

The Perfect Number Theorem and Wilson's Theorem

Marco Riccardi
Casella Postale 49
54038 Montignoso, Italy

Summary. This article formalizes proofs of some elementary theorems of number theory (see [1, 26]): Wilson's theorem (that n is prime iff $n > 1$ and $(n - 1)! \cong -1 \pmod{n}$), that all primes $(1 \pmod{4})$ equal the sum of two squares, and two basic theorems of Euclid and Euler about perfect numbers. The article also formally defines Euler's sum of divisors function ϕ , proves that ϕ is multiplicative and that $\sum_{k|n} \phi(k) = n$.

MML identifier: NAT_5, version: 7.11.02 4.120.1050

The articles [14], [38], [28], [32], [39], [11], [40], [13], [33], [12], [5], [4], [2], [6], [10], [37], [36], [25], [3], [15], [19], [35], [24], [30], [18], [34], [16], [9], [22], [21], [41], [17], [20], [7], [31], [29], [8], [23], and [27] provide the notation and terminology for this paper.

1. PRELIMINARIES

We adopt the following convention: k, n, m, l, p denote natural numbers and n_0, m_0 denote non zero natural numbers.

We now state several propositions:

- (1) $2^{n+1} < 2^{n+2} - 1$.
- (2) If n_0 is even, then there exist k, m such that m is odd and $k > 0$ and $n_0 = 2^k \cdot m$.
- (3) If $n = 2^k$ and m is odd, then n and m are relative prime.
- (4) $\{n\}$ is a finite subset of \mathbb{N} .
- (5) $\{n, m\}$ is a finite subset of \mathbb{N} .

In the sequel f is a finite sequence and x, X, Y are sets.

The following four propositions are true:

- (6) If f is one-to-one, then $f_{\upharpoonright n}$ is one-to-one.
- (7) If f is one-to-one and $n \in \text{dom } f$, then $f(n) \notin \text{rng}(f_{\upharpoonright n})$.
- (8) If $x \in \text{rng } f$ and $x \notin \text{rng}(f_{\upharpoonright n})$, then $x = f(n)$.
- (9) Let f_1 be a finite sequence of elements of \mathbb{N} and f_2 be a finite sequence of elements of X . If $\text{rng } f_1 \subseteq \text{dom } f_2$, then $f_2 \cdot f_1$ is a finite sequence of elements of X .

In the sequel f_1, f_2, f_3 are finite sequences of elements of \mathbb{R} .

Next we state four propositions:

- (10) If $X \cup Y = \text{dom } f_1$ and X misses Y and $f_2 = f_1 \cdot \text{Sgm } X$ and $f_3 = f_1 \cdot \text{Sgm } Y$, then $\sum f_1 = \sum f_2 + \sum f_3$.
- (11) If $f_2 = f_1 \cdot \text{Sgm } X$ and $\text{dom } f_1 \setminus f_1^{-1}(\{0\}) \subseteq X \subseteq \text{dom } f_1$, then $\sum f_1 = \sum f_2$.
- (12) $\sum f_1 = \sum(f_1 - \{0\})$.
- (13) Every finite sequence of elements of \mathbb{N} is a finite sequence of elements of \mathbb{R} .

In the sequel n_1, n_2, m_1, m_2 denote natural numbers.

We now state several propositions:

- (14) If $n_1 \in \text{NatDivisors } n$ and $m_1 \in \text{NatDivisors } m$ and n and m are relative prime, then n_1 and m_1 are relative prime.
- (15) If $n_1 \in \text{NatDivisors } n$ and $m_1 \in \text{NatDivisors } m$ and $n_2 \in \text{NatDivisors } n$ and $m_2 \in \text{NatDivisors } m$ and n and m are relative prime and $n_1 \cdot m_1 = n_2 \cdot m_2$, then $n_1 = n_2$ and $m_1 = m_2$.
- (16) If $n_1 \in \text{NatDivisors } n_0$ and $m_1 \in \text{NatDivisors } m_0$, then $n_1 \cdot m_1 \in \text{NatDivisors}(n_0 \cdot m_0)$.
- (17) If n_0 and m_0 are relative prime, then $k \text{ gcd } n_0 \cdot m_0 = (k \text{ gcd } n_0) \cdot (k \text{ gcd } m_0)$.
- (18) If n_0 and m_0 are relative prime and $k \in \text{NatDivisors}(n_0 \cdot m_0)$, then there exist n_1, m_1 such that $n_1 \in \text{NatDivisors } n_0$ and $m_1 \in \text{NatDivisors } m_0$ and $k = n_1 \cdot m_1$.
- (19) If p is prime, then $\text{NatDivisors}(p^n) = \{p^k; k \text{ ranges over elements of } \mathbb{N}; k \leq n\}$.
- (20) If $0 \neq l$ and $p > l$ and $p > n_1$ and $p > n_2$ and $l \cdot n_1 \text{ mod } p = l \cdot n_2 \text{ mod } p$ and p is prime, then $n_1 = n_2$.
- (21) If p is prime, then $p\text{-count}(n_0 \text{ gcd } m_0) = \min(p\text{-count}(n_0), p\text{-count}(m_0))$.

2. WILSON'S THEOREM

One can prove the following proposition

(22) n is prime iff $((n - 1)! + 1) \bmod n = 0$ and $n > 1$.

3. ALL PRIMES CONGRUENT TO 1 MODULO 4 ARE THE SUM OF TWO SQUARES

Next we state the proposition

(23) If p is prime and $p \bmod 4 = 1$, then there exist n, m such that $p = n^2 + m^2$.

4. THE SUM OF DIVISORS FUNCTION

Let I be a set, let f be a function from I into \mathbb{N} , and let J be a finite subset of I . Then $f \upharpoonright J$ is a bag of J .

Let I be a set, let f be a function from I into \mathbb{N} , and let J be a finite subset of I . Observe that $\sum(f \upharpoonright J)$ is natural.

We now state two propositions:

(24) Let f be a function from \mathbb{N} into \mathbb{N} , F be a function from \mathbb{N} into \mathbb{R} , and J be a finite subset of \mathbb{N} . If $f = F$ and there exists k such that $J \subseteq \text{Seg } k$, then $\sum(f \upharpoonright J) = \sum \text{FuncSeq}(F, \text{Sgm } J)$.

(25) Let I be a non empty set, F be a partial function from I to \mathbb{R} , f be a function from I into \mathbb{N} , and J be a finite subset of I . If $f = F$, then $\sum(f \upharpoonright J) = \sum_{\kappa=0}^J F(\kappa)$.

We follow the rules: I, j denote sets, f, g denote functions from I into \mathbb{N} , and J, K denote finite subsets of I .

We now state three propositions:

(26) If J misses K , then $\sum(f \upharpoonright (J \cup K)) = \sum(f \upharpoonright J) + \sum(f \upharpoonright K)$.

(27) $\sum(f \upharpoonright (\{j\})) = f(j)$.

(28) $\sum((\cdot_{\mathbb{N}} \cdot (f \times g)) \upharpoonright (J \times K)) = \sum(f \upharpoonright J) \cdot \sum(g \upharpoonright K)$.

Let k be a natural number. The functor $\text{EXP } k$ yielding a function from \mathbb{N} into \mathbb{N} is defined by:

(Def. 1) For every natural number n holds $(\text{EXP } k)(n) = n^k$.

Let k, n be natural numbers. The functor $\sigma_k(n)$ yields an element of \mathbb{N} and is defined as follows:

(Def. 2)(i) For every non zero natural number m such that $n = m$ holds $\sigma_k(n) = \sum(\text{EXP } k \upharpoonright \text{NatDivisors } m)$ if $n \neq 0$,

(ii) $\sigma_k(n) = 0$, otherwise.

Let k be a natural number. The functor Σk yields a function from \mathbb{N} into \mathbb{N} and is defined by:

(Def. 3) For every natural number n holds $(\Sigma k)(n) = \sigma_k(n)$.

Let n be a natural number. The functor $\sigma(n)$ yields an element of \mathbb{N} and is defined as follows:

(Def. 4) $\sigma(n) = \sigma_1(n)$.

The following propositions are true:

$$(29) \quad \sigma_k(1) = 1.$$

$$(30) \quad \text{If } p \text{ is prime, then } \sigma(p^n) = \frac{p^{n+1}-1}{p-1}.$$

$$(31) \quad \text{If } m \mid n_0 \text{ and } n_0 \neq m \neq 1, \text{ then } 1 + m + n_0 \leq \sigma(n_0).$$

$$(32) \quad \text{If } m \mid n_0 \text{ and } k \mid n_0 \text{ and } n_0 \neq m \text{ and } n_0 \neq k \text{ and } m \neq 1 \text{ and } k \neq 1 \text{ and } m \neq k, \text{ then } 1 + m + k + n_0 \leq \sigma(n_0).$$

$$(33) \quad \text{If } \sigma(n_0) = n_0 + m \text{ and } m \mid n_0 \text{ and } n_0 \neq m, \text{ then } m = 1 \text{ and } n_0 \text{ is prime.}$$

Let f be a function from \mathbb{N} into \mathbb{N} . We say that f is multiplicative if and only if:

(Def. 5) For all non zero natural numbers n_0, m_0 such that n_0 and m_0 are relative prime holds $f(n_0 \cdot m_0) = f(n_0) \cdot f(m_0)$.

One can prove the following propositions:

(34) Let f, F be functions from \mathbb{N} into \mathbb{N} . Suppose f is multiplicative and for every n_0 holds $F(n_0) = \sum(f \upharpoonright \text{NatDivisors } n_0)$. Then F is multiplicative.

(35) $\text{EXP } k$ is multiplicative.

(36) Σk is multiplicative.

(37) If n_0 and m_0 are relative prime, then $\sigma(n_0 \cdot m_0) = \sigma(n_0) \cdot \sigma(m_0)$.

5. TWO BASIC THEOREMS ON PERFECT NUMBERS

Let n_0 be a non zero natural number. We say that n_0 is perfect if and only if:

(Def. 6) $\sigma(n_0) = 2 \cdot n_0$.

We now state two propositions:

(38) If $2^p - 1$ is prime and $n_0 = 2^{p-1} \cdot (2^p - 1)$, then n_0 is perfect.

(39) If n_0 is even and perfect, then there exists a natural number p such that $2^p - 1$ is prime and $n_0 = 2^{p-1} \cdot (2^p - 1)$.

6. A FORMULA INVOLVING EULER'S ϕ FUNCTION

The function ϕ from \mathbb{N} into \mathbb{N} is defined by:

(Def. 7) For every element k of \mathbb{N} holds $\phi(k) = \text{Euler } k$.

The following proposition is true

$$(40) \quad \sum(\phi \upharpoonright \text{NatDivisors } n_0) = n_0.$$

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. König's theorem. *Formalized Mathematics*, 1(3):589–593, 1990.
- [5] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(1):91–96, 1990.
- [6] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(1):107–114, 1990.
- [7] Józef Białas. Infimum and supremum of the set of real numbers. Measure theory. *Formalized Mathematics*, 2(1):163–171, 1991.
- [8] Czesław Byliński. Basic functions and operations on functions. *Formalized Mathematics*, 1(1):245–254, 1990.
- [9] Czesław Byliński. The complex numbers. *Formalized Mathematics*, 1(3):507–513, 1990.
- [10] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(3):529–536, 1990.
- [11] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(1):55–65, 1990.
- [12] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(1):153–164, 1990.
- [13] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(2):357–367, 1990.
- [14] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(1):47–53, 1990.
- [15] Czesław Byliński. The sum and product of finite sequences of real numbers. *Formalized Mathematics*, 1(4):661–668, 1990.
- [16] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(1):165–167, 1990.
- [17] Yoshinori Fujisawa and Yasushi Fuwa. The Euler's function. *Formalized Mathematics*, 6(4):549–551, 1997.
- [18] Yoshinori Fujisawa, Yasushi Fuwa, and Hidetaka Shimizu. Public-key cryptography and Pepin's test for the primality of Fermat numbers. *Formalized Mathematics*, 7(2):317–321, 1998.
- [19] Krzysztof Hryniewiecki. Basic properties of real numbers. *Formalized Mathematics*, 1(1):35–40, 1990.
- [20] Krzysztof Hryniewiecki. Recursive definitions. *Formalized Mathematics*, 1(2):321–328, 1990.
- [21] Magdalena Jastrzębska and Adam Grabowski. On the properties of the Möbius function. *Formalized Mathematics*, 14(1):29–36, 2006, doi:10.2478/v10037-006-0005-0.
- [22] Artur Korniłowicz and Piotr Rudnicki. Fundamental Theorem of Arithmetic. *Formalized Mathematics*, 12(2):179–186, 2004.
- [23] Jarosław Kotowicz and Yuji Sakai. Properties of partial functions from a domain to the set of real numbers. *Formalized Mathematics*, 3(2):279–288, 1992.
- [24] Rafał Kwiatek. Factorial and Newton coefficients. *Formalized Mathematics*, 1(5):887–890, 1990.
- [25] Rafał Kwiatek and Grzegorz Zwara. The divisibility of integers and integer relative primes. *Formalized Mathematics*, 1(5):829–832, 1990.
- [26] W. J. LeVeque. *Fundamentals of Number Theory*. Dover Publication, New York, 1996.
- [27] Takaya Nishiyama and Yasuho Mizuhara. Binary arithmetics. *Formalized Mathematics*, 4(1):83–86, 1993.

- [28] Beata Padlewska. Families of sets. *Formalized Mathematics*, 1(1):147–152, 1990.
- [29] Piotr Rudnicki. Little Bezout theorem (factor theorem). *Formalized Mathematics*, 12(1):49–58, 2004.
- [30] Piotr Rudnicki and Andrzej Trybulec. Abian’s fixed point theorem. *Formalized Mathematics*, 6(3):335–338, 1997.
- [31] Piotr Rudnicki and Andrzej Trybulec. Multivariate polynomials with arbitrary number of variables. *Formalized Mathematics*, 9(1):95–110, 2001.
- [32] Andrzej Trybulec. Binary operations applied to functions. *Formalized Mathematics*, 1(2):329–334, 1990.
- [33] Andrzej Trybulec. Tuples, projections and Cartesian products. *Formalized Mathematics*, 1(1):97–105, 1990.
- [34] Andrzej Trybulec. On the sets inhabited by numbers. *Formalized Mathematics*, 11(4):341–347, 2003.
- [35] Andrzej Trybulec and Czesław Byliński. Some properties of real numbers. *Formalized Mathematics*, 1(3):445–449, 1990.
- [36] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(3):501–505, 1990.
- [37] Wojciech A. Trybulec. Non-contiguous substrings and one-to-one finite sequences. *Formalized Mathematics*, 1(3):569–573, 1990.
- [38] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(1):67–71, 1990.
- [39] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1(1):73–83, 1990.
- [40] Edmund Woronowicz. Relations defined on sets. *Formalized Mathematics*, 1(1):181–186, 1990.
- [41] Hiroshi Yamazaki, Yasunari Shidama, and Yatsuka Nakamura. Bessel’s inequality. *Formalized Mathematics*, 11(2):169–173, 2003.

Received March 3, 2009
