Arithmetical Congruence Preservation: from Finite to Infinite

Patrick Cégielski[1] ⋆, Serge Grigorieff[2] ⋆, and Irène Guessarian[2] ⋆ ⋆⋆

[1] LACL, EA 4219, Université Paris-Est Créteil, IUT Fontainebleau-Sénart, France
[2] LIAFA, CNRS UMR 7089, Université Paris 7 Denis Diderot, France

To Yuri, on his 75th birthday, with thanks for many stimulating discussions on Logic and Computation

Abstract. Various problems on integers lead to the class of functions defined on a ring of numbers (or a subset of such a rings) METTRE RING AU SINGULIER and verifying $a - b$ divides $f(a) - f(b)$ for all a, b. We say that such functions are "congruence preserving". In previous works, we characterized these classes of functions for the cases $\mathbb{N} \to \mathbb{Z}$, $\mathbb{Z} \to \mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ in terms of sums series of rational polynomials (taking only integral values) and the function giving the least common multiple of $1, 2, \ldots, k$. In this paper we relate the finite and infinite cases via a notion of "lifting": if $\pi \colon X \to Y$ is a surjective morphism and f is a function $Y \to Y$ a lifting of f is a function $F : X \to X$ such that $\pi \circ F = f \circ \pi$. We prove that the finite case $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ can be so lifted to the infinite cases $\mathbb{N} \to \mathbb{N}$ and $\mathbb{Z} \to \mathbb{Z}$. We also use such liftings to extend the characterization to the rings of p-adic and profinite integers, using Mahler representation of continuous functions on these rings.

1 **Introduction** 1
2 **Switching between finite and infinite** 2
2.1 Lifting functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ to $\mathbb{N} \to \mathbb{N}$ and $\mathbb{Z} \to \mathbb{Z}$ 2
2.2 Representation of congruence preserving functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ 6
2.3 Lifting functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ to $\mathbb{Z}/r\mathbb{Z} \to \mathbb{Z}/r\mathbb{Z}$ 7
C'EST to $\mathbb{Z}/r\mathbb{Z} \to \mathbb{Z}/s$ s ET NON r
3 **Congruence preservation on p-adic/profinite integers** 8
3.1 Continuity of congruence preserving functions 9
3.2 Congruence preserving functions and inverse limits 9
3.3 Extension of congruence preserving functions $\mathbb{N} \to \mathbb{N}$ 12
3.4 Representation of congruence preserving functions $\mathbb{Z}_p \to \mathbb{Z}_p$ 12
Appendix 1 Basic definitions of p-adic and profinite integers 15
Appendix 2 $\mathbb{N}$ and $\mathbb{Z}$ in $\mathbb{Z}_p$ and $\widehat{\mathbb{Z}}$ 16

1 Introduction

A function f (on $\mathbb{N}$ or $\mathbb{Z}$) is said to be congruence preserving if $a - b$ divides $f(a) - f(b)$. Polynomial functions are obvious examples of congruence preserving

⋆ Partially supported by TARMAC ANR agreement 12 BS02 007 01.
⋆⋆ Emeritus at UPMC Université Paris 6.

functions. In [3,4] we characterized such functions $\mathbb{N} \to \mathbb{Z}$ and $\mathbb{Z} \to \mathbb{Z}$ (which we named "functions having the integral difference ratio property"). In [5] we extended the characterization to functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ with $n, m \geq 1$ (for the suitable notion of congruence preservation).

In the present paper, we prove in §2 that every congruence preserving function $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ (with m dividing n) can be lifted to congruence preserving functions $\mathbb{N} \to \mathbb{N}$ and $\mathbb{Z} \to \mathbb{Z}$ (i.e. it is the modular projection of such a function). As a corollary (i) we show that such a lift also works replacing $\mathbb{N}$ with $\mathbb{Z}/qn\mathbb{Z}$ and (ii) we give an alternative proof of a representation (obtained in [5]) of congruence preserving functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ as linear sums of "rational" polynomials.

In §3 we consider the rings of p-adic integers (resp. profinite integers) and prove that congruence preserving functions on these rings are inverse limits of congruence preserving functions on the $\mathbb{Z}/p^k\mathbb{Z}$ (resp. on the $\mathbb{Z}/n\mathbb{Z}$). Considering the Mahler representation of continuous functions by series, we prove that congruence preserving functions correspond to those series for which the linear coefficient with rank k is divisible by the least common multiple of $1, \ldots, k$.

2 Switching between finite and infinite

In order to characterize congruence preserving functions on $\mathbb{Z}/n\mathbb{Z}$, we first lift each such function into a congruence preserving function $\mathbb{N} \to \mathbb{N}$. In a second step, we use our characterization of congruence preserving functions $\mathbb{N} \to \mathbb{Z}$ to characterize the congruence preserving functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$.

2.1 Lifting functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ to $\mathbb{N} \to \mathbb{N}$ and $\mathbb{Z} \to \mathbb{Z}$

Definition 1. *Let X be a subset of a commutative ring $(R, +, \times)$. A function $f\colon X \to R$ is said to be congruence preserving if*

$$\forall x, y \in X \quad \exists d \in R \quad f(x) - f(y) = d(x - y)\,, \quad \text{i.e. } x - y \textit{ divides } f(x) - f(y)\,.$$

Definition 2 (Lifting). *Let $\sigma\colon X \to N$ and $\rho\colon Y \to M$ be surjective maps. A function $F\colon X \to Y$ is said to be a (σ, ρ)-*lifting *of a function $f\colon N \to M$ (or simply* lifting *if σ, ρ are clear from the context) if the following diagram commutes:*

$$\begin{array}{ccc} X & \xrightarrow{F} & Y \\ \sigma\big\downarrow & & \big\downarrow\rho \\ N & \xrightarrow{f} & M \end{array} \qquad \textit{i.e.} \quad \rho \circ F = f \circ \sigma\,.$$

We will consider elements of $\mathbb{Z}/k\mathbb{Z}$ as integers and vice versa via the following modular projection maps.

Notation 3 *1. Let $\pi_k\colon \mathbb{Z} \to \mathbb{Z}/k\mathbb{Z}$ be the canonical surjective homomorphism associating to an integer its class in $\mathbb{Z}/k\mathbb{Z}$.*

2. Let $\iota_k \colon \mathbb{Z}/k\mathbb{Z} \to \mathbb{N}$ be the injective map associating to an element $x \in \mathbb{Z}/kZ$ its representative in $\{0, \ldots, k-1\}$.
3. Let $\pi_{n,m} \colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ be the map $\pi_{n,m} = \pi_m \circ \iota_n$.
If $m \leq n$ let $\iota_{m,n} \colon \mathbb{Z}/m\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ be the injective map $\iota_{m,n} = \pi_n \circ \iota_m$.

Lemma 4. *If m divides n then $\pi_m = \pi_{n,m} \circ \pi_n$ and $\pi_{n,m}$ is a surjective homomorphism.*

The next theorem insures that congruence preserving functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ can be lifted to congruence preserving functions $\mathbb{N} \to \mathbb{N}$ and $\mathbb{N} \to \mathbb{Z}$.

Theorem 5 (Lifting functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ to $\mathbb{N} \to \mathbb{N}$). *Let $f \colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ with $m \geq 2$. The following conditions are equivalent:*

(1) f is congruence preserving.
(2) f can be (π_n, π_n)-lifted to a congruence preserving function $F : \mathbb{N} \to \mathbb{N}$.
(3) f can be (π_n, π_n)-lifted to a congruence preserving function $F : \mathbb{N} \to \mathbb{Z}$.

In view of applications in the context of p-adic and profinite integers, we state and prove a slightly more general version. As $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}/m\mathbb{Z}$ are different rings we use an extension of the notion of congruence preservation introduced in Chen [6] and studied in Bhargava [1]) which we recall below.

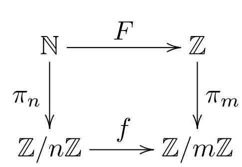
Definition 6. *A function $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is congruence preserving if*

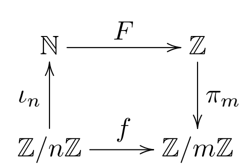
$$\text{for all } x, y \in \mathbb{Z}/n\mathbb{Z}, \quad \pi_{n,m}(x-y) \text{ divides } f(x) - f(y) \text{ in } \mathbb{Z}/m\mathbb{Z}. \tag{1}$$

Theorem 7 (Lifting functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ to $\mathbb{N} \to \mathbb{N}$). *Let $f \colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ with m divides n and $m \geq 2$. The following conditions are equivalent:*

(1) f is congruence preserving.
(2) f can be (π_n, π_m)-lifted to a congruence preserving function $F : \mathbb{N} \to \mathbb{N}$.
(3) f can be (π_n, π_m)-lifted to a congruence preserving function $F : \mathbb{N} \to \mathbb{Z}$.

Proof. (2) $\Rightarrow$ (3) is trivial.
(3) $\Rightarrow$ (1). Assume f lifts to the congruence preserving function $F : \mathbb{N} \to \mathbb{Z}$, i.e. $f \circ \pi_n = \pi_m \circ F$. Since $\pi_n \circ \iota_n$ is the identity we get $f = i_m \circ F \circ \iota_n$. The following diagrams are thus commutative:





Let $x, y \in \mathbb{Z}/n\mathbb{Z}$. As F is congruence preserving, $\iota_n(x) - \iota_n(y)$ divides $F(\iota_n(x)) - F(\iota_n(y))$, hence $F(\iota_n(x)) - F(\iota_n(y)) = (\iota_n(x) - \iota_n(y))\,\delta$. Since π_m is a morphism and $\pi_m \circ \iota_n = \pi_{n,m}$, we get $\pi_m(F(\iota_n(x))) - \pi_m(F(\iota_n(x))) = \pi_{n,m}(x-y)\,\pi_m(\delta)$. As F lifts f we have $\pi_m(F(\iota_n(x))) - \pi_m(F(\iota_n(y))) = f(x) - f(y)$ whence (1).

(1) $\Rightarrow$ (2). By induction on $t \in \mathbb{N}$ we define a sequence of functions $\varphi_t \colon \{0, \ldots, t\} \to \mathbb{N}$ for $t \in \mathbb{N}$ such that φ_{t+1} extends φ_t and (*) and (**) below hold.

$$\left\{ \begin{array}{rl} (*) & \varphi_t \text{ is congruence preserving,} \\ (**) & \pi_m(\varphi_t(u)) = f(\pi_n(u)), \text{ for all } u \in \{0, \ldots, t\}, \\ & \text{i.e. the following diagram commutes:} \quad \begin{array}{ccc} \{0, \ldots, t\} & \xrightarrow{\varphi_t} & \mathbb{Z} \\ \pi_n \downarrow & & \downarrow \pi_m \\ \mathbb{Z}/n\mathbb{Z} & \xrightarrow{f} & \mathbb{Z}/m\mathbb{Z} \end{array} \end{array} \right.$$

Basis. We choose $\varphi_0(0) \in \mathbb{N}$ such that $\pi_m(\varphi_0(0)) = f(\pi_n(0))$. Properties (*) and (**) clearly hold for φ_0.

Induction: from φ_t to φ_{t+1}. Since the wanted φ_{t+1} has to extend φ_t to the domain $\{0, \ldots, t, t+1\}$, we only have to find a convenient value for $\varphi_{t+1}(t+1)$. By the induction hypothesis, (*) and (**) hold for φ_t; in order for φ_{t+1} to satisfy (*) and (**), we have to find $\varphi_{t+1}(t+1)$ such that $t+1-i$ divides $\varphi_{t+1}(t+1) - \varphi_t(i)$, for $i = 0, \ldots, t$, and $\pi_m(\varphi_{t+1}(t+1)) = f(\pi_n(t+1))$. Rewritten in terms of congruences, these conditions amount to say that $\varphi_{t+1}(t+1)$ is a solution of the following system of congruence equations:

$$\left. \begin{array}{r|ll} \star(0) & \varphi_{t+1}(t+1) \equiv \varphi_t(0) & \pmod{t+1} \\ & \vdots & \\ \star(\mathrm{i}) & \varphi_{t+1}(t+1) \equiv \varphi_t(i) & \pmod{t+1-i} \\ & \vdots & \\ \star(\mathrm{t\text{-}1}) & \varphi_{t+1}(t+1) \equiv \varphi_t(t-1) & \pmod{2} \\ \star\star & \varphi_{t+1}(t+1) \equiv \iota_m(f(\pi_n(t+1))) & \pmod{m} \end{array} \right\} \qquad (2)$$

Recall the Generalized Chinese Remainder Theorem (cf. §3.3, exercice 9 p. 114, in Rosen's textbook [13]): a system of congruence equations

$$\bigwedge_{i=0,\ldots,t} x \equiv a_i \pmod{n_i}$$

has a solution if and only if $a_i \equiv a_j \mod \gcd(n_i, n_j)$ for all $0 \leq i < j \leq t$.

Let us show that the conditions of application of the Generalized Chinese Remainder Theorem are satisfied for system (2).

- Lines $\star$(i) and $\star$(j) of system (2) (with $0 \leq i < j \leq t-1$).
  Every common divisor to $t+1-i$ and $t+1-j$ divides their difference $j-i$ hence $\gcd(t+1-i, t+1-j)$ divides $j-i$. Since φ_t satisfies (*), $j-i$ divides $\varphi_t(j) - \varphi_t(i)$ and a fortiori $\gcd(t+1-i, t+1-j)$ divides $\varphi_t(j) - \varphi_t(i)$.
- Lines $\star$(i) and $\star\star$ of system (2) (with $0 \leq i \leq t-1$).
  Let $d = \gcd(t+1-i, m)$. We have to show that d divides $\iota_m(f(\pi_n(t+1))) - \varphi_t(i)$. Since f is congruence preserving, $\pi_{n,m}(\pi_n(t+1) - \pi_n(i))$ divides $f(\pi_n(t+1)) - f(\pi_n(i))$. As m divides n, by Lemma 4, $\pi_{n,m}(\pi_n(t+1) - \pi_n(i)) =$

$\pi_m(t+1)-\pi_m(i)=\pi_m(t+1-i)$ and $f(\pi_n(t+1))-f(\pi_n(i))=k\pi_m(t+1-i)$ for some $k\in\mathbb{Z}/m\mathbb{Z}$. Applying ι_m, there exists $\lambda\in\mathbb{Z}$ such that

$$\iota_m(f(\pi_n(t+1)))-\iota_m(f(\pi_n(i)))=\iota_m(k)\iota_m(\pi_m(t+1-i))+\lambda m$$

as $\iota_m(\pi_m(u))\equiv u \pmod{m}$ for every $u\in\mathbb{Z}$, there exists $\mu\in\mathbb{Z}$ such that

$$\iota_m(f(\pi_n(t+1)))-\iota_m(f(\pi_n(i)))=\iota_m(k)(t+1-i)+\mu m+\lambda m\,. \qquad (3)$$

Since φ_t satisfies (**), we have $\pi_m(\varphi_t(i))=f(\pi_n(i))$ hence $\varphi_t(i)\equiv\iota_m(f(\pi_n(i))) \pmod{m}$. Thus equation (3) can be rewritten

$$\iota_m(f(\pi_n(t+1)))-\varphi_t(i)=(t+1-i)\iota_m(k)+\nu m \quad \text{for some } \nu\,. \qquad (4)$$

As $d=\gcd(t+1-i,m)$ divides m and $t+1-i$, (4) shows that d divides $\iota_n(f(\pi_n(t+1)))-\varphi_t(i)$ as wanted.

Thus, we can apply the Generalized Chinese Theorem and get the wanted value of $\varphi_{t+1}(t+1)$, concluding the induction step.

Finally, taking the union of the φ_t's, $t\in\mathbb{N}$, we get a function $F:\mathbb{N}\to\mathbb{N}$ which is congruence preserving and lifts f. □

Example 8 (counterexample to Theorem 7). Lemma 4 and Theorem 7 do not hold if m does not divide n. Consider $f\colon\mathbb{Z}/6\mathbb{Z}\to\mathbb{Z}/8\mathbb{Z}$ defined by $f(0)=0$, $f(1)=3$, $f(2)=4$, $f(3)=1$, $f(4)=4$, $f(5)=7$. Note first that, in $\mathbb{Z}/8\mathbb{Z}$, 1, 3 and 5 are invertible, hence f is congruence preserving iff for $k\in\{2,\ 4\}$, for all $x\in\mathbb{Z}/6\mathbb{Z}$, k divides $f(x+k)-f(x)$ which is easily checked; nevertheless, f has no congruence preserving lift $F\colon\mathbb{Z}\to\mathbb{Z}$. If such a lift F existed, we should have

(1) because F lifts f, $\pi_8(F(0))=f(\pi_6(0))=0$ and $\pi_8(F(8))=f(\pi_6(8))=f(2)=4$;
(2) as F is congruence preserving, 8 must divide $F(8)-F(0)$; we already noted that 8 divides $F(0)$, hence 8 divides $F(8)$ and $\pi_8(F(8))=0$, contradicting $\pi_8(F(8))=4$.

Note that $\pi_{6,8}$ is neither a homomorphism nor surjective and $0=\pi_8(8)\neq\pi_{6,8}\circ\pi_6(8)=2$. □

We can also lift congruence preserving functions from $\mathbb{Z}/n\mathbb{Z}\to\mathbb{Z}/m\mathbb{Z}$ to $\mathbb{Z}\to\mathbb{Z}$ instead of $\mathbb{N}\to\mathbb{N}$.

Theorem 9 (Lifting functions $\mathbb{Z}/n\mathbb{Z}\to\mathbb{Z}/m\mathbb{Z}$ to $\mathbb{Z}\to\mathbb{Z}$). *Let $f\colon\mathbb{Z}/n\mathbb{Z}\to\mathbb{Z}/m\mathbb{Z}$ with m divides n and $m\geq 2$. The following conditions are equivalent:*

(1) f is congruence preserving.
(2) f can be (π_n,π_m)-lifted to a congruence preserving function $F:\mathbb{Z}\to\mathbb{Z}$.

Proof. (2) ⇒ (1). The proof is the same as that of (3) ⇒ (1) in Theorem 7.
(1) ⇒ (2). The argument is a slight modification of that for the same implication in Theorem 7. We define the lift $F:\mathbb{Z}\to\mathbb{Z}$ of $f:\mathbb{Z}/n\mathbb{Z}\to\mathbb{Z}/m\mathbb{Z}$ as the union of a series of functions φ_t, $t\in\mathbb{N}$ such that
- φ_{2t} has domain $\{-t,\dots,t\}$ and φ_{2t+1} has domain $\{-t,\dots,t+1\}$,
- φ_{t+1} extends φ_t,
- φ_t is congruence preserving. The induction step is done exactly as in Theorem 7 via a system of congruence equations and an application of the Generalized Chinese Remainder Theorem.

2.2 Representation of congruence preserving functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$

As a first corollary of Theorem 7 we get a new proof of the representations of congruence preserving functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ as finite linear sums of polynomials with rational coefficients (cf. [5]). Let us recall the so-called binomial polynomials.

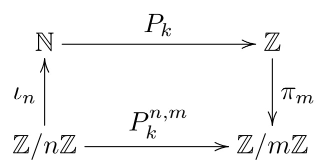
Definition 10. *For $k \in \mathbb{N}$, let $P_k(x) = \binom{x}{k} = \frac{1}{k!} \prod_{\ell=0}^{\ell=k-1} (x-\ell)$.*

Though P_k has rational coefficients, it maps $\mathbb{N}$ into $\mathbb{Z}$. Also, observe that $P_k(x)$ takes value 0 for all $k > x$. This implies that for any sequence of integers $(a_k)_{k\in\mathbb{N}}$, the infinite sum $\sum_{k\in\mathbb{N}} a_k\, P_k(x)$ reduces to a finite sum for any $x \in \mathbb{N}$ hence defines a function $\mathbb{N} \to \mathbb{Z}$.

Definition 11. *We denote by $lcm(k)$ the least common multiple of integers $1, \ldots, k$ (with the convention $lcm(0) = 1$).*

Definition 12. *To each binomial polynomial P_k, $k \in \mathbb{N}$, we associate a function $P_k^{n,m} \colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ which sends an element $x \in \mathbb{Z}/n\mathbb{Z}$ to $(\pi_m \circ P_k \circ \iota_n)(x) \in \mathbb{Z}/m\mathbb{Z}$.*

In other words, consider the representative t of x lying in $\{0, \ldots, n-1\}$, evaluate $P_k(t)$ in $\mathbb{N}$ and then take the class of the result in $\mathbb{Z}/m\mathbb{Z}$. Hence, the following diagram commutes:



Lemma 13. *If $lcm(k)$ divides a_k in $\mathbb{Z}$, then the function $\pi_m(a_k)P_k^{n,m} \colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ (represented by $a_k P_k$) is congruence preserving.*

Proof. In [3] we proved that if $lcm(k)$ divides a_k then $a_k P_k$ is a congruence preserving function on $\mathbb{N}$. Let us now show that $\pi_m(a_k)P_k^{n,m} \colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is also congruence preserving. Let $x, y \in \mathbb{Z}/n\mathbb{Z}$: as $a_k P_k$ is congruence preserving, $\iota_n(x) - \iota_n(y)$ divides $a_k P_k(\iota_n(x)) - a_k P_k(\iota_n(y))$. As m divides n, π_m is a morphism (cf. Lemma 4) hence $\pi_m(\iota_n(x)) - \pi_m(\iota_n(y))$ divides $\pi_m(a_k)\pi_m(P_k(\iota_n(x))) - \pi_m(a_k)\pi_m(P_k(\iota_n(y))) = \pi_m(a_k)P_k^{n,m}(x) - \pi_m(a_k)P_k^{n,m}(x)$. As $\pi_m \circ \iota_n = \pi_{n,m}$ we have $\pi_m(\iota_n(x)) - \pi_m(\iota_n(y)) = \pi_{n,m}(x)) - \pi_{n,m}(y)$ and we conclude that $\pi_m(a_k)P_k^{n,m}$ is congruence preserving. □

Corollary 14 ([5]). *Let $1 \leq m = p_1^{\alpha_1} \cdots p_\ell^{\alpha_\ell}$, p_i prime. Suppose m divides n and let $\nu(m) = \max_{i=1,\ldots,\ell}\ p_i^{\alpha_i}$. A function $f \colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is congruence preserving if and only if it is represented by a finite $\mathbb{Z}$-linear sum $f = \sum_{k=0}^{\nu(m)-1} \pi_m(a_k)P_k^{n,m}$ such that $lcm(k)$ divides a_k (in $\mathbb{Z}$) for all $k < \nu(m)$. Moreover, such a representation is unique.*

Proof. Assume $f\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is congruence preserving. Applying Theorem 7, lift f to $F\colon \mathbb{N} \to \mathbb{N}$ which is congruence preserving.

$$\begin{array}{ccc} \mathbb{N} & \xrightarrow{\;F = \sum_{k=0}^{\nu(m)-1} a_k\, P_k\;} & \mathbb{Z} \\ \pi_n \downarrow & & \downarrow \pi_m \\ \mathbb{Z}/n\mathbb{Z} & \xrightarrow{\quad f \quad} & \mathbb{Z}/m\mathbb{Z} \end{array} \qquad f \circ \pi_n = \pi_m \circ F$$

We proved in [5] that every congruence preserving function $F\colon \mathbb{N} \to \mathbb{N}$ is of the form $F = \sum_{k=0}^{\infty} a_k P_k$ where $lcm(k)$ divides a_k for all k. As π_m is a morphism (because m divides n) and F lifts f, we have, for $u \in \mathbb{Z}$

$$\begin{aligned} f(\pi_n(u)) \;&=\; \pi_m(F(u)) \;=\; \pi_m(\sum_{k=0}^{\infty} a_k\, P_k(u)) \\ &= \sum_{k=0}^{\infty} \pi_m(a_k)\, \pi_m(P_k(u)) \;=\; \sum_{k=0}^{k=\nu(m)-1} \pi_m(a_k)\, \pi_m(P_k(u)) \end{aligned} \tag{5}$$

The last equality is obtained by noting that for $k \geq \nu(m)$, m divides $lcm(k)$ hence as a_k is a multiple of $lcm(k)$, $\pi_m(a_k) = 0$. From (5) we get $f(\pi_n(u)) = \sum_{k=0}^{k=\nu(m)-1} \pi_m(a_k)\, \pi_m(P_k(u)) = \pi_m(\sum_{k=0}^{k=\nu(m)-1} a_k\, P_k(u))$. This proves that f is lifted to the rational polynomial function $\sum_{k=0}^{k=\nu(m)-1} a_k\, P_k$. Since $P_k(k) = 1$ for all $k \in \mathbb{N}$, and $P_k(i) = 0$ for $k > i$, we obtain the unicity of the representation.

The converse follows from Lemma 13 and the fact that any finite sum of congruence preserving functions is congruence preserving. □

2.3 Lifting functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ to $\mathbb{Z}/r\mathbb{Z} \to \mathbb{Z}/s\mathbb{Z}$

As a second corollary of Theorem 7 we can lift congruence preserving functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ to congruence preserving functions $\mathbb{Z}/qn\mathbb{Z} \to \mathbb{Z}/qn\mathbb{Z}$.

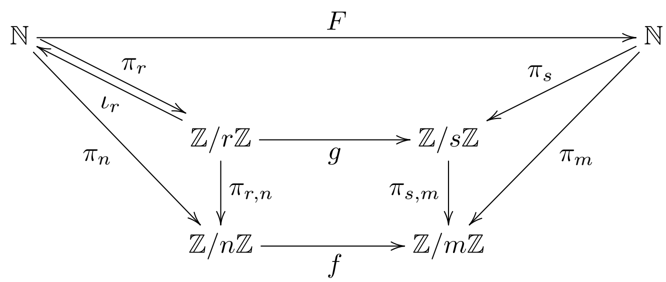
We state a slightly more general result.

Corollary 15. *Assume $m, n, s, r \geq 1$, m divides both n and s, and n, s both divide r. If $f\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is congruence preserving then it can be $(\pi_{r,n}, \pi_{s,m})$-lifted to $g\colon \mathbb{Z}/r\mathbb{Z} \to \mathbb{Z}/s\mathbb{Z}$ which is also congruence preserving.*

n DIVIDES r IS A CONSEQUENCE
NON je ne pense pas

Proof. As m divides n, using Theorem 7, we lift f to a congruence preserving $F : \mathbb{N} \to \mathbb{N}$ and set $g = \pi_s \circ F \circ \iota_r$.

We first show that the rectangular subdiagram around f, g commutes:



$$
\begin{aligned}
\pi_{s,m} \circ g &= \pi_{s,m} \circ (\pi_s \circ F \circ \iota_r) \\
&= (\pi_m \circ F) \circ \iota_r && m \text{ divides } s \text{ yields } \pi_m = \pi_{s,m} \circ \pi_s \text{ (Lemma 4)} \\
&= (f \circ \pi_n) \circ \iota_r && \text{since } F \text{ lifts } f \\
&= f \circ \pi_{r,n} && \text{since } \pi_n \circ \iota_r = \pi_{r,n}
\end{aligned}
$$

Thus, $\pi_{s,m} \circ g = f \circ \pi_{r,n}$, i.e. g lifts f.
Finally, if $x, y \in \mathbb{Z}/r\mathbb{Z}$ then $\iota_r(x) - \iota_r(y)$ divides $F(\iota_r(x)) - F(\iota_r(y))$ (by congruence preservation of F). As π_s is a morphism, and $\pi_s = \pi_{r,s} \circ \pi_r$ (because s divides r), and $\pi_r \circ \iota_r$ is the identity on $\mathbb{Z}/r\mathbb{Z}$, we deduce that $\pi_s(\iota_r(x)) - \pi_s(\iota_r(y)) = (\pi_{r,s} \circ \pi_r \circ \iota_r)(x) - (\pi_{r,s} \circ \pi_r \circ \iota_r)(y) = \pi_{r,s}(x - y)$ divides $\pi_s(F(\iota_r(x))) - \pi_s(F(\iota_r(y)) = g(x) - g(y)$ (by definition of g). We thus conclude that g is congruence preserving. □

Remark 16. Let us check that the previous diagram is completely commutative. The large trapezoid around F, f commutes because F lifts f. The upper trapezoid F, g, ι_r, π_s commutes by definition of g. The upper trapezoid F, g, π_r, π_s commutes since $g \circ \pi_r = (\pi_s \circ F \circ \iota_r) \circ \pi_r = \pi_s \circ F$ (as $\iota_r \circ \pi_r$ is the identity). The left and right triangles $\pi_n, \pi_r, \pi_{r,n}$ and $\pi_m, \pi_s, \pi_{s,m}$ commute by Lemma 4 as n divides r and m divides s. Finally, the triangle $\pi_n, \iota_r, \pi_{r,n}$ commutes by definition of $\pi_{r,n}$ (cf. Notation 3).

3 Congruence preservation on p-adic/profinite integers

All along this section, p is a prime number; we study congruence preserving functions on the rings $\mathbb{Z}_p$ of p-adic integers and $\widehat{\mathbb{Z}}$ of profinite integers. $\mathbb{Z}_p$ is the projective limit $\varprojlim \mathbb{Z}/p^n\mathbb{Z}$ relative to the projections π_{p^n,p^m}. Usually, $\widehat{\mathbb{Z}}$ is defined as the projective limit $\varprojlim \mathbb{Z}/n\mathbb{Z}$ of the finite rings $\mathbb{Z}/n\mathbb{Z}$ relative to the projections $\pi_{n,m}$, for m dividing n. We here use the following equivalent definition which allows to get completely similar proofs for $\mathbb{Z}_p$ and $\widehat{\mathbb{Z}}$.

$$\widehat{\mathbb{Z}} = \varprojlim \mathbb{Z}/n!\mathbb{Z} = \{\hat{x} = (x_n)_{n=1}^{\infty} \in \prod_{n=1}^{\infty} \mathbb{Z}/n!\mathbb{Z} \mid \forall m < n,\ x_m \equiv x_n \pmod{m!}\}$$

Recall that $\mathbb{Z}_p$ (resp. $\widehat{\mathbb{Z}}$) contains the ring $\mathbb{Z}$ and is a compact topological ring for the topology given by the ultrametric d such that $d(x, y) = 2^{-n}$ where n is largest such that p^n (resp. $n!$) divides $x - y$, i.e. x and y have the same first n digits in their base p (resp. base factorial) representation. We refer to the Appendix for some basic definitions, representations and facts that we use about the compact topological rings $\mathbb{Z}_p$ and $\widehat{\mathbb{Z}}$.

We first prove that on $\mathbb{Z}_p$ and $\widehat{\mathbb{Z}}$ every congruence preserving function is continuous (Proposition 18).

3.1 Congruence preserving functions are continuous

Definition 17. *1. Let $\mu : \mathbb{N} \to \mathbb{N}$ be increasing. A function $\Psi : \mathbb{Z}_p \to \mathbb{Z}_p$ admits μ as modulus of uniform continuity if and only if $d(x, y) \leq 2^{-\mu(n)}$ implies $d(\Psi(x), \Psi(y)) \leq 2^{-n}$.*
2. Φ is 1-Lipschitz if it admits the identity as modulus of uniform continuity.

Since the rings $\mathbb{Z}_p$ and $\widehat{\mathbb{Z}}$ are compact, every continuous function admits a modulus of uniform continuity. For congruence preserving function, we get a tight bound on the modulus.

Proposition 18. *Every congruence preserving function $\Psi : \mathbb{Z}_p \to \mathbb{Z}_p$ is 1-Lipschitz (hence continuous). Idem with $\widehat{\mathbb{Z}}$ in place of $\mathbb{Z}_p$.*

Proof. If $d(x, y) \leq 2^{-n}$ then p^n divides $x - y$ hence (by congruence preservation) p^n also divides $\Psi(x) - \Psi(y)$ which yields $d(\Psi(x), \Psi(y)) \leq 2^{-n}$. □

The converse of Proposition 18 is false: a 1-Lipschitz function is not necessarily congruence preserving as will be seen in Example 31.

Note the following quite expectable result.

Corollary 19. *There are functions $\mathbb{Z}_p \to \mathbb{Z}_p$ (resp. $\widehat{\mathbb{Z}} \to \widehat{\mathbb{Z}}$) which are not continuous hence not congruence preserving.*

Proof. As $\mathbb{Z}_p$ has cardinality $2^{\aleph_0}$ there are $2^{2^{\aleph_0}}$ functions $\mathbb{Z}_p \to \mathbb{Z}_p$. Since $\mathbb{N}$ is dense in $\mathbb{Z}_p$, $\mathbb{Z}_p$ is a separable space, hence there are at most $2^{\aleph_0}$ continuous functions. □

3.2 Congruence preserving functions and inverse limits

In general an arbitrary continuous function on $\mathbb{Z}_p$ is not the inverse limit of a sequence of functions $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$'s. However, this is true for congruence preserving functions. We first recall how any continuous function $\Psi : \mathbb{Z}_p \to \mathbb{Z}_p$ is the inverse limit of an inverse system of continuous functions $\psi_n : \mathbb{Z}/p^{\mu(n)}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$, $n \in \mathbb{N}$, i.e. the diagram of Figure 1 commutes for any $m \leq n$. For legibility, we use notations adapted to $\mathbb{Z}_p$.

Notation 20 *We write $\widehat{\pi_n}$ for $\pi_{p^n} : \mathbb{Z}_p \to \mathbb{Z}/p^n\mathbb{Z}$ and $\widehat{\iota_n}$ for $\iota_{p^n} : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}_p$.*

Lemma 4 has an avatar in the profinite framework.

Lemma 21. *$\widehat{\pi_n} \circ \widehat{\iota_n}$ is the identity on $\mathbb{Z}/p^n\mathbb{Z}$. If $m \leq n$ then $\widehat{\pi_m} = \pi_{p^n,p^m} \circ \widehat{\pi_n}$.*

Proposition 22. *Consider $\Psi : \mathbb{Z}_p \to \mathbb{Z}_p$ and a strictly increasing $\mu : \mathbb{N} \to \mathbb{N}$. Define $\psi_n : \mathbb{Z}/p^{\mu(n)}\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ as $\psi_n = \widehat{\pi_n} \circ \Psi \circ \widehat{\iota_{\mu(n)}}$ for all $n \in \mathbb{N}$. Then the following conditions are equivalent :*

(1) Ψ is uniformly continuous and admits μ as a modulus of uniform continuity.
(2) The sequence $(\psi_n)_{n\in\mathbb{N}}$ is an inverse system with Ψ as inverse limit (in other words, for all $1 \le m \le n$, the diagrams of Figure 1 commute)
(3) For all $n \ge 1$, the upper half (dealing with Ψ and ψ_n) of the diagram of Figure 1 commutes.

Idem with $\widehat{\mathbb{Z}}$ in place of $\mathbb{Z}_p$.

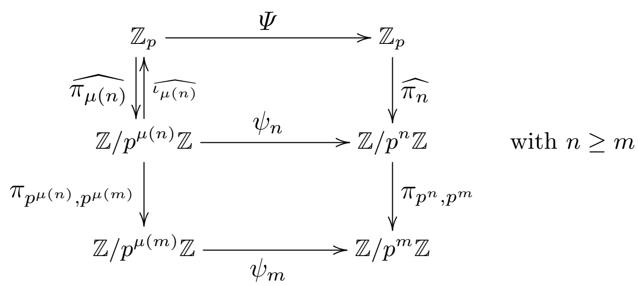


Fig. 1. The inverse system $(\psi_n)_{n\in\mathbb{N}}$ and its inverse limit Ψ.

Proof. (1) $\Rightarrow$ (2). We first show $\widehat{\pi_n} \circ \Psi = \psi_n \circ \widehat{\pi_{\mu(n)}}$. Let $u \in \mathbb{Z}_p$. Since $\widehat{\pi_{\mu(n)}} \circ \widehat{\iota_{\mu(n)}}$ is the identity on $\mathbb{Z}/p^{\mu(n)}\mathbb{Z}$, we have $\widehat{\pi_{\mu(n)}}(u) = \widehat{\pi_{\mu(n)}}(\widehat{\iota_{\mu(n)}}(\widehat{\pi_{\mu(n)}}(u)))$ hence $p^{\mu(n)}$ (considered as an element of $\mathbb{Z}_p$) divides the difference $u - \widehat{\iota_{\mu(n)}}(\widehat{\pi_{\mu(n)}}(u))$, i.e. the distance between these two elements is at most $2^{-\mu(n)}$. As μ is a modulus of uniform continuity for Ψ, the distance between their images under Ψ is at most 2^{-n}, i.e. p^n divides their difference, hence $\widehat{\pi_n}(\Psi(u)) = \widehat{\pi_n}(\Psi(\widehat{\iota_{\mu(n)}}(\widehat{\pi_{\mu(n)}}(u))))$. By definition, $\psi_n = \widehat{\pi_n} \circ \Psi \circ \widehat{\iota_{\mu(n)}}$. Thus, $\widehat{\pi_n}(\Psi(u)) = \psi_n(\widehat{\pi_{\mu(n)}}(u))$, which proves that Ψ lifts ψ_n.
We now show $\pi_{p^n,p^m} \circ \psi_n = \psi_m \circ \pi_{p^{\mu(n)},p^{\mu(m)}}$. Observe that, since $n \ge m$ and μ is increasing, p^m divides p^n and $p^{\mu(m)}$ divides $p^{\mu(n)}$. We just proved above equality $\widehat{\pi_m} \circ \Psi = \psi_m \circ \widehat{\pi_{\mu(m)}}$. Applying three times Lemma 21, we get

$$\begin{aligned} \widehat{\pi_m} \circ \Psi \circ \widehat{\iota_{\mu(n)}} &= \psi_m \circ \widehat{\pi_{\mu(m)}} \circ \widehat{\iota_{\mu(n)}} \\ (\pi_{p^n,p^m} \circ \widehat{\pi_n}) \circ \Psi \circ \widehat{\iota_{\mu(n)}} &= \psi_m \circ (\pi_{p^{\mu(n)},p^{\mu(m)}} \circ \widehat{\pi_{\mu(n)}}) \circ \widehat{\iota_{\mu(n)}} \\ \pi_{p^n,p^m} \circ \psi_n &= \psi_m \circ \pi_{p^{\mu(n)},p^{\mu(m)}} \qquad \text{as } \widehat{\pi_{\mu(n)}} \circ \widehat{\iota_{\mu(n)}} \text{ is the identity.} \end{aligned}$$

The last equality means that ψ_n lifts ψ_m.
(2) $\Rightarrow$ (3). Trivial
(3) $\Rightarrow$ (1). The fact that Ψ lifts ψ_n shows that two elements of $\mathbb{Z}_p$ with the same first $\mu(n)$ digits (in the p-adic representation) have images with the same first n digits. This proves that μ is a modulus of uniform continuity for Ψ. ☐

For congruence preserving functions $\Phi : \mathbb{Z}_p \to \mathbb{Z}_p$, the representation of Proposition 22 as an inverse limit gets smoother since then $\mu(n) = n$.

Theorem 23. *For a function $\Phi : \mathbb{Z}_p \to \mathbb{Z}_p$, letting $\varphi_n : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^n\mathbb{Z}$ be defined as $\varphi_n = \widehat{\pi_n} \circ \Phi \circ \widehat{\iota_n}$, the following conditions are equivalent.*

(1) Φ is congruence preserving.
(2) All φ_n's are congruence preserving function and the sequence $(\varphi_n)_{n\geq 1}$ is an inverse system with Φ as inverse limit (in other words, for all $1 \leq m \leq n$, the diagrams of Figure 2 commute).

A similar equivalence also holds for functions $\Phi : \widehat{\mathbb{Z}} \to \widehat{\mathbb{Z}}$.

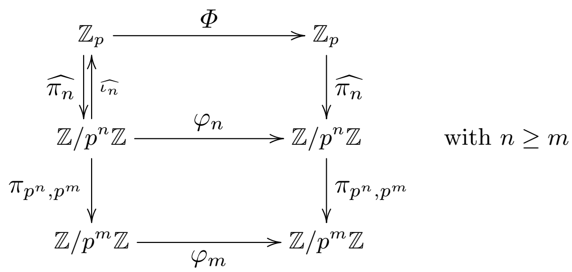


Fig. 2. Φ as the inverse limit of the φ_n's, $n \in \mathbb{N}$.

Proof. (1) $\Rightarrow$ (2). Proposition 18 insures that Φ is 1-Lipschitz. The implication (1) $\Rightarrow$ (2) in Proposition 22, applied with the identity as μ, insures that the sequence $(\varphi_n)_{n\geq 1}$ is an inverse system with Φ as inverse limit. It remains to show that φ_n is congruence preserving. Since Φ is congruence preserving, if $x, y \in \mathbb{Z}/p^n\mathbb{Z}$ then $\widehat{\iota_n}(x) - \widehat{\iota_n}(y)$ divides $\Phi(\widehat{\iota_n}(x)) - \Phi(\widehat{\iota_n}(y))$. Now, the canonical projection $\widehat{\pi_n}$ is a morphism hence $\widehat{\pi_n}(\widehat{\iota_n}(x)) - \widehat{\pi_n}(\widehat{\iota_n}(y))$ divides $\widehat{\pi_n}(\Phi(\widehat{\iota_n}(x))) - \widehat{\pi_n}(\Phi(\widehat{\iota_n}(y)))$. As $\widehat{\pi_n} \circ \widehat{\iota_n}$ is the identity on $\mathbb{Z}/p^n\mathbb{Z}$, $x - y$ divides $\widehat{\pi_n}(\Phi(\widehat{\iota_n}(x))) - \widehat{\pi_n}(\Phi(\widehat{\iota_n}(y))) = \varphi_n(x) - \varphi_n(y)$ as wanted.

(2) $\Rightarrow$ (1). Let $x, y \in \mathbb{Z}_p$. Since φ_n is congruence preserving $\widehat{\pi_n}(x) - \widehat{\pi_n}(y)$ divides $\varphi_n(\widehat{\pi_n}(x)) - \varphi_n(\widehat{\pi_n}(y))$. Let

$$U_n^{x,y} = \{u \in \mathbb{Z}/p^n\mathbb{Z} \mid \varphi_n(\widehat{\pi_n}(x)) - \varphi_n(\widehat{\pi_n}(y)) = (\widehat{\pi_n}(x) - \widehat{\pi_n}(y))\, u\}\,.$$

If $m \leq n$ and $u \in U_n^{x,y}$ then, applying π_{p^n,p^m} to the equality defining $U_n^{x,y}$, using the commutative diagrams of Figure 2 and letting $v = \pi_{p^n,p^m}(u)$, we get

$$\begin{aligned}
\varphi_n(\widehat{\pi_n}(x)) - \varphi_n(\widehat{\pi_n}(y)) &= \big(\widehat{\pi_n}(x) - \widehat{\pi_n}(y)\big)\, u\\
\pi_{p^n,p^m}(\varphi_n(\widehat{\pi_n}(x)) - \pi_{p^n,p^m}(\varphi_n(\widehat{\pi_n}(y)) &= \big(\pi_{p^n,p^m}(\widehat{\pi_n}(x)) - \pi_{p^n,p^m}(\widehat{\pi_n}(y)\big)\, v\\
\varphi_m(\pi_{p^n,p^m}(\widehat{\pi_n}(x))) - \varphi_m(\pi_{p^n,p^m}(\widehat{\pi_n}(y))) &= \big(\widehat{\pi_m}(x) - \widehat{\pi_m}(y)\big)\, v\\
\varphi_m(\widehat{\pi_m}(x)) - \varphi_m(\widehat{\pi_m}(y)) &= \big(\widehat{\pi_m}(x) - \widehat{\pi_m}(y)\big)\, v
\end{aligned}$$

Thus, if $u \in U_n^{x,y}$ then $v = \pi_{p^n,p^m}(u) \in U_m^{x,y}$.

Consider the tree $\mathcal{T}$ of finite sequences $(u_0, \ldots, u_n)$ such that $u_i \in U_i^{x,y}$ and $u_i = \pi_{p^n,p^i}(u_n)$ for all $i = 0, \ldots, n$. Since each $U_n^{x,y}$ is nonempty, the tree $\mathcal{T}$ is infinite. Since it is at most p-branching, using König's Lemma, we can pick an infinite branch $(u_n)_{n\in\mathbb{N}}$ in $\mathcal{T}$. This branch defines an element $z \in \mathbb{Z}_p$. The commutative diagrams of Figure 2 show that the sequences $(\widehat{\pi_n}(x) - \widehat{\pi_n}(y))_{n\in\mathbb{N}}$ and $\varphi_n(\widehat{\pi_n}(x)) - \varphi_n(\widehat{\pi_n}(y))$ represent $x - y$ and $\Phi(x) - \Phi(y)$ in Z_p. Equality $\varphi_m(\widehat{\pi_m}(x)) - \varphi_m(\widehat{\pi_m}(y)) = (\widehat{\pi_m}(x) - \widehat{\pi_m}(y))\, \pi_{p^n,p^m}(u)$ shows that (going to the projective limits) $\Phi(x) - \Phi(y) = (x - y)\, z$. This proves that Φ is congruence preserving. □

3.3 Extension of congruence preserving functions $\mathbb{N} \to \mathbb{N}$

Congruence preserving functions $\mathbb{Z}_p \to \mathbb{Z}_p$ (resp. $\widehat{\mathbb{Z}} \to \widehat{\mathbb{Z}}$) are determined by their restrictions to $\mathbb{N}$ since $\mathbb{N}$ is dense in $\mathbb{Z}_p$ (resp. $\widehat{\mathbb{Z}}$). Let us state a (partial) converse result.

Theorem 24. *Every congruence preserving function $F : \mathbb{N} \to \mathbb{Z}$ has a unique extension to a congruence preserving function $\Phi : \mathbb{Z}_p \to \mathbb{Z}_p$ (resp. $\widehat{\mathbb{Z}} \to \widehat{\mathbb{Z}}$).*

Proof. Let us denote by $\widetilde{\mathbb{N}}$ and $\widetilde{\mathbb{Z}}$ the canonical copies of $\mathbb{N}$ and $\mathbb{Z}$ in $\mathbb{Z}_p$ and by $\widetilde{F} : \widetilde{\mathbb{N}} \to \widetilde{\mathbb{Z}}$ the copy of F as a partial function on $\mathbb{Z}_p$. As F is congruence preserving so is $\widetilde{F}$, which is thus also uniformly continuous (as a partial function on $\mathbb{Z}_p$). Since $\widetilde{\mathbb{N}}$ is dense in $\mathbb{Z}_p$, $\widetilde{F}$ has a unique uniformly continuous extension $\Phi : \mathbb{Z}_p \to \mathbb{Z}_p$. To show that this extension Φ is congruence preserving, observe that Φ, being uniformly continuous, is the inverse limit of the $\varphi_n = \widehat{\pi_n} \circ \Phi \circ \widehat{\iota_n}$. Now, since $\widehat{\iota_n}$ has range exactly $\widetilde{\mathbb{N}}$ we see that $\varphi_n = \widehat{\pi_n} \circ \widetilde{F} \circ \widehat{\iota_n}$; as $\widetilde{F}$ is congruence preserving so is φ_n. Finally, Theorem 23 insures that Φ is also congruence preserving. □

Polynomials in $\mathbb{Z}_p[X]$ obviously define congruence preserving functions $\mathbb{Z}_p \to \mathbb{Z}_p$. But non polynomial functions can also be congruence preserving.

Consequence 25 *The extensions to $\mathbb{Z}_p$ and $\widehat{\mathbb{Z}}$ of the $\mathbb{N} \to \mathbb{Z}$ functions [3,4]*

$$x \mapsto \lfloor e^{1/a}\, a^x\, x! \rfloor \quad (\text{for } a \in \mathbb{Z} \setminus \{0,1\}) \quad , \quad x \mapsto \textbf{\textit{if}}\ x = 0\ \textbf{\textit{then}}\ 1\ \textbf{\textit{else}}\ \lfloor e\, x! \rfloor$$

and the Bessel like function $f(n) = \sqrt{\frac{e}{\pi}} \times \frac{\Gamma(1/2)}{2 \times 4^n \times n!} \int_1^\infty e^{-t/2}(t^2 - 1)^n dt$ *are congruence preserving.*

3.4 Representation of congruence preserving functions $\mathbb{Z}_p \to \mathbb{Z}_p$

We now characterize congruence preserving functions via their representation as infinite linear sums of the P_k's (suitably extended to $\mathbb{Z}_p$). This representation is a refinement of Mahler's characterization of continuous functions (Theorem 28). First recall the notion of valuation.

Definition 26. *The p-valuation (resp. the factorial valuation) $Val(x)$ of $x \in \mathbb{Z}_p$, or $x \in \mathbb{Z}/p^n\mathbb{Z}$ (resp. $x \in \widehat{\mathbb{Z}}$) is the largest s such that p^s (resp. $s!$) divides x or is $+\infty$ in case $x = 0$. It is also the length of the initial block of zeros in the p-adic (resp. factorial) representation of x.*

Note that for any polynomial P_k (or more generally any polynomial), the below diagram commutes for any $m \leq n$ (recall that $P_k^{p^n,p^n} = \pi_{p^n} \circ P_k \circ \iota_{p^n}$, cf. Definition 12):

$$\begin{array}{ccc} \mathbb{Z}/p^n\mathbb{Z} & \xrightarrow{P_k^{p^n,p^n}} & \mathbb{Z}/p^n\mathbb{Z} \\ \pi_{p^n,p^m}\downarrow & & \downarrow\pi_{p^n,p^m} \\ \mathbb{Z}/p^m\mathbb{Z} & \xrightarrow{P_k^{p^m,p^m}} & \mathbb{Z}/p^m\mathbb{Z} \end{array} \quad \text{i.e.} \quad \pi_{p^n,p^m} \circ P_k^{p^n,p^n} = P_k^{p^m,p^m} \circ \pi_{p^n,p^m}\,.$$

This allows to define the interpretation $\widehat{P_k}$ of P_k in $\mathbb{Z}_p$ (resp. $\widehat{\mathbb{Z}}$) as an inverse limit.

Definition 27. *$\widehat{P_k} \colon \mathbb{Z}_p \to \mathbb{Z}_p$ is the inverse limit of the inverse system $(P_k^{p^n,p^n})_{n\geq 1}$. Otherwise stated, for $x \in \mathbb{Z}_p$ such that $x = \varprojlim_{n\in\mathbb{N}} x_n$, we have*

$$\widehat{P_k}(x) = \varprojlim_{n\in\mathbb{N}} P_k^{p^n,p^n}(x_n) = \varprojlim_{n\in\mathbb{N}} \pi_{p^n}(P_k(\iota_{p^n}(x_n)))$$

Thus, the following diagram commutes for all n :

$$\begin{array}{ccc} \mathbb{Z}_p & \xrightarrow{\widehat{P_k}} & \mathbb{Z}_p \\ \widehat{\pi_n}\downarrow & & \downarrow\widehat{\pi_n} \\ \mathbb{Z}/p^n\mathbb{Z} & \xrightarrow{P_k^{p^n,p^n}} & \mathbb{Z}/p^n\mathbb{Z} \\ \iota_{p^n}\downarrow & & \downarrow\iota_{p^n} \\ \mathbb{N} & \xrightarrow{P_k} & \mathbb{N} \end{array}$$

Recall Mahler's characterization of continuous functions on $\mathbb{Z}_p$ (resp. $\widehat{Z}$).

Theorem 28 (Mahler, 1956 [10]). *1. A series $\sum_{k\in\mathbb{N}} a_k \widehat{P_k}(x)$, $a_k \in \mathbb{Z}_p$, is convergent in $\mathbb{Z}_p$ if and only if $\lim_{k\to\infty} a_k = 0$, i.e. the corresponding sequence of valuations $(Val(a_k))_{k\in\mathbb{N}}$ tends to $+\infty$.*
2. A function $\mathbb{Z}_p \to \mathbb{Z}_p$ is represented by a convergent series if and only if it is continuous. Moreover, such a representation is unique.
Idem with $\widehat{\mathbb{Z}}$.

Theorem 29 refines Mahler's characterization to congruence preserving functions.

Theorem 29. *A function $\Phi : \mathbb{Z}_p \to \mathbb{Z}_p$ represented by a series $\Phi = \sum_{k\in\mathbb{N}} a_k \widehat{P_k}$ is congruence preserving if and only if $lcm(k)$ divides a_k for all k.*

Note. The condition "$lcm(k)$ divides a_k for all k" is stronger than $\lim_{k\to\infty} a_k = 0$.

Proof. Suppose Φ is congruence preserving and let $\varphi_n = \widehat{\pi_n} \circ \Phi \circ \widehat{\iota_n}$. Theorem 23 insures that $\Phi = \varprojlim_{n\in\mathbb{N}} \varphi_n$ and the φ_n's are congruence preserving on $\mathbb{Z}/p^n\mathbb{Z}$. Using Corollary 14, we get $\varphi_n = \sum_{k=0}^{\nu(n)-1} b_k^n \, P_k^{p^n,p^n}$ with $lcm(k)$ dividing b_k^n for all $k \le \nu(n)-1$. By Proposition 18, Φ is uniformly continuous hence by Mahler's Theorem 28, $\Phi = \sum_{k\in\mathbb{N}} a_k \widehat{P_k}$ with $a_k \in \mathbb{Z}_p$ such that $\lim_{k\to\infty} a_k = 0$. Equation $\varphi_n = \widehat{\pi_n} \circ \Phi \circ \widehat{\iota_n}$ then yields

$$\varphi_n = \widehat{\pi_n} \circ (\sum_{k\in\mathbb{N}} a_k \widehat{P_k}) \circ \widehat{\iota_n} = \sum_{k\in\mathbb{N}} \widehat{\pi_n}(a_k)\, \widehat{\pi_n} \circ \widehat{P_k} \circ \widehat{\iota_n} = \sum_{k\in\mathbb{N}} \widehat{\pi_n}(a_k)\, P_k^{p^n,p^n} \,.$$

The unicity of the representation of φ_n (cf. Corollary 14) insures that $b_k^n = \widehat{\pi_n}(a_k)$. Similarly, $b_k^m = \widehat{\pi_m}(a_k)$; as for $m \le n$, $\widehat{\pi_m} = \pi_{p^n,p^m} \circ \widehat{\pi_n}$ (Lemma 21), we obtain $b_k^m = \pi_{p^n,p^m}(b_k^n)$. Thus, $(b_k^n)_{n\in\mathbb{N}}$ is an inverse system such that $a_k = \varprojlim_{n\in\mathbb{N}} b_k^n$. Since φ_n is congruence preserving Corollary 14 insures that $lcm(k)$ divides b_k^n; applying Lemma 30, we see that for all n, $\nu_p(k) \le Val(b_k^n)$. Noting that $Val(a_k) = Val(b_k^n)$, we deduce that $\nu_p(k) \le Val(a_k)$, hence $p^{\nu_p(k)}$ and thus also $lcm(k)$ divide a_k. In particular, this implies that $d(a_k, 0) \le 2^{-\nu_p(k)}$ and $\lim_{k\to\infty} a_k = 0$.

Conversely, if $\Phi = \sum_{k\in\mathbb{N}} a_k \widehat{P_k}$ and $lcm(k)$ divides a_k for all k then $lcm(k)$ divides $\widehat{\pi_n}(a_k)$ for all n, k. Thus, the associated φ_n are congruence preserving which implies that so is Φ by Theorem 23. □

Lemma 30. *Let $\nu_p(k)$ be the largest i such that $p^i \le k < p^{i+1}$. In $\mathbb{Z}/p^n\mathbb{Z}$, $lcm(k)$ divides a number x iff $\nu_p(k) \le Val(x)$.*

Proof. In $\mathbb{Z}/p^n\mathbb{Z}$ all numbers are invertible except multiples of p. Hence $lcm(k)$ divides x iff $p^{\nu_p(k)}$ divides x. □

Example 31. Let $\Phi = \sum_{k\in\mathbb{N}} a_k \, P_k$ with $a_k = p^{\nu_p(k)-1}$, with $\nu_p(k)$ as in Lemma 30. Φ is uniformly continuous by Theorem 28. By Lemma 30, $lcm(k)$ does not divide a_k; hence by Theorem 29, Φ is *not* congruence preserving.

4 Conclusion

We here studied functions having congruence preserving properties. These functions appeared as uniformly continuous functions in a variety of finite groups (see [11]).

The contribution of the present paper is to *characterize congruence preserving functions* on various sets derived from $\mathbb{Z}$ such as $\mathbb{Z}/n\mathbb{Z}$, (resp. $\mathbb{Z}_p, \widehat{\mathbb{Z}}$) via polynomials (resp. series) with *rational coefficients* which share the following common property: $lcm(k)$ divides the k-th coefficient. Examples of *non polynomial* (Bessel like) congruence preserving functions can be found in [4].

Acknowledgments

We thank the anonymous referee for careful reading and valuable comments.

References

1. M. Bhargava, *Congruence preservation and polynomial functions from $\mathbb{Z}_n$ to $\mathbb{Z}_m$*, Discrete Mathematics 173, 15 – 21, 1997.
2. M. Benois, Parties Rationnelles du Groupe Libre, *C. R. Acad. Sci. Paris Série A*, 269, 1188-1190, 1969.
3. P. Cégielski, S. Grigorieff and I. Guessarian, Newton representation of functions over natural integers having integral difference ratios. To be published in Int. J. Number Theory. Preliminary version on arXiv, 2013.
4. P. Cégielski, S. Grigorieff and I. Guessarian, *Integral Difference Ratio functions on Integers*, LNCS 8808, Computing with new resources, Festschrift for Jozef Gruska, C, Calude, R. Freivalds, I. Kazuo (Eds.), Springer, 277–291, 2014.
5. P. Cégielski, S. Grigorieff and I. Guessarian, *Characterizing congruence preserving functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ via rational polynomials*, Submitted, 2015.
6. Z. Chen, *On polynomial functions from $\mathbb{Z}_n$ to $\mathbb{Z}_m$*, Disc. Math. 137, 137–145, 1995.
7. S. Lang, *Algebra 3rd ed.*, Springer, 2002.
8. H.W. Lenstra, Profinite Fibonacci numbers. *Nieuw Arch. Wiskd.*, (5) 6, n.4, 297–300, 2005.
9. H.W. Lenstra, Profinite groups. *Lecture notes available on the web.*
10. K. Mahler, An Interpolation Series for Continuous Functions of a p-adic Variable. *Journal für die reine und angewandte Mathematik*, 199, 23–34, 1956.
11. 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.
12. A. Robert, *A course in p-adic analysis*, Springer, 2000.
13. K. Rosen, *Elementary number theory and its applications*, Addison,-Wesley, 1984.

Appendix

Appendix 1: Basics on p-adic and profinite integers

Recall some classical equivalent approaches to the topological rings of p-adic integers and profinite integers, cf. Lenstra [8,9], Lang [7] and Robert [12].

Proposition 32. *Let p be prime. The three following approaches lead to isomorphic structures, called the topological ring $\mathbb{Z}_p$ of p-adic integers.*

- *The ring $\mathbb{Z}_p$ is the inverse limit of the following inverse system:*
  - *the family of rings $\mathbb{Z}/p^n\mathbb{Z}$ for $n \in \mathbb{N}$, endowed with the discrete topology,*
  - *the family of surjective morphisms $\pi_{p^n,p^m} : \mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$ for $0 \leq n \geq m$.*
- *The ring $\mathbb{Z}_p$ is the set of infinite sequences $\{0, \ldots, p-1\}^{\mathbb{N}}$ endowed with the Cantor topology and addition and multiplication which extend the usual way to perform addition and multiplication on base p representations of natural integers.*
- *The ring $\mathbb{Z}_p$ is the Cauchy completion of the metric topological ring $(\mathbb{N}, +, \times)$ relative to the following ultrametric: $d(x, x) = 0$ and for $x \neq y$, $d(x, y) = 2^{-n}$ where n is the p-valuation of $|x-y|$, i.e. the maximum k such that p^k divides $x - y$.*

Recall the factorial representation of integers.

Lemma 33. *Every positive integer n has a unique representation as*

$$n = c_k k! + c_{k-1}(k-1)! + ... + c_2 2! + c_1 1!$$

where $c_k \neq 0$ and $0 \leq c_i \leq i$ for all $i = 1, ..., k$.

Proposition 34. *The four following approaches lead to isomorphic structures, called the topological ring $\widehat{\mathbb{Z}}$ of profinite integers.*

- *The ring $\widehat{\mathbb{Z}}$ is the inverse limit of the following inverse system:*
  - *the family of rings $\mathbb{Z}/k\mathbb{Z}$ for $k \geq 1$, endowed with the discrete topology,*
  - *the family of surjective morphisms $\pi_{n,m} : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ for $m \mid n$.*
- *The ring $\widehat{\mathbb{Z}}$ is the inverse limit of the following inverse system:*
  - *the family of rings $\mathbb{Z}/k!\mathbb{Z}$ for $k \geq 1$, endowed with the discrete topology,*
  - *the family of surjective morphisms $\pi_{(n+1)!,n!} : \mathbb{Z}/n!\mathbb{Z} \to \mathbb{Z}/m!\mathbb{Z}$ for $n \geq m$.*
- *The ring $\widehat{\mathbb{Z}}$ is the set of infinite sequences $\prod_{n \geq 1}\{0, \ldots, n\}$ endowed with the product topology and addition and multiplication which extend the obvious way to perform addition and multiplication on factorial representations of natural integers.*
- *The ring $\widehat{\mathbb{Z}}$ is the Cauchy completion of the metric topological ring $(\mathbb{N}, +, \times)$ relative to the following ultrametric: for $x \neq y \in \mathbb{N}$, $d(x, x) = 0$ and $d(x, y) = 2^{-n}$ where n is the maximum k such that $k!$ divides $x - y$.*
- *The ring $\widehat{\mathbb{Z}}$ is the product ring $\prod_{p\ prime} \mathbb{Z}_p$ endowed with the product topology.*

Proposition 35. *The topological rings $\mathbb{Z}_p$ and $\widehat{\mathbb{Z}}$ are compact and zero dimensional (i.e. they have a basis of closed open sets).*

Appendix 2: $\mathbb{N}$ and $\mathbb{Z}$ in $\mathbb{Z}_p$ and $\widehat{\mathbb{Z}}$

Proposition 36. *Let $\lambda : \mathbb{N} \to \mathbb{Z}_p$ (resp. $\lambda : \mathbb{N} \to \widehat{\mathbb{Z}}$) be the function which maps $n \in \mathbb{N}$ to the element of $\mathbb{Z}_p$ (resp. $\widehat{\mathbb{Z}}$) with base p (resp. factorial) representation obtained by suffixing an infinite tail of zeros to the base p (resp. factorial) representation of n.*
The function λ is an embedding of the semiring $\mathbb{N}$ onto a topologically dense semiring in the ring $\mathbb{Z}_p$ (resp. $\widehat{\mathbb{Z}}$).

Remark 37. In the base p representation, the opposite of an element $f \in \mathbb{Z}_p$ is the element $-f$ such that, for all $m \in \mathbb{N}$,

$$(-f)(i) = \begin{cases} 0 & \textit{if } \ \forall s \leq i \ f(s) = 0\,, \\ p - f(i) & \textit{if } \ i \textit{ is least such that } f(i) \neq 0\,, \\ p - 1 - f(i) & \textit{if } \ \exists s < i \ f(s) \neq 0\,. \end{cases}$$

In particular,
– Integers in $\mathbb{N}$ correspond in $\mathbb{Z}_p$ to infinite base p representations with a tail of 0's.
– Integers in $\mathbb{Z} \setminus \mathbb{N}$ correspond in $\mathbb{Z}_p$ to infinite base p representations with a tail of digits $p - 1$.
Similar results hold for the infinite factorial representation of profinite integers.