FORMALIZED MATHEMATICS
2006, Vol. 14, No. 2, Pages 47–52
DOI: 10.2478/v10037-006-0007-y

Pocklington's Theorem and Bertrand's Postulate

Marco Riccardi
Casella Postale 49
54038 Montignoso, Italy

Summary. The first four sections of this article include some auxiliary theorems related to number and finite sequence of numbers, in particular a primality test, the Pocklington's theorem (see [19]). The last section presents the formalization of Bertrand's postulate closely following the book [1], pp. 7–9.

MML identifier: NAT_4, version: 7.7.01 4.66.942

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

1. Some Theorems on Real and Natural Numbers

The following propositions are true:

(1) For all real numbers r, s such that $0 \leq r$ and $s \cdot s < r \cdot r$ holds $s < r$.

(2) For all real numbers r, s such that $1 < r$ and $r \cdot r \leq s$ holds $r < s$.

(3) For all natural numbers a, n such that $a > 1$ holds $a^n > n$.

(4) For all natural numbers n, k, m such that $k \leq n$ and $m = \lfloor \frac{n}{2} \rfloor$ holds $\binom{n}{m} \geq \binom{n}{k}$.

(5) For all natural numbers n, m such that $m = \lfloor \frac{n}{2} \rfloor$ and $n \geq 2$ holds $\binom{n}{m} \geq \frac{2^n}{n}$.

(6) For every natural number n holds $\binom{2 \cdot n}{n} \geq \frac{4^n}{2 \cdot n}$.

(7) For all natural numbers n, p such that $p > 0$ and $n \mid p$ and $n \neq 1$ and $n \neq p$ holds $1 < n$ and $n < p$.

ISSN 1426–2630

(8) Let p be a natural number. Given a natural number n such that $n \mid p$ and $1 < n$ and $n < p$. Then there exists a natural number n such that $n \mid p$ and $1 < n$ and $n \cdot n \leq p$.

(9) For all natural numbers i, j, k, l such that $i = j \cdot k + l$ and $l < j$ and $0 < l$ holds $j \nmid i$.

(10) For all natural numbers n, q, b such that $\gcd(q, b) = 1$ and $q \neq 0$ and $b \neq 0$ holds $\gcd(q^n, b) = 1$.

(11) For all natural numbers a, b, c holds $a^{2 \cdot b} \bmod c = (a^b \bmod c) \cdot (a^b \bmod c) \bmod c$.

(12) Let p be a natural number. Then p is not prime if and only if one of the following conditions is satisfied:

(i) $p \leq 1$, or

(ii) there exists a natural number n such that $n \mid p$ and $1 < n$ and $n < p$.

(13) Let n, k be natural numbers. Suppose $n \mid k$ and $1 < n$. Then there exists a natural number p such that $p \mid k$ and $p \leq n$ and p is prime.

(14) Let p be a natural number. Then p is prime if and only if the following conditions are satisfied:

(i) $p > 1$, and

(ii) for every natural number n such that $1 < n$ and $n \cdot n \leq p$ and n is prime holds $n \nmid p$.

(15) For all natural numbers a, p, k such that $a^k \bmod p = 1$ and $k \geq 1$ and p is prime holds a and p are relative prime.

(16) Let p be a prime number, a be a natural number, and x be a set. Suppose $a \neq 0$ and $x = p^{p\text{-count}(a)}$. Then there exists a natural number b such that $b = x$ and $1 \leq b$ and $b \leq a$.

(17) For all natural numbers k, q, n, d such that q is prime and $d \mid k \cdot q^{n+1}$ and $d \nmid k \cdot q^n$ holds $q^{n+1} \mid d$.

(18) For all natural numbers q_1, q, n_1 such that $q_1 \mid q^{n_1}$ and q is prime and q_1 is prime and $n_1 > 0$ holds $q = q_1$.

(19) For every prime number p and for every natural number n such that $n < p$ holds $p \nmid n!$.

(20) Let a, b be non empty natural numbers. Suppose that for every natural number p such that p is prime holds $p\text{-count}(a) \leq p\text{-count}(b)$. Then there exists a natural number c such that $b = a \cdot c$.

(21) Let a, b be non empty natural numbers. Suppose that for every natural number p such that p is prime holds $p\text{-count}(a) = p\text{-count}(b)$. Then $a = b$.

(22) For all prime numbers p_1, p_2 and for every non empty natural number m such that ${p_1}^{p_1\text{-count}(m)} = {p_2}^{p_2\text{-count}(m)}$ and $p_1\text{-count}(m) > 0$ holds $p_1 = p_2$.

2. Pocklington's Theorem

One can prove the following propositions:

(23) Let n, k, q, p, n_1, p, a be natural numbers. Suppose $n - 1 = k \cdot q^{n_1}$ and $k > 0$ and $n_1 > 0$ and q is prime and $a^{n -' 1} \bmod n = 1$ and p is prime and $p \mid n$. Then $p \mid a^{(n -' 1) \div q} -' 1$ or $p \bmod q^{n_1} = 1$.

(24) Let n, f, c be natural numbers. Suppose that

(i) $n - 1 = f \cdot c$,

(ii) $f > c$,

(iii) $c > 0$,

(iv) $\gcd(f, c) = 1$, and

(v) for every natural number q such that $q \mid f$ and q is prime there exists a natural number a such that $a^{n -' 1} \bmod n = 1$ and $\gcd(a^{(n -' 1) \div q} -' 1, n) = 1$.

Then n is prime.

(25) Let n, f, d, n_1, a, q be natural numbers. Suppose $n - 1 = q^{n_1} \cdot d$ and $q^{n_1} > d$ and $d > 0$ and $\gcd(q, d) = 1$ and q is prime and $a^{n -' 1} \bmod n = 1$ and $\gcd(a^{(n -' 1) \div q} -' 1, n) = 1$. Then n is prime.

3. Some Prime Numbers

The following propositions are true:

(26) 7 is prime.

(27) 11 is prime.

(28) 13 is prime.

(29) 19 is prime.

(30) 23 is prime.

(31) 37 is prime.

(32) 43 is prime.

(33) 83 is prime.

(34) 139 is prime.

(35) 163 is prime.

(36) 317 is prime.

(37) 631 is prime.

(38) 1259 is prime.

(39) 2503 is prime.

(40) 4001 is prime.

4. Some Theorems on Finite Sequence of Numbers

One can prove the following propositions:

(41) For all finite sequences f, f_0, f_1 of elements of $\mathbb{R}$ such that $f = f_0 + f_1$ holds $\mathrm{dom}\, f = \mathrm{dom}\, f_0 \cap \mathrm{dom}\, f_1$.

(42) Let F be a finite sequence of elements of $\mathbb{R}$. If for every natural number k such that $k \in \mathrm{dom}\, F$ holds $F(k) > 0$, then $\prod F > 0$.

(43) For every set X_1 and for every finite set X_2 such that $X_1 \subseteq X_2$ and $X_2 \subseteq \mathbb{N}$ and $\emptyset \notin X_2$ holds $\prod \mathrm{Sgm}\, X_1 \leq \prod \mathrm{Sgm}\, X_2$.

(44) Let a, k be natural numbers, X be a set, F be a finite sequence of elements of Prime, and p be a prime number such that $X \subseteq$ Prime and $X \subseteq \mathrm{Seg}\, k$ and $F = \mathrm{Sgm}\, X$ and $a = \prod F$. Then

(i) if $p \in \mathrm{rng}\, F$, then p-count$(a) = 1$, and

(ii) if $p \notin \mathrm{rng}\, F$, then p-count$(a) = 0$.

(45) For every natural number n holds $\prod \mathrm{Sgm}\{p; p$ ranges over prime numbers: $p \leq n+1\} \leq 4^n$.

(46) For every real number x such that $x \geq 2$ holds $\prod \mathrm{Sgm}\{p; p$ ranges over prime numbers: $p \leq x\} \leq 4^{x-1}$.

(47) Let n be a natural number and p be a prime number. Suppose $n \neq 0$. Then there exists a finite sequence f of elements of $\mathbb{N}$ such that

(i) $\mathrm{len}\, f = n$,

(ii) for every natural number k such that $k \in \mathrm{dom}\, f$ holds $f(k) = 1$ iff $p^k \mid n$ and $f(k) = 0$ iff $p^k \nmid n$, and

(iii) p-count$(n) = \sum f$.

(48) Let n be a natural number and p be a prime number. Then there exists a finite sequence f of elements of $\mathbb{N}$ such that $\mathrm{len}\, f = n$ and for every natural number k such that $k \in \mathrm{dom}\, f$ holds $f(k) = \lfloor \frac{n}{p^k} \rfloor$ and p-count$(n!) = \sum f$.

(49) Let n be a natural number and p be a prime number. Then there exists a finite sequence f of elements of $\mathbb{R}$ such that $\mathrm{len}\, f = 2 \cdot n$ and for every natural number k such that $k \in \mathrm{dom}\, f$ holds $f(k) = \lfloor \frac{2 \cdot n}{p^k} \rfloor - 2 \cdot \lfloor \frac{n}{p^k} \rfloor$ and p-count$(\binom{2 \cdot n}{n}) = \sum f$.

Let f be a finite sequence of elements of $\mathbb{N}$ and let p be a prime number. The functor p-count(f) yielding a finite sequence of elements of $\mathbb{N}$ is defined by:

(Def. 1) $\mathrm{len}(p\text{-count}(f)) = \mathrm{len}\, f$ and for every set i such that $i \in \mathrm{dom}(p\text{-count}(f))$ holds $(p\text{-count}(f))(i) = p\text{-count}(f(i))$.

One can prove the following propositions:

(50) For every prime number p and for every finite sequence f of elements of $\mathbb{N}$ such that $f = \emptyset$ holds p-count$(f) = \emptyset$.

(51) For every prime number p and for all finite sequences f_1, f_2 of elements of $\mathbb{N}$ holds $p\text{-count}(f_1 \frown f_2) = (p\text{-count}(f_1)) \frown (p\text{-count}(f_2))$.

(52) For every prime number p and for every non empty natural number n holds $p\text{-count}(\langle n \rangle) = \langle p\text{-count}(n) \rangle$.

(53) For every finite sequence f of elements of $\mathbb{N}$ and for every prime number p such that $\prod f \neq 0$ holds $p\text{-count}(\prod f) = \sum(p\text{-count}(f))$.

(54) Let f_1, f_2 be finite sequences of elements of $\mathbb{R}$. Suppose $\operatorname{len} f_1 = \operatorname{len} f_2$ and for every natural number k such that $k \in \operatorname{dom} f_1$ holds $f_1(k) \leq f_2(k)$ and $f_1(k) > 0$. Then $\prod f_1 \leq \prod f_2$.

(55) For every natural number n and for every real number r such that $r > 0$ holds $\prod(n \mapsto r) = r^n$.

In this article we present several logical schemes. The scheme *scheme1* concerns a ternary predicate $\mathcal{P}$, and states that:

> Let p be a prime number, n be a natural number, m be a non empty natural number, and X be a set. If $X = \{p'^{p'\text{-count}(m)}; p'$ ranges over prime numbers: $\mathcal{P}[n, m, p']\}$, then $\prod \operatorname{Sgm} X > 0$

for all values of the parameters.

The scheme *scheme2* concerns a ternary predicate $\mathcal{P}$, and states that:

> Let p be a prime number, n be a natural number, m be a non empty natural number, and X be a set. If $X = \{p'^{p'\text{-count}(m)}; p'$ ranges over prime numbers: $\mathcal{P}[n, m, p']\}$ and $p^{p\text{-count}(m)} \notin X$, then $p\text{-count}(\prod \operatorname{Sgm} X) = 0$

for all values of the parameters.

The scheme *scheme3* concerns a ternary predicate $\mathcal{P}$, and states that:

> Let p be a prime number, n be a natural number, m be a non empty natural number, and X be a set. If $X = \{p'^{p'\text{-count}(m)}; p'$ ranges over prime numbers: $\mathcal{P}[n, m, p']\}$ and $p^{p\text{-count}(m)} \in X$, then $p\text{-count}(\prod \operatorname{Sgm} X) = p\text{-count}(m)$

for all values of the parameters.

The scheme *scheme4* deals with a binary functor $\mathcal{F}$ yielding a set and a binary predicate $\mathcal{P}$, and states that:

> Let n, m be natural numbers, r be a real number, and X be a finite set. If $X = \{\mathcal{F}(p, m); p$ ranges over prime numbers: $p \leq r \ \wedge\ \mathcal{P}[p, m]\}$ and $r \geq 0$, then $\operatorname{card} X \leq \lfloor r \rfloor$

for all values of the parameters.

5. Bertrand's Postulate

The following proposition is true

(56) For every natural number n such that $n \geq 1$ there exists a prime number p such that $n < p$ and $p \leq 2 \cdot n$.

References

[1] M. Aigner and G. M. Ziegler. *Proofs from THE BOOK*. Springer-Verlag, Berlin Heidelberg New York, 2004.

[2] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.

[3] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.

[4] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 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] Czesław Byliński. Binary operations applied to finite sequences. *Formalized Mathematics*, 1(**4**):643–649, 1990.

[8] Czesław Byliński. The complex numbers. *Formalized Mathematics*, 1(**3**):507–513, 1990.

[9] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.

[10] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**):55–65, 1990.

[11] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.

[12] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.

[13] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(**4**):661–668, 1990.

[14] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.

[15] Andrzej Kondracki. The Chinese Remainder Theorem. *Formalized Mathematics*, 6(**4**):573–577, 1997.

[16] Artur Korniłowicz and Piotr Rudnicki. Fundamental Theorem of Arithmetic. *Formalized Mathematics*, 12(**2**):179–186, 2004.

[17] Rafał Kwiatek. Factorial and Newton coefficients. *Formalized Mathematics*, 1(**5**):887–890, 1990.

[18] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relative primes. *Formalized Mathematics*, 1(**5**):829–832, 1990.

[19] W. J. LeVeque. *Fundamentals of Number Theory*. Dover Publication, New York, 1996.

[20] Takaya Nishiyama and Yasuho Mizuhara. Binary arithmetics. *Formalized Mathematics*, 4(**1**):83–86, 1993.

[21] Library Committee of the Association of Mizar Users. Binary operations on numbers. *To appear in Formalized Mathematics*.

[22] Konrad Raczkowski and Andrzej Nędzusiak. Real exponents and logarithms. *Formalized Mathematics*, 2(**2**):213–216, 1991.

[23] Piotr Rudnicki and Andrzej Trybulec. Multivariate polynomials with arbitrary number of variables. *Formalized Mathematics*, 9(**1**):95–110, 2001.

[24] Andrzej Trybulec. Subsets of complex numbers. *To appear in Formalized Mathematics*.

[25] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(**2**):329–334, 1990.

[26] Andrzej Trybulec. Tarski Grothendieck set theory. *Formalized Mathematics*, 1(**1**):9–11, 1990.

[27] Andrzej Trybulec. On the sets inhabited by numbers. *Formalized Mathematics*, 11(**4**):341–347, 2003.

[28] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.

[29] Wojciech A. Trybulec. Non-contiguous substrings and one-to-one finite sequences. *Formalized Mathematics*, 1(**3**):569–573, 1990.

[30] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(**1**):73–83, 1990.

[31] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(**1**):181–186, 1990.

Received May 17, 2006