FORMALIZED MATHEMATICS
Vol. **16**, No. **2**, Pages 103–107, **2008**

# Uniqueness of Factoring an Integer and Multiplicative Group $\mathbb{Z}/p\mathbb{Z}^*$

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Yasunari Shidama
Shinshu University
Nagano, Japan

**Summary.** In the [20], it had been proven that the Integers modulo $p$, in this article we shall refer as $\mathbb{Z}/p\mathbb{Z}$, constitutes a field if and only if $p$ is a prime. Then the prime modulo $\mathbb{Z}/p\mathbb{Z}$ is an additive cyclic group and $\mathbb{Z}/p\mathbb{Z}^* = \mathbb{Z}/p\mathbb{Z}\setminus\{0\}$ is a multiplicative cyclic group, too. The former has been proven in the [23]. However, the latter had not been proven yet. In this article, first, we prove a theorem concerning the LCM to prove the existence of primitive elements of $\mathbb{Z}/p^*$. Moreover we prove the uniqueness of factoring an integer. Next we define the multiplicative group $\mathbb{Z}/p\mathbb{Z}^*$ and prove it is cyclic.

MML identifier: `INT_7`, version: `7.8.10 4.99.1005`

The articles [31], [3], [9], [1], [25], [2], [32], [8], [24], [4], [19], [29], [28], [13], [7], [26], [22], [11], [17], [18], [12], [16], [30], [23], [27], [5], [14], [15], [20], [21], [6], and [10] provide the terminology and notation for this paper.

## 1. Uniqueness of Factoring an Integer

In this paper $x$, $X$ denote sets.

Next we state four propositions:

(1) For every many sorted set $p$ indexed by $X$ such that $\operatorname{support} p = \{x\}$ holds $p = (X \longmapsto 0) +\cdot (x, p(x))$.

(2) Let $X$ be a set and $p$, $q$, $r$ be real-valued many sorted sets indexed by $X$. If $\operatorname{support} p \cap \operatorname{support} q = \emptyset$ and $\operatorname{support} p \cup \operatorname{support} q = \operatorname{support} r$ and $p \restriction \operatorname{support} p = r \restriction \operatorname{support} p$ and $q \restriction \operatorname{support} q = r \restriction \operatorname{support} q$, then $p + q = r$.




ISSN 1426–2630(p), 1898-9934(e)

(3) For every set $X$ and for all many sorted sets $p$, $q$ indexed by $X$ such that $p \restriction \operatorname{support} p = q \restriction \operatorname{support} q$ holds $p = q$.

(4) For every set $X$ and for all bags $p$, $q$ of $X$ such that $\operatorname{support} p = \emptyset$ and $\operatorname{support} q = \emptyset$ holds $p = q$.

Let $p$ be a bag of Prime. We say that $p$ is prime-factorization-like if and only if:

(Def. 1) For every prime number $x$ such that $x \in \operatorname{support} p$ there exists a natural number $n$ such that $0 < n$ and $p(x) = x^n$.

Let $n$ be a non empty natural number. Note that $\mathrm{PPF}(n)$ is prime-factorization-like.

Next we state a number of propositions:

(5) For all prime numbers $p$, $q$ and for all natural numbers $n$, $m$ such that $p \mid m \cdot q^n$ and $p \neq q$ holds $p \mid m$.

(6) Let $f$ be a finite sequence of elements of $\mathbb{N}$, $b$ be a bag of Prime, and $a$ be a prime number. Suppose $b$ is prime-factorization-like and $\prod b \neq 1$ and $a \mid \prod b$ and $\prod b = \prod f$ and $f = b \cdot \mathrm{CFS}(\operatorname{support} b)$. Then $a \in \operatorname{support} b$.

(7) For all bags $p$, $q$ of Prime such that $\operatorname{support} p \subseteq \operatorname{support} q$ and $p \restriction \operatorname{support} p = q \restriction \operatorname{support} p$ holds $\prod p \mid \prod q$.

(8) Let $p$ be a bag of Prime and $x$ be a prime number. If $p$ is prime-factorization-like, then $x \mid \prod p$ iff $x \in \operatorname{support} p$.

(9) For all non empty natural numbers $n$, $m$, $k$ such that $k = \operatorname{lcm}(n, m)$ holds $\operatorname{support} \mathrm{PPF}(k) = \operatorname{support} \mathrm{PPF}(n) \cup \operatorname{support} \mathrm{PPF}(m)$.

(10) For every set $X$ and for all bags $b_1$, $b_2$ of $X$ holds $\operatorname{support} \min(b_1, b_2) = \operatorname{support} b_1 \cap \operatorname{support} b_2$.

(11) For all non empty natural numbers $n$, $m$, $k$ such that $k = n \operatorname{gcd} m$ holds $\operatorname{support} \mathrm{PPF}(k) = \operatorname{support} \mathrm{PPF}(n) \cap \operatorname{support} \mathrm{PPF}(m)$.

(12) Let $p$, $q$ be bags of Prime. Suppose $p$ is prime-factorization-like and $q$ is prime-factorization-like and $\operatorname{support} p$ misses $\operatorname{support} q$. Then $\prod p$ and $\prod q$ are relative prime.

(13) For every bag $p$ of Prime such that $p$ is prime-factorization-like holds $\prod p \neq 0$.

(14) For every bag $p$ of Prime such that $p$ is prime-factorization-like holds $\prod p = 1$ iff $\operatorname{support} p = \emptyset$.

(15) Let $p$, $q$ be bags of Prime. Suppose $p$ is prime-factorization-like and $q$ is prime-factorization-like and $\prod p = \prod q$. Then $p = q$.

(16) Let $p$ be a bag of Prime and $n$ be a non empty natural number. If $p$ is prime-factorization-like and $n = \prod p$, then $\mathrm{PPF}(n) = p$.

(17) Let $n$, $m$ be elements of $\mathbb{N}$. Suppose $1 \leq n$ and $1 \leq m$. Then there exist elements $m_0$, $n_0$ of $\mathbb{N}$ such that $\operatorname{lcm}(n, m) = n_0 \cdot m_0$ and $n_0 \operatorname{gcd} m_0 = 1$

and $n_0 \mid n$ and $m_0 \mid m$ and $n_0 \neq 0$ and $m_0 \neq 0$.

## 2. Multiplicative Group $\mathbb{Z}/p\mathbb{Z}^*$

Let $n$ be a natural number. Let us assume that $1 < n$. The functor $\mathbb{Z}_n^*$ yields a non empty finite subset of $\mathbb{N}$ and is defined by:

(Def. 2) $\mathbb{Z}_n^* = \mathbb{Z}_n \setminus \{0\}$.

We now state the proposition

(18) For every natural number $n$ such that $1 < n$ holds $\overline{\overline{\mathbb{Z}_n^*}} = n - 1$.

Let $n$ be a prime number. The functor $\cdot_{\mathbb{Z}_n^*}$ yielding a binary operation on $\mathbb{Z}_n^*$ is defined by:

(Def. 3) $\cdot_{\mathbb{Z}_n^*} = \cdot_{\mathbb{Z}_n} \upharpoonright \mathbb{Z}_n^*$.

One can prove the following proposition

(19) For every prime number $p$ holds $\langle \mathbb{Z}_p^*, \cdot_{\mathbb{Z}_p^*} \rangle$ is associative, commutative, and group-like.

Let $p$ be a prime number. The functor $\mathbb{Z}/p\mathbb{Z}^*$ yielding a commutative group is defined by:

(Def. 4) $\mathbb{Z}/p\mathbb{Z}^* = \langle \mathbb{Z}_p^*, \cdot_{\mathbb{Z}_p^*} \rangle$.

The following three propositions are true:

(20) Let $p$ be a prime number, $x$, $y$ be elements of $\mathbb{Z}/p\mathbb{Z}^*$, and $x_1$, $y_1$ be elements of $\mathbb{Z}_p^{\mathrm{R}}$. If $x = x_1$ and $y = y_1$, then $x \cdot y = x_1 \cdot y_1$.

(21) For every prime number $p$ holds $\mathbf{1}_{\mathbb{Z}/p\mathbb{Z}^*} = 1$ and $\mathbf{1}_{\mathbb{Z}/p\mathbb{Z}^*} = 1_{\mathbb{Z}_p^{\mathrm{R}}}$.

(22) For every prime number $p$ and for every element $x$ of $\mathbb{Z}/p\mathbb{Z}^*$ and for every element $x_1$ of $\mathbb{Z}_p^{\mathrm{R}}$ such that $x = x_1$ holds $x^{-1} = {x_1}^{-1}$.

Let $p$ be a prime number. One can verify that $\mathbb{Z}/p\mathbb{Z}^*$ is finite.

We now state several propositions:

(23) For every prime number $p$ holds $\mathrm{ord}(\mathbb{Z}/p\mathbb{Z}^*) = p - 1$.

(24) Let $G$ be a group, $a$ be an element of $G$, and $i$ be an integer. Suppose $a$ is not of order 0. Then there exist elements $n$, $k$ of $\mathbb{N}$ such that $a^i = a^n$ and $n = k \cdot \mathrm{ord}(a) + i$.

(25) Let $G$ be a commutative group, $a$, $b$ be elements of $G$, and $n$, $m$ be natural numbers. If $G$ is finite and $\mathrm{ord}(a) = n$ and $\mathrm{ord}(b) = m$ and $n \gcd m = 1$, then $\mathrm{ord}(a \cdot b) = n \cdot m$.

(26) For every non empty zero structure $L$ and for every polynomial $p$ of $L$ such that $0 \leq \deg p$ holds $p$ is non-zero.

(27) For every field $L$ and for every polynomial $f$ of $L$ such that $0 \leq \deg f$ holds $\mathrm{Roots}\, f$ is a finite set and $\overline{\overline{\mathrm{Roots}\, f}} \leq \deg f$.

(28) Let $p$ be a prime number, $z$ be an element of $\mathbb{Z}/p\mathbb{Z}^*$, and $y$ be an element of $\mathbb{Z}_p^{\mathrm{R}}$. If $z = y$, then for every element $n$ of $\mathbb{N}$ holds $\mathrm{power}_{\mathbb{Z}/p\mathbb{Z}^*}(z, n) = \mathrm{power}_{\mathbb{Z}_p^{\mathrm{R}}}(y, n)$.

(29) Let $p$ be a prime number, $a$, $b$ be elements of $\mathbb{Z}/p\mathbb{Z}^*$, and $n$ be a natural number. If $0 < n$ and $\mathrm{ord}(a) = n$ and $b^n = 1$, then $b$ is an element of $\mathrm{gr}(\{a\})$.

(30) Let $G$ be a group, $z$ be an element of $G$, and $d$, $l$ be elements of $\mathbb{N}$. If $G$ is finite and $\mathrm{ord}(z) = d \cdot l$, then $\mathrm{ord}(z^d) = l$.

(31) For every prime number $p$ holds $\mathbb{Z}/p\mathbb{Z}^*$ is a cyclic group.

## References

[1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.
[2] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.
[3] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[4] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[5] Grzegorz Bancerek and Andrzej Trybulec. Miscellaneous facts about functions. *Formalized Mathematics*, 5(**4**):485–492, 1996.
[6] Józef Białas. Group and field definitions. *Formalized Mathematics*, 1(**3**):433–439, 1990.
[7] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.
[8] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[9] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[10] Krzysztof Hryniewiecki. Recursive definitions. *Formalized Mathematics*, 1(**2**):321–328, 1990.
[11] Andrzej Kondracki. The Chinese Remainder Theorem. *Formalized Mathematics*, 6(**4**):573–577, 1997.
[12] Artur Korniłowicz and Piotr Rudnicki. Fundamental Theorem of Arithmetic. *Formalized Mathematics*, 12(**2**):179–186, 2004.
[13] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[14] Rafał Kwiatek. Factorial and Newton coefficients. *Formalized Mathematics*, 1(**5**):887–890, 1990.
[15] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relative primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.
[16] Robert Milewski. Fundamental theorem of algebra. *Formalized Mathematics*, 9(**3**):461–470, 2001.
[17] Robert Milewski. The ring of polynomials. *Formalized Mathematics*, 9(**2**):339–346, 2001.
[18] Piotr Rudnicki. Little Bezout theorem (factor theorem). *Formalized Mathematics*, 12(**1**):49–58, 2004.
[19] Piotr Rudnicki and Andrzej Trybulec. Multivariate polynomials with arbitrary number of variables. *Formalized Mathematics*, 9(**1**):95–110, 2001.
[20] Christoph Schwarzweller. The ring of integers, euclidean rings and modulo integers. *Formalized Mathematics*, 8(**1**):29–34, 1999.
[21] Christoph Schwarzweller and Agnieszka Rowińska-Schwarzweller. Schur's theorem on the stability of networks. *Formalized Mathematics*, 14(**4**):135–142, 2006.
[22] Christoph Schwarzweller and Andrzej Trybulec. The evaluation of multivariate polynomials. *Formalized Mathematics*, 9(**2**):331–338, 2001.
[23] Dariusz Surowik. Cyclic groups and some of their properties – part I. *Formalized Mathematics*, 2(**5**):623–627, 1991.
[24] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.

[25] Andrzej Trybulec. Domains and their Cartesian products. *Formalized Mathematics*, 1(**1**):115–122, 1990.
[26] Andrzej Trybulec. Many-sorted sets. *Formalized Mathematics*, 4(**1**):15–22, 1993.
[27] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[28] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
[29] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
[30] Wojciech A. Trybulec. Lattice of subgroups of a group. Frattini subgroup. *Formalized Mathematics*, 2(**1**):41–47, 1991.
[31] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[32] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.

*Received January 31, 2008*