#A50 INTEGERS 16 (2016)

CHARACTERIZING CONGRUENCE PRESERVING FUNCTIONS $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ VIA RATIONAL POLYNOMIALS

Patrick Cégielski [1]
LACL, EA 4219, Université Paris-Est Créteil, France
IUT Sénart-Fontainebleau
cegielski@u-pec.fr

Serge Grigorieff[1]
IRIF, CNRS and Université Paris-Diderot, France
seg@irif.univ-paris-diderot.fr

Irène Guessarian[1] [2]
IRIF, CNRS and Université Paris-Diderot, France
ig@irif.univ-paris-diderot.fr

Received: 3/19/15, Revised: 10/26/15, Accepted: 6/15/16, Published:

Abstract

Using a simple basis of rational polynomial-like functions $P_0, \ldots, P_{n-1}$ for the free module of functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$, we characterize the subfamily of congruence preserving functions as the set of linear combinations of the products $\mathrm{lcm}(k)\, P_k$ where $\mathrm{lcm}(k)$ is the least common multiple of $2, \ldots, k$ (viewed in $\mathbb{Z}/m\mathbb{Z}$). As a consequence, when $n \geq m$, the number of such functions is independent of n.

1. Introduction

The notion of a congruence preserving function on rings of residue classes was introduced in Chen [3] and studied in Bhargava [1].

Definition 1.1. Let $m, n \geq 1$. A function $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is said to be *congruence preserving* if for all d dividing m

$$\text{for all } a, b \in \{0, \ldots, n-1\} \quad a \equiv b \pmod d \text{ implies } f(a) \equiv f(b) \pmod d. \tag{1}$$

Remark 1.2. 1. If $n \in \{1, 2\}$ or $m = 1$ then every function $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is trivially congruence preserving.

[1] Partially supported by TARMAC ANR agreement 12 BS02 007 01.
[2] Emeritus at UPMC Université Paris 6. Corresponding author

2. Observe that since d is assumed to divide m, equivalence modulo d is a congruence on $(\mathbb{Z}/m\mathbb{Z}, +, \times)$. However, since d is not supposed to divide n, equivalence modulo d may not be a congruence on $(\mathbb{Z}/n\mathbb{Z}, +, \times)$.

Example 1.3. 1. For functions $\mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z}$, condition (1) reduces to the conditions $f(3) \equiv f(0) \pmod 3$, $f(4) \equiv f(1) \pmod 3$, $f(5) \equiv f(2) \pmod 3$.
2. For functions $\mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/8\mathbb{Z}$, condition (1) reduces to $f(2) \equiv f(0) \pmod 2$, $f(3) \equiv f(1) \pmod 2$, $f(4) \equiv f(0) \pmod 4$, $f(5) \equiv f(1) \pmod 4$.

In this paper, we characterize congruence preserving functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$.

We denote by $\mathbb{Z}$ the set of integers and by $\mathbb{N}$ the set of nonnegative integers (including zero).

Definition 1.4. The unary *lcm* function $\mathbb{N} \to \mathbb{N}$ maps 0 to 1 and $k \geq 1$ to the least common multiple of $1, 2, \ldots, k$.

A natural way to associate with each map from $\mathbb{N}$ to $\mathbb{Z}$ a map from $\mathbb{Z}/n\mathbb{Z}$ to $\mathbb{Z}/m\mathbb{Z}$ is to restrict F to $\{0, \cdots, n-1\}$ and take its values modulo m.

Definition 1.5. With each map $F : \mathbb{N} \to \mathbb{Z}$, we associate the map $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ defined by $f = \pi_m \circ F \circ \iota_n$, where $\pi_m(x) = x \pmod m$, and $\iota_n(z)$ is the unique element of $\pi_n^{-1}(z) \cap \{0, \ldots, n-1\}$.

Definition 1.5 is best pictured by the commutativity of diagram (2).

$$\begin{tikzcd} \mathbb{N} \arrow[r, "F"] & \mathbb{Z} \arrow[d, "\pi_m"] \\ \mathbb{Z}/n\mathbb{Z} \arrow[u, "\iota_n"] \arrow[r, "f"] & \mathbb{Z}/m\mathbb{Z} \end{tikzcd} \tag{2}$$

Applying Definition 1.5 to binomial coefficients, we obtain a basis of the $(\mathbb{Z}/m\mathbb{Z})$-module of functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$.

Proposition 1.6. *Let $P_k : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ be associated with the $\mathbb{N} \to \mathbb{N}$ binomial function $x \mapsto \binom{x}{k}$. For every function $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ there is a unique sequence $(a_0, \ldots, a_{n-1})$ of elements of $\mathbb{Z}/m\mathbb{Z}$ such that*

$$f \quad = \quad \sum_{k=0}^{k=n-1} a_k \, P_k \ . \tag{3}$$

In other words, the family $\{P_0, \ldots, P_{n-1}\}$ is a basis of the $(\mathbb{Z}/m\mathbb{Z})$-module of functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$.

Our main result can be stated as

Theorem 1.7. *A function $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is congruence preserving if and only if, for each $k = 0, \ldots, n-1$, in equation* (3) *the coefficient a_k is a multiple of the residue of* $\mathrm{lcm}(k)$ *in $\mathbb{Z}/m\mathbb{Z}$.*

The paper is organized as follows.

Proposition 1.6 is proved in Section 2 where, after recalling Chen's notion of a polynomial function $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ (cf. [3]), we extend it to a notion of a rational polynomial function.

The proof of our main result, Theorem 1.7, is given in Section 3. We adapt the techniques of our paper [2], exploiting similarities between Definition 1.1 and the condition studied in [2] for functions $f : \mathbb{N} \to \mathbb{Z}$ (namely, $x-y$ divides $f(x)-f(y)$ for all $x, y \in \mathbb{N}$). As a consequence of Theorem 1.7, the number of congruence preserving functions is independent of n for $n \geq m$ and even for $n \geq gpp(m)$ (the greatest prime power dividing m). Also, every congruence preserving function $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is a rational polynomial for a polynomial of degree strictly less than the minimum of n and $gpp(m)$.

In Section 4 we use our main theorem to count the congruence preserving functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$. We thus get an expression equivalent to that obtained by Bhargava in [1] and which makes apparent the fact that, for $n \geq gpp(m)$ (hence for $n \geq m$), this number depends only on m and is independent of n.

2. Representing Functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ by Rational Polynomials

In [3, 1], congruence preserving functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ are introduced and studied together with an original notion of polynomial function $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$.

Definition 2.1 (Chen [3])**.** A function $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is *polynomial* if it is associated (in the sense of Definition 1.5) with a function $F : \mathbb{N} \to \mathbb{Z}$ given by a polynomial in $\mathbb{Z}[X]$.

Polynomial functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ are obviously congruence preserving. Are all congruence preserving functions polynomial? Chen [3] observed that this is not the case for some values of n, m, for instance $n = 6$, $m = 8$. He also proves that a stronger identity holds for infinitely many ordered pairs $\langle n, m\rangle$: *every function $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is polynomial if and only n is not greater than the first prime factor of m* (in particular, this is the case when $n = m$ and m is prime, cf. Kempner [4]). Using counting arguments, Bhargava [1] characterizes the ordered pairs $\langle n, m\rangle$ such that every congruence preserving function $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is polynomial.

Some polynomials in $\mathbb{Q}[X]$ (i.e., polynomials with rational coefficients) happen to map integers into integers.

Definition 2.2. For $k \in \mathbb{N}$, let $P_k \in \mathbb{Q}[X]$ be the following polynomial:

$$P_k(x) = \binom{x}{k} = \frac{\prod_{i=0}^{k-1}(x-i)}{k!}.$$

We will use the following examples later on:
$P_0(x) = 1$, $P_1(x) = x$, $P_2(x) = x(x-1)/2$, $P_3(x) = x(x-1)(x-2)/6$, $P_4(x) = x(x-1)(x-2)(x-3)/24$, $P_5(x) = x(x-1)(x-2)(x-3)(x-4)/120$.

In [5], Pólya used the P_k's to give the following very elegant and elementary characterization of polynomials in $\mathbb{Q}[X]$ mapping integers to integers.

Theorem 2.3 (Pólya)**.** *A polynomial in $\mathbb{Q}[X]$ is integer-valued on $\mathbb{Z}$ if and only if it can be written as a $\mathbb{Z}$-linear combination of the polynomials P_k, $k = 0, 1, 2, \ldots$.*

It turns out that the representation of functions $\mathbb{N} \to \mathbb{Z}$ as $\mathbb{Z}$-linear combinations of the P_k's used in [2] also fits in the case of functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$: every such function is a $(\mathbb{Z}/m\mathbb{Z})$-linear combination of the P_k's.

Definition 2.4. 1. A function $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is *rat-polynomial* if is associated in the sense of Definition 1.5 with some polynomial in $\mathbb{Q}[X]$.
2. The *degree* of a rat-polynomial function is the smallest degree of an associated polynomial in $\mathbb{Q}[X]$.
3. We denote by $P_k^{n,m}$ the rat-polynomial function $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ associated with the polynomial P_k of Definition 2.2 in the sense of Definition 1.5. When there is no ambiguity, $P_k^{n,m}$ will be denoted simply as P_k.

Remark 2.5. In Definition 2.4, the polynomial *crucially depends* on the choice of representatives of elements of $\mathbb{Z}/n\mathbb{Z}$: e.g., for $n = m = 6$, $0 \equiv 6 \pmod 6$ but $0 = P_2(0) \not\equiv P_2(6) = 3 \pmod 6$. The chosen representatives for elements of $\mathbb{Z}/n\mathbb{Z}$ will always be $0, 1, \ldots, n-1$.

We now prove the representation result by the P_k's.

Proof of Proposition 1.6. Let us start with uniqueness. We have $f(0) = a_0$, and hence a_0 is $f(0)$. We have $f(1) = a_0 + a_1$, and hence $a_1 = f(1) - f(0)$. By induction, letting $Q_k = \sum_{\ell=0}^{\ell=k-1} a_\ell P_\ell$, and noting that $P_k(k) = 1$, we have $f(k) = Q_k(k) + a_k P_k(k) = Q_k(k) + a_k$, and hence $a_k = f(k) - Q_k(k)$. We thus are able to determine a_k in $\mathbb{Z}/m\mathbb{Z}$.

For existence, argue backwards to see that this sequence suits. □

Remark 2.6. The evaluation of $a_k\, P_k(x)$ in $\mathbb{Z}/m\mathbb{Z}$ has to be done as follows: for x an element of $\mathbb{Z}/n\mathbb{Z}$, we consider it as an element of $\{0, \ldots, n-1\} \subseteq \mathbb{N}$ and we evaluate $P_k(x) = \dfrac{1}{k!} \prod_{i=0}^{k-1}(x-i)$ as an element of $\mathbb{Z}$, then we consider the remainder modulo m, and finally we multiply the result by a_k in $\mathbb{Z}/m\mathbb{Z}$. For instance, for

$n = m = 8$, we have $4\,P_2(3) = 4 \times \dfrac{3 \times 2}{2} = 4 \times 3 = 4$, but we might be tempted to evaluate it as $4\,P_2(3) = \dfrac{4 \times 3 \times 2}{2} = \dfrac{0}{2} = 0$, which does *not* correspond to our definition. However, dividing a_k by a factor of the denominator is allowed.

Corollary 2.7. *1. Every function $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is rat-polynomial with degree less than n.*
2. The family of rat-polynomial functions $\{P_k \mid k = 0, 1, \ldots, n-1\}$ is a basis of the $(\mathbb{Z}/m\mathbb{Z})$-module of functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$.

Example 2.8. The function $f\colon \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/6\mathbb{Z}$ such that $f(0) = 0$, $f(1) = 3$, $f(2) = 4$, $f(3) = 3$, $f(4) = 0$, $f(5) = 1$, is represented by the rational polynomial $P_f(x) = 3x + 4\,\dfrac{x(x-1)}{2}$ which can be simplified to $P_f(x) = 3x - x(x-1)$ on $\mathbb{Z}/6\mathbb{Z}$.

Example 2.9. The function $f\colon \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/8\mathbb{Z}$ given by Chen [3] as a non-polynomial congruence preserving function, namely the function such that $f(0) = 0$, $f(1) = 3$, $f(2) = 4$, $f(3) = 1$, $f(4) = 4$, $f(5) = 7$, is represented by the rational polynomial with coefficients $a_0 = 0$, $a_1 = 3$, $a_2 = 6$, $a_3 = 2$, $a_4 = 4$, $a_5 = 4$. Thus,

$$\begin{aligned} f(x) &= 3x + 6\,\frac{x(x-1)}{2} + 2\,\frac{x(x-1)(x-2)}{2} + 4\,\frac{x(x-1)(x-2)(x-3)}{8} \\ &\quad + 4\,\frac{x(x-1)(x-2)(x-3)(x-4)}{8} \\ &= 3x + 3x(x-1) + x(x-1)(x-2) + \frac{x(x-1)(x-2)(x-3)}{2} \\ &\quad + \frac{x(x-1)(x-2)(x-3)(x-4)}{2}. \end{aligned}$$

3. Characterizing Congruence Preserving Functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$

Congruence preserving functions $f\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ can be characterized by a simple condition on the coefficients of the rat-polynomial representation of f given in Proposition 1.6.

3.1. Proof of Theorem 1.7

For proving Theorem 1.7 we will need some relations involving binomial coefficients and the unary lcm function; these relations are stated in the next three lemmata. The proofs are elementary but technical and can be found in our paper [2].

Lemma 3.1. *If $0 \le n - k < p \le n$ then p divides $\mathrm{lcm}(k)\binom{n}{k}$ in $\mathbb{N}$.*

Lemma 3.2. *If $k \le b$ then n divides $A^n_{k,b} = \mathrm{lcm}(k)\left(\binom{b+n}{k} - \binom{b}{k}\right)$ in $\mathbb{N}$.*

The following is an immediate consequence of Lemma 3.2 (set $a = b + n$).

Lemma 3.3. *If $a \geq b$ and $k \leq b$, then $a - b$ divides $\operatorname{lcm}(k)\left(\binom{a}{k} - \binom{b}{k}\right)$ in $\mathbb{N}$.*

Besides these lemmata which deal with divisibility on integers, we shall use a classical result in $\mathbb{Z}/m\mathbb{Z}$. For $x, y \in \mathbb{Z}$ we say *x divides y in $\mathbb{Z}/m\mathbb{Z}$* if and only if the residue class of x divides the residue class of y in $\mathbb{Z}/m\mathbb{Z}$.

Lemma 3.4. *Let $1 \leq c_1, \ldots, c_k \leq m$ and let c be their least common multiple in $\mathbb{N}$. If $c_1, \ldots, c_k$ all divide a in $\mathbb{Z}/m\mathbb{Z}$ then so does c.*

Proof. It suffices to consider the case $k = 2$ since the passage to any k is done via a straightforward induction. Let $c = c_1 b_1 = c_2 b_2$ with b_1, b_2 coprime. Let t, u be such that $a = c_1 t = c_2 u$ in $\mathbb{Z}/m\mathbb{Z}$. Then $a \equiv c_1 t \equiv c_2 u \pmod{m}$. Using Bézout's identity, let $\alpha, \beta \in \mathbb{Z}$ be such that $\alpha b_1 + \beta b_2 = 1$. Then $c(t\alpha + u\beta) = c_1 b_1 t\alpha + c_2 b_2 u\beta \equiv a\alpha b_1 + a\beta b_2 \pmod{m}$, and hence $c(t\alpha + u\beta) \equiv a \pmod{m}$, proving that c divides a in $\mathbb{Z}/m\mathbb{Z}$. $\square$

Proof of the "only if" part of Theorem 1.7. Assume $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is congruence preserving and consider its decomposition $f(x) = \sum_{k=0}^{n-1} a_k P_k(x)$ given by Proposition 1.6. We show that $\operatorname{lcm}(k)$ divides a_k in $\mathbb{Z}/m\mathbb{Z}$ for all $k < n$. The cases $k = 0$ and $k = 1$ are trivial since $\operatorname{lcm}(0) = \operatorname{lcm}(1) = 1$.

Claim 1. *For all $2 \leq k < n$, k divides a_k in $\mathbb{Z}/m\mathbb{Z}$.*

Proof. Recall that $f(k) = \sum_{i=0}^{n-1} a_i \binom{k}{i} = \sum_{i=0}^{k} a_i \binom{k}{i}$ since $\binom{k}{i} = 0$ for $i > k$. We argue by induction on $k \geq 2$.

`Base case` $k = 2$. If 2 does not divide m then 2 and m are coprime, and hence 2 is invertible and divides a_2 in $\mathbb{Z}/m\mathbb{Z}$. Assume 2 divides m. As 2 divides $2 - 0$ and f is congruence preserving, 2 also divides $f(2) - f(0) = 2a_1 + a_2$, and hence 2 divides a_2.

`Inductive step`. Let $2 < k < n - 1$. The inductive hypothesis ensures that ℓ divides a_ℓ in $\mathbb{Z}/m\mathbb{Z}$ for every $\ell \leq k$. Let $a_\ell \equiv \ell q_\ell \pmod{m}$ for $0 \leq \ell \leq k$. We prove that $k + 1$ divides a_{k+1} in $\mathbb{Z}/m\mathbb{Z}$. First, observe that

$$\begin{aligned} f(k+1) - f(0) &= (k+1)a_1 + \left(\sum_{i=2}^{k} \binom{k+1}{i} a_i\right) + a_{k+1} \\ &\equiv (k+1)a_1 + \left(\sum_{i=2}^{k} \binom{k+1}{i} i q_i\right) + a_{k+1} \pmod{m} \\ f(k+1) - f(0) &= (k+1)a_1 + \left(\sum_{i=2}^{k} (k+1) \binom{k}{i-1} q_i\right) + \alpha m + a_{k+1} \qquad (4) \end{aligned}$$

for some α. Let $d = gcd(k+1, m)$. Since d divides m and $k+1-0$ and f is congruence preserving, d also divides $f(k+1) - f(0)$. Using equality (4), we see that d divides the last term a_{k+1} of the sum. Using Bézout's identity, let u, v be such that $u(k+1) + vm = d$. Then $u(k+1) \equiv d \pmod{m}$, and hence $k+1$ divides d in $\mathbb{Z}/m\mathbb{Z}$. Since d divides a_{k+1}, we conclude that $k+1$ divides a_{k+1} in $\mathbb{Z}/m\mathbb{Z}$. $\square$

Claim 2. *(i) For all $2 \le p \le k < n$, p divides a_k in $\mathbb{Z}/m\mathbb{Z}$.*
(ii) For all $2 \le k < n$, $\mathrm{lcm}(k)$ divides a_k in $\mathbb{Z}/m\mathbb{Z}$.

Proof. Assertion *(ii)* is a direct application of Lemma 3.4 and assertion *(i)*. We prove *(i)* by induction on $p \ge 2$. Both the base case and the inductive step of this induction are proved by induction on k.

`Base case` $p = 2$. We have to prove that 2 divides a_k for all $k \ge 2$. If 2 does not divide m, then 2 is invertible and divides all numbers in $\mathbb{Z}/m\mathbb{Z}$. Assume now that 2 divides m. We argue by induction on $k \ge 2$.

`Base case.` Apply Claim 1: 2 divides a_2.

`Inductive step.` Let $k < n-1$. Assuming that 2 divides a_i for all $2 \le i \le k$, we prove that 2 divides a_{k+1}. Two cases can occur.

`Subcase 1:` $k+1$ `is odd.` Then 2 divides k and hence, by congruence preservation, 2 divides $f(k+1) - f(1)$. As $f(k+1) - f(1) = ka_1 + \left(\sum_{i=2}^{k} a_i \binom{k+1}{i}\right) + a_{k+1}$, and 2 divides k and also, by the induction hypothesis, 2 divides a_i for $2 \le i \le k$, we see that 2 divides a_{k+1}.

`Subcase 2:` $k+1$ `is even.` By congruence preservation, 2 divides $f(k+1) - f(0) = (k+1)a_1 + \left(\sum_{i=2}^{k} a_i \binom{k+1}{i}\right) + a_{k+1}$. Since 2 divides $k+1$ and a_i for $2 \le i \le k$ (induction hypothesis), we infer that 2 divides a_{k+1}.

`Inductive step`. Let $2 \le p < n-1$ and assume that

$$\text{for all } q \le p \text{ and all } \ell \text{ such that } q \le \ell < n,\ q \text{ divides } a_\ell \text{ in } \mathbb{Z}/m\mathbb{Z}. \tag{5}$$

By induction on $k \ge p+1$, we prove that $p+1$ divides a_k for all k such that $p+1 \le k < n$.

`Base case` $k = p+1$. Apply Claim 1: $p+1$ divides a_{p+1}.

`Inductive step.` Let $k < n-1$. Assuming that $p+1$ divides a_i in $\mathbb{Z}/m\mathbb{Z}$ for all i

such that $p+1 \leq i \leq k$, we prove that $p+1$ divides a_{k+1} in $\mathbb{Z}/m\mathbb{Z}$. We have

$$f(k+1) - f(k-p) = \sum_{i=1}^{k-p} a_i \left(\binom{k+1}{i} - \binom{k-p}{i} \right) + \left(\sum_{i=k+1-p}^{k} a_i \binom{k+1}{i} \right) + a_{k+1} \quad (6)$$

We first look at the terms of the first sum on the right side of (6) corresponding to $1 \leq i \leq p$. Applying (5) with $\ell = i$, we see that q divides a_i in $\mathbb{Z}/m\mathbb{Z}$ for all $q \leq \min(p, i) = i$. Using Lemma 3.4, we conclude that $\mathrm{lcm}(i)$ divides a_i in $\mathbb{Z}/m\mathbb{Z}$. Observing that $(k+1) = (k-p)+(p+1)$, we can apply Lemma 3.2 (with $k-p$, $p+1$ and i in place of b, n and k) and conclude that $p+1$ divides $\mathrm{lcm}(i)\left(\binom{k+1}{i} - \binom{k-p}{i}\right)$ in $\mathbb{N}$. Thus, $p+1$ divides $a_i\left(\binom{k+1}{i} - \binom{k-p}{i}\right)$ in $\mathbb{Z}/m\mathbb{Z}$.

We now turn to the terms of the first sum on the right side of (6) corresponding to $p+1 \leq i \leq k-p$ (if there are any). Each of these terms is divisible by $p+1$ in $\mathbb{Z}/m\mathbb{Z}$, because the induction hypothesis on k ensures that $p+1$ divides a_i in $\mathbb{Z}/m\mathbb{Z}$ whenever $p+1 \leq i \leq k$.

Consider next the terms of the second sum on the right side of (6). For those terms corresponding to values of i such that $p+1 \leq i \leq k$, divisibility by $p+1$ in $\mathbb{Z}/m\mathbb{Z}$ follows from the fact that, by the induction hypothesis on k, $p+1$ divides a_i. It remains to look at the terms associated with the i's such that $k+1-p \leq i \leq p$ (there are such i's in case $k+1-p < p+1$). For such i's we have $0 \leq (k+1)-i \leq (k+1)-p < p+1 \leq k+1$ and Lemma 3.1 (used with $k+1, i$ and $p+1$ in place of n, k and p) implies that $p+1$ divides $\mathrm{lcm}(i)\binom{k+1}{i}$. Now, for such i's, the induction hypothesis (5) on p shows that $\mathrm{lcm}(i)$ divides a_i in $\mathbb{Z}/m\mathbb{Z}$. A fortiori, $p+1$ divides $a_i\binom{k+1}{i}$ in $\mathbb{Z}/m\mathbb{Z}$.

Let $d = gcd(p+1, m)$. As $p+1$ divides in $\mathbb{Z}/m\mathbb{Z}$ all terms of the two sums on the right side of (6) so does d. Since d divides m and $k+1-(k-p) = p+1$ and f is congruence preserving, d also divides $f(k+1) - f(k-p)$. Using equality (6), we conclude that d divides in $\mathbb{Z}/m\mathbb{Z}$ the last term a_{k+1}. Using Bézout's identity, let u, v be such that $u(p+1) + vm = d$. Then $u(p+1) \equiv d \pmod{m}$, and hence $p+1$ divides d in $\mathbb{Z}/m\mathbb{Z}$. As d divides a_{k+1} in $\mathbb{Z}/m\mathbb{Z}$, we conclude that $p+1$ divides a_{k+1} in $\mathbb{Z}/m\mathbb{Z}$.

This ends the proof of the induction in the inductive step, and hence also the proof of Claim 2 and of the "only if" part of the Theorem. □

Proof of the "if" part of Theorem 1.7. Assume $f = \sum_{k=0}^{k=n-1} a_k P_k$ and that all of the a_k's are divisible by $lcm(k)$ in $\mathbb{Z}/m\mathbb{Z}$. We can write f in the form $f(n) = \sum_{k=0}^{n} c_k \mathrm{lcm}(k) \binom{n}{k}$. We prove that f is congruence preserving, i.e., if $0 \leq b < a \leq$

$n-1$ and d divides both m and $a-b$ then d also divides $f(a)-f(b)$. Observe that

$$f(a)-f(b)=\left(\sum_{k=0}^{b} c_k \mathrm{lcm}(k)\left(\binom{a}{k}-\binom{b}{k}\right)\right)+\sum_{k=b+1}^{a} c_k \mathrm{lcm}(k)\binom{a}{k}.$$

By Lemma 3.3, $a-b$ divides each term of the first sum. Consider the terms of the second sum. For $b+1 \leq k \leq a$, we have $0 \leq a-k < a-b \leq a$ and Lemma 3.1 (used with a, k and $a-b$ in place of n, k and p) shows that $a-b$ divides $\mathrm{lcm}(k)\binom{a}{k}$. Thus, $a-b$ divides $f(a)-f(b)$. □

3.2. On a Family of Generators

We now sharpen the degree of the rat-polynomial representing a congruence preserving function $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$. We first state some properties of the lcm function in $\mathbb{N}$.

Lemma 3.5. *Let $m \geq 1$ be an integer with prime factorization $m = p_1^{\alpha_1} \cdots p_\ell^{\alpha_\ell}$. Then $\mathrm{lcm}(k) = u \prod_{i=1}^{\ell} p_i^{\alpha_{i,k}}$, where u is coprime with m and $\alpha_{i,k} = \max\{\beta_i \mid p_i^{\beta_i} \leq k\}$.*

Definition 3.6. Let $m \geq 1$ be an integer with prime factorization $m = p_1^{\alpha_1} \cdots p_\ell^{\alpha_\ell}$. We let $gpp(m) = \max\left\{p_i^{\alpha_i} \mid i \in \{1, \ldots, \ell\}\right\}$ be the greatest power of prime dividing m in $\mathbb{N}$.

Lemma 3.7. *The number $gpp(m)$ is the least integer k such that m divides $\mathrm{lcm}(k)$.*

Example 3.8. We have $gpp(8) = 8$, $gpp(12) = 4$ and $gpp(14) = 7$. The successive values of the residues in $\mathbb{Z}/m\mathbb{Z}$ of $\mathrm{lcm}(k)$ are

k	1	2	3	4	5	6	7	8
$\mathrm{lcm}(k)$ in $\mathbb{Z}/8\mathbb{Z}$	1	2	2	4	4	4	4	0
$\mathrm{lcm}(k)$ in $\mathbb{Z}/12\mathbb{Z}$	1	2	6	0	0	0	0	0
$\mathrm{lcm}(k)$ in $\mathbb{Z}/14\mathbb{Z}$	1	2	6	12	4	4	0	0

.

For all $\ell \geq gpp(m)$, $\mathrm{lcm}(\ell)$ is zero in $\mathbb{Z}/m\mathbb{Z}$.

Remark 3.9. 1. Either $gpp(m) = m$ or $gpp(m) \leq m/2$.
2. In general, $gpp(m)$ is greater than $\lambda(m)$, the least k such that m divides $k!$ (a function considered in [3]): for $m = 8$, $gpp(m) = 8$ whereas $\lambda(m) = 4$.

Using Lemma 3.7, we can get a better version of Theorem 1.7.

Theorem 3.10. *A function $f\colon \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is congruence preserving if and only if it is associated in the sense of Definition 1.5 with a rational polynomial $P = \sum_{k=0}^{d-1} a_k \binom{x}{k}$ where $d = \min(n, gpp(m))$ and such that lcm(k) divides a_k in $\mathbb{Z}/m\mathbb{Z}$ for all $k < d$.*

Proof. For $k \geq gpp(m)$, m divides $lcm(k)$ hence the coefficient a_k is 0. $\square$

Theorem 3.11. *(i) Every congruence preserving function $f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is rat-polynomial with degree less than $gpp(m)$.*
(ii) The family of rat-polynomial functions

$$\mathcal{F} = \{lcm(k)P_k \mid 0 \leq k < \min(n, gpp(m))\}$$

generates the set of congruence preserving functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$.
(iii) $\mathcal{F}$ is a basis of the set of congruence preserving functions if and only if m has no prime divisor $p < \min(n, m)$ (in case $n \geq m$ this means that m is prime).

Proof. Assertions *(i)* and *(ii)* are restatements of Theorem 3.10. Let us prove *(iii)*.

"Only If" part. Asssume m has a prime divisor $p < \min(n, m)$ and let p be the least one. Then $\mathrm{lcm}(p) = pa$ with a coprime with m, and hence $\mathrm{lcm}(p) \neq 0$ in $\mathbb{Z}/m\mathbb{Z}$. Since $P_p(p) = 1$ this shows that $\mathrm{lcm}(p)\, P_p$ is not the null function. However $(m/p)\,\mathrm{lcm}(p) = 0$ in $\mathbb{Z}/m\mathbb{Z}$, and hence $(m/p)\,\mathrm{lcm}(p)\, P_p$ is the null function. As $(m/p) \neq 0$ in $\mathbb{Z}/m\mathbb{Z}$, this proves that $\mathcal{F}$ cannot be a basis.

"If" part. Assume that m has no prime divisor $p < \min(n, m)$. We prove that $\mathcal{F}$ is $(\mathbb{Z}/m\mathbb{Z})$-linearly independent. Suppose that the $(\mathbb{Z}/m\mathbb{Z})$-linear combination $L = \sum_{k=0}^{\min(n,gpp(m))-1} a_k\,\mathrm{lcm}(k)\, P_k$ is the null function $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$. By induction on $k = 0, \ldots, \min(n, gpp(m)) - 1$ we prove that $a_k = 0$.

- *Basic cases* $k = 0, 1$. From $L(0) = a_0$ and $L(1) = a_0 + a_1$ we deduce $a_0 = a_1 = 0$.
- *Induction step.* Assuming $k \geq 2$ and $a_i = 0$ for $i = 0, \ldots, k-1$, we prove that $a_k = 0$. Observe that $P_\ell(k) = \binom{k}{\ell} = 0$ for $k < \ell < n$. Since $a_i = 0$ for $i = 0, \ldots, k-1$, and $P_k(k) = 1$ we get $L(k) = a_k\,\mathrm{lcm}(k\,)$. As $k < \min(n, gpp(m)) \leq \min(n, m)$ and m has no prime divisor $p < \min(n, m)$, the numbers $\mathrm{lcm}(k)$ and m are coprime. Thus, $\mathrm{lcm}(k)$ is invertible in $\mathbb{Z}/m\mathbb{Z}$ and equality $L(k) = a_k\,\mathrm{lcm}(k) = 0$ implies $a_k = 0$. $\square$

4. Counting Congruence Preserving Functions

We now compute the number of congruence preserving functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$. As two different rational polynomials correspond to different functions by Proposition 1.6 (uniqueness of the representation by a rational polynomial), the number of congruence preserving functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is equal to the number of polynomials representing them.

Proposition 4.1. *Let $CP(n, m)$ be the number of congruence preserving functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$. Let $m = p_1^{e_1} p_2^{e_2} \cdots p_\ell^{e_\ell}$ be the decomposition of m in powers of* *primes. Let* $\mathcal{I} = \{i \mid p_i^{e_i} < gpp(m)\}$ *and* $\mathcal{J} = \{i \mid p_i^{e_i} \geq gpp(m)\}$. *Then*

$$CP(n,m) = \begin{cases} p_1^{p_1+p_1^2+\cdots+p_1^{e_1}} \times \cdots \times p_\ell^{p_\ell+p_\ell^2+\cdots+p_\ell^{e_\ell}} & \text{if } n \geq gpp(m), \\ \prod_{i\in\mathcal{I}} p_i^{p_i+p_i^2+\cdots+p_i^{e_i}} \times \prod_{i\in\mathcal{J}} p_i^{p_i+p_i^2+\cdots+p_i^{\lfloor \log_p n\rfloor}+n(e-\lfloor \log_p n\rfloor)} & \text{if } n < gpp(m). \end{cases}$$

Equivalently, writing $E(p,\alpha)$ *instead of* p^α *for better readability, we have*

$$CP(n,m) = \begin{cases} \prod_{i=1}^{\ell} E(p_i, \sum_{k=1}^{e_i} p_i^k) & \text{if } n \geq gpp(m), \\ \prod_{i\in\mathcal{I}} E(p_i, \sum_{k=1}^{e_i} p_i^k) \times \prod_{i\in\mathcal{J}} E(p_i, (\sum_{k=1}^{\lfloor \log_p n\rfloor} p_i^k) + n(e - \lfloor \log_p n\rfloor)) & \text{if } n < gpp(m). \end{cases}$$

Corollary 4.2. *For* $n \geq gpp(m)$, $CP(n,m)$ *does* not *depend on* n.

Proof of Proposition 4.1. By Theorem 3.10, we must count the number of n-tuples of coefficients $(a_0,\ldots,a_{n-1})$, with, for $k = 0,\ldots,n-1$, a_k being a multiple of $lcm(k)$ in $\mathbb{Z}/m\mathbb{Z}$.

Claim 1. *For* $m = p_1^{e_1}p_2^{e_2}\cdots p_\ell^{e_\ell}$, *for all* n, $CP(n,m) = \prod_{i=1}^{\ell} CP(n,p_i^{e_i})$.

Proof of Claim 1. Let $E(r,k)$ be the set of multiples in $\mathbb{Z}/r\mathbb{Z}$ of $\mathrm{lcm}(k)$ and $\lambda(r,k)$ be the cardinal of $E(r,k)$. The Chinese remainder theorem shows that the map $\rho : z \mapsto \big(z \pmod{p_i^{e_i}}\big)_{i=1,\ldots,\ell}$ is an isomorphism and also that ρ maps the set $E(m,k)$ onto the Cartesian product $P = \prod_{i=1}^{\ell} E(p_i^{e_i},k)$. Indeed, let $(t_i)_{i=1,\ldots,\ell} \in P$. For each $i = 1,\ldots,\ell$, there is $0 \leq q_i < p_i^{e_i}$ such that $t_i \equiv q_i\,\mathrm{lcm}(k) \pmod{p_i^{e_i}}$. Applying the Chinese remainder theorem, there are $0 \leq t,q < m$ such that $t \equiv t_i \pmod{p_i^{e_i}}$ and $q \equiv q_i \pmod{p_i^{e_i}}$. Then $t \equiv q\,\mathrm{lcm}(k) \pmod{m}$, and hence $\rho(t) = (t_i)_{i=1,\ldots,\ell}$. This proves that $\lambda(m,k) = \prod_{i=1}^{\ell} \lambda(p_i^{e_i},k)$ for each k. Thus, the number $CP(n,m)$ of n-tuples $(a_0,\ldots,a_{n-1})$ such that $lcm(k)$ divides a_k is equal to

$$CP(n,m) = \prod_{k<n} \lambda(m,k) = \prod_{k<n}\prod_{i=1}^{\ell} \lambda(p_i^{e_i},k) = \prod_{i=1}^{\ell}\prod_{k<n} \lambda(p_i^{e_i},k) = \prod_{i=1}^{\ell} CP(n,p_i^{e_i}). \quad \square$$

Claim 1 reduces the problem to that of counting the congruence preserving functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/p_i^{e_i}\mathbb{Z}$. We will use Theorem 3.10 to this end.

Claim 2. *Letting* $\ell = \lfloor \log_p n\rfloor$ *(and using the* $E(p,\alpha)$ *notation for* p^α*), we have*

$$CP(n,p^e) = \begin{cases} E(p, p+p^2+\cdots+p^e) & \text{if } n \geq p^e, \\ E(p, p+p^2+\cdots+p^\ell + (e-\ell)n) & \text{if } p^\ell \leq n < p^e. \end{cases}$$

Proof of Claim 2. By Theorem 3.10, as $gpp(p^e) = p^e$, letting $\nu = \inf(n,p^e)$, we have $CP(n,p^e) = CP(\nu,p^e) = \prod_{k=0}^{\nu-1} \lambda(p^e,k)$. As we noted in the proof of Claim 1, for

$p^j \le k < p^{j+1}$, the order $\lambda(p^e,k)$ of the subgroup generated by $lcm(k)$ in $\mathbb{Z}/p^e\mathbb{Z}$ is p^{e-j}, and there are $p^{j+1}-p^j$ such k's. For $k=0$, $\mathrm{lcm}(0)=1$ yields $\lambda(p^e,0)=p^e$.

• If $n \ge p^e$ then $CP(n,p^e) = CP(p^e,p^e) = p^e \prod_{j=0}^{e-1}\prod_{k=p^j}^{p^{j+1}-1} p^{e-j} = p^M$ with

$$M \quad = \quad e + \sum_{j=0}^{e-1}(e-j)(p^{j+1}-p^j) = p + p^2 + \cdots + p^e$$

• If $n < p^e$ then $p^\ell \le n < p^e$ and

$$\begin{aligned}
CP(n,p^e) &= \textstyle\prod_{k=0}^{n-1}\lambda(p^e,k) \\
&= p^e(\textstyle\prod_{j=0}^{\ell-1}\prod_{k=p^j}^{p^{j+1}-1} p^{e-j})(\prod_{k=p^\ell}^{n-1} p^{e-\ell}) = p^M \text{ with} \\
M &= e + \sum_{j=0}^{\ell-1}(e-j)(p^{j+1}-p^j) + \sum_{k=p^\ell}^{n-1}(e-\ell) \\
&= (e-\ell)p^\ell + (p+p^2+\cdots+p^\ell) + (n-p^\ell)(e-\ell) \\
&= (p+p^2+\cdots+p^\ell) + n(e-\ell) \qquad \square
\end{aligned}$$

This finishes the proof of Proposition 4.1. $\square$

Remark 4.3. In [1] the number of congruence preserving functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/p^e\mathbb{Z}$ is shown to be equal to $E(p, en - \sum_{k=1}^{n-1}\min\{e, \lfloor \log_p k\rfloor\})$. For $p^i \le k < p^{i+1}$, we have $\lfloor \log_p k\rfloor = i$, and hence $\min\{e, \lfloor \log_p k\rfloor\} = \lfloor \log_p k\rfloor$ for $k \le p^e$, and $\min\{e, \lfloor \log_p k\rfloor\} = e$ for $k \ge p^e$. Thus, we have

• if $n \ge p^e$, then
$\sum_{k=1}^{n-1}\min\{e, \lfloor \log_p k\rfloor\} = \sum_{k=1}^{p^e-1}\lfloor \log_p k\rfloor + \sum_{k=p^e}^{n-1} e = \sum_{j=0}^{e-1} j(p^{j+1}-p^j) + e(n-p^e)$ $= -(p+\cdots+p^e)+ep^e+e(n-p^e)$, and hence $en-\sum_{k=1}^{n-1}\min\{e, \lfloor \log_p k\rfloor\} = p+\cdots+p^e$. This coincides with our counting in Claim 2.

• if $n < p^e$, and $l = \lfloor \log_p n\rfloor$, then, similarly,
$\sum_{k=1}^{n-1}\lfloor \log_p k\rfloor = \sum_{k=1}^{\ell-1}\lfloor \log_p k\rfloor + \sum_{k=l}^{n-1}\lfloor \log_p k\rfloor = \sum_{j=0}^{\ell-1} j(p^{j+1}-p^j) + \ell(n-p^\ell) =$ $-(p+\cdots+p^\ell)+n\ell$, and hence $en - \sum_{k=1}^{n-1}\lfloor \log_p k\rfloor = p+\cdots+p^\ell+(e-\ell)n$. Again, this coincides with our counting in Claim 2.

5. Conclusion

We proved that the rational polynomials $\mathrm{lcm}(k)\,P_k$ generate the $\mathbb{Z}/m\mathbb{Z}$ submodule of congruence preserving functions $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$. When n is larger than the greatest prime power dividing m, the number of functions in this submodule is independent of n. An open problem is the existence of a basis of this submodule.

Acknowledgments. We are grateful to the anonymous referee for insightful reading and valuable comments which helped improve the paper. We are also thankful to the managing editor Bruce Landman whose advices improved the English, the typographic style, and the general readability.

References

[1] M. Bhargava, Congruence preservation and polynomial functions from $\mathbb{Z}_n$ to $\mathbb{Z}_m$, *Discrete Math.* **173** (1997), 15–21.

[2] P. Cégielski, S. Grigorieff, I. Guessarian, Newton expansion of functions over natural integers having integral difference ratios, *Int. J. Number Theory*, **11 No 7** (2015), 2109–2139.

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

[4] A.J. Kempner, Polynomials and their residue systems, *Amer. Math. Soc. Trans.* **22** (1921), 240–288.

[5] G. Pólya, Über ganzwertige ganze Funktionen, *Rend. Circ. Mat. Palermo* **40** (1915), 1–16.