alpha\, e!$ and $x \mapsto \alpha\, a^x\, x!$ are uniformly close to NO congruence preserving function*

Proof of 4. Use Koksma's theorem : If $\inf_{m<n} |\lambda_m - \lambda_n| > 0$ then

for almost all α the sequence $(\alpha\lambda_n)_{n\in\mathbb{N}}$ is uniformly distributed modulo 1

Congruence preserving functions $\mathbb{Z} \to \mathbb{Z}$

À la Newton representation of functions $\mathbb{Z} \to \mathbb{Z}$

Replace the binomial polynomials $\binom{x}{n}$'s by

$$P_0 = 1 \quad P_{2\ell} = \frac{\prod_{k=-\ell+1}^{k=\ell} x-k}{(2\ell)!} \quad P_{2\ell+1} = \frac{\prod_{k=-\ell}^{k=\ell} x-k}{(2\ell+1)!}$$

Again, P_n is in $\mathbb{Q}[x]$, coefficients are rational numbers. But,

Proposition (à la Pólya, 1915)

finite $\mathbb{Z}$-linear combinations of the P_n's

$$\overset{1\text{-}1}{\equiv} \quad \textit{polynomials in } \mathbb{R}[x] \textit{ mapping } \mathbb{Z} \textit{ into } \mathbb{Z}$$

Proposition (à la Newton, 1687)

infinite $\mathbb{Z}$-linear combinations of the P_n's

$$\overset{1\text{-}1}{\equiv} \quad \textit{functions } \mathbb{Z} \to \mathbb{Z}$$

À la Newton representation of congruence preserving functions $\mathbb{Z} \to \mathbb{Z}$

$P_0 = 1 \quad P_{2\ell} = \dfrac{\prod_{k=-\ell+1}^{k=\ell} x - k}{(2\ell)!} \quad P_{2\ell+1} = \dfrac{\prod_{k=-\ell}^{k=\ell} x - k}{(2\ell+1)!}$

$f : \mathbb{Z} \to \mathbb{Z}$ congruence preserving $\iff \forall x, y \; \boxed{x - y \text{ divides } f(x) - f(y)}$

$lcm(k) = lcm(1, 2, \ldots, k) \qquad lcm(0) = 1$ (Unary *least common multiple*)

Theorem (CGG)

Let $f : \mathbb{Z} \to \mathbb{Z}, \quad f = \sum_{n \in \mathbb{N}} a_n P_n(x)$ *with* $a_n \in \mathbb{Z}$

f *is congruence preserving* $\iff \forall n \in \mathbb{N}$ $lcm(n)$ *divides* a_n

Proof analogous to that for the $\mathbb{N} \to \mathbb{Z}$ case
but needs more combinatorics of the binomial numbers

The extension problem

Lemma (Let $X \subseteq Y \subseteq \mathbb{Z}$ be finite)

Every $\varphi : X \to \mathbb{Z}$ such that $\forall x, y \in X \quad x - y$ *divides* $\varphi(x) - \varphi(y)$
can be extended to $\psi : Y \to \mathbb{Z}$ such that $\forall x, y \in Y \quad x - y$ *divides* $\psi(x) - \psi(y)$

Proof. Reduce to $Y = X \cup \{a\}$. Use the Chinese Remainder Theorem : $\bigwedge_{x \in X} b - \varphi(x) \equiv 0 \bmod |a - x|$ has a solution since, for $x, y \in X$,

$$(b - \varphi(x)) - (b - \varphi(y)) = \varphi(y) - \varphi(x) \equiv 0 \bmod |y - x|$$
$$\equiv 0 \bmod \gcd(|a - x|, |a - y|) \quad \text{since } \gcd(|a - x|, |a - y|) \text{ divides } y - x$$

But NOT every congruence preserving function $f : \mathbb{N} \to \mathbb{Z}$ extends to a congr. pres. function $\widehat{f} : \mathbb{N} \cup \{-1\} \to \mathbb{Z}$

The infinite version of the Chinese Remainder Theorem gives solutions in p-adic or profinite integers

Example of congruence preserving functions

Example of congruence preserving function $\mathbb{Z} \to \mathbb{Z}$ (CGG)

$$f(x) = \sum_{k\in\mathbb{N}} \frac{(2k)!}{k!} P_{2k}(x) \qquad \textit{observe } lcm(k) \textit{ divides } (2k)!/k!$$

$$= \begin{cases} \sqrt{\frac{e}{\pi}} \frac{\Gamma(1/2)}{2^{2x+1}\ x!} \int_1^\infty e^{-t/2}(t^2-1)^x dt & \textit{if } x \geq 0 \\ f(|x|-1) & \textit{if } x < 0 \end{cases}$$

Proof. Known identity around modified Bessel function of the 2d kind
Thus, $x - y$ divides the difference of this expression on x and on y

Not very intuitive property. . .

Congruence preserving functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$

In this finite framework,
the notion was already considered $\sim$ 1995

Chen & Bhargava notion of congruence preserving function $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$

Definition (Zhibo Chen, 1995)

Let $m, n \geq 1$. $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ *congruence preserving* if
$\forall d$ dividing m $\forall a, b \in \{0, \ldots, n-1\}$
$$(a \equiv b \mod d \Longrightarrow f(a) \equiv f(b) \mod d)$$

Denomination *"congruence preserving"* a bit abusive in some cases :

$$\{(x, y) \in \{0, \ldots, k-1\} \times \{0, \ldots, k-1\} \mid x \equiv y \bmod d\}$$

is NOT a congruence on $\mathbb{Z}/k\mathbb{Z}$ when $d < k$ and d does not divide k

Saying *"congruence preserving"* is fully justified when m divides n

The reason for this definition is that it is true for polynomials in $\mathbb{Z}[x]$
$x \in \{0, \ldots, n-1\} \mapsto P(x) \bmod m$
is congruence preserving $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$

Alternative definitions in case m divides n

$f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ *is congruence preserving à la Chen* if
$\forall d$ dividing m $\quad \forall a, b \in \{0, \ldots, n-1\}$ $(a \equiv b \mod d \implies f(a) \equiv f(b) \mod d)$

$f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ *is congruence preserving à la Grätzer* if
$\forall \theta$ congruence on $\mathbb{Z}/n\mathbb{Z}$ $\quad \forall a, b \in \mathbb{Z}/n\mathbb{Z}$ $(\, a\,\theta\, b \implies f(a)\,\theta\, f(b)\,)$

Proposition Case $m = n$ $\qquad f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$

The following conditions are equivalent

1. $\forall a, b \in \mathbb{Z}/n\mathbb{Z}$ $\quad a - b$ *divides* $f(a) - f(b)$ *(in the ring $\mathbb{Z}/n\mathbb{Z}$)*
2. f *is congruence preserving à la Chen*
3. f *is congruence preserving à la Grätzer*

Proof. $2 \Rightarrow 3.$

let $d = \gcd(m, a-b) = \alpha m + \beta(a-b)$ (by Bézout)
d divides m and $a \equiv b \mod d$ hence $f(a) \equiv f(b) \mod d$
$f(a) - f(b) = d\delta = (\alpha m + \beta(a-b))\delta = \beta\delta(a-b)$ in $\mathbb{Z}/m\mathbb{Z}$

Proposition Case m divides n $\qquad f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$

The following conditions are equivalent

1. $\forall a, b \in \mathbb{Z}/n\mathbb{Z}$ $\quad \pi_{n,m}(a-b)$ *divides* $f(a) - f(b)$ *(in the ring $\mathbb{Z}/m\mathbb{Z}$)*
2. f *is congruence preserving à la Chen*

Chen & Bhargava motivation (in the vein of Grätzer) : the scope of polynomial functions

When are all functions polynomial?

- *[Kempner, 1921] Every function* $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ *is polynomial* $\iff$ *n is prime*
- *[Chen & Mullen, 2006]*
  The $(0,1)$ *transposition function* $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ *is polynomial* $\iff$ *n is prime*
- *[Chen, 1995] Every function* $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ *is polynomial*
  $\iff$ $n \leq$ *least prime factor of m*

When does congruence preserving = polynomial? (Bhargava, 1997)

Every <u>congruence preserving</u> function $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ *is polynomial*

$$\iff \quad n < \gamma(m) \quad \text{with} \quad \left|\begin{array}{rcl} \gamma(p^k) & = & \begin{cases} \infty & \text{if } k = 1 \\ \infty & \text{if } p^k = 4 \\ 2p+1 & \text{otherwise} \end{cases} \\ \gamma(\prod_i p_i^{k_i}) & = & \min\{\gamma(p_i^{k_i}) \mid i\} \end{array}\right.$$

Every <u>congruence preserving</u> function $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ *is polynomial*

$\iff$ *8 does not divide n and* $\forall p$ *prime* > 2 $\quad p^2$ *does not divide n*

Density of such n's $= 7/\pi^2$

Newton representation of functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$

We want to represent functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$

Polynomial in $\mathbb{Z}[x]$ may not suffice

But it is OK with polynomials in $\mathbb{Q}[x]$ mapping $\mathbb{N}$ into $\mathbb{Z}$

Binomial polynomial function $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$

$$\binom{x}{k}_{n,m} : x \in \{0, \ldots, n-1\} \mapsto \binom{x}{k} \bmod m$$

Proposition

Every function $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is a unique

$\mathbb{Z}/m\mathbb{Z}$-linear combination of the $\binom{x}{k}_{n,m}$'s, $k = 0, \ldots, n-1$

In other words, the $\binom{x}{k}_{n,m}$'s, $k = 0, \ldots, n-1$, are a basis of the $\mathbb{Z}/m\mathbb{Z}$-module of functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$

Same proof as in the infinite case $\mathbb{N} \to \mathbb{Z}$

Newton representation of congruence preserving functions

Unary *least common multiple function* $\quad lcm(k) = lcm(1, 2, \ldots, k) \quad lcm(0) = 1$

Theorem (CGG)

Let $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, $f = \sum_{k=0}^{k=n-1} a_k \binom{x}{k}_{n,m}$ *with* $a_k \in \{0, \ldots, m-1\}$

f *is congruence preserving* $\iff$

$\forall k = 0, \ldots, n-1 \quad lcm(k) \bmod m$ *divides* a_k *in* $\mathbb{Z}/m\mathbb{Z}$

Proposition

$lcm(k) \equiv 0 \bmod m$ *for* $k \geq \mu(m) =$ *largest power of prime dividing* m

Corollary (CGG)

$\mathcal{S} = \{lcm(k) \bmod m) [\binom{x}{k}]_{n,m} \mid 0 \leq k < \min(n, \mu(m))\}$

$\mathcal{M} = \mathbb{Z}/m\mathbb{Z}$-*module of congruence preserving functions* $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$

$\mathcal{S}$ *generates* $\mathcal{M}$ $\quad$ $\mathcal{S}$ *is a basis of* $\mathcal{M}$ $\iff$ m *is prime*

Alternative proof :

Lifting congruence preserving functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$

In case m divides n, to represent congruence preserving functions
the $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ case reduces to the $\mathbb{N} \to \mathbb{Z}$ case

Theorem (CGG)

Assume m divides n
Every congruence preserving $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$
can be lifted to a congruence preserving $F : \mathbb{N} \to \mathbb{N}$

$$\begin{array}{ccc} \mathbb{N} & \xrightarrow{F} & \mathbb{N} \\ \pi_n \big\downarrow & & \big\downarrow \pi_m \\ \mathbb{Z}/n\mathbb{Z} & \xrightarrow{f} & \mathbb{Z}/m\mathbb{Z} \end{array}$$

Proof : Chinese Remainder Theorem (with infinitely many congruence equations)

Congruence preserving functions on p-adic and profinite integers

Back to the topological motivation of congruence preservation
with profinite distances on $\mathbb{N}$ *and* $\mathbb{Z}$

Back to the extension problem

$$\mathbb{N} \to \mathbb{Z} \qquad \rightsquigarrow \qquad \mathbb{Z} \to \mathbb{Z}$$

p-adic integers   (p prime)

p prime

$\boxed{\mathbb{Z}_p = \text{family of formal series } \sum_{n\in\mathbb{N}} a_n p^n}$,
$a_n \in \{0, \ldots, p-1\}$

Addition and multiplication are done as with
usual base p (finite) expansions of natural numbers

$\mathbb{Z}_p$ **is a ring** : $-1 = \sum_n (p-1)\, p^n$
Inversible elements : the $\sum_{n\in\mathbb{N}} a_n p^n$'s such that $a_0 \neq 0$

The ring $\mathbb{Z}_p$ is the projective limit of the rings $\mathbb{Z}/p^n\mathbb{Z}$
for the projective system $(\pi_{p^n,p^m} : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z})_{n\geq m}$

Profinite integers

Factorial expansions of natural integers :

$n = a_1\,1! + a_2\,2! + a_3\,3! + \cdots + a_n\,n!$ with $a_k \in \{0, \ldots, k\}$

Care : a_k can take the value k

Addition and multiplication are done with carry propagation

(as in the usual fixed base case)

Going to infinite such expansions,

$\widehat{\mathbb{Z}}$ = family of formal series $\sum_{k\geq 1} a_k\,k!$, $a_k \in \{0, \ldots, k\}$

Addition and multiplication are as expected

$\widehat{\mathbb{Z}}$ **is a ring** : $-1 = \sum_{k\geq 1} k\,k!$

$\sum_{k\geq 1} a_k\,k!$ is inversible $\iff a_1 \neq 0$

- The ring $\widehat{\mathbb{Z}}$ is the projective limit of the rings $\mathbb{Z}/n!\mathbb{Z}$ for the projective system $(\pi_{n!,m!} : \mathbb{Z}/n!\mathbb{Z} \to \mathbb{Z}/m!\mathbb{Z})_{n\geq m}$
- $\widehat{\mathbb{Z}}$ also the projective limit of the $\mathbb{Z}/k\mathbb{Z}$'s wrt $(\pi_{k,\ell} : \mathbb{Z}/k\mathbb{Z} \to \mathbb{Z}/\ell\mathbb{Z})_{\ell \text{ divides } k}$
- $\widehat{\mathbb{Z}} = \prod_{p \text{ prime}} \mathbb{Z}_p$

Topology on p-adic / profinite integers

p-adic distance on $\mathbb{N}$ $\quad d_p(x,y) = 2^{-Val_p(x-y)}$ with

$$\begin{array}{rcll} Val_p(u) & = & max\{k \mid p^k \text{ divides } u\} & \text{(the } p\text{-valuation of } u) \\ & = & \text{length of the prefix of 0's in the } p\text{-expansion of } u \end{array}$$

p-adic distance on $\mathbb{Z}_p$ $\quad d_p(x,y) = 2^{-Val_p(x-y)}$ with
$Val_p(u) =$ length of the prefix of 0's in the infinite word u

$(\mathbb{Z}_p, d_p)$ is the Cauchy completion of $(\mathbb{N}, d_p)$ $\qquad \mathbb{N}$ is dense in $\mathbb{Z}_p$
$\mathbb{Z}_p$ is compact and totally discontinuous

. . . .

profinite distance $d_!(x,y)$ on $\widehat{\mathbb{Z}}$
Similar with $\widehat{\mathbb{Z}}$ and $Val_!$

Congruence preserving functions $\mathbb{Z}_p \to \mathbb{Z}_p$

Definition

$f : \mathbb{Z}_p \to \mathbb{Z}_p$ is congruence preserving if, for all $x, y \in \mathbb{Z}_p$

$$x - y \text{ divides } f(x) - f(y)$$

Proposition

For $f : \mathbb{Z}_p \to \mathbb{Z}_p$ the following conditions are equivalent

1. *f is congruence preserving*
2. *f is congruence preserving à la Grätzer*

$$\forall \text{ congruence } \theta \text{ on } \mathbb{Z}_p \ \ \forall a, b \in \widehat{\mathbb{Z}} \ \ (\ a\,\theta\, b \implies f(a)\,\theta\, f(b)\ )$$

Proof

Congruences on a ring correspond to ideals (congruence $\theta \leftrightarrow \theta$-class of 0)
In the ring $\mathbb{Z}_p$ every ideal is principal

This equivalence holds for any principal ring

Congruence preserving functions $\mathbb{Z}_p \to \mathbb{Z}_p$ are 1-Lipschitz

Definition

$f : \mathbb{Z}_p \to \mathbb{Z}_p$ is 1-Lipschitz if

$$\begin{array}{rcl} d_p(f(x), f(y)) & \leq & d_p(x, y) \\ \text{i.e.} \quad Val_p(f(x) - f(y)) & \geq & Val_p(x - y) \end{array}$$

i.e. the identity map $2^{-n} \mapsto 2^{-n}$ is a modulus of uniform continuity

Proposition

Congruence preserving functions $\mathbb{Z}_p \to \mathbb{Z}_p$ are 1-Lipschitz

Proof. $x - y$ divides $f(x) - f(y) \implies f$ is 1-Lipschitz

Projective limits of functions $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$

Definition

$(\varphi_n : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^n Z)_{n\in\mathbb{N}}$ is a projective system if these diagrams are commutative for all $n \geq m$

$$\begin{array}{ccc} \mathbb{Z}/p^n\mathbb{Z} & \xrightarrow{\varphi_{p^n}} & \mathbb{Z}/p^n\mathbb{Z} \\ \pi p^n, p^m \big\downarrow & & \big\downarrow \pi_{p^n,p^m} \\ \mathbb{Z}/p^m\mathbb{Z} & \xrightarrow{\varphi_{p^m}} & \mathbb{Z}/p^m\mathbb{Z} \end{array}$$

Proposition (CGG)

$f : \mathbb{Z}_p \to \mathbb{Z}_p$ is 1-Lipschitz $\iff$ f is the projective limit of a projective system $(\varphi_{p^n} : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z})_{n\in\mathbb{N}}$

Proof. φ_{p^n} witnesses that $f(x) - f(y) \leq 2^{-n}$ whenever $x - y \leq 2^{-n}$

Theorem (CGG)

$f : \mathbb{Z}_p \to \mathbb{Z}_p$ is congruence preserving $\iff$

f is the projective limit of a projective system of congruence preserving functions $(\varphi_n : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z})_{n\in\mathbb{N}}$

Mahler representation of continuous functions $\mathbb{Z}_p \to \mathbb{Z}_p$ on p-adic integers

Binomial function $\binom{x}{n}$ is d_p-uniformly continuous $\mathbb{N} \to \mathbb{N}$
hence extends to $\mathbb{Z}_p \to \mathbb{Z}_p$

Theorem (Mahler, 1956)

Let $a_k \in \mathbb{Z}_p$ (p-adic integers)

A Newton series $\sum_{k \in \mathbb{N}} a_k \binom{x}{n}$ is convergent in $\mathbb{Z}_p$

$$\iff \lim_{k\to\infty} a_k = 0 \quad \text{in } \mathbb{Z}_p \text{ relative to } d_p$$

$$\iff \lim_{k\to\infty} Val_p(a_k) = +\infty$$

Theorem (Mahler, 1956)

Continuous functions $\mathbb{Z}_p \to \mathbb{Z}_p$

$$\overset{1\text{-}1}{\equiv} \quad \text{Newton series } \sum_{k\in\mathbb{N}} a_k \binom{x}{n} \text{ with } \lim_{k\to\infty} a_k = 0 \quad (\text{wrt } d_p)$$

Idem with the ring $\widehat{\mathbb{Z}}$ of profinite integers

Representation of congruence preserving functions

$f : \mathbb{Z}_p \to \mathbb{Z}_p$ congruence preserving if $\forall x, y \in \mathbb{Z}_p \quad x - y$ divides $f(x) - f(y)$

Theorem (CGG)

Let $f : \mathbb{Z}_p \to \mathbb{Z}_p$, $\quad f = \sum_{n\in\mathbb{N}} a_n \binom{x}{n}$ with $a_n \in \mathbb{Z}_p$

f is congruence preserving $\iff \forall n \in \mathbb{N}\ \ lcm(n)$ divides a_n (in $\mathbb{Z}_p$)

Corollary

Thus, every congruence preserving $f : \mathbb{N} \to \mathbb{Z}$ extends to unique congruence preserving functions $\widehat{f}_{\mathbb{Z}} : \mathbb{Z} \to \mathbb{Z}_p$, $\widehat{f} : \mathbb{Z}_p \to \mathbb{Z}_p$

Care : The extension $\widehat{f}_Z : \mathbb{Z} \to \mathbb{Z}_p$ from $\mathbb{N}$ to $\mathbb{Z}$ does not map $\mathbb{Z}$ into $\mathbb{Z}$ but into $\mathbb{Z}_p$

Idem with the ring $\widehat{\mathbb{Z}}$ of profinite integers

THANK YOU FOR YOUR ATTENTION

BIBLIOGRAPHY

- M. Bhargava, Congruence preservation and polynomial functions from $\mathbb{Z}_n$ to $\mathbb{Z}_m$, Discrete Mathematics 173 (1997), p. 15 – 21.

- Z. Chen, On polynomial functions from $\mathbb{Z}_n$ to $\mathbb{Z}_m$,
Discrete Math. 137 (1995), p. 137–145.

- K. Mahler, An Interpolation Series for Continuous Functions of a p-adic Variable.
Journal für die reine und angewandte Mathematik, 199 :23–34, 1956.

- J.-É. Pin and P.V. Silva, On profinite uniform structures defined by varieties of finite monoids,
International Journal of Algebra and Computation, 21 :295-314, 2011.