FORMALIZED MATHEMATICS
Volume 12, Number 2, 2004
University of Białystok

Fundamental Theorem of Arithmetic[1]

Artur Korniłowicz
University of Białystok

Piotr Rudnicki
University of Alberta
Edmonton

Summary. We formalize the notion of the prime-power factorization of a natural number and prove the Fundamental Theorem of Arithmetic. We prove also how prime-power factorization can be used to compute: products, quotients, powers, greatest common divisors and least common multiples.

MML Identifier: `NAT_3`.

The notation and terminology used in this paper are introduced in the following papers: [25], [27], [12], [7], [3], [4], [1], [24], [13], [2], [19], [18], [28], [8], [9], [6], [16], [15], [11], [26], [22], [23], [10], [14], [20], [5], [21], and [17].

1. Preliminaries

We follow the rules: a, b, n denote natural numbers, r denotes a real number, and f denotes a finite sequence of elements of $\mathbb{R}$.

Let X be an empty set. Observe that $\operatorname{card} X$ is empty.

One can check that every binary relation which is natural-yielding is also real-yielding.

Let us mention that there exists a finite sequence which is natural-yielding.

Let a be a non empty natural number and let b be a natural number. Observe that a^b is non empty.

One can verify that every prime number is non empty.

In the sequel p denotes a prime number.

One can verify that Prime is infinite.

The following propositions are true:

[1] A. Korniłowicz has been supported by a post-doctoral fellowship at Shinshu University, Nagano, Japan. P. Rudnicki has been supported by NSERC Grant OGP9207.

ISSN 1426–2630

(1) For all natural numbers a, b, c, d such that $a \mid c$ and $b \mid d$ holds $a \cdot b \mid c \cdot d$.

(2) If $1 < a$, then $b \leqslant a^b$.

(3) If $a \neq 0$, then $n \mid n^a$.

(4) For all natural numbers i, j, m, n such that $i < j$ and $m^j \mid n$ holds $m^{i+1} \mid n$.

(5) If $p \mid a^b$, then $p \mid a$.

(6) For every prime number a such that $a \mid p^b$ holds $a = p$.

(7) For every finite sequence f of elements of $\mathbb{N}$ such that $a \in \operatorname{rng} f$ holds $a \mid \prod f$.

(8) For every finite sequence f of elements of Prime such that $p \mid \prod f$ holds $p \in \operatorname{rng} f$.

Let f be a real-yielding finite sequence and let a be a natural number. The functor f^a yielding a finite sequence is defined as follows:

(Def. 1) $\operatorname{len}(f^a) = \operatorname{len} f$ and for every set i such that $i \in \operatorname{dom}(f^a)$ holds $f^a(i) = f(i)^a$.

Let f be a real-yielding finite sequence and let a be a natural number. One can verify that f^a is real-yielding.

Let f be a natural-yielding finite sequence and let a be a natural number. Note that f^a is natural-yielding.

Let f be a finite sequence of elements of $\mathbb{R}$ and let a be a natural number. Then f^a is a finite sequence of elements of $\mathbb{R}$.

Let f be a finite sequence of elements of $\mathbb{N}$ and let a be a natural number. Then f^a is a finite sequence of elements of $\mathbb{N}$.

Next we state several propositions:

(9) $f^0 = \operatorname{len} f \mapsto 1$.

(10) $f^1 = f$.

(11) $(\varepsilon_{\mathbb{R}})^a = \varepsilon_{\mathbb{R}}$.

(12) $\langle r \rangle^a = \langle r^a \rangle$.

(13) $(f \frown \langle r \rangle)^a = (f^a) \frown \langle r \rangle^a$.

(14) $\prod(f^{b+1}) = \prod(f^b) \cdot \prod f$.

(15) $\prod(f^a) = (\prod f)^a$.

2. More about Bags

Let X be a set. Note that there exists a many sorted set indexed by X which is natural-yielding and finite-support.

Let X be a set, let b be a real-yielding many sorted set indexed by X, and let a be a natural number. The functor $a \cdot b$ yielding a many sorted set indexed by X is defined as follows:

(Def. 2) For every set i holds $(a \cdot b)(i) = a \cdot b(i)$.

Let X be a set, let b be a real-yielding many sorted set indexed by X, and let a be a natural number. One can verify that $a \cdot b$ is real-yielding.

Let X be a set, let b be a natural-yielding many sorted set indexed by X, and let a be a natural number. Note that $a \cdot b$ is natural-yielding.

Let X be a set and let b be a real-yielding many sorted set indexed by X. Note that $\mathrm{support}(0 \cdot b)$ is empty.

Next we state the proposition

(16) For every set X and for every real-yielding many sorted set b indexed by X such that $a \neq 0$ holds $\mathrm{support}\, b = \mathrm{support}(a \cdot b)$.

Let X be a set, let b be a real-yielding finite-support many sorted set indexed by X, and let a be a natural number. One can check that $a \cdot b$ is finite-support.

Let X be a set and let b_1, b_2 be real-yielding many sorted sets indexed by X. The functor $\min(b_1, b_2)$ yields a many sorted set indexed by X and is defined by:

(Def. 3) For every set i holds if $b_1(i) \leqslant b_2(i)$, then $(\min(b_1, b_2))(i) = b_1(i)$ and if $b_1(i) > b_2(i)$, then $(\min(b_1, b_2))(i) = b_2(i)$.

Let X be a set and let b_1, b_2 be real-yielding many sorted sets indexed by X. Note that $\min(b_1, b_2)$ is real-yielding.

Let X be a set and let b_1, b_2 be natural-yielding many sorted sets indexed by X. Observe that $\min(b_1, b_2)$ is natural-yielding.

We now state the proposition

(17) For every set X and for all real-yielding finite-support many sorted sets b_1, b_2 indexed by X holds $\mathrm{support} \min(b_1, b_2) \subseteq \mathrm{support}\, b_1 \cup \mathrm{support}\, b_2$.

Let X be a set and let b_1, b_2 be real-yielding finite-support many sorted sets indexed by X. Observe that $\min(b_1, b_2)$ is finite-support.

Let X be a set and let b_1, b_2 be real-yielding many sorted sets indexed by X. The functor $\max(b_1, b_2)$ yielding a many sorted set indexed by X is defined as follows:

(Def. 4) For every set i holds if $b_1(i) \leqslant b_2(i)$, then $(\max(b_1, b_2))(i) = b_2(i)$ and if $b_1(i) > b_2(i)$, then $(\max(b_1, b_2))(i) = b_1(i)$.

Let X be a set and let b_1, b_2 be real-yielding many sorted sets indexed by X. Observe that $\max(b_1, b_2)$ is real-yielding.

Let X be a set and let b_1, b_2 be natural-yielding many sorted sets indexed by X. One can check that $\max(b_1, b_2)$ is natural-yielding.

One can prove the following proposition

(18) For every set X and for all real-yielding finite-support many sorted sets b_1, b_2 indexed by X holds $\mathrm{support} \max(b_1, b_2) \subseteq \mathrm{support}\, b_1 \cup \mathrm{support}\, b_2$.

Let X be a set and let b_1, b_2 be real-yielding finite-support many sorted sets indexed by X. Observe that $\max(b_1, b_2)$ is finite-support.

Let A be a set and let b be a bag of A. The functor $\prod b$ yields a natural number and is defined by:

(Def. 5) There exists a finite sequence f of elements of $\mathbb{N}$ such that $\prod b = \prod f$ and $f = b \cdot \mathrm{CFS}(\mathrm{support}\, b)$.

Let A be a set and let b be a bag of A. Then $\prod b$ is a natural number.

One can prove the following proposition

(19) For every set X and for all bags a, b of X such that support a misses support b holds $\prod(a + b) = \prod a \cdot \prod b$.

Let X be a set, let b be a real-yielding many sorted set indexed by X, and let n be a non empty natural number. The functor b^n yielding a many sorted set indexed by X is defined by:

(Def. 6) $\mathrm{support}(b^n) = \mathrm{support}\, b$ and for every set i holds $b^n(i) = b(i)^n$.

Let X be a set, let b be a natural-yielding many sorted set indexed by X, and let n be a non empty natural number. One can verify that b^n is natural-yielding.

Let X be a set, let b be a real-yielding finite-support many sorted set indexed by X, and let n be a non empty natural number. Observe that b^n is finite-support.

The following proposition is true

(20) For every set A holds $\prod \mathrm{EmptyBag}\, A = 1$.

3. Multiplicity of a Divisor

Let n, d be natural numbers. Let us assume that $d \neq 1$ and $n \neq 0$. The functor $d\text{-count}(n)$ yields a natural number and is defined by:

(Def. 7) $d^{d\text{-count}(n)} \mid n$ and $d^{d\text{-count}(n)+1} \nmid n$.

One can prove the following propositions:

(21) If $n \neq 1$, then $n\text{-count}(1) = 0$.

(22) If $1 < n$, then $n\text{-count}(n) = 1$.

(23) If $b \neq 0$ and $b < a$ and $a \neq 1$, then $a\text{-count}(b) = 0$.

(24) If $a \neq 1$ and $a \neq p$, then $a\text{-count}(p) = 0$.

(25) If $1 < b$, then $b\text{-count}(b^a) = a$.

(26) If $b \neq 1$ and $a \neq 0$ and $b \mid b^{b\text{-count}(a)}$, then $b \mid a$.

(27) If $b \neq 1$, then $a \neq 0$ and $b\text{-count}(a) = 0$ iff $b \nmid a$.

(28) For all non empty natural numbers a, b holds $p\text{-count}(a \cdot b) = p\text{-count}(a) + p\text{-count}(b)$.

(29) For all non empty natural numbers a, b holds $p^{p\text{-count}(a \cdot b)} = p^{p\text{-count}(a)} \cdot p^{p\text{-count}(b)}$.

(30) For all non empty natural numbers a, b such that $b \mid a$ holds $p\text{-count}(b) \leqslant p\text{-count}(a)$.

(31) For all non empty natural numbers a, b such that $b \mid a$ holds p-count$(a \div b) = p$-count$(a) -' p$-count(b).

(32) For every non empty natural number a holds p-count$(a^b) = b \cdot p$-count(a).

4. Exponents in Prime-Power Factorization

Let n be a natural number. The functor PrimeExponents(n) yields a many sorted set indexed by Prime and is defined as follows:

(Def. 8) For every prime number p holds $(\mathrm{PrimeExponents}(n))(p) = p$-count$(n)$.

We introduce PFExp(n) as a synonym of PrimeExponents(n).

One can prove the following three propositions:

(33) For every set x such that $x \in \mathrm{dom}\,\mathrm{PFExp}(n)$ holds x is a prime number.

(34) For every set x such that $x \in \mathrm{support}\,\mathrm{PFExp}(n)$ holds x is a prime number.

(35) If $a > n$ and $n \neq 0$, then $(\mathrm{PFExp}(n))(a) = 0$.

Let n be a natural number. Note that PFExp(n) is natural-yielding.

One can prove the following two propositions:

(36) If $a \in \mathrm{support}\,\mathrm{PFExp}(b)$, then $a \mid b$.

(37) If b is non empty and a is a prime number and $a \mid b$, then $a \in \mathrm{support}\,\mathrm{PFExp}(b)$.

Let n be a non empty natural number. Observe that PFExp(n) is finite-support.

We now state two propositions:

(38) For every non empty natural number a such that $p \mid a$ holds $(\mathrm{PFExp}(a))(p) \neq 0$.

(39) $\mathrm{PFExp}(1) = \mathrm{EmptyBag}\,\mathrm{Prime}$.

One can verify that support PFExp(1) is empty.

One can prove the following four propositions:

(40) $(\mathrm{PFExp}(p^a))(p) = a$.

(41) $(\mathrm{PFExp}(p))(p) = 1$.

(42) If $a \neq 0$, then $\mathrm{support}\,\mathrm{PFExp}(p^a) = \{p\}$.

(43) $\mathrm{support}\,\mathrm{PFExp}(p) = \{p\}$.

Let p be a prime number and let a be a non empty natural number. Observe that support PFExp(p^a) is non empty and trivial.

Let p be a prime number. Observe that support PFExp(p) is non empty and trivial.

Next we state several propositions:

(44) For all non empty natural numbers a, b such that a and b are relative prime holds support PFExp(a) misses support PFExp(b).

(45) For all non empty natural numbers a, b holds support PFExp$(a) \subseteq$ support PFExp$(a \cdot b)$.

(46) For all non empty natural numbers a, b holds support PFExp$(a \cdot b) =$ support PFExp$(a) \cup$ support PFExp(b).

(47) For all non empty natural numbers a, b such that a and b are relative prime holds card support PFExp$(a \cdot b) =$ card support PFExp$(a) +$ card support PFExp(b).

(48) For all non empty natural numbers a, b holds support PFExp$(a) =$ support PFExp(a^b).

In the sequel n, m are non empty natural numbers.

Next we state several propositions:

(49) $\mathrm{PFExp}(n \cdot m) = \mathrm{PFExp}(n) + \mathrm{PFExp}(m)$.

(50) If $m \mid n$, then $\mathrm{PFExp}(n \div m) = \mathrm{PFExp}(n) -' \mathrm{PFExp}(m)$.

(51) $\mathrm{PFExp}(n^a) = a \cdot \mathrm{PFExp}(n)$.

(52) If support PFExp$(n) = \emptyset$, then $n = 1$.

(53) For all non empty natural numbers m, n holds $\mathrm{PFExp}(\gcd(n, m)) = \min(\mathrm{PFExp}(n), \mathrm{PFExp}(m))$.

(54) For all non empty natural numbers m, n holds $\mathrm{PFExp}(\mathrm{lcm}(n, m)) = \max(\mathrm{PFExp}(n), \mathrm{PFExp}(m))$.

5. Prime-Power Factorization

Let n be a non empty natural number. The functor PrimeFactorization(n) yielding a many sorted set indexed by Prime is defined as follows:

(Def. 9) support PrimeFactorization$(n) =$ support PFExp(n) and for every natural number p such that $p \in$ support PFExp(n) holds $(\mathrm{PrimeFactorization}(n))(p) = p^{p\text{-count}(n)}$.

We introduce PPF(n) as a synonym of PrimeFactorization(n).

Let n be a non empty natural number. Observe that PPF(n) is natural-yielding and finite-support.

The following propositions are true:

(55) If p-count$(n) = 0$, then $(\mathrm{PPF}(n))(p) = 0$.

(56) If p-count$(n) \neq 0$, then $(\mathrm{PPF}(n))(p) = p^{p\text{-count}(n)}$.

(57) If support PPF$(n) = \emptyset$, then $n = 1$.

(58) For all non empty natural numbers a, b such that a and b are relative prime holds $\mathrm{PPF}(a \cdot b) = \mathrm{PPF}(a) + \mathrm{PPF}(b)$.

(59) $(\mathrm{PPF}(p^n))(p) = p^n$.

(60) $\mathrm{PPF}(n^m) = (\mathrm{PPF}(n))^m$.

(61) $\prod \mathrm{PPF}(n) = n$.

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. Sequences of ordinal numbers. *Formalized Mathematics*, 1(**2**):281–290, 1990.
[5] Grzegorz Bancerek. Joining of decorated trees. *Formalized Mathematics*, 4(**1**):77–82, 1993.
[6] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[7] Józef Białas. Group and field definitions. *Formalized Mathematics*, 1(**3**):433–439, 1990.
[8] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.
[9] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[10] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.
[11] Marek Chmur. The lattice of natural numbers and the sublattice of it. The set of prime numbers. *Formalized Mathematics*, 2(**4**):453–459, 1991.
[12] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[13] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(**1**):35–40, 1990.
[14] Andrzej Kondracki. The Chinese Remainder Theorem. *Formalized Mathematics*, 6(**4**):573–577, 1997.
[15] Jarosław Kotowicz. Monotone real sequences. Subsequences. *Formalized Mathematics*, 1(**3**):471–475, 1990.
[16] Jarosław Kotowicz. Real sequences and basic operations on them. *Formalized Mathematics*, 1(**2**):269–272, 1990.
[17] Eugeniusz Kusak, Wojciech Leończuk, and Michał Muzalewski. Abelian groups, fields and vector spaces. *Formalized Mathematics*, 1(**2**):335–342, 1990.
[18] Rafał Kwiatek. Factorial and Newton coefficients. *Formalized Mathematics*, 1(**5**):887–890, 1990.
[19] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relative primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.
[20] Takaya Nishiyama and Yasuho Mizuhara. Binary arithmetics. *Formalized Mathematics*, 4(**1**):83–86, 1993.
[21] Piotr Rudnicki. Little Bezout theorem (factor theorem). *Formalized Mathematics*, 12(**1**):49–58, 2003.
[22] Piotr Rudnicki and Andrzej Trybulec. Multivariate polynomials with arbitrary number of variables. *Formalized Mathematics*, 9(**1**):95–110, 2001.
[23] Christoph Schwarzweller and Andrzej Trybulec. The evaluation of multivariate polynomials. *Formalized Mathematics*, 9(**2**):331–338, 2001.
[24] Andrzej Trybulec. Subsets of complex numbers. *To appear in Formalized Mathematics.*
[25] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.
[26] Andrzej Trybulec. Many-sorted sets. *Formalized Mathematics*, 4(**1**):15–22, 1993.
[27] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.
[28] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.

Received February 13, 2004