FORMALIZED MATHEMATICS
Vol. 24, No. 3, Pages 187–198, 2016
DOI: 10.1515/forma-2016-0015

DE GRUYTER OPEN
degruyter.com/view/j/forma

Prime Factorization of Sums and Differences of Two Like Powers

Rafał Ziobro
Department of Carbohydrate Technology
University of Agriculture
Krakow, Poland

Summary. Representation of a non zero integer as a signed product of primes is unique similarly to its representations in various types of positional notations [4], [3]. The study focuses on counting the prime factors of integers in the form of sums or differences of two equal powers (thus being represented by 1 and a series of zeroes in respective digital bases).

Although the introduced theorems are not particularly important, they provide a couple of shortcuts useful for integer factorization, which could serve in further development of Mizar projects [2]. This could be regarded as one of the important benefits of proof formalization [9].

MSC: 11A51 03B35

Keywords: integers; factorization; primes

MML identifier: NEWTON03, version: 8.1.05 5.37.1275

From now on a, b, c, d, x, j, k, l, m, n, o denote natural numbers, p, q, t, z, u, v denote integers, and a_1, b_1, c_1, d_1 denote complexes.

Now we state the propositions:

(1) $a_1{}^{n+k} + b_1{}^{n+k} = a_1{}^{n} \cdot (a_1{}^{k} + b_1{}^{k}) + b_1{}^{k} \cdot (b_1{}^{n} - a_1{}^{n})$.

(2) $a_1{}^{n+k} - b_1{}^{n+k} = a_1{}^{n} \cdot (a_1{}^{k} - b_1{}^{k}) + b_1{}^{k} \cdot (a_1{}^{n} - b_1{}^{n})$.

(3) $a_1{}^{m+2} + b_1{}^{m+2} = (a_1 + b_1) \cdot (a_1{}^{m+1} + b_1{}^{m+1}) - a_1 \cdot b_1 \cdot (a_1{}^{m} + b_1{}^{m})$.

Let a be a natural number. Let us note that a is trivial if and only if the condition (Def. 1) is satisfied.

(Def. 1) $a \leqslant 1$.

Let a be a complex. Let us note that the functor $a^{\mathbf{2}}$ yields a set and is defined by the term

ISSN 1426–2630(Print), 1898-9934(Online)

(Def. 2) a^2.

Let a, b be integers. The functors: $\gcd(a, b)$ and $\mathrm{lcm}(a, b)$ yielding natural numbers are defined by terms

(Def. 3) $\gcd(|a|, |b|)$,

(Def. 4) $\mathrm{lcm}(|a|, |b|)$,

respectively. Let a, b be positive real numbers. Note that $\max(a, b)$ is positive and $\min(a, b)$ is positive.

Let a be a non zero integer and b be an integer. One can check that $\gcd(a, b)$ is non zero.

Let a be a non zero complex and n be a natural number. Let us observe that a^n is non zero.

Let a be a non trivial natural number and n be a non zero natural number. Note that a^n is non trivial.

Let a be an integer. One can check that $|a|$ is natural.

Let a be an even integer. Note that $|a|$ is even.

Let a be a natural number. Let us note that $\mathrm{lcm}(a, a)$ reduces to a and $\gcd(a, a)$ reduces to a.

Let a be a non zero integer and b be an integer. Note that $\gcd(a, b)$ is positive.

Let a, b be integers. One can check that $\gcd(a, \gcd(a, b))$ reduces to $\gcd(a, b)$ and $\mathrm{lcm}(a, \mathrm{lcm}(a, b))$ reduces to $\mathrm{lcm}(a, b)$.

Let a be an integer. Observe that $\gcd(a, 1)$ reduces to 1 and $\gcd(a + 1, a)$ reduces to 1.

Now we state the proposition:

(4) Let us consider integers t, z. Then $\gcd(t^n, z^n) = (\gcd(t, z))^n$.

Let a be an integer and n be a natural number.

One can verify that $\gcd((a + 1)^n, a^n)$ reduces to 1.

Let us consider a_1 and b_1. One can verify that ${a_1}^0 - {b_1}^0$ reduces to 0.

Let a be a non negative real number and n be a natural number. One can verify that a^n is non negative and there exists an odd natural number which is non trivial and there exists an even natural number which is non trivial.

Let a be a positive real number and n be a natural number. One can verify that a^n is positive.

Let a be an integer. One can verify that $a \cdot a$ is square and $\frac{a}{a}$ is square and there exists an element of $\mathbb{N}$ which is non square and every element of $\mathbb{N}$ which is prime is also non square and there exists a prime natural number which is even and there exists a prime natural number which is odd and every integer which is prime is also non square.

Let a be a square element of $\mathbb{N}$. Observe that $\sqrt{a}$ is natural.

Let a be an integer. Let us note that a^2 is square and $a \cdot a$ is square and there exists an integer which is non square and every natural number which is zero is also trivial and there exists a natural number which is square and there exists an element of $\mathbb{N}$ which is non zero and there exists a square element of $\mathbb{N}$ which is non trivial and every natural number which is trivial is also square and every integer which is non square is also non zero.

Now we state the propositions:

(5) Let us consider integers a, b, c, d. If $a \mid b$ and $c \mid d$, then $a \cdot c \mid b \cdot d$.

(6) Let us consider integers a, b. Then $a \mid b$ if and only if $\operatorname{lcm}(a, b) = |b|$.
PROOF: If $a \mid b$, then $\operatorname{lcm}(a, b) = |b|$ by [8, (16)], [7, (44)]. □

Let a be an integer. Observe that $\operatorname{lcm}(a, 0)$ reduces to 0.

Let a be a natural number. Note that $\operatorname{lcm}(a, 1)$ reduces to a.

Let us consider a and b. Let us observe that $\operatorname{lcm}(a \cdot b, a)$ reduces to $a \cdot b$ and $\operatorname{lcm}(\gcd(a, b), b)$ reduces to b and $\gcd(a, \operatorname{lcm}(a, b))$ reduces to a.

Let us consider integers a, b. Now we state the propositions:

(7) $|a \cdot b| = (\gcd(a, b)) \cdot \operatorname{lcm}(a, b)$.

(8) $\operatorname{lcm}(a^n, b^n) = \operatorname{lcm}(a, b)^n$. The theorem is a consequence of (4) and (7).

Let a be a square element of $\mathbb{N}$ and b be a square element of $\mathbb{N}$. One can check that $\gcd(a, b)$ is square and $\operatorname{lcm}(a, b)$ is square.

Let a, b be square integers. One can verify that $\gcd(a, b)$ is square and $\operatorname{lcm}(a, b)$ is square.

Now we state the proposition:

(9) Let us consider an integer t. Then t is odd if and only if $\gcd(t, 2) = 1$.
PROOF: If t is odd, then $\gcd(t, 2) = 1$ by [13, (1)], [14, (5)]. □

Let t be an integer. One can check that t is odd if and only if the condition (Def. 5) is satisfied.

(Def. 5) $\gcd(t, 2) = 1$.

Let a be an odd integer. Let us observe that $|a|$ is odd and $-a$ is odd.

Let a, b be even integers. Note that $\gcd(a, b)$ is even.

Let a be an integer and b be an odd integer. Note that $\gcd(a, b)$ is odd.

Let a be a natural number. One can check that $|-a|$ reduces to a.

Let t, z be even integers. One can check that $t + z$ is even and $t - z$ is even and $t \cdot z$ is even.

Let t, z be odd integers. Note that $t + z$ is even and $t - z$ is even and $t \cdot z$ is odd.

Let t be an odd integer and z be an even integer. Let us observe that $t + z$ is odd and $t - z$ is odd and $t \cdot z$ is even.

Now we state the proposition:

(10) Let us consider a non zero, square integer a, and an integer b. If $a \cdot b$ is square, then b is square.

Let a be a square element of $\mathbb{N}$ and n be a natural number. Let us observe that a^n is square.

Let a be a square integer. Note that a^n is square.

Let a be a non zero, square integer and b be a non square integer. Let us note that $a \cdot b$ is non square.

Let a be an element of $\mathbb{N}$ and b be an even natural number. Note that a^b is square.

Let a be a non square element of $\mathbb{N}$ and b be an odd natural number. Note that a^b is non square.

Let a be a non zero, square integer. Note that $a+1$ is non square.

Let a be a non zero, square element of $\mathbb{N}$. Let us observe that $a+1$ is non square.

Let a be a non zero, square object and b be a non square element of $\mathbb{N}$. Let us observe that $a \cdot b$ is non square.

Let a be a non zero, square integer and n, m be natural numbers. Let us observe that $a^n + a^m$ is non square.

Let a be a non zero, square element of $\mathbb{N}$. Let us note that $a^n + a^m$ is non square.

Let a be a non zero, square integer and p be a prime natural number. Note that $p \cdot a$ is non square.

Let a be a non trivial element of $\mathbb{N}$. One can verify that $a-1$ is non zero.

Let q be a square integer. Let us observe that $|q|$ is square.

Let x be a non zero integer. Let us observe that $|x|$ is non zero.

Let a be a non trivial, square element of $\mathbb{N}$. Let us observe that $a-1$ is non square.

Let a be a non trivial element of $\mathbb{N}$. Let us note that $a \cdot (a-1)$ is non square.

Let a, b be integers and n, m be natural numbers. One can verify that $(a^n + b^n) \cdot (a^m - b^m) + (a^m + b^m) \cdot (a^n - b^n)$ is even and $(a^n + b^n) \cdot (a^m + b^m) + (a^m - b^m) \cdot (a^n - b^n)$ is even.

Let a be an even integer. Let us note that $\frac{a}{2}$ is integer.

Let a, b be non zero natural numbers. Note that $a+b$ is non trivial.

Let b be a non zero natural number and a, c be non trivial natural numbers. Let us observe that c-count$(c^{a\text{-count}(b)})$ reduces to a-count(b).

Let a, b be non zero integers. Let us note that $\frac{a}{\gcd(a,b)}$ is integer and $\frac{\operatorname{lcm}(a,b)}{b}$ is integer and $\frac{\operatorname{lcm}(a,b)}{\gcd(a,b)}$ is integer.

Let a be an even integer. One can verify that $\gcd(a, 2)$ reduces to 2.

Let us observe that there exists an even natural number which is non zero.

Let a be an even integer and n be a non zero natural number. Let us observe that $a \cdot n$ is even and a^n is even.

Let a be an integer and n be a zero natural number. One can check that $a \cdot n$ is even and a^n is odd.

Let a be an element of $\mathbb{N}$. Note that $|a|$ reduces to a.

One can check that every integer which is non negative is also natural.

Let a be a non negative real number and n be a non zero natural number. Let us note that $\sqrt[n]{a^n}$ reduces to a and $(\sqrt[n]{a})^n$ reduces to a.

Now we state the propositions:

(11) If $a \nmid b$, then $a \cdot c \nmid b$.

(12) Let us consider non negative real numbers a, b, and a positive natural number n. Then $a^n = b^n$ if and only if $a = b$.

Let a be a real number and n be an even natural number. One can verify that a^n is non negative.

Let a be a negative real number and n be an odd natural number. One can verify that a^n is negative.

Now we state the propositions:

(13) Let us consider real numbers a, b, and an odd natural number n. Then $a^n = b^n$ if and only if $a = b$. The theorem is a consequence of (12).

(14) If a and b are relatively prime, then for every non zero natural number n, $a \cdot b = c^n$ iff $\sqrt[n]{a}, \sqrt[n]{b} \in \mathbb{N}$ and $c = \sqrt[n]{a} \cdot \sqrt[n]{b}$.
Proof: If $a \cdot b = c^n$, then $\sqrt[n]{a}, \sqrt[n]{b} \in \mathbb{N}$ and $c = \sqrt[n]{a} \cdot \sqrt[n]{b}$ by [14, (30)], [11, (11)], [1, (14)]. □

(15) Let us consider a non zero natural number n, an integer a, and an integer b. Then $b^n \mid a^n$ if and only if $b \mid a$.
Proof: If $b^n \mid a^n$, then $b \mid a$ by [10, (1)], [14, (3)], (4), [5, (3)]. □

(16) Let us consider an integer a, and natural numbers m, n. If $m \geqslant n$, then $a^n \mid a^m$.

(17) Let us consider integers a, b. If $a \mid b$ and $b^m \mid c$, then $a^m \mid c$. The theorem is a consequence of (4).

(18) Let us consider integers a, p. If $p^{2 \cdot n+k} \mid a^2$, then $p^n \mid a$. The theorem is a consequence of (16), (4), and (12).

(19) Let us consider odd, square elements a, b of $\mathbb{N}$. Then $8 \mid a - b$.

Let us consider odd natural numbers a, b. Now we state the propositions:

(20) If $4 \mid a - b$, then $4 \nmid a^n + b^n$.

(21) If $4 \mid a^n + b^n$, then $4 \nmid a^{2 \cdot n} + b^{2 \cdot n}$.

(22) If $4 \mid a^n - b^n$, then $4 \nmid a^{2 \cdot n} + b^{2 \cdot n}$.

(23) Let us consider odd natural numbers a, b. If $2^m \mid a^n - b^n$, then $2^{m+1} \mid a^{2 \cdot n} - b^{2 \cdot n}$.

(24) ${a_1}^3 - {b_1}^3 = (a_1 - b_1) \cdot ({a_1}^2 + {b_1}^2 + a_1 \cdot b_1)$. The theorem is a consequence of (2).

(25) Let us consider an odd natural number n. Then $3 \mid a^n + b^n$ if and only if $3 \mid a + b$.

PROOF: Consider k such that $n = 2 \cdot k + 1$. If $3 \mid a^n + b^n$, then $3 \mid a + b$ by [14, (173)], [5, (4)], [8, (1), (10)]. □

(26) Let us consider an integer c. If $c \mid a - b$, then $c \mid a^n - b^n$.

(27) Let us consider an odd natural number n. Then $3 \mid a^n - b^n$ if and only if $3 \mid a - b$.

PROOF: Consider k such that $n = 2 \cdot k + 1$. If $3 \mid a^n - b^n$, then $3 \mid a - b$ by [14, (173)], [8, (10)], [5, (4)], [8, (1)]. □

(28) Let us consider a natural number n. Then $a^n \equiv (a - b)^n \pmod{b}$.

(29) Let us consider a non trivial natural number a. Then there exists a prime natural number n such that $n \mid a$.

(30) Let us consider a prime natural number p. If $p \mid (p+(k+1)) \cdot (p-(k+1))$, then $k + 1 \geqslant p$.

(31) Let us consider a prime natural number p, and a non zero natural number k. If $k < p$, then $p \nmid p^2 - k^2$. The theorem is a consequence of (30).

(32) Let us consider integers a, b, and an odd, prime natural number p. If $p \nmid b$, then if $p \mid a - b$, then $p \nmid a + b$.

(33) Let us consider a non zero, square element a of $\mathbb{N}$, and a prime natural number p. If $p \mid a$, then $a + p$ is not square.

(34) Let us consider a non zero, square element a of $\mathbb{N}$, and a prime natural number p. If $a + p$ is square, then $p = 2 \cdot \sqrt{a} + 1$.

(35) Let us consider integers a, b, c. Suppose a and b are relatively prime. Then $\gcd(c, a \cdot b) = (\gcd(c, a)) \cdot (\gcd(c, b))$.

(36) Let us consider a prime natural number p. If $a \mid p^n$, then there exists k such that $a = p^k$.

Let us consider non zero natural numbers a, b and a prime natural number p. Now we state the propositions:

(37) If $a + b = p$, then a and b are relatively prime.

(38) If $a^n + b^n = p^n$, then a and b are relatively prime.

(39) Let us consider non zero natural numbers a, b. If $c \geqslant a + b$, then $c^{k+1} \cdot (a + b) > a^{k+2} + b^{k+2}$.

(40) Let us consider natural numbers a, c, and a non zero natural number b. If $a \cdot b < c < a \cdot (b+1)$, then $a \nmid c$ and $c \nmid a$.

(41) Let us consider real numbers a, b. Then $a + b = \min(a, b) + \max(a, b)$.

(42) Let us consider non negative real numbers a, b. Then

(i) $\max(a^n, b^n) = (\max(a, b))^n$, and

(ii) $\min(a^n, b^n) = (\min(a, b))^n$.

(43) Let us consider a prime natural number p. Suppose $a \cdot b = p^n$. Then there exist natural numbers k, l such that

(i) $a = p^k$, and

(ii) $b = p^l$, and

(iii) $k + l = n$.

(44) Let us consider non trivial natural numbers a, b. If a and b are relatively prime, then $a \nmid b$ and $b \nmid a$.

(45) Let us consider a non trivial natural number a, and a prime natural number p. If $p > a$, then $p \nmid a$ and $a \nmid p$. The theorem is a consequence of (44).

(46) Let us consider a prime natural number p. Then

(i) $\gcd(a, p) = 1$, or

(ii) $\gcd(a, p) = p$.

(47) Let us consider a non trivial natural number a, and a prime natural number p. If $a \mid p^n$, then $p \mid a$. The theorem is a consequence of (46).

(48) Let us consider odd natural numbers a, b, and an even natural number m. Then $2\text{-count}(a^m + b^m) = 1$.

(49) Let us consider a non zero natural number a. Then there exists an odd natural number k such that $a = 2^{2\text{-count}(a)} \cdot k$.

(50) Let us consider a non zero natural number b. Suppose $a > b$. Then there exists a prime natural number p such that $p\text{-count}(a) > p\text{-count}(b)$.
PROOF: If for every prime natural number p, $p\text{-count}(a) \leqslant p\text{-count}(b)$, then $a \leqslant b$ by [12, (20)], [1, (14)]. $\square$

(51) Let us consider natural numbers a, b, c. Suppose $a \neq 1$ and $b \neq 0$ and $c \neq 0$ and $b > a\text{-count}(c)$. Then $a^b \nmid c$. The theorem is a consequence of (11).

Let us consider a non zero integer b and an integer a. Now we state the propositions:

(52) If $|a| \neq 1$, then $a^{|a|\text{-count}(|b|)} \mid b$ and $a^{(|a|\text{-count}(|b|))+1} \nmid b$.

(53) If $|a| \neq 1$, then if $a^n \mid b$ and $a^{n+1} \nmid b$, then $n = |a|\text{-count}(|b|)$.

(54) Let us consider a non zero natural number b, and a non trivial natural number a. Then $a \mid b$ if and only if a-count$(\gcd(a, b)) = 1$.
PROOF: If $a \mid b$, then a-count$(\gcd(a, b)) = 1$ by [14, (3)], [6, (22)]. □

(55) Let us consider non zero natural numbers b, n, and a non trivial natural number a. Then a-count$(\gcd(a, b)) = 1$ if and only if a^n-count$((\gcd(a, b))^n) = 1$. The theorem is a consequence of (15), (54), and (4).

(56) Let us consider a non zero natural number b, and a non trivial natural number a. Then a-count$(\gcd(a, b)) = 0$ if and only if a-count$(\gcd(a, b)) \neq 1$. The theorem is a consequence of (54).

Let a, b be integers. The functor a-count(b) yielding a natural number is defined by the term

(Def. 6) $|a|$-count$(|b|)$.

Let a be an integer. Assume $|a| \neq 1$. Let b be a non zero integer. One can check that the functor a-count(b) is defined by

(Def. 7) $a^{it} \mid b$ and $a^{it+1} \nmid b$.

Now we state the propositions:

(57) Let us consider a prime natural number p, and non zero integers a, b. Then p-count$(a \cdot b) = (p$-count$(a)) + (p$-count$(b))$.

(58) Let us consider a non trivial natural number a, and a non zero natural number b. Then $a^{a\text{-count}(b)} \leqslant b$.

(59) Let us consider a non trivial natural number a, and a non zero integer b. Then $a^n \mid b$ if and only if $n \leqslant a$-count(b).
PROOF: If $a^n \mid b$, then $n \leqslant a$-count(b) by [8, (9)], [7, (89)], [1, (13)]. If $a^n \nmid b$, then a-count$(b) < n$ by [8, (9)], [7, (89)]. □

(60) Let us consider a non trivial natural number a, a non zero integer b, and a non zero natural number n. Then $n \cdot (a$-count$(b)) \leqslant a$-count$(b^n) < n \cdot ((a$-count$(b)) + 1)$. The theorem is a consequence of (4) and (59).

(61) Let us consider a non trivial natural number a, and non zero natural numbers b, n. If $b < a$, then a-count$(b^n) < n$. The theorem is a consequence of (60).

(62) Let us consider a non trivial natural number a, and a non zero natural number b. If $b < a^n$, then a-count$(b) < n$. The theorem is a consequence of (59).

(63) Let us consider non zero natural numbers a, b, and a non trivial natural number n. Then $a + b$-count$(a^n + b^n) < n$. The theorem is a consequence of (62).

(64) Let us consider non zero natural numbers a, b. Then $\gcd(a, b) = 1$ if and only if for every non trivial natural number c, $(c$-count$(a)) \cdot (c$-count$(b)) = 0$.

Proof: If $\gcd(a,b) = 1$, then for every non trivial natural number c, $(c\text{-count}(a)) \cdot (c\text{-count}(b)) = 0$ by [6, (27)]. If for every prime natural number c, $(c\text{-count}(a)) \cdot (c\text{-count}(b)) = 0$, then $\gcd(a,b) = 1$ by [6, (27)]. $\square$

Let us consider a non zero, even natural number m and odd natural numbers a, b. Now we state the propositions:

(65) If $a \neq b$, then $2\text{-count}(a^{2 \cdot m} - b^{2 \cdot m}) \geqslant (2\text{-count}(a^m - b^m)) + 1$. The theorem is a consequence of (12), (23), and (59).

(66) If $a \neq b$, then $2\text{-count}(a^{2 \cdot m} - b^{2 \cdot m}) = (2\text{-count}(a^m - b^m)) + 1$. The theorem is a consequence of (12), (57), and (48).

Let us consider a prime natural number p and integers a, b. Now we state the propositions:

(67) If $|a| \neq |b|$, then $p\text{-count}(a^2 - b^2) = (p\text{-count}(a - b)) + (p\text{-count}(a + b))$.

(68) If $|a| \neq |b|$, then $p\text{-count}(a^3 - b^3) = (p\text{-count}(a - b)) + (p\text{-count}(a^2 + a \cdot b + b^2))$. The theorem is a consequence of (24).

(69) Let us consider non zero natural numbers a, b. Then $\frac{a}{\gcd(a,b)} = \frac{\operatorname{lcm}(a,b)}{b}$.

Let us consider a non zero natural number b. Now we state the propositions:

(70) $\operatorname{lcm}(a, a \cdot n + b) = ((\frac{a \cdot n}{b}) + 1) \cdot \operatorname{lcm}(a,b)$. The theorem is a consequence of (69).

(71) $\operatorname{lcm}(a, (n \cdot a + 1) \cdot b) = (n \cdot a + 1) \cdot \operatorname{lcm}(a,b)$. The theorem is a consequence of (70).

(72) Let us consider a non trivial natural number a, and non zero natural numbers n, b. Then $a\text{-count}(b) \geqslant n \cdot (a^n\text{-count}(b))$. The theorem is a consequence of (51).

Let us consider odd integers a, b. Now we state the propositions:

(73) $4 \mid a - b$ if and only if $4 \nmid a + b$.

(74) $2\text{-count}(a^2 + b^2) = 1$. The theorem is a consequence of (5) and (73).

(75) Let us consider a prime natural number p, and natural numbers a, b. Suppose $a \neq b$. Then $p\text{-count}(a + b) \geqslant p\text{-count}(\gcd(a,b))$.

(76) Let us consider a non zero integer a, a non trivial natural number b, and an integer c. If $a = b^{b\text{-count}(a)} \cdot c$, then $b \nmid c$.

Let a be a non zero integer and b be a non trivial natural number. Let us note that $\frac{a}{b^{b\text{-count}(a)}}$ is integer and $\frac{a}{2^{2\text{-count}(a)}}$ is integer and $\frac{a}{2^{2\text{-count}(a)}}$ is odd.

Now we state the proposition:

(77) Let us consider a non zero integer a, and a non trivial natural number b. Then $b\text{-count}(a) = 0$ if and only if $b \nmid a$.

Let a be an odd integer. Observe that $2\text{-count}(a)$ is zero.

Observe that $\frac{a}{2^{2\text{-count}(a)}}$ reduces to a.

Now we state the propositions:

(78) Let us consider a prime natural number a, a non zero integer b, and a natural number c. Then a-count$(b^c) = c \cdot (a\text{-count}(b))$.

(79) Let us consider non zero natural numbers a, b, and an odd natural number n. Then $\frac{a^{n+2}+b^{n+2}}{a+b} = a^{n+1} + b^{n+1} - a \cdot b \cdot (\frac{a^n+b^n}{a+b})$. The theorem is a consequence of (3).

(80) Let us consider odd integers a, b, and a natural number n. Then 2-count$(a^{2 \cdot n+1} - b^{2 \cdot n+1}) =$ 2-count$(a - b)$. The theorem is a consequence of (13), (2), and (57).

(81) Let us consider odd integers a, b, and an odd natural number m. Then 2-count$(a^m + b^m) =$ 2-count$(a + b)$. The theorem is a consequence of (80).

(82) Let us consider odd natural numbers a, b. Suppose $a \neq b$. Then $1 = \min(2\text{-count}(a - b), 2\text{-count}(a + b))$.

Let us consider a non trivial natural number a and non zero integers b, c. Now we state the propositions:

(83) If a-count$(b) > a$-count(c), then $a^{a\text{-count}(c)} \mid b$ and $a^{a\text{-count}(b)} \nmid c$.

(84) If $a^{a\text{-count}(b)} \mid c$ and $a^{a\text{-count}(c)} \mid b$, then a-count$(b) = a$-count(c). The theorem is a consequence of (83).

(85) Let us consider integers a, b, and natural numbers m, n. If $a^n \mid b$ and $a^m \nmid b$, then $m > n$. The theorem is a consequence of (16).

Let us consider a non trivial natural number a and non zero integers b, c. Now we state the propositions:

(86) If a-count$(b) = a$-count(c) and $a^n \mid b$, then $a^n \mid c$. The theorem is a consequence of (85).

(87) a-count$(b) = a$-count(c) if and only if for every natural number n, $a^n \mid b$ iff $a^n \mid c$.

PROOF: If a-count$(b) \neq a$-count(c), then there exists a natural number n such that $a^n \mid b$ and $a^n \nmid c$ or $a^n \mid c$ and $a^n \nmid b$ by (83), [1, (13)], [7, (89)], [8, (9)]. □

(88) Let us consider odd integers a, b. Suppose $|a| \neq |b|$. Then

(i) 2-count$((a - b)^2) \neq$ 2-count$((a + b)^2)$, and

(ii) 2-count$((a - b)^2) \neq (2\text{-count}(a^2)) - b^2$.

The theorem is a consequence of (78), (73), and (87).

(89) Let us consider a non trivial natural number b, and a non zero integer a. Then b-count$(a) \neq 0$ if and only if $b \mid a$.

PROOF: b-count$(|a|) \neq 0$ iff $b \mid |a|$ by [6, (27)]. □

(90) Let us consider a non trivial natural number b, and a non zero natural number a. Then $b\text{-count}(a) = 0$ if and only if $a \bmod b \neq 0$. The theorem is a consequence of (89).

(91) Let us consider a prime natural number p, and a non trivial natural number a. Then $a\text{-count}(p) \leqslant 1$.

(92) Let us consider non trivial natural numbers a, b, and a non zero natural number c. Then $a^{(a\text{-count}(b))\cdot(b\text{-count}(c))} \leqslant c$. The theorem is a consequence of (58).

(93) Let us consider a prime natural number p, a non trivial natural number a, and a non zero natural number b. Then $a\text{-count}(p^b) \leqslant b$. The theorem is a consequence of (89) and (59).

(94) Let us consider a prime natural number p, and a non trivial natural number a. Then $(p\text{-count}(a))\cdot(a\text{-count}(p^n)) \leqslant n$. The theorem is a consequence of (92).

(95) Let us consider non trivial natural numbers a, b, and a non zero natural number c. Then $(a\text{-count}(b)) \cdot (b\text{-count}(c)) \leqslant a\text{-count}(c)$. The theorem is a consequence of (17).

(96) Let us consider a non zero natural number a, and an odd natural number b. Then $2\text{-count}(a \cdot b) = 2\text{-count}(a)$.

Let us consider a non trivial natural number a. Now we state the propositions:

(97) $a^{n+1} + a^n < a^{n+2}$.

(98) $(a+1)^n + (a+1)^n < (a+1)^{n+1}$.

(99) Let us consider a non trivial, odd natural number a. Then $a^n+a^n < a^{n+1}$. The theorem is a consequence of (98).

(100) Let us consider a non trivial natural number p. If $a \nmid b$, then $(p^a)^c \neq p^b$.

(101) Let us consider non zero integers a, b, and a non zero natural number n. Suppose there exists a prime natural number p such that $n \nmid p\text{-count}(a)$. Then $a \neq b^n$.

(102) Let us consider non zero integers a, b, and a non zero natural number n. Suppose $a = b^n$. Let us consider a prime natural number p. Then $n \mid p\text{-count}(a)$.

(103) Let us consider positive real numbers a, b, and a non trivial natural number n. Then $(a+b)^n > a^n + b^n$. The theorem is a consequence of (42) and (41).

(104) Let us consider non zero integers a, b, and an odd, prime natural number p. Suppose $|a| \neq |b|$ and $p \nmid b$. Then $p\text{-count}(a^2 - b^2) = \max(p\text{-count}(a - b), p\text{-count}(a+b))$. The theorem is a consequence of (32), (77), and (57).

(105) Let us consider a non trivial natural number a, and a non zero integer b. Then a-count$(a^n \cdot b) = n + (a\text{-count}(b))$.

Acknowledgement: Ad Maiorem Dei Gloriam

References

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

[2] Grzegorz Bancerek, Czesław Byliński, Adam Grabowski, Artur Korniłowicz, Roman Matuszewski, Adam Naumowicz, Karol Pąk, and Josef Urban. Mizar: State-of-the-art and beyond. In Manfred Kerber, Jacques Carette, Cezary Kaliszyk, Florian Rabe, and Volker Sorge, editors, *Intelligent Computer Mathematics*, volume 9150 of *Lecture Notes in Computer Science*, pages 261–279. Springer International Publishing, 2015. ISBN 978-3-319-20614-1. doi:10.1007/978-3-319-20615-8_17.

[3] Paul Erdős and János Surányi. *Topics in the Theory of Numbers*, chapter Divisibility, the Fundamental Theorem of Number Theory, pages 1–37. Springer New York, 2003. doi:10.1007/978-1-4613-0015-1_1.

[4] Jacek Gancarzewicz. *Arytmetyka*. Wydawnictwo UJ, Kraków, 2000. In Polish.

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

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

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

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

[9] Adam Naumowicz. An example of formalizing recent mathematical results in Mizar. *Journal of Applied Logic*, 4(4):396–413, 2006. doi:10.1016/j.jal.2005.10.003. Towards Computer Aided Mathematics.

[10] Akira Nishino and Yasunari Shidama. The Maclaurin expansions. *Formalized Mathematics*, 13(**3**):421–425, 2005.

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

[12] Marco Riccardi. Pocklington's theorem and Bertrand's postulate. *Formalized Mathematics*, 14(**2**):47–52, 2006. doi:10.2478/v10037-006-0007-y.

[13] Piotr Rudnicki and Andrzej Trybulec. Abian's fixed point theorem. *Formalized Mathematics*, 6(**3**):335–338, 1997.

[14] Rafał Ziobro. Fermat's Little Theorem via divisibility of Newton's binomial. *Formalized Mathematics*, 23(**3**):215–229, 2015. doi:10.1515/forma-2015-0018.

Received June 30, 2016

The English version of this volume of Formalized Mathematics was financed under agreement 548/P-DUN/2016 with the funds from the Polish Minister of Science and Higher Education for the dissemination of science.