

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.

The notation and terminology used here are introduced in the following papers: [16], [21], [20], [17], [22], [4], [5], [14], [10], [12], [13], [3], [8], [7], [15], [18], [2], [6], [11], [9], [1], and [19].

1. THE RING OF INTEGERS

The binary operation multint on \mathbb{Z} is defined as follows:

(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 as follows:

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

The double loop structure INT.Ring is defined by:

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

Let us mention that INT.Ring is strict and non empty.

Let us mention 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 the carrier 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 the carrier of INT.Ring . The functor $|a|$ yields an element of the carrier of INT.Ring and is defined as follows:

(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 as follows:

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

One can prove the following two propositions:

- (1) For every element a of the carrier of INT.Ring holds $(\text{absint})(a) = |a|$.
- (2) Let a, b, q_1, q_2, r_1, r_2 be elements of the carrier of INT.Ring . Suppose $b \neq 0_{\text{INT.Ring}}$ and $a = q_1 \cdot b + r_1$ and $0_{\text{INT.Ring}} \leq r_1$ and $r_1 < |b|$ and $a = q_2 \cdot b + r_2$ and $0_{\text{INT.Ring}} \leq r_2$ and $r_2 < |b|$. Then $q_1 = q_2$ and $r_1 = r_2$.

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

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

Let a, b be elements of the carrier of INT.Ring . Let us assume that $b \neq 0_{\text{INT.Ring}}$. The functor $a \bmod b$ yields an element of the carrier of INT.Ring and is defined as follows:

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

Next we state the proposition

- (3) For all elements a, b of the carrier of INT.Ring such that $b \neq 0_{\text{INT.Ring}}$ 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 the carrier of I if $b \neq 0_I$, then there exist elements q, r of the carrier of I such that $a = q \cdot b + r$ but $r = 0_I$ or $f(r) < f(b)$.

One can check that `INT.Ring` is Euclidian.

Let us observe that there exists a ring which is strict, Euclidian, integral domain-like, non degenerated, well unital, and distributive.

A `EuclidianRing` is a Euclidian integral domain-like non degenerated well unital distributive ring.

Let us mention that there exists a `EuclidianRing` which is strict.

Let E be a 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 it satisfies the condition (Def. 10).

- (Def. 10) Let a, b be elements of the carrier of E . Suppose $b \neq 0_E$. Then there exist elements q, r of the carrier of E such that $a = q \cdot b + r$ but $r = 0_E$ or $\text{it}(r) < \text{it}(b)$.

Next we state the proposition

- (4) Every `EuclidianRing` is a `gcdDomain`.

Let us note 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 observe 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

The following propositions are true:

- (7) Let n be a natural number. Suppose $n > 0$. Let a be an integer and a' be a natural number. If $a' = a$, then $a \div n = a' \div n$ and $a \bmod n = a' \bmod n$.
- (8) 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 $a \equiv b \pmod{n}$.
- (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 $\text{multint } n$ yielding a binary operation on \mathbb{Z}_n is defined as follows:

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

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

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

Next we state three propositions:

- (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 $(\text{multint } n)(a, b) = a \cdot b - k \cdot n$.
- (19) Let n be a natural number. Suppose $n > 0$. Let a be an element of \mathbb{Z}_n .
Then
- (i) $a = 0$ iff $(\text{compint } n)(a) = 0$, and
 - (ii) $a \neq 0$ iff $(\text{compint } n)(a) = n - a$.

Let n be a natural number. The functor $\text{INT.Ring } n$ yields a double loop structure and is defined by:

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

Let n be a natural number. Observe that $\text{INT.Ring } n$ is strict and non empty.

We now state the proposition

- (20) $\text{INT.Ring } 1$ is degenerated and $\text{INT.Ring } 1$ is a ring and $\text{INT.Ring } 1$ is field-like, well unital, and distributive.

Let us note that there exists a ring which is strict, degenerated, well unital, distributive, and field-like.

One can prove the following propositions:

- (21) For every natural number n such that $n > 1$ holds $\text{INT.Ring } n$ is non degenerated and $\text{INT.Ring } n$ is a well unital distributive ring.
- (22) Let p be a natural number. Suppose $p > 1$. Then $\text{INT.Ring } p$ 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. Observe that $\text{INT.Ring } p$ 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. *Formalized Mathematics*, 1(1):41–46, 1990.
- [2] Grzegorz Bancerek and Andrzej Trybulec. Miscellaneous facts about functions. *Formalized Mathematics*, 5(4):485–492, 1996.
- [3] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(1):175–180, 1990.
- [4] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(1):55–65, 1990.
- [5] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(1):153–164, 1990.
- [6] Marek Chmur. The lattice of natural numbers and the sublattice of it. The set of prime numbers. *Formalized Mathematics*, 2(4):453–459, 1991.
- [7] Agata Darmochwał. The Euclidean space. *Formalized Mathematics*, 2(4):599–603, 1991.
- [8] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(1):35–40, 1990.
- [9] Krzysztof Hryniewiecki. Recursive definitions. *Formalized Mathematics*, 1(2):321–328, 1990.
- [10] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(2):335–342, 1990.
- [11] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relative primes. *Formalized Mathematics*, 1(5):829–832, 1990.
- [12] Michał Muzalewski. Construction of rings and left-, right-, and bi-modules over a ring. *Formalized Mathematics*, 2(1):3–11, 1991.
- [13] Henryk Oryszczyszyn and Krzysztof Prażmowski. Real functions spaces. *Formalized Mathematics*, 1(3):555–561, 1990.
- [14] Christoph Schwarzeweller. The correctness of the generic algorithms of Brown and Henrici concerning addition and multiplication in fraction fields. *Formalized Mathematics*, 6(3):381–388, 1997.
- [15] Dariusz Surowik. Cyclic groups and some of their properties - part I. *Formalized Mathematics*, 2(5):623–627, 1991.
- [16] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(1):9–11, 1990.
- [17] Andrzej Trybulec. Tuples, projections and Cartesian products. *Formalized Mathematics*, 1(1):97–105, 1990.

- [18] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
- [19] Wojciech A. Trybulec. Groups. *Formalized Mathematics*, 1(**5**):821–827, 1990.
- [20] Wojciech A. Trybulec. Vectors in real linear space. *Formalized Mathematics*, 1(**2**):291–296, 1990.
- [21] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
- [22] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.

Received February 4, 1999
