JOURNAL OF FORMALIZED MATHEMATICS
Volume 11, Released 1999, Published 2003
Inst. of Computer Science, Univ. of Białystok

The Ring of Integers, Euclidean Rings and Modulo Integers

Christoph Schwarzweller
University of Tübingen

Summary. In this article we introduce the ring of Integers, Euclidean rings and Integers modulo p. In particular we prove that the Ring of Integers is an Euclidean ring and that the Integers modulo p constitutes a field if and only if p is a prime.

MML Identifier: `INT_3`.

WWW: `http://mizar.org/JFM/Vol11/int_3.html`

The articles [15], [20], [2], [16], [18], [21], [5], [6], [13], [10], [12], [4], [9], [8], [14], [17], [3], [7], [11], [1], and [19] provide the notation and terminology for this paper.

1. The Ring of Integers

The binary operation multint on $\mathbb{Z}$ is defined by:

(Def. 1) For all elements a, b of $\mathbb{Z}$ holds $(\text{multint})(a,b) = \cdot_{\mathbb{R}}(a,b)$.

The unary operation compint on $\mathbb{Z}$ is defined by:

(Def. 2) For every element a of $\mathbb{Z}$ holds $(\text{compint})(a) = -_{\mathbb{R}}(a)$.

The double loop structure INT.Ring is defined as follows:

(Def. 3) $\text{INT.Ring} = \langle \mathbb{Z}, +_{\mathbb{Z}}, \text{multint}, 1 (\in \mathbb{Z}), 0 (\in \mathbb{Z}) \rangle$.

One can check that INT.Ring is strict and non empty.

One can check that INT.Ring is Abelian, add-associative, right zeroed, right complementable, well unital, distributive, commutative, associative, integral domain-like, and non degenerated.

Let a, b be elements of INT.Ring. The predicate $a \leq b$ is defined by:

(Def. 4) There exist integers a', b' such that $a' = a$ and $b' = b$ and $a' \leq b'$.

Let us notice that the predicate $a \leq b$ is reflexive and connected. We introduce $b \geq a$ as a synonym of $a \leq b$. We introduce $b < a$ and $a > b$ as antonyms of $a \leq b$.

Let a be an element of INT.Ring. The functor $|a|$ yields an element of INT.Ring and is defined by:

(Def. 5) $|a| = \begin{cases} a, & \text{if } a \geq 0_{\text{INT.Ring}}, \\ -a, & \text{otherwise.} \end{cases}$

The function absint from the carrier of INT.Ring into $\mathbb{N}$ is defined by:

(Def. 6) For every element a of INT.Ring holds $(\text{absint})(a) = |\square|_{\mathbb{R}}(a)$.

Next we state two propositions:

(1) For every element a of INT.Ring holds $(\mathrm{absint})(a) = |a|$.

(2) Let a, b, q_1, q_2, r_1, r_2 be elements of INT.Ring. Suppose $b \neq 0_{\mathrm{INT.Ring}}$ and $a = q_1 \cdot b + r_1$ and $0_{\mathrm{INT.Ring}} \leq r_1$ and $r_1 < |b|$ and $a = q_2 \cdot b + r_2$ and $0_{\mathrm{INT.Ring}} \leq r_2$ and $r_2 < |b|$. Then $q_1 = q_2$ and $r_1 = r_2$.

Let a, b be elements of INT.Ring. Let us assume that $b \neq 0_{\mathrm{INT.Ring}}$. The functor $a \div b$ yields an element of INT.Ring and is defined by:

(Def. 7) There exists an element r of INT.Ring such that $a = (a \div b) \cdot b + r$ and $0_{\mathrm{INT.Ring}} \leq r$ and $r < |b|$.

Let a, b be elements of INT.Ring. Let us assume that $b \neq 0_{\mathrm{INT.Ring}}$. The functor $a \bmod b$ yielding an element of INT.Ring is defined by:

(Def. 8) There exists an element q of INT.Ring such that $a = q \cdot b + (a \bmod b)$ and $0_{\mathrm{INT.Ring}} \leq a \bmod b$ and $a \bmod b < |b|$.

We now state the proposition

(3) For all elements a, b of INT.Ring such that $b \neq 0_{\mathrm{INT.Ring}}$ holds $a = (a \div b) \cdot b + (a \bmod b)$.

2. Euclidean Rings

Let I be a non empty double loop structure. We say that I is Euclidian if and only if the condition (Def. 9) is satisfied.

(Def. 9) There exists a function f from the carrier of I into $\mathbb{N}$ such that for all elements a, b of I if $b \neq 0_I$, then there exist elements q, r of I such that $a = q \cdot b + r$ but $r = 0_I$ or $f(r) < f(b)$.

One can verify that INT.Ring is Euclidian.

One can check that there exists a ring which is strict, Euclidian, integral domain-like, non degenerated, well unital, distributive, and commutative.

An EuclidianRing is an Euclidian integral domain-like non degenerated well unital distributive commutative ring.

Let us note that there exists an EuclidianRing which is strict.

Let E be an Euclidian non empty double loop structure. A function from the carrier of E into $\mathbb{N}$ is said to be a DegreeFunction of E if:

(Def. 10) For all elements a, b of E such that $b \neq 0_E$ there exist elements q, r of E such that $a = q \cdot b + r$ but $r = 0_E$ or $\mathrm{it}(r) < \mathrm{it}(b)$.

Next we state the proposition

(4) Every EuclidianRing is a gcdDomain.

One can verify that every integral domain-like non degenerated Abelian add-associative right zeroed right complementable associative commutative right unital right distributive non empty double loop structure which is Euclidian is also gcd-like.

absint is a DegreeFunction of INT.Ring.

One can prove the following proposition

(5) Every commutative associative left unital field-like right zeroed non empty double loop structure is Euclidian.

Let us note that every non empty double loop structure which is commutative, associative, left unital, field-like, right zeroed, and field-like is also Euclidian.

One can prove the following proposition

(6) Let F be a commutative associative left unital field-like right zeroed non empty double loop structure. Then every function from the carrier of F into $\mathbb{N}$ is a DegreeFunction of F.

3. Some Theorems about Div and Mod

Next we state several propositions:

(8)[1] For every natural number n such that $n > 0$ and for all integers a, k holds $(a+n\cdot k) \div n = (a \div n) + k$ and $(a+n\cdot k) \bmod n = a \bmod n$.

(9) For every natural number n such that $n > 0$ and for every integer a holds $a \bmod n \geq 0$ and $a \bmod n < n$.

(10) Let n be a natural number. Suppose $n > 0$. Let a be an integer. Then

(i) if $0 \leq a$ and $a < n$, then $a \bmod n = a$, and

(ii) if $0 > a$ and $a \geq -n$, then $a \bmod n = n + a$.

(11) For every natural number n such that $n > 0$ and for every integer a holds $a \bmod n = 0$ iff $n \mid a$.

(12) For every natural number n such that $n > 0$ and for all integers a, b holds $a \bmod n = b \bmod n$ iff $a \equiv b (\bmod n)$.

(13) For every natural number n such that $n > 0$ and for every integer a holds $a \bmod n \bmod n = a \bmod n$.

(14) For every natural number n such that $n > 0$ and for all integers a, b holds $(a+b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n$.

(15) For every natural number n such that $n > 0$ and for all integers a, b holds $a \cdot b \bmod n = (a \bmod n) \cdot (b \bmod n) \bmod n$.

(16) For all integers a, b there exist integers s, t such that $a \gcd b = s \cdot a + t \cdot b$.

4. Modulo Integers

Let n be a natural number. Let us assume that $n > 0$. The functor multint$n$ yields a binary operation on $\mathbb{Z}_n$ and is defined as follows:

(Def. 11) For all elements k, l of $\mathbb{Z}_n$ holds $(\mathrm{multint}\,n)(k, l) = k \cdot l \bmod n$.

Let n be a natural number. Let us assume that $n > 0$. The functor compint$n$ yields a unary operation on $\mathbb{Z}_n$ and is defined as follows:

(Def. 12) For every element k of $\mathbb{Z}_n$ holds $(\mathrm{compint}\,n)(k) = (n-k) \bmod n$.

The following three propositions are true:

(17) Let n be a natural number. Suppose $n > 0$. Let a, b be elements of $\mathbb{Z}_n$. Then

(i) $a+b < n$ iff $+_n(a, b) = a+b$, and

(ii) $a+b \geq n$ iff $+_n(a, b) = (a+b)-n$.

(18) Let n be a natural number. Suppose $n > 0$. Let a, b be elements of $\mathbb{Z}_n$ and k be a natural number. Then $k \cdot n \leq a \cdot b$ and $a \cdot b < (k+1) \cdot n$ if and only if $(\mathrm{multint}\,n)(a, b) = a \cdot b - k \cdot n$.

(19) Let n be a natural number. Suppose $n > 0$. Let a be an element of $\mathbb{Z}_n$. Then

(i) $a = 0$ iff $(\mathrm{compint}\,n)(a) = 0$, and

(ii) $a \neq 0$ iff $(\mathrm{compint}\,n)(a) = n-a$.

Let n be a natural number. The functor INT.Ring$n$ yielding a double loop structure is defined by:

[1] The proposition (7) has been removed.

(Def. 13) INT.Ring $n = \langle \mathbb{Z}_n, +_n, \mathrm{multint}\, n, 1(\in \mathbb{Z}_n), 0(\in \mathbb{Z}_n) \rangle$.

Let n be a natural number. One can check that INT.Ring n is strict and non empty.

Next we state the proposition

(20) INT.Ring 1 is degenerated and INT.Ring 1 is a ring and INT.Ring 1 is field-like, well unital, distributive, and commutative.

One can verify that there exists a ring which is strict, degenerated, well unital, distributive, field-like, and commutative.

Next we state two propositions:

(21) Let n be a natural number. Suppose $n > 1$. Then INT.Ring n is non degenerated and INT.Ring n is a well unital distributive commutative ring.

(22) Let p be a natural number. Suppose $p > 1$. Then INT.Ring p is an add-associative right zeroed right complementable Abelian commutative associative left unital distributive field-like non degenerated non empty double loop structure if and only if p is a prime number.

Let p be a prime number. Note that INT.Ring p is add-associative, right zeroed, right complementable, Abelian, commutative, associative, left unital, distributive, field-like, and non degenerated.

REFERENCES

[1] Grzegorz Bancerek. The fundamental properties of natural numbers. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/nat_1.html`.

[2] Grzegorz Bancerek. Sequences of ordinal numbers. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/ordinal2.html`.

[3] Grzegorz Bancerek and Andrzej Trybulec. Miscellaneous facts about functions. *Journal of Formalized Mathematics*, 8, 1996. `http://mizar.org/JFM/Vol8/funct_7.html`.

[4] Czesław Byliński. Binary operations. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/binop_1.html`.

[5] Czesław Byliński. Functions and their basic properties. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/funct_1.html`.

[6] Czesław Byliński. Functions from a set to a set. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/funct_2.html`.

[7] Marek Chmur. The lattice of natural numbers and the sublattice of it. The set of prime numbers. *Journal of Formalized Mathematics*, 3, 1991. `http://mizar.org/JFM/Vol3/nat_lat.html`.

[8] Agata Darmochwał. The Euclidean space. *Journal of Formalized Mathematics*, 3, 1991. `http://mizar.org/JFM/Vol3/euclid.html`.

[9] Krzysztof Hryniewiecki. Basic properties of real numbers. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/real_1.html`.

[10] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/vectsp_1.html`.

[11] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relatively primes. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/int_2.html`.

[12] Michał Muzalewski. Construction of rings and left-, right-, and bi-modules over a ring. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/vectsp_2.html`.

[13] Christoph Schwarzweller. The correctness of the generic algorithms of Brown and Henrici concerning addition and multiplication in fraction fields. *Journal of Formalized Mathematics*, 9, 1997. `http://mizar.org/JFM/Vol9/gcd_1.html`.

[14] Dariusz Surowik. Cyclic groups and some of their properties — part I. *Journal of Formalized Mathematics*, 3, 1991. `http://mizar.org/JFM/Vol3/gr_cy_1.html`.

[15] Andrzej Trybulec. Tarski Grothendieck set theory. *Journal of Formalized Mathematics*, Axiomatics, 1989. `http://mizar.org/JFM/Axiomatics/tarski.html`.

[16] Andrzej Trybulec. Subsets of real numbers. *Journal of Formalized Mathematics*, Addenda, 2003. `http://mizar.org/JFM/Addenda/numbers.html`.

[17] Michał J. Trybulec. Integers. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/int_1.html`.

[18] Wojciech A. Trybulec. Vectors in real linear space. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/rlvect_1.html`.

[19] Wojciech A. Trybulec. Groups. *Journal of Formalized Mathematics*, 2, 1990. `http://mizar.org/JFM/Vol2/group_1.html`.

[20] Zinaida Trybulec. Properties of subsets. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/subset_1.html`.

[21] Edmund Woronowicz. Relations and their basic properties. *Journal of Formalized Mathematics*, 1, 1989. `http://mizar.org/JFM/Vol1/relat_1.html`.

Received February 4, 1999

Published January 2, 2004