

Article

Polyadic Rings of P -adic Integers

Steven Duplij

Center for Information Technology (WWU IT), Universität Münster, Röntgenstrasse 7-13
D-48149 Münster, Deutschland

MSC: 17A42; 20N15; 11A07; 11S31

Abstract. In this note we, first, recall that the sets of all representatives of some special ordinary residue classes become (m, n) -rings. Second, we introduce a possible p -adic analog of the residue class modulo a p -adic integer. Then, we find the relations which determine, when the representatives form a (m, n) -ring.

Keywords: polyadic semigroup, polyadic ring, arity, querelement, residue class, representative, p -adic integer

1. INTRODUCTION

The fundamental conception of p -adic numbers is based on a special extension of rational numbers which is alternative to the real and complex numbers. The main idea is a completion of rational numbers with respect to the p -adic norm, which is non-Archimedean. Nowadays, p -adic methods are widely used in number theory [1,2] and arithmetic geometry [3,4], mathematical physics [5,6] and algorithmic computations [7]. For general reviews, see [8–10].

We have found that in the study of p -adic integers some polyadic structures, that is (m, n) -rings, can appear naturally, if we introduce informally a p -adic analog of the residue classes for ordinary integers and investigate the set of its representatives along the lines of [11–13].

2. (m, n) -RINGS OF INTEGER NUMBERS FROM RESIDUE CLASSES

Here we recall that representatives of special residue (congruence) classes can form polyadic rings, as was found in [11,12] (see also notation from [13]).

Let us denote the residue (congruence) class of an integer a modulo b by

$$[a]_b = \{\{r_k(a, b)\} \mid k \in \mathbb{Z}, a \in \mathbb{Z}_+, b \in \mathbb{N}, 0 \leq a \leq b - 1\}, \quad (2.1)$$

where $r_k(a, b) = a + bk$ is a generic representative element of the class $[a]_b$. The canonical representative is the least nonnegative number among these. Informally, a is the remainder of $r_k(a, b)$ when divided by b . The corresponding equivalence relation (congruence modulo b) is denoted by

$$r = a \pmod{b}. \quad (2.2)$$

Introducing the binary operations between classes $(+_{cl}, \times_{cl})$, the addition $[a_1]_b +_{cl} [a_2]_b = [a_1 + a_2]_b$ and multiplication $[a_1]_b \times_{cl} [a_2]_b = [a_1 a_2]_b$, the residue class (binary) finite commutative ring $\mathbb{Z}/b\mathbb{Z}$ (with identity) is defined in the standard way (which was named “external” [11]). If $a \neq 0$ and b is prime, then $\mathbb{Z}/b\mathbb{Z}$ becomes a finite field.

The set of representatives $\{r_k(a, b)\}$ in a given class $[a]_b$ does not form a binary ring, because there are no binary operations (addition and multiplication) which are simultaneously closed for arbitrary a and b . Nevertheless, the following polyadic operations on representatives $r_k = r_k(a, b)$, m -ary addition ν_m

$$\nu_m[r_{k_1}, r_{k_2}, \dots, r_{k_m}] = r_{k_1} + r_{k_2} + \dots + r_{k_m}, \quad (2.3)$$

and n -ary multiplication μ_n

$$\mu_n[r_{k_1}, r_{k_2}, \dots, r_{k_n}] = r_{k_1} r_{k_2} \dots r_{k_n}, \quad r_{k_i} \in [a]_b, \quad k_i \in \mathbb{Z}, \quad (2.4)$$

can be closed, but only for special values of $a = a_q$ and $b = b_q$, which defines the nonderived (m, n) -ary ring

$$\mathbb{Z}_{(m,n)}(a_q, b_q) = \left\langle [a_q]_{b_q} \mid \nu_m, \mu_n \right\rangle \quad (2.5)$$

of polyadic integers (that was called the “internal” way [11]). The conditions of closure for the operations between representatives can be formulated in terms of the (arity shape [12]) invariants (which may be seen as some kind of “quantization”)

$$(m-1) \frac{a_q}{b_q} = I_m(a_q, b_q) \in \mathbb{N}, \quad (2.6)$$

$$a_q^{n-1} \frac{a_q - 1}{b_q} = J_n(a_q, b_q) \in \mathbb{N}, \quad (2.7)$$

or, equivalently, using the congruence relations [11]

$$ma_q \equiv a_q \pmod{b_q}, \quad (2.8)$$

$$a_q^n \equiv a_q \pmod{b_q}, \quad (2.9)$$

where we have denoted by a_q and b_q the concrete solutions of the “quantization” equations (2.6)–(2.9). The arity shape of the ring of polyadic integers $\mathbb{Z}_{(m,n)}(a_q, b_q)$ (2.5) is the (surjective) mapping

$$(a_q, b_q) \implies (m, n). \quad (2.10)$$

The mapping (2.10) for the lowest values of a_q, b_q is given in TABLE 1 ($I = I_m(a_q, b_q)$, $J = J_n(a_q, b_q)$). 26

Table 1. The arity shape mapping (2.10) for the polyadic ring $\mathbb{Z}_{(m,n)}(a_q, b_q)$ (2.5).

| $a_q \setminus b_q$ | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---------------------|--|--|--|---|---|---|---|--|--|
| 1 | $m = 3$ $n = 2$ $I = 1$ $J = 0$ | $m = 4$ $n = 2$ $I = 1$ $J = 0$ | $m = 5$ $n = 2$ $I = 1$ $J = 0$ | $m = 6$ $n = 2$ $I = 1$ $J = 0$ | $m = 7$ $n = 2$ $I = 1$ $J = 0$ | $m = 8$ $n = 2$ $I = 1$ $J = 0$ | $m = 9$ $n = 2$ $I = 1$ $J = 0$ | $m = 10$ $n = 2$ $I = 1$ $J = 0$ | $m = 11$ $n = 2$ $I = 1$ $J = 0$ |
| 2 | | $m = 4$ $n = 3$ $I = 2$ $J = 2$ | | $m = 6$ $n = 5$ $I = 2$ $J = 6$ | $m = 4$ $n = 3$ $I = 1$ $J = 1$ | $m = 8$ $n = 4$ $I = 2$ $J = 2$ | | $m = 10$ $n = 7$ $I = 2$ $J = 14$ | $m = 6$ $n = 5$ $I = 1$ $J = 3$ |
| 3 | | | $m = 5$ $n = 3$ $I = 3$ $J = 6$ | $m = 6$ $n = 5$ $I = 3$ $J = 48$ | $m = 3$ $n = 2$ $I = 1$ $J = 1$ | $m = 8$ $n = 7$ $I = 3$ $J = 312$ | $m = 9$ $n = 3$ $I = 3$ $J = 3$ | | $m = 11$ $n = 5$ $I = 3$ $J = 24$ |
| 4 | | | | $m = 6$ $n = 4$ $I = 4$ $J = 12$ | $m = 4$ $n = 2$ $I = 2$ $J = 2$ | $m = 8$ $n = 4$ $I = 4$ $J = 36$ | | $m = 10$ $n = 4$ $I = 4$ $J = 28$ | $m = 6$ $n = 3$ $I = 2$ $J = 6$ |
| 5 | | | | | $m = 7$ $n = 3$ $I = 5$ $J = 20$ | $m = 8$ $n = 7$ $I = 11$ $J = 11160$ | $m = 9$ $n = 3$ $I = 5$ $J = 15$ | $m = 10$ $n = 7$ $I = 5$ $J = 8680$ | $m = 3$ $n = 2$ $I = 1$ $J = 2$ |
| 6 | | | | | | $m = 8$ $n = 3$ $I = 6$ $J = 30$ | | | $m = 6$ $n = 2$ $I = 3$ $J = 3$ |
| 7 | | | | | | | $m = 9$ $n = 3$ $I = 7$ $J = 42$ | $m = 10$ $n = 4$ $I = 7$ $J = 266$ | $m = 11$ $n = 5$ $I = 7$ $J = 1680$ |
| 8 | | | | | | | | $m = 10$ $n = 3$ $I = 8$ $J = 56$ | $m = 6$ $n = 5$ $I = 4$ $J = 3276$ |
| 9 | | | | | | | | | $m = 11$ $n = 3$ $I = 9$ $J = 72$ |

The binary ring of ordinary integers \mathbb{Z} corresponds to $(a_q = 0, b_q = 1) \implies (2, 2)$ or $\mathbb{Z} = \mathbb{Z}_{(2,2)}(0, 1)$, $I = J = 0$. 27
28

3. REPRESENTATIONS OF p -ADIC INTEGERS

Let us explore briefly some well-known definitions regarding p -adic integers to establish notations (for reviews, see [8,9,14]).

A p -adic integer is an infinite formal sum of the form

$$x = x(p) = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \dots + \alpha_{i-1} p^{i-1} + \alpha_i p^i + \alpha_{i+1} p^{i+1} + \dots, \quad \alpha_i \in \mathbb{Z}, \quad (3.1)$$

where the digits (denoted by Greek letters from the beginning of alphabet) $0 \leq \alpha_i \leq p - 1$, and $p \geq 2$ is a fixed prime number. The expansion (3.1) is called standard (or canonical), and α_i are the p -adic digits which are usually written from the right to the left (positional notation) $x = \dots \alpha_{i+1} \alpha_i \alpha_{i-1} \dots \alpha_2 \alpha_1 \alpha_0$ or sometimes $x = \{\alpha_0, \alpha_1, \alpha_2, \dots, \alpha_{i-1}, \alpha_i, \alpha_{i+1}, \dots\}$. The set of p -adic integers is a commutative ring (of p -adic integers) denoted by $\mathbb{Z}_p = \{x\}$, and the ring of ordinary integers (sometimes called “rational” integers) \mathbb{Z} is its (binary) subring.

The so called coherent representation of \mathbb{Z}_p is based on the (inverse) projective limit of finite fields $\mathbb{Z}/p^l \mathbb{Z}$, because the surjective map $\mathbb{Z}_p \rightarrow \mathbb{Z}/p^l \mathbb{Z}$ defined by

$$\alpha_0 + \alpha_1 p + \alpha_2 p^2 + \dots + \alpha_i p^i + \dots \mapsto (\alpha_0 + \alpha_1 p + \alpha_2 p^2 + \dots + \alpha_{i-1} p^{i-1}) \bmod p^i \quad (3.2)$$

is a ring homomorphism. In this case, a p -adic integer is the infinite Cauchy sequence that converges to

$$x = x(p) = \{x_i(p)\}_{i=1}^{\infty} = \{x_1(p), x_2(p), \dots, x_i(p), \dots\}, \quad (3.3)$$

where

$$x_i(p) = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \dots + \alpha_{i-1} p^{i-1} \quad (3.4)$$

with the coherency condition

$$x_{i+1}(p) \equiv x_i(p) \bmod p^i, \quad \forall i \geq 1, \quad (3.5)$$

and the p -adic digits are $0 \leq \alpha_i \leq p - 1$.

If $0 \leq x_i(p) \leq p^i - 1$ for all $i \geq 1$, then the coherent representation (3.3) is called reduced. The ordinary integers $x \in \mathbb{Z}$ embed into p -adic integers as constant infinite sequences by $x \mapsto \{x, x, \dots, x, \dots\}$.

Using the fact that the process of reducing modulo p^i is equivalent to vanishing the last i digits, the coherency condition (3.5) leads to a sequence of partial sums [14]

$$x = x(p) = \{y_i(p)\}_{i=1}^{\infty} = \{y_1(p), y_2(p), \dots, y_i(p), \dots\}, \quad (3.6)$$

where

$$y_1(p) = \alpha_0, \quad y_2(p) = \alpha_0 + \alpha_1 p, \quad y_3(p) = \alpha_0 + \alpha_1 p + \alpha_2 p^2, \quad y_4(p) = \alpha_0 + \alpha_1 p + \alpha_2 p^2 + \alpha_3 p^3, \quad \dots \quad (3.7)$$

Sometimes the partial sum representation (3.6) is simpler for p -adic integer computations.

4. (m, n) -RINGS OF p -ADIC INTEGERS

As may be seen from SECTION 2 and [11,12], the construction of the nonderived (m, n) -rings of ordinary (“rational”) integers $\mathbb{Z}_{(m,n)}(a_q, b_q)$ (2.5) can be done in terms of residue class representatives (2.1). To introduce a p -adic analog of the residue class (2.1), one needs some ordering concept, which does not exist for p -adic integers [14]. Nevertheless, one could informally define the following analog of ordering,

Definition 1. A “componentwise strict order” $<_{\text{comp}}$ is a multicomponent binary relation between p -adic numbers $\mathbf{a} = \{\alpha_i\}_{i=0}^{\infty}$, $0 \leq \alpha_i \leq p-1$ and $\mathbf{b} = \{\beta_i\}_{i=0}^{\infty}$, $0 \leq \beta_i \leq p-1$, such that

$$\mathbf{a} <_{\text{comp}} \mathbf{b} \iff \alpha_i < \beta_i, \text{ for all } i = 0, \dots, \infty, \mathbf{a}, \mathbf{b} \in \mathbb{Z}_p, \alpha_i, \beta_i \in \mathbb{Z}. \quad (4.1)$$

A “componentwise nonstrict order” \leq_{comp} is defined in the same way, but using the nonstrict order \leq for component integers from \mathbb{Z} (digits). 52
53

Using this definition we can define a p -adic analog of the residue class informally by changing \mathbb{Z} to \mathbb{Z}_p in (2.1). 54
55

Definition 2. A p -adic analog of the residue class of \mathbf{a} modulo \mathbf{b} is

$$[\mathbf{a}]_{\mathbf{b}} = \{ \{r_k(\mathbf{a}, \mathbf{b})\} \mid \mathbf{a}, \mathbf{b}, k \in \mathbb{Z}_p, 0 \leq \mathbf{a} < \mathbf{b} \}, \quad (4.2)$$

and the generic representative of the class is

$$r_k(\mathbf{a}, \mathbf{b}) = \mathbf{a} +_p \mathbf{b} \bullet_p k, \quad (4.3)$$

where $+_p$ and \bullet_p are the binary sum and the binary product of p -adic integers (we treat them componentwise in the partial sum representation (3.7)), and the i th component of (4.3) r.h.s. is computed by $\text{mod } p^i$. 56
57
58

As with the ordinary (“rational”) integers (2.1), the p -adic integer \mathbf{a} can be treated as some kind of remainder for the representative $r_k(\mathbf{a}, \mathbf{b})$ when divided by the p -adic integer \mathbf{b} . We denote the corresponding p -adic analog of (2.2) (informally, a p -adic analog of the congruence modulo \mathbf{b}) as

$$\mathbf{r} = \mathbf{a} (\text{Mod}_p \mathbf{b}). \quad (4.4)$$

Remark 1. In general, to build a nonderived (m, n) -ring along the lines of SECTION 2, we do not need any analog of the residue class at all, but only the concrete form of the representative (4.3). Then demanding the closure of m -ary addition (2.3) and n -ary multiplication (2.4), we obtain conditions on the parameters (now digits of p -adic integers), similarly to (2.6)–(2.7). 59
60
61
62

In the partial sum representation (3.6), the case of ordinary (“rational”) integers corresponds to the first component (first digit α_0) of the p -adic integer (3.7), and higher components can be computed using the explicit formulas for sum and product of p -adic integers [15]. Because they are too cumbersome, we present here the “block-schemes” of the computations, while concrete examples can be obtained componentwise using (3.7). 63
64
65
66
67

Lemma 1. The p -adic analog of the residue class (4.2) is a commutative m -ary group $\langle [\mathbf{a}]_{\mathbf{b}} \mid \mathbf{v}_m \rangle$, if

$$(m-1)\mathbf{a} = \mathbf{b} \bullet_p \mathbf{I}, \quad (4.5)$$

where \mathbf{I} is a p -adic integer (addition shape invariant), and the nonderived m -ary addition \mathbf{v}_m is the repeated binary sum of m representatives $\mathbf{r}_k = r_k(\mathbf{a}, \mathbf{b})$

$$\mathbf{v}_m [\mathbf{r}_{k_1}, \mathbf{r}_{k_2}, \dots, \mathbf{r}_{k_m}] = \mathbf{r}_{k_1} +_p \mathbf{r}_{k_2} +_p \dots +_p \mathbf{r}_{k_m}. \quad (4.6)$$

Proof. The condition of closure for the m -ary addition \mathbf{v}_m is $\mathbf{r}_{k_1} +_p \mathbf{r}_{k_2} +_p \dots +_p \mathbf{r}_{k_m} = \mathbf{r}_{k_0}$ in the notation of (4.2). Using (4.3) it gives $m\mathbf{a} + \mathbf{b} \bullet_p (k_1 +_p k_2 +_p \dots +_p k_m) = \mathbf{a} +_p \mathbf{b} \bullet_p k_0$, which is equivalent to (4.5), where $\mathbf{I} = k_0 -_p (k_1 +_p k_2 +_p \dots +_p k_m)$. The querelement $\mathbf{r}_{\bar{k}}$ [16] satisfies

$$\mathbf{v}_m [\mathbf{r}_k, \mathbf{r}_k, \dots, \mathbf{r}_k, \mathbf{r}_{\bar{k}}] = \mathbf{r}_k, \quad (4.7)$$

which has a unique solution $\bar{k} = (2-m)k - \mathbf{I}$. Therefore, each element of $[\mathbf{a}]_{\mathbf{b}}$ is invertible with respect to \mathbf{v}_m , and $\langle [\mathbf{a}]_{\mathbf{b}} \mid \mathbf{v}_m \rangle$ is a commutative m -ary group. \square 68
69

Lemma 2. The p -adic analog of the residue class (4.2) is a commutative n -ary semigroup $\langle [a]_b \mid \mu_n \rangle$, if

$$a^n - a = b \bullet_p J, \quad (4.8)$$

where J is a p -adic integer (multiplication shape invariant), and the nonderived m -ary multiplication ν_m is the repeated binary product of n representatives

$$\mu_n [r_{k_1}, r_{k_2}, \dots, r_{k_n}] = r_{k_1} r_{k_2} \dots r_{k_n}. \quad (4.9)$$

Proof. The condition of closure for the n -ary multiplication μ_n is $r_{k_1} \bullet_p r_{k_2} \bullet_p \dots \bullet_p r_{k_m} = r_{k_0}$. Using (4.3) and opening brackets we obtain $na + b \bullet_p J_1 = a +_p b \bullet_p k_0$, where J_1 is some p -adic integer, which gives (4.8) with $J = k_0 -_p J_1$. \square

Combining the conditions (4.5) and (4.8), we arrive at

Theorem 1. The p -adic analog of the residue class (4.2) becomes a (m, n) -ring with m -ary addition (4.6) and n -ary multiplication (4.9)

$$\mathbb{Z}_{(m,n)}(a_q, b_q) = \left\langle [a_q]_{b_q} \mid \nu_m, \mu_n \right\rangle, \quad (4.10)$$

when the p -adic integers $a_q, b_q \in \mathbb{Z}_p$ are solutions of the equations

$$ma_q = a_q (\text{Mod}_p b_q), \quad (4.11)$$

$$a_q^n = a_q (\text{Mod}_p b_q). \quad (4.12)$$

Proof. The conditions (4.11)–(4.12) are equivalent to (4.5) and (4.8), respectively, which shows that $[a_q]_{b_q}$ (considered as a set of representatives (4.3)) is simultaneously an m -ary group with respect to ν_m , and an n -ary semigroup with respect to μ_n , and is therefore a (m, n) -ring. \square

If we work in the partial sum representation (3.7), the procedure of finding the digits of p -adic integers $a_q, b_q \in \mathbb{Z}_p$ such that $[a_q]_{b_q}$ becomes a (m, n) -ring with initially fixed arities is recursive. To find the first digits α_0 and β_0 that are ordinary integers, we use the equations (2.6)–(2.9), and for their arity shape TABLE 1. Next we consider the second components of (3.7) to find the digits α_1 and β_1 of a_q and b_q by solving the equations (4.5) and (4.8) (these having initially given arities m and n from the first step) by application of the exact formulas from [15]. In this way, we can find as many digits $(\alpha_0, \alpha_{i_{\max}})$ and $(\beta_0, \beta_{i_{\max}})$ of a_q and b_q , as needed for our accuracy preferences in building the polyadic ring of p -adic integers $\mathbb{Z}_{(m,n)}(a_q, b_q)$ (4.10).

Further development and examples will appear elsewhere.

Acknowledgements. The author is grateful to Branko Dragovich, Mike Hewitt, Vladimir Tkach and Raimund Vogl for useful discussions and valuable help.

1. Neurklich, J. *Algebraic Number Theory*; Springer: Berlin-New York, 1999.
2. Samuel, P. *Algebraic theory of numbers*; Hermann: Paris, 1972.
3. Berthelot, P.; Ogus, A. *Notes on Crystalline Cohomology*; Princeton Univ. Press: Princeton, 1978.
4. Le Stum, B. *Rigid cohomology*; Cambridge Univ. Press: Cambridge, 2007.
5. Dragovich, B.; Khrennikov, A.Y.; Kozyrev, S.V.; Volovich, I.V.; Zelenov, E.I. p -Adic mathematical physics: the first 30 years. *P-Adic Num. Ultrametr. Anal. Appl.* 2017, 9, 87–121. <https://doi.org/10.1134/s2070046617020017>.
6. Vladimirov, V.S.; Volovich, I.V.; Zelenov, E.I. *P-Adic Analysis And Mathematical Physics*; World Sci.: Singapore, 1994; p. 319.
7. Caruso, X. Computations with p -adic numbers. *Les cours du C.I.R.M., Course no II*, 2017, 5, 1–75. <https://arxiv.org/abs/1701.06794>.

8. Koblitz, N. *p-Adic Numbers, p-adic Analysis, and Zeta-functions*, 2nd ed.; Springer: New York, 1996; p. 150. 102
103
9. Robert, A.M. *A Course in p-adic Analysis*; Springer: New York, 2000. <https://doi.org/10.1007/978-1-4757-3254-2>. 104
105
10. Schikhof, W.H. *Ultrametric Calculus*; Cambridge Univ. Press: Cambridge, 1984. 106
11. Duplij, S. Polyadic integer numbers and finite (m, n) -fields. *p-Adic Numbers, Ultrametric Analysis and Appl.* **2017**, *9*, 257–281. arXiv:math.RA/1707.00719. 107
108
12. Duplij, S. Arity shape of polyadic algebraic structures. *J. Math. Physics, Analysis, Geometry* **2019**, *15*, 3–56. 109
110
13. Duplij, S. *Polyadic Algebraic Structures*; IOP Publishing: Bristol, 2022; p. 461. <https://doi.org/10.1088/978-0-7503-2648-3>. 111
112
14. Gouvêa, F.Q. *p-Adic Numbers. An introduction*, 3rd ed.; Springer: Cham, 2020. <https://doi.org/10.1007/978-3-030-47295-5>. 113
114
15. Xu, K.; Dai, Z.; Dai, Z. The formulas for the coefficients of the sum and product of p -adic integers with applications to Witt vectors. *Acta Arith.* **2011**, *150*, 361–384. <https://doi.org/10.4064/aa150-4-3>. 115
116
117
16. Dörnte, W. Unterschungen über einen verallgemeinerten Gruppenbegriff. *Math. Z.* **1929**, *29*, 1–19. 118
119