FORMALIZED MATHEMATICS
Vol. **23**, No. **3**, Pages 215–229, **2015**
DOI: 10.1515/forma-2015-0018

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

Fermat's Little Theorem via Divisibility of Newton's Binomial

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

Summary. Solving equations in integers is an important part of the number theory [29]. In many cases it can be conducted by the factorization of equation's elements, such as the Newton's binomial. The article introduces several simple formulas, which may facilitate this process. Some of them are taken from relevant books [28], [14].

In the second section of the article, Fermat's Little Theorem is proved in a classical way, on the basis of divisibility of Newton's binomial. Although slightly redundant in its content (another proof of the theorem has earlier been included in [12]), the article provides a good example, how the application of registrations could shorten the length of Mizar proofs [9], [17].

MSC: 11A51 11Y55 03B35

Keywords: factorization; primes; Fermat

MML identifier: NEWTON02, version: 8.1.04 5.32.1246

The notation and terminology used in this paper have been introduced in the following articles: [26], [1], [5], [4], [10], [6], [30], [22], [21], [3], [15], [32], [19], [7], [23], and [8].

1. Divisibility of Newton's Binomial

From now on a, b, c, d, m, x, n, j, k, l denote natural numbers, t, u, v, z denote integers, f, F denote finite sequences of elements of $\mathbb{N}$, p, q, r, s denote real numbers.

Let a be a complex. Note that $1 \cdot a^0$ reduces to 1.

Let n be a non zero natural number. One can check that 0^n reduces to 0.

Let a be a natural number. Let us observe that $|a|$ reduces to a.

Let us note that $\gcd(a, 0)$ reduces to a.

Let us consider t and z. Let us note that $(t \bmod z) \bmod z$ reduces to $t \bmod z$.

Observe that $0 \bmod t$ reduces to 0.

Let us consider u and z. One can check that $0 + u \cdot z \bmod z$ reduces to 0.

Let r be a non zero real number and n be an even, natural number. One can verify that r^n is positive.

Now we state the propositions:

(1) $\gcd(t, z) = \gcd(-t, z)$.

(2) If $t \mid z$ and $u \mid v$, then $t \cdot u \mid z \cdot v$.

(3) $t \mid z$ if and only if $\gcd(t, z) = |t|$.

(4) $t \cdot u \mid z \cdot u$ if and only if $|u| \cdot (\gcd(t, z)) = |u| \cdot |t|$. The theorem is a consequence of (3).

(5) (i) $\gcd(t + u \cdot z, z) = \gcd(t, z)$, and

(ii) $\gcd(t - u \cdot z, z) = \gcd(t, z)$.

(6) If $n > 0$, then $t \mid t^n$.

(7) $\gcd(a^n, b^n) = (\gcd(a, b))^n$.

Proof: If $\gcd(a, b) = k$, then $\gcd(a^n, b^n) = k^n$ by [22, (21)], [16, (12)], [11, (15)], [21, (7), (11), (4)]. □

(8) If $a > b$ and a and b are relatively prime, then $\gcd(a + b, a - b) \leqslant 2$. The theorem is a consequence of (5).

(9) $\gcd(t, z)$ is even if and only if t is even and z is even.

Proof: If $\gcd(t, z)$ is even, then t is even and z is even by [22, (21)]. □

(10) (i) $t \mid (t + z)^n - z^n$, and

(ii) $z \mid (t + z)^n - t^n$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv t \mid (t + z)^{\$_1} - z^{\$_1}$ and $z \mid (t + z)^{\$_1} - t^{\$_1}$. $\mathcal{P}[0]$ by [21, (4)], [30, (11)]. If $\mathcal{P}[x]$, then $\mathcal{P}[x+1]$ by [16, (4)], [21, (8)]. For every m, $\mathcal{P}[m]$ from [2, Sch. 2]. □

(11) $u \mid (u + z)^n$ if and only if $u \mid z^n$. The theorem is a consequence of (10).

(12) If $t \mid (t + z)^n$, then $t \mid (t + z)^n + z^n$. The theorem is a consequence of (11).

(13) $t + u \mid (t + 2 \cdot u)^n - u^n$. The theorem is a consequence of (10).

(14) If $l > 0$ and $t \mid z$, then $t \mid z^l$.

(15) If $t \mid z$, then $t^n \mid z^n$. The theorem is a consequence of (7) and (3).

(16) If $n > 0$ and $t \nmid (t + z)^n$, then $t \nmid z$. The theorem is a consequence of (14).

(17) If $m > 0$, then $t \cdot z \mid (t+z)^m - (t^m + z^m)$.
Proof: Consider n such that $m = 1 + n$. $t \cdot z \mid (t+z)^{n+1} - (t^{n+1} + z^{n+1})$ by [22, (12), (2)], [21, (6)], [22, (1)]. □

(18) $t - z \mid t^m - z^m$. The theorem is a consequence of (11) and (10).

(19) If $n > 0$, then $t \cdot z \mid (t-z)^n - (t^n + (-z)^n)$. The theorem is a consequence of (17).

(20) $t \cdot z \mid (t+z)^n - (t-z)^n + ((-z)^n - z^n)$. The theorem is a consequence of (17) and (19).

(21) If $n > 0$, then $t \mid (t+z)^n + (t^n - z^n)$. The theorem is a consequence of (6) and (10).

(22) If $u \mid t + z$ and $u \mid t - z$, then $u \mid 2 \cdot t$ and $u \mid 2 \cdot z$.

(23) $t \cdot z \mid (t+z)^{2 \cdot n} - (t-z)^{2 \cdot n}$. The theorem is a consequence of (20).

(24) If $n > 0$, then $t \cdot z \mid (t-z)^{2 \cdot n} - (t^{2 \cdot n} + z^{2 \cdot n})$. The theorem is a consequence of (19).

(25) $t \cdot z \mid (t-z)^{2 \cdot n+1} - (t^{2 \cdot n+1} - z^{2 \cdot n+1})$. The theorem is a consequence of (19).

(26) If $k > 0$ and $x \mid a + k$ and $x \mid a - k$, then $x \leqslant 2 \cdot k$. The theorem is a consequence of (22).

(27) If $k > 0$, then $\gcd(a, b) \leqslant \gcd(a, b \cdot k)$.

(28) If $n > 0$, then $\gcd(\gcd(a, b), b^n) = \gcd(a, b)$.

(29) $t + z$ and t are relatively prime if and only if $t + z$ and z are relatively prime.

(30) If a and b are relatively prime and $a \cdot b = c^n$, then there exists k such that $k^n = a$. The theorem is a consequence of (7).

(31) If a and b are relatively prime and $a + b > 2$, then $a + b \mid a^n + b^n$ iff $a + b \nmid a^n - b^n$.
Proof: $b > 0$. If $a + b \mid a^n - b^n$, then $a + b \nmid a^n + b^n$ by [16, (4)]. □

(32) If a and b are relatively prime and $a + b > 2$ and n is odd, then $a + b \nmid a^n - b^n$. The theorem is a consequence of (31).

(33) If a and b are relatively prime and $a + b > 2$ and n is even, then $a + b \nmid a^n + b^n$. The theorem is a consequence of (31).

Let us assume that a and b are relatively prime. Now we state the propositions:

(34) $a \cdot b$ and $a^{n+1} + b^{n+1}$ are relatively prime. The theorem is a consequence of (5).

(35) $a \cdot b$ and $a^{n+1} - b^{n+1}$ are relatively prime. The theorem is a consequence of (5).

(36) If $q > 0$ and $n > 0$, then there exists r such that $q = r^n$.

(37) If $k > 0$ and $a + b > k$ and $a + b \mid k \cdot a$, then a and b are not relatively prime.

(38) If $k > 1$, then $k \nmid (k + 1)^n$. The theorem is a consequence of (11).

(39) If $a > 1$ and $b > 0$ and $\gcd(a, b) = 1$, then $a \nmid (a + b)^n$. The theorem is a consequence of (11).

(40) If $c > 0$, then for every non negative real numbers r, s, $r < s$ iff $r^c < s^c$.
PROOF: if $r < s$, then $r^c < s^c$ and if $r^c < s^c$, then $r < s$ by [24, (6)], [2, (14)], [21, (11)], [25, (37)]. □

(41) Let us consider non negative real numbers r, s. If $r \geqslant s$, then $r^n \geqslant s^n$. The theorem is a consequence of (40).

(42) If $a > 0$ and $n > 0$, then there exists r such that $a^n + b^n = r^n$.

(43) There exists b such that $b^{n+1} \leqslant a < (b + 1)^{n+1}$.
PROOF: Define $\mathcal{P}$[natural number] $\equiv$ there exists b such that $b^{n+1} \leqslant \$_1 < (b + 1)^{n+1}$. $\mathcal{P}[0]$. If $\mathcal{P}[k]$, then $\mathcal{P}[k+1]$ by [2, (13)], (40). For every x, $\mathcal{P}[x]$ from [2, Sch. 2]. □

(44) If $n > 0$ and $a > b$ and a and b are relatively prime, then $\gcd(a^n + b^n, a^n - b^n) \leqslant 2$. The theorem is a consequence of (40) and (8).

(45) If $a + b \mid c$ and a and c are relatively prime, then a and b are relatively prime. The theorem is a consequence of (5).

(46) If t and z are relatively prime and t and u are relatively prime and t is even, then $u + z$ is even and $u - z$ is even and $u \cdot z$ is odd.

(47) If a and b are relatively prime and c is even and $a^n + b^n = c^n$, then $a + b$ is even and $a - b$ is even.

(48) If a is even and a and b are relatively prime, then $a - b$ and $a + b$ are relatively prime. The theorem is a consequence of (9), (8), and (1).

(49) If a and b are relatively prime, then $a + b$ and $a \cdot b$ are relatively prime. The theorem is a consequence of (5).

(50) If $3 \nmid a \cdot b$, then $3 \mid (a + b) \cdot (a - b)$. The theorem is a consequence of (3).

(51) $3 \mid (a + b) \cdot (a - b) + a \cdot b$ if and only if $3 \mid a$ and $3 \mid b$.

(52) If $b^2 = a \cdot (a - b)$, then $3 \mid a$ and $3 \mid b$. The theorem is a consequence of (51).

(53) If a and b are relatively prime, then $3 \nmid (a+b) \cdot (a-b) + a \cdot b$. The theorem is a consequence of (51).

(54) If $a > b$ and $a + b \geqslant 2^{n+1}$, then $a > 2^n$.

(55) If $a \neq b$, then $2 \cdot a \cdot b < a^2 + b^2$.

(56) If $n > 0$ and $a \neq b$, then $2 \cdot a^n \cdot b^n < a^{2 \cdot n} + b^{2 \cdot n}$. The theorem is a consequence of (55).

(57) If $b > 0$, then there exists n such that $b \geqslant 2^n$ and $b < 2^{n+1}$.

Proof: Consider a such that $b = 1+a$. There exists n such that $a+1 \geqslant 2^n$ and $a + 1 < 2^{n+1}$ by [21, (6)]. □

(58) Let us consider odd natural numbers a, b. Then $4 \mid a + b$ if and only if $4 \nmid a - b$.

Proof: Consider t, z such that $a + b = 2 \cdot t$ and $a - b = 2 \cdot z$. t is odd iff z is even. If $2 \cdot 2 \mid a + b$, then $2 \cdot 2 \nmid a - b$ by (3), [27, (16)]. If $2 \cdot 2 \nmid a + b$, then $2 \cdot 2 \mid a - b$ by (3), [27, (16)]. □

(59) If $\gcd(b + c, b) = 1$ and c is odd, then $\gcd(2 \cdot b + c, c) = 1$.

(60) If $a + b = k \cdot a + k \cdot b$ and $a \cdot b > 0$, then $k = 1$.

(61) If $t \cdot z = t + z$, then $t = z$.

(62) $(2 \cdot n + 1)^2 = 4 \cdot n \cdot (n + 1) + 1$.

(63) If a is odd and b is odd, then $8 \mid a^2 - b^2$. The theorem is a consequence of (62).

(64) Let us consider odd natural numbers a, b. If $4 \mid a - b$, then $4 \mid a^n - b^n$.

(65) Let us consider odd natural numbers a, b, and an even natural number m. Then $4 \mid a^m - b^m$.

Proof: Consider n such that $m = 2 \cdot n$. If $4 \mid a + b$, then $4 \mid a^m - b^m$ by [34, (36)], [22, (9)]. If $4 \mid a - b$, then $4 \mid a^m - b^m$. □

(66) If t is even and $4 \nmid t$, then there exists u such that $u = t/2$ and u is odd.

(67) If a is odd and $2^n \mid a \cdot b$, then $2^n \mid b$.

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

(68) $4 \mid a^m + b^m$ if and only if $4 \mid a + b$.

Proof: Consider n such that $m = 2 \cdot n + 1$. If $4 \mid a^{2 \cdot n+1} + b^{2 \cdot n+1}$, then $4 \mid a + b$ by [21, (81)], (65), [22, (2)], (58). □

(69) $4 \mid a - b$ if and only if $4 \nmid a^m + b^m$. The theorem is a consequence of (58) and (68).

Now we state the propositions:

(70) If $a^2 + b^2 = c^2$, then there exists t such that $b^2 = (2 \cdot a + t) \cdot t$.

(71) If $b^2 = (2 \cdot a + t) \cdot t$, then there exists c such that $a^2 + b^2 = c^2$.

(72) If a is odd and b is odd and m is even, then $a^m + b^m \neq c^m$.

Proof: If a is odd and b is odd, then $a^{2 \cdot n} + b^{2 \cdot n} \neq c^{2 \cdot n}$ by [21, (9)]. □

(73) If t and z^n are relatively prime and $n > 0$, then t and z are relatively prime. The theorem is a consequence of (6).

Let us assume that a and b are relatively prime. Now we state the propositions:

(74) $\gcd((a+b)^2, a^2+b^2-(n-2)\cdot a\cdot b) = \gcd(a^2+b^2-(n-2)\cdot a\cdot b, n)$. The theorem is a consequence of (34) and (5).

(75) $a+b$ and $a^2+b^2+a\cdot b$ are relatively prime. The theorem is a consequence of (74) and (73).

(76) $\gcd((a-b)^2, a^2+b^2+(n-2)\cdot a\cdot b) = \gcd(a^2+b^2+(n-2)\cdot a\cdot b, n)$. The theorem is a consequence of (35), (5), and (1).

Now we state the propositions:

(77) $a \mid k\cdot(a\cdot n+1)$ if and only if $a \mid k$.

Proof: If $a \mid k\cdot(a\cdot n+1)$, then $a \mid k$ by [22, (1)]. □

(78) Let us consider a positive natural number n. Then $a \mid k\cdot(a^n+1)$ if and only if $a \mid k$. The theorem is a consequence of (77).

(79) Let us consider positive natural numbers a, b. If $a \bmod b = b \bmod a$, then $a = b$.

(80) $k\cdot(a\cdot n+1) \bmod a = k \bmod a$.

Let us consider a positive natural number n. Now we state the propositions:

(81) $k\cdot(a^n+1) \bmod a = k \bmod a$. The theorem is a consequence of (80).

(82) $k\cdot(a^n+1)^m \bmod a = k \bmod a$. The theorem is a consequence of (81).

(83) $b\cdot(a^n+1)^m + c\cdot(a^n+1)^l \bmod a = b+c \bmod a$. The theorem is a consequence of (82).

Now we state the propositions:

(84) Let us consider positive natural numbers a, n. Then $a \mid b\cdot(a^n+1)^m + c\cdot(a^n+1)^l$ if and only if $a \mid b+c$. The theorem is a consequence of (83).

(85) If $|t| < a$, then $t \bmod a = |t|$ or $t \bmod a = a - |t|$.

(86) $-t \bmod a = u\cdot a - (t \bmod a) \bmod a$.

(87) Let us consider an odd natural number n. Then $t^n \bmod 3 = t \bmod 3$.

(88) $t + (u \bmod z) \bmod z = t + u \bmod z$.

(89) Let us consider an odd natural number n. Then $a+b-c \bmod 3 = a^n+b^n-c^n \bmod 3$. The theorem is a consequence of (87).

(90) Let us consider a positive natural number k. Then $t \bmod k = k-1$ if and only if $t+1 \bmod k = 0$. The theorem is a consequence of (88).

(91) If $a^2+b^2=c^2$, then $3 \mid a\cdot b\cdot c$. The theorem is a consequence of (14) and (50).

(92) Let us consider non zero natural numbers a, n. Suppose $t \bmod a = z \bmod a$. Then $t^n \bmod a = z^n \bmod a$.

(93) If $3 \mid t-z$, then $3 \mid t^n - z^n$. The theorem is a consequence of (18).

(94) Let us consider an odd natural number n. Then $3 \mid a+b-c$ if and only if $3 \mid a^n + b^n - c^n$.
Proof: If $3 \mid a+b-c$, then $3 \mid a^n + b^n - c^n$ by [30, (62)], (89). $a+b-c \bmod 3 = 0$. □

(95) $(t+u-z)^2 \equiv t^2+u^2+z^2 \pmod{2}$.

(96) $(t+u-z)^3 \equiv t^3+u^3-z^3 \pmod{3}$.

(97) $6 \mid a^3 - a$. The theorem is a consequence of (50).

(98) Let us consider odd natural numbers a, b, c. Then $3 \mid t^a + t^b + t^c$. The theorem is a consequence of (87) and (88).

(99) (i) $2^m - 1 \mid 2^{2 \cdot m+1} - 2$, and
(ii) $2^m + 1 \mid 2^{2 \cdot m+1} - 2$.

(100) If $u+t+z$ is even, then $u \cdot t \cdot z$ is even.

(101) If $t^n + u^n = z^n$, then $2^n \mid (t \cdot u \cdot z)^n$. The theorem is a consequence of (100) and (15).

(102) $t^n \equiv t^m \pmod{t-1}$. The theorem is a consequence of (18).

2. Fermat's Little Theorem Revisited

In the sequel a, b, c, d, m, x, n, k, l denote natural numbers, t, z denote integers, f, F, G denote finite sequences of elements of $\mathbb{R}$, q, r, s denote real numbers, and D denotes a set.

Now we state the propositions:

(103) Let us consider a finite sequence f. Then f is D-valued if and only if f is a finite sequence of elements of D.

(104) $k+1 \in \operatorname{Seg} n$ if and only if $k < n$.
Proof: If $k+1 \in \operatorname{Seg} n$, then $k < n$ by [4, (1)], [2, (13)]. □

(105) $n+1 \leqslant \operatorname{len} f$ if and only if $n+1 \in \operatorname{dom} f$.
Proof: If $n+1 \leqslant \operatorname{len} f$, then $n+1 \in \operatorname{dom} f$ by [2, (13)], (104). $n < \operatorname{len} f$. □

(106) $k \in \mathbb{Z}_n$ if and only if $k+1 \in \operatorname{Seg} n$.

(107) If $n \in \operatorname{dom} f$ and $1 \leqslant m \leqslant n$, then $f(m) = (f{\restriction}n)(m)$.

(108) Suppose f is a finite sequence of elements of D. Then
(i) $f{\restriction}n$ is a finite sequence of elements of D, and
(ii) $f_{\lfloor n}$ is a finite sequence of elements of D.

(109) If $n \in \operatorname{dom} f$, then $(f{\restriction}n)(1) = f(1)$. The theorem is a consequence of (107).

(110) Let us consider a finite sequence f of elements of $\mathbb{R}$. If $n \in \operatorname{dom} f$, then $\operatorname{len}(f{\restriction}n) = n$.

Let us consider s. Observe that $\langle s \rangle$ is $\mathbb{R}$-valued.

Let us consider D. Let f be a D-valued finite sequence. Let us consider n. Let us note that $f{\restriction}n$ is D-valued.

Let f be a finite sequence of elements of D. Observe that $f_{\downharpoonleft n}$ is D-valued.

Now we state the proposition:

(111) Let us consider a finite sequence f of elements of $\mathbb{C}$. If $k \in \operatorname{dom}(f{\restriction}n)$, then $k \in \operatorname{dom} f$.

Let us consider n. Note that $\emptyset_{\downharpoonleft n}$ is empty.

Let us consider f. One can check that $(f{\restriction}n)_{\downharpoonleft n}$ is empty.

Let us consider D. Let f be a D-valued finite sequence. One can verify that $f_{\downharpoonleft n}$ is D-valued.

Let f be a finite sequence of elements of $\mathbb{N}$. Observe that $f(n)$ is natural.

Let us consider k. One can verify that $(f{\restriction}n)(k)$ is natural and $(f{\restriction}n)_{\downharpoonleft 1}(k)$ is natural.

Now we state the propositions:

(112) $\sum(f \smallfrown F) = \sum f + \sum F$.

(113) Let us consider a finite sequence f of elements of $\mathbb{R}$. Suppose $k \in \operatorname{dom} f_{\downharpoonleft n}$ and $n \in \operatorname{dom} f$. Then $n + k \in \operatorname{dom} f$. The theorem is a consequence of (110).

(114) Let us consider a positive natural number k. If $n + k \in \operatorname{dom} f$, then $k \in \operatorname{dom} f_{\downharpoonleft n}$.

(115) Let us consider a positive natural number n. Suppose $n + 1 = \operatorname{len} f$. Then $\sum f = \sum(f{\restriction}n)_{\downharpoonleft 1} + f(1) + f(n+1)$. The theorem is a consequence of (112) and (109).

(116) If $n + 1 = \operatorname{len} f$, then $f_{\downharpoonleft n} = \langle f(n+1) \rangle$.

Let us assume that $(f{\restriction}n)_{\downharpoonleft 1}$ is not empty. Now we state the propositions:

(117) $\operatorname{len}(f{\restriction}n)_{\downharpoonleft 1} \leqslant \operatorname{len} f - 1$. The theorem is a consequence of (110).

(118) $\operatorname{len}(f{\restriction}n)_{\downharpoonleft 1} < n$. The theorem is a consequence of (110).

Now we state the propositions:

(119) If n is prime and $k \neq 0$ and $k \neq n$, then $n \mid \binom{n}{k}$.

(120) If $b \geqslant 2$, then $(b+1)! > 2^b$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv (\$_1 + 1)! > 2^{\$_1}$. $\mathcal{P}[2]$ by [21, (14), (15), (81)]. For every natural number k such that $k \geqslant 2$ and $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [21, (6), (15)]. For every natural number x such that $x \geqslant 2$ holds $\mathcal{P}[x]$ from [2, Sch. 8]. □

(121) $b > 1$ if and only if $b! > 1$.

Proof: If $b > 1$, then $b! > 1$ by [2, (13)], [20, (55)]. □

(122) If $b \geqslant 2$, then $b! < b^b$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv \$_1! < {\$_1}^{\$_1}$. $\mathcal{P}[2]$ by [21, (81), (14)]. For every natural number k such that $k \geqslant 2$ and $\mathcal{P}[k]$ holds $\mathcal{P}[k+1]$ by [24, (10)], [21, (15), (6)]. For every natural number x such that $x \geqslant 2$ holds $\mathcal{P}[x]$ from [2, Sch. 8]. □

(123) $(b+1)! \geqslant 2^b$. The theorem is a consequence of (120).

(124) $b! \leqslant b^b$. The theorem is a consequence of (122).

(125) If $b > 0$ and a and $b!$ are relatively prime, then a and b are relatively prime. The theorem is a consequence of (121).

(126) If a and $(a+b)!$ are relatively prime, then $a = 1$ or $a = 0$ and ($b = 0$ or $b = 1$). The theorem is a consequence of (121).

(127) If $n \in \operatorname{dom} f$ and $m \in \operatorname{dom}(f{\restriction}n)_{\downharpoonright 1}$, then $(f{\restriction}n)_{\downharpoonright 1}(m) = f(m+1)$. The theorem is a consequence of (113), (105), (110), and (107).

Let us consider n. One can verify that $\langle \binom{n}{0}, \ldots, \binom{n}{n} \rangle$ is non empty.

Let us consider m. One can check that $\langle \binom{n}{0}, \ldots, \binom{n}{n} \rangle(m)$ is natural and $\langle \binom{n}{0}, \ldots, \binom{n}{n} \rangle$ is $\mathbb{N}$-valued.

Let h be a finite sequence of elements of $\mathbb{N}$. One can verify that $\sum h$ is natural.

Now we state the propositions:

(128) If $n > 0$, then $n \in \operatorname{dom}\langle \binom{n}{0}, \ldots, \binom{n}{n} \rangle$.

(129) $\langle \binom{n}{0}, \ldots, \binom{n}{n} \rangle$ is a finite sequence of elements of $\mathbb{N}$.

(130) $\langle \binom{n}{0}, \ldots, \binom{n}{n} \rangle(n+1) = 1$. The theorem is a consequence of (105).

(131) $\langle \binom{k}{0}, \ldots, \binom{k}{k} \rangle(1) = 1$.

Proof: $\langle \binom{k}{0} 1^0 1^k, \ldots, \binom{k}{k} 1^k 1^0 \rangle(1) = 1$ by [21, (28)]. □

Let us consider a positive natural number n. Now we state the propositions:

(132) $\sum\langle \binom{n}{0}, \ldots, \binom{n}{n} \rangle = \sum(\langle \binom{n}{0}, \ldots, \binom{n}{n} \rangle{\restriction}n)_{\downharpoonright 1} + \langle \binom{n}{0}, \ldots, \binom{n}{n} \rangle(1) + \langle \binom{n}{0}, \ldots, \binom{n}{n} \rangle(n+1)$. The theorem is a consequence of (128), (112), and (109).

(133) $\sum\langle \binom{n}{0}, \ldots, \binom{n}{n} \rangle = \sum(\langle \binom{n}{0}, \ldots, \binom{n}{n} \rangle{\restriction}n)_{\downharpoonright 1} + 2$. The theorem is a consequence of (132), (130), and (131).

Now we state the propositions:

(134) $\sum\langle \binom{n}{0}, \ldots, \binom{n}{n} \rangle = \sum(\langle \binom{n}{0}, \ldots, \binom{n}{n} \rangle{\restriction}n) + 1$. The theorem is a consequence of (103).

(135) $\operatorname{len}(\langle \binom{n}{0}, \ldots, \binom{n}{n} \rangle{\restriction}n) = n$.

(136) Suppose $m \in \operatorname{dom}(\langle \binom{n}{0}, \ldots, \binom{n}{n} \rangle{\restriction}n)_{\downharpoonright 1}$. Then $(\langle \binom{n}{0}, \ldots, \binom{n}{n} \rangle{\restriction}n)_{\downharpoonright 1}(m) = \langle \binom{n}{0}, \ldots, \binom{n}{n} \rangle(m+1)$. The theorem is a consequence of (128) and (127).

(137) If n is prime, then $n \mid (\langle \binom{n}{0}, \ldots, \binom{n}{n} \rangle \upharpoonright n)_{\downharpoonleft 1}(k)$.

PROOF: If n is prime and $k \geqslant n$, then $n \mid (\langle \binom{n}{0}, \ldots, \binom{n}{n} \rangle \upharpoonright n)_{\downharpoonleft 1}(k)$ by (128), (110), [2, (13)], [31, (25)]. If n is prime and $k < n$, then $n \mid (\langle \binom{n}{0}, \ldots, \binom{n}{n} \rangle \upharpoonright n)_{\downharpoonleft 1}(k)$ by [31, (25)], (128), (110), [2, (13)]. □

(138) Let us consider a prime natural number n. Then $n \mid 2^n - 2$. The theorem is a consequence of (103), (137), and (133).

Let k be a positive natural number. Let us consider n. Let us note that $n^k - n$ is natural.

Now we state the propositions:

(139) Let us consider prime natural numbers k, n. Then $n \cdot k \mid (2^n - 2) \cdot (2^k - 2)$. The theorem is a consequence of (138).

(140) Let us consider an odd prime number n. If $n = 2 \cdot k + 1$, then $n \mid 2^k - 1$ iff $n \nmid 2^k + 1$.

PROOF: $n \mid 2^k - 1$ or $n \mid 2^k + 1$ by (138), [21, (6)], [33, (7)], [21, (9)]. □

Let n be a natural number. The functor $n\setminus$ yielding a finite sequence of elements of $\mathbb{R}$ is defined by the term

(Def. 1) $\langle \binom{n}{0} 1^0 1^n, \ldots, \binom{n}{n} 1^n 1^0 \rangle$.

Let us consider n. We identify $\langle \binom{n}{0}, \ldots, \binom{n}{n} \rangle$ with $n\setminus$. We identify $n\setminus$ with $\langle \binom{n}{0}, \ldots, \binom{n}{n} \rangle$. Now we state the proposition:

(141) If $n > 0$, then $n \in \operatorname{dom} \langle \binom{n}{0} a^0 b^n, \ldots, \binom{n}{n} a^n b^0 \rangle$.

Let us consider a, b, n, and m. Let us observe that $\langle \binom{n}{0} a^0 b^n, \ldots, \binom{n}{n} a^n b^0 \rangle(m)$ is natural and $\langle \binom{n}{0} a^0 b^n, \ldots, \binom{n}{n} a^n b^0 \rangle$ is $\mathbb{N}$-valued.

Now we state the propositions:

(142) If $k + l$ is prime and $k > 0$ and $l > 0$, then $k + l \mid \langle \binom{k+l}{0} a^0 b^{k+l}, \ldots, \binom{k+l}{k+l} a^{k+l} b^0 \rangle(k+1)$. The theorem is a consequence of (119).

(143) If $a \neq 0$, then $\langle \binom{m}{0} a^0 b^m, \ldots, \binom{m}{m} a^m b^0 \rangle(1) \neq 0$.

(144) Let us consider a non zero natural number m. Then $a = 0$ if and only if $\langle \binom{m}{0} a^0 b^m, \ldots, \binom{m}{m} a^m b^0 \rangle(1) = 0$.

PROOF: For every non zero natural number m such that $a = 0$ holds $\langle \binom{m}{0} a^0 b^m, \ldots, \binom{m}{m} a^m b^0 \rangle(1) = 0$ by [21, (28)]. □

(145) If $\langle \binom{m}{0} a^0 b^m, \ldots, \binom{m}{m} a^m b^0 \rangle(1) = 0$, then $m \neq 0$.

(146) Let us consider a positive natural number m. Then $\sum \langle \binom{m}{0} a^0 b^m, \ldots, \binom{m}{m} a^m b^0 \rangle = a^m + b^m + \sum (\langle \binom{m}{0} a^0 b^m, \ldots, \binom{m}{m} a^m b^0 \rangle \upharpoonright m)_{\downharpoonleft 1}$. The theorem is a consequence of (115).

(147) $\sum \langle \binom{m+n}{0} a^0 b^{m+n}, \ldots, \binom{m+n}{m+n} a^{m+n} b^0 \rangle = \sum \langle \binom{m}{0} a^0 b^m, \ldots, \binom{m}{m} a^m b^0 \rangle \cdot \sum \langle \binom{n}{0} a^0 b^n, \ldots, \binom{n}{n} a^n b^0 \rangle$.

(148) If $l > 0$, then there exists x such that $\langle \binom{k+l}{0} a^0 b^{k+l}, \ldots, \binom{k+l}{k+l} a^{k+l} b^0 \rangle (k+1) = a \cdot x$.

(149) If $m > 0$, then there exists k such that $\langle \binom{m}{0} a^0 b^m, \ldots, \binom{m}{m} a^m b^0 \rangle (1) = a \cdot k$. The theorem is a consequence of (148).

(150) If $l > 0$, then there exists x such that $\langle \binom{k+l}{0} a^0 b^{k+l}, \ldots, \binom{k+l}{k+l} a^{k+l} b^0 \rangle (l) = a \cdot x$.

(151) If $n = \langle \binom{k+l}{0} a^0 b^{k+l}, \ldots, \binom{k+l}{k+l} a^{k+l} b^0 \rangle (k+1)$ and $l > 0$, then $a \mid n$. The theorem is a consequence of (148).

Let us consider a prime natural number n and positive natural numbers a, b. Now we state the propositions:

(152) $n \cdot a \cdot b \mid (\langle \binom{n}{0} a^0 b^n, \ldots, \binom{n}{n} a^n b^0 \rangle \upharpoonright n)_{\lfloor 1}(k)$.

Proof: If $k \notin \mathrm{dom}(\langle \binom{n}{0} a^0 b^n, \ldots, \binom{n}{n} a^n b^0 \rangle \upharpoonright n)_{\lfloor 1}$, then $n \cdot a \cdot b \mid (\langle \binom{n}{0} a^0 b^n, \ldots, \binom{n}{n} a^n b^0 \rangle \upharpoonright n)_{\lfloor 1}(k)$. If n is prime and $k \in \mathrm{dom}(\langle \binom{n}{0} a^0 b^n, \ldots, \binom{n}{n} a^n b^0 \rangle \upharpoonright n)_{\lfloor 1}$, then $n \cdot a \cdot b \mid (\langle \binom{n}{0} a^0 b^n, \ldots, \binom{n}{n} a^n b^0 \rangle \upharpoonright n)_{\lfloor 1}(k)$ by [31, (25)], (118), [2, (13), (10)]. □

(153) $n \cdot a \cdot b \mid (a+b)^n - (a^n + b^n)$. The theorem is a consequence of (103), (152), and (146).

Now we state the propositions:

(154) Let us consider a prime natural number n. Then $n \cdot a \mid (a+1)^n - (a^n + 1)$. The theorem is a consequence of (153).

(155) Let us consider positive natural numbers a, b. Then $2 \cdot a \cdot b \mid (a+b)^2 - (a^2 + b^2)$.

(156) Let us consider a prime natural number n. Then $n \mid a^n - a$.

Proof: Define $\mathcal{P}[\text{natural number}] \equiv n \mid {\$_1}^n - \$_1$. If $\mathcal{P}[k]$, then $\mathcal{P}[k+1]$ by (154), [22, (2)], [16, (4)]. For every natural number x, $\mathcal{P}[x]$ from [2, Sch. 2]. □

(157) Let us consider a natural number k. If $k+1$ is prime and $k+1 \nmid a$, then $k+1 \mid a^k - 1$. The theorem is a consequence of (156).

(158) Let us consider a prime natural number n. Then $n \mid a+b$ if and only if $n \mid a^n + b^n$. The theorem is a consequence of (156).

(159) $163 \mid a+b$ if and only if $163 \mid a^{163} + b^{163}$.

Let us consider a prime natural number n. Now we state the propositions:

(160) $n \mid a$ if and only if $n \mid a^n$.

(161) $n \mid a^n + 1$ if and only if $n \mid a+1$. The theorem is a consequence of (158).

(162) $n \mid a^n + b^n$ if and only if $n \mid (a+b)^n$.

Now we state the propositions:

(163) $7 \mid a^7 + 1$ if and only if $7 \mid a+1$.

(164) If $7 \nmid a$, then $7 \mid a^6 - 1$. The theorem is a consequence of (156).

Let us consider a prime natural number n and positive natural numbers a, b. Now we state the propositions:

(165) $n \cdot a \cdot b \mid (a+b)^{k \cdot n} - (a^n + b^n)^k$. The theorem is a consequence of (153).

(166) If $n \cdot a \cdot b \mid (a+t)^n - (a^n + b^n)$, then $n \cdot a \cdot b \mid (a+b)^n - (a+t)^n$. The theorem is a consequence of (153).

Now we state the proposition:

(167) Let us consider a prime natural number n, and positive natural numbers a, b, c. If $n \cdot a \cdot b \mid c - b$, then $n \cdot a \cdot b \mid a^n + b^n - (a+c)^n$. The theorem is a consequence of (153).

Let us consider a prime natural number p. Now we state the propositions:

(168) If $p = 2 \cdot n + 1$, then $p \mid a$ or $p \mid a^n - 1$ or $p \mid a^n + 1$. The theorem is a consequence of (156).

(169) If $p \nmid a$, then there exists n such that $p \mid a^n - 1$ and $0 < n < p$. The theorem is a consequence of (157).

Now we state the propositions:

(170) $5 \mid a^3 - 1$ if and only if $5 \mid a - 1$.

PROOF: If $5 \mid a^3 - 1$, then $5 \mid a - 1$ by [13, (59)], (156), [22, (13)], [18, (3)]. □

(171) If $k+1$ is prime, then $k + 1 \mid a^{n \cdot k + 1} - a$. The theorem is a consequence of (157).

(172) $2 \mid a^{n+1} - a$. The theorem is a consequence of (171).

(173) $3 \mid a^{2 \cdot n + 1} - a$. The theorem is a consequence of (171).

(174) $5 \mid a^{4 \cdot n + 1} - a$. The theorem is a consequence of (171).

(175) $7 \mid a^{6 \cdot n + 1} - a$. The theorem is a consequence of (171).

(176) If $k \neq l$ and $k+1$ is odd and prime and $l+1$ is odd and prime, then $2 \cdot (k+1) \cdot (l+1) \mid a^{k \cdot l + 1} - a$. The theorem is a consequence of (171) and (172).

(177) $154 \mid a^{61} - a$. The theorem is a consequence of (176).

(178) $6 \mid a^{2 \cdot n + 1} - a$. The theorem is a consequence of (172) and (173).

(179) $30 \mid a^{4 \cdot n + 1} - a$. The theorem is a consequence of (172), (173), and (174).

(180) $42 \mid a^{6 \cdot n + 1} - a$. The theorem is a consequence of (172), (173), and (175).

(181) Let us consider a prime natural number n. Then $n \mid a^{n+k} - a^{k+1}$. The theorem is a consequence of (156).

(182) If $2 \cdot n + 1$ is prime, then for every k such that $2 \cdot n > k > 1$ holds $2 \cdot n + 1 \nmid a^n - k$ and $2 \cdot n + 1 \nmid a^n + k$. The theorem is a consequence of (168).

(183) (i) $5 \nmid a^2 - 2$, and

(ii) $5 \nmid a^2 + 2$, and

(iii) $5 \nmid a^2 - 3$, and

(iv) $5 \nmid a^2 + 3$.

The theorem is a consequence of (182).

(184) If $a^2 + b^2 = c^2$, then $5 \mid a$ or $5 \mid b$ or $5 \mid c$. The theorem is a consequence of (168) and (183).

(185) (i) $7 \nmid a^3 - 2$, and

(ii) $7 \nmid a^3 + 2$, and

(iii) $7 \nmid a^3 - 3$, and

(iv) $7 \nmid a^3 + 3$, and

(v) $7 \nmid a^3 - 4$, and

(vi) $7 \nmid a^3 + 4$, and

(vii) $7 \nmid a^3 - 5$, and

(viii) $7 \nmid a^3 + 5$.

The theorem is a consequence of (182).

(186) $2 \mid 2^n - 1$ if and only if $n = 0$.

Proof: If $2 \mid 2^n - 1$, then $n = 0$ by [18, (3)], [22, (13)]. □

(187) If $2^{k+l} \mid 2^{n+k} - 2^k$, then $l = 0$ or $n = 0$. The theorem is a consequence of (186).

(188) (i) $3 \mid b$, or

(ii) $3 \mid b - 1$, or

(iii) $3 \mid b + 1$.

The theorem is a consequence of (168).

(189) If $3 \nmid b$, then $3 \nmid b^2 + c^2$.

Proof: If $3 \nmid b$ and $3 \nmid c$, then $3 \nmid b^2 + c^2$ by (157), [13, (41)], [16, (4)], [22, (1), (27)]. If $3 \nmid b$ and $3 \mid c$, then $3 \nmid b^2 + c^2$ by [18, (3)], [22, (9)], [18, (5)], [13, (41)]. □

(190) (i) $3 \nmid b^2 + 1$, and

(ii) $3 \nmid b^2 - 2$.

The theorem is a consequence of (189).

(191) $3 \nmid b^3 + b^2 - b + 1$. The theorem is a consequence of (190) and (156).

(192) Let us consider a positive natural number a. If b and c are relatively prime and $a + 1 \mid b$, then $a + 1 \nmid c$.

(193) If b and c are relatively prime, then $3 \nmid b^2 + c^2$. The theorem is a consequence of (192) and (189).

(194) Let us consider a prime natural number p. If $p \mid a$, then $p \mid a^{n+1}$.

(195) If b and c are relatively prime and $b^2 + c^2 = a^2$, then $3 \nmid a$. The theorem is a consequence of (193) and (194).

Let us consider a prime natural number p. Now we state the propositions:

(196) If $p \mid a + b$, then $p \mid a^{2 \cdot n+1} + b^{2 \cdot n+1}$.

(197) If $p \nmid a^{2 \cdot n+1} + b^{2 \cdot n+1}$ and $p \mid a^2 - b^2$, then $p \mid a - b$. The theorem is a consequence of (196).

Now we state the propositions:

(198) (i) $3 \mid a \cdot b$, or

(ii) $3 \mid a + b$, or

(iii) $3 \mid a - b$.

The theorem is a consequence of (188).

(199) If $3 \nmid a$ and $3 \nmid b$, then $3 \mid a^{2 \cdot n+1} + b^{2 \cdot n+1}$ or $3 \mid a^{2 \cdot n+1} - b^{2 \cdot n+1}$. The theorem is a consequence of (188).

(200) If $a^3 + b^3 = c^3$, then $7 \mid a$ or $7 \mid b$ or $7 \mid c$. The theorem is a consequence of (168) and (185).

Acknowledgement: Ad Maiorem Dei Gloriam

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 and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.

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

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

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

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

[9] Marco B. Caminati and Giuseppe Rosolini. Custom automations in Mizar. *Journal of Automated Reasoning*, 50(2):147–160, 2013.

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

[11] Yoshinori Fujisawa and Yasushi Fuwa. The Euler's function. *Formalized Mathematics*, 6 (**4**):549–551, 1997.

[12] Yoshinori Fujisawa, Yasushi Fuwa, and Hidetaka Shimizu. Euler's Theorem and small Fermat's Theorem. *Formalized Mathematics*, 7(**1**):123–126, 1998.

[13] 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.

[14] Jacek Gancarzewicz. Arytmetyka, 2000. In Polish.

[15] Krzysztof Hryniewiecki. Recursive definitions. *Formalized Mathematics*, 1(**2**):321–328, 1990.

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

[17] Artur Korniłowicz. On rewriting rules in Mizar. *Journal of Automated Reasoning*, 50(2): 203–210, 2013.

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

[19] Jarosław Kotowicz. Functions and finite sequences of real numbers. *Formalized Mathematics*, 3(**2**):275–278, 1992.

[20] Richard Krueger, Piotr Rudnicki, and Paul Shelley. Asymptotic notation. Part II: Examples and problems. *Formalized Mathematics*, 9(**1**):143–154, 2001.

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

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

[23] Beata Padlewska. Families of sets. *Formalized Mathematics*, 1(**1**):147–152, 1990.

[24] Konrad Raczkowski. Integer and rational exponents. *Formalized Mathematics*, 2(**1**):125–130, 1991.

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

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

[27] Christoph Schwarzweller. Modular integer arithmetic. *Formalized Mathematics*, 16(**3**): 247–252, 2008. doi:10.2478/v10037-008-0029-8.

[28] Wacław Sierpiński. Teoria liczb. 1950. In Polish.

[29] Wacław Sierpiński. O rozwiązywaniu rownań w liczbach całkowitych, 1956. In Polish.

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

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

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

[33] Li Yan, Xiquan Liang, and Junjie Zhao. Gauss lemma and law of quadratic reciprocity. *Formalized Mathematics*, 16(**1**):23–28, 2008. doi:10.2478/v10037-008-0004-4.

[34] Rafał Ziobro. Some remarkable identities involving numbers. *Formalized Mathematics*, 22(**3**):205–208, 2014. doi:10.2478/forma-2014-0023.

Received June 30, 2015