

# Application of Complex Classes to Number Theory

Rafał Ziobro

Department of Carbohydrate Technology and Cereal Processing  
University of Agriculture  
Kraków, Poland

**Summary.** The paper extends the use of registrations for Mizar proofs [2], [5]. The classes proposed for complex numbers [13] are applied here to integer and natural numbers, which seems to facilitate the proofs. The article is not solving any of “250 Problems in Elementary Number Theory” by Waław Sierpiński [11], but its contents are closely related to the series of Mizar articles “Elementary Number Theory Problems” [10].

MSC: 40-04 03B35 68V20

Keywords: integer numbers; multiplication; division; rounding

MML identifier: NEWTON06, version: 8.1.14 5.92.1491

Let  $a$  be a weightless complex number. One can check that  $|a|$  is weightless.

Let  $a$  be a light complex number. One can check that  $|a|$  is light.

Let  $a$  be a heavy complex number. One can check that  $|a|$  is heavy.

Let  $a$  be a heavy, positive real number and  $b$  be a negative real number. Observe that  $a - b$  is heavy.

Let  $a$  be a heavy, negative real number and  $b$  be a positive real number. One can check that  $a - b$  is heavy.

Let  $a$  be a non light, positive real number and  $b$  be a negative real number. Let us note that  $a - b$  is heavy.

Let  $a$  be a non light, negative real number and  $b$  be a positive real number. Let us observe that  $a - b$  is heavy.

Let  $a$  be a non heavy real number and  $b$  be a heavy, negative real number. One can check that  $a - b$  is positive.

Let  $a$  be a light real number and  $b$  be a non light, negative real number. Let us note that  $a - b$  is positive.

Let  $a$  be a non heavy real number. Note that  $a - b$  is non negative.

Let  $b$  be a heavy, positive real number. Let us note that  $a - b$  is negative.

Let  $a$  be a light real number and  $b$  be a non light, positive real number. Let us observe that  $a - b$  is negative.

Let  $a$  be a non heavy real number. Observe that  $a - b$  is non positive.

Let  $a$  be a light, positive real number and  $b$  be a light, positive real number. Note that  $a - b$  is light.

Let  $a$  be a non heavy, positive real number and  $b$  be a non heavy, positive real number. Let us observe that  $a - b$  is non heavy.

Let  $a$  be a real number. Observe that  $\text{frac } a$  is light and non negative.

One can check that  $\text{frac } \text{frac } a$  reduces to  $\text{frac } a$ .

Let  $a$  be an integer real number. Observe that  $\text{frac } a$  is zero and there exists an even integer which is weightless and there exists an odd integer which is weightless and there exists an integer which is heavy and every integer which is non weightless is also heavy and there exists an odd integer which is heavy and there exists an even integer which is heavy and there exists a positive integer which is heavy and there exists a negative integer which is heavy.

Now we state the proposition:

- (1) Let us consider non weightless integers  $a$ ,  $b$ . If  $a$  and  $b$  are relatively prime, then  $a \nmid b$  and  $b \nmid a$ .

Let us observe that there exists a real number which is non integer.

Let  $a$  be a non integer complex number. Observe that  $-a$  is non integer.

Let  $a$  be a non integer real number. Observe that  $\text{frac } a$  is light and positive.

Let  $a$  be a non integer complex number and  $b$  be a non zero integer. One can verify that  $a + b$  is non integer and  $a - b$  is non integer and  $\frac{a}{b}$  is non integer.

Let  $b$  be a light, positive real number. One can check that  $\lceil b \rceil$  is weightless and positive and  $\lfloor b \rfloor$  is zero.

One can check that  $\text{frac } b$  reduces to  $b$ . Let  $a$  be an integer. Observe that  $\lfloor a + b \rfloor$  reduces to  $a$  and  $\lceil a - b \rceil$  reduces to  $a$  and  $\text{frac}(a + b)$  reduces to  $b$ .

Let  $a$  be a positive real number. Observe that  $\lfloor a \rfloor$  is non negative and  $\lceil a \rceil$  is positive.

Let  $a$  be a heavy, positive real number. Observe that  $\lfloor a \rfloor$  is positive.

Let  $a$  be a negative real number. Let us note that  $\lfloor a \rfloor$  is negative and  $\lceil a \rceil$  is non positive.

Let  $a$  be a heavy, negative real number. Observe that  $\lceil a \rceil$  is negative.

Let  $a$  be an integer and  $b$  be a light, negative real number. One can verify that  $\lfloor a - b \rfloor$  reduces to  $a$  and  $\lceil a + b \rceil$  reduces to  $a$ .

Now we state the proposition:

(2) Let us consider positive real numbers  $a, b$ . Then  $[a] \cdot [b] \leq [a] \cdot b \leq a \cdot b$ .

Let us consider positive real numbers  $a, b$ . Now we state the propositions:

(3)  $[a] \cdot [b] \leq [a \cdot b]$ . The theorem is a consequence of (2).

(4)  $\frac{[a]}{b} \leq \frac{a}{b}$ .

Now we state the propositions:

(5) Let us consider a positive real number  $a$ , and a heavy, positive real number  $b$ . Then  $\frac{a}{[b]} \geq \frac{a}{b}$ .

(6) Let us consider an integer  $a$ , and a non zero integer  $b$ . Then  $b \mid a$  if and only if  $a \bmod b = 0$ .

(7) Let us consider a positive real number  $a$ , and a natural number  $n$ . Then  $[n \cdot a] \geq n \cdot [a]$ .

Let  $a$  be an integer. Let us observe that  $a \bmod 1$  is zero and  $a \bmod -1$  is zero and  $a \bmod 0$  is zero.

Let  $b$  be a weightless integer. Note that  $a \bmod b$  is zero.

Let  $b$  be a non zero natural number. One can check that  $a^b \bmod a$  is zero.

Let  $b$  be a non negative integer. Let us observe that  $a \bmod b$  is natural.

Let  $a$  be an odd integer and  $b$  be a non zero, even integer. Let us observe that  $a \bmod b$  is odd.

Let  $a$  be an even integer. Let us observe that  $a \bmod b$  is even and  $a^4 \bmod 8$  is zero and there exists square natural number which is odd.

Let  $a, b$  be odd integers. Note that  $\frac{a^2-b^2}{2}$  is even and  $\frac{a^2+b^2}{2}$  is odd.

Let  $a$  be square integer. Let us note that  $\sqrt[2]{a}$  is natural.

One can check that  $\sqrt[2]{a} \cdot \sqrt[2]{a}$  reduces to  $a$ .

Let  $a$  be an even, a square integer. One can verify that  $\sqrt[2]{a}$  is even and  $\frac{a}{2}$  is even.

Let  $b$  be an odd, a square integer. Let us observe that  $a - b$  is non square.

Let  $a$  be an odd, a square integer. One can verify that  $\sqrt[2]{a}$  is odd and  $\frac{a+b}{2}$  is odd and  $\frac{a-b}{2}$  is even.

Let  $a$  be a non negative real number. Let us observe that  $\sqrt[2]{a}$  is non negative and there exists square integer which is even and there exists square integer which is odd and there exists square natural number which is even.

Let  $n$  be a non zero natural number. Observe that  $\sqrt[n]{1}$  reduces to 1 and  $\sqrt[n]{0}$  reduces to 0.

Let  $a$  be a positive real number. Let us observe that  $\sqrt[n]{a}$  is positive.

Now we state the proposition:

(8) Let us consider a natural number  $a$ . Then  $a$  is a square and square-free if and only if  $a = 1$ .

PROOF: If  $a$  is a square and square-free, then  $a = 1$  by [12, (3)], [8, (31)], [6, (5)], [3, (14)].  $\square$

One can check that there exists a natural number which is square-free and square.

Let  $a$  be an even, a square integer. Note that  $\frac{a}{4}$  is a square and integer.

Let  $a$  be a non zero, a square integer. Let us observe that  $2 \cdot a$  is non square and  $a + a$  is non square.

Let  $a$  be an integer and  $b, c$  be non zero natural numbers. Note that  $(a \bmod b) \bmod b \cdot c$  reduces to  $a \bmod b$ .

Let  $b$  be a non trivial natural number. Let us note that  $1 \bmod b$  reduces to 1. Let  $a$  be a natural number. Note that  $a \cdot b + 1 \bmod b$  reduces to 1. Let  $n$  be a natural number. One can check that  $(a \cdot b + 1)^n \bmod b$  reduces to 1.

Let  $n$  be an even natural number. Let us note that  $(b - 1)^n \bmod b$  reduces to 1.

Let  $n$  be an odd natural number. One can verify that  $(b - 1)^n \bmod b$  reduces to  $b - 1$ .

Now we state the proposition:

(9) Let us consider a natural number  $a$ , and a prime number  $p$ . Then

(i)  $a^{p-1} \bmod p = 0$ , or

(ii)  $a^{p-1} \bmod p = 1$ .

Let  $a$  be a natural number. Let us note that  $a \bmod 2$  is a square and  $a^2 \bmod 3$  is a square and  $a^2 \bmod 4$  is a square and  $a^2 \bmod 5$  is a square and  $a^2 \bmod 8$  is a square.

Let  $p$  be a prime natural number. Let us observe that  $a^{p-1} \bmod p$  is a square.

Now we state the proposition:

(10) Let us consider a non integer real number  $a$ . Then  $\text{frac } a + \text{frac}(-a) = 1$ .

Let  $a$  be a non integer real number. Observe that  $\text{frac } a + \text{frac}(-a)$  is non zero and trivial.

Now we state the propositions:

(11) Let us consider a non integer real number  $a$ . Then  $-1 < \text{frac } a - \text{frac}(-a) < 1$ . The theorem is a consequence of (10).

(12) Let us consider a non integer real number  $a$ . Then  $\text{frac } a = \text{frac}(-a)$  if and only if  $2 \cdot a$  is an odd integer.

Let us consider real numbers  $a, b$ . Now we state the propositions:

(13)  $\text{frac } a \cdot b = \text{frac}(a \cdot (\text{frac } b) + b \cdot (\text{frac } a) - (\text{frac } a) \cdot (\text{frac } b))$ .

(14)  $\text{frac } a \cdot b = \text{frac}(\lfloor a \rfloor \cdot (\text{frac } b) + \lfloor b \rfloor \cdot (\text{frac } a) + (\text{frac } a) \cdot (\text{frac } b))$ .

Now we state the proposition:

(15) Let us consider a real number  $a$ , and an integer  $b$ . Then  $\text{frac } a \cdot b = \text{frac } b \cdot (\text{frac } a)$ . The theorem is a consequence of (14).

Let us consider a real number  $a$ . Now we state the propositions:

- (16)  $\text{frac } a \cdot a = \text{frac}(2 \cdot a \cdot (\text{frac } a) - (\text{frac } a) \cdot (\text{frac } a))$ . The theorem is a consequence of (13).
- (17)  $\text{frac } a \cdot a = \text{frac}(2 \cdot \lfloor a \rfloor \cdot (\text{frac } a) + (\text{frac } a) \cdot (\text{frac } a))$ . The theorem is a consequence of (14).

Let us consider a positive real number  $a$ . Now we state the propositions:

- (18) If  $\text{frac } a = \frac{1}{2}$ , then  $\text{frac } 2 \cdot a = 0$ . The theorem is a consequence of (15).
- (19) If  $\frac{1}{2} > \text{frac } a$ , then  $\text{frac } 2 \cdot a = 2 \cdot (\text{frac } a)$ . The theorem is a consequence of (15).
- (20) If  $\frac{1}{2} < \text{frac } a$ , then  $\text{frac } 2 \cdot a < \text{frac } a$ . The theorem is a consequence of (15).

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

- (21) If  $b \nmid a$ , then  $(a \text{ div } b) + (-a \text{ div } b) = -1$ .
- (22)  $b \nmid a$  if and only if  $(a \text{ mod } b) + (-a \text{ mod } b) = b$ .
- PROOF: If  $b \nmid a$ , then  $(a \text{ mod } b) + (-a \text{ mod } b) = b$ . If  $b \mid a$ , then  $(a \text{ mod } b) + (-a \text{ mod } b) = 0$  by (6), [8, (10)].  $\square$

Now we state the propositions:

- (23) Let us consider integers  $a, b$ . Then
- (i)  $(a \text{ mod } b) + (-a \text{ mod } b) = 0$ , or
- (ii)  $(a \text{ mod } b) + (-a \text{ mod } b) = b$ .

The theorem is a consequence of (6) and (22).

- (24) Let us consider an even integer  $a$ , and an odd integer  $b$ . Then  $a \text{ div } b$  is odd if and only if  $a \text{ mod } b$  is odd.
- (25) Let us consider odd integers  $a, b$ . Then  $a \text{ mod } b$  is odd if and only if  $a \text{ div } b$  is even.
- (26) Let us consider an integer  $a$ , and an odd integer  $b$ . Suppose  $b \nmid a$ . Then  $a \text{ mod } b$  is odd if and only if  $-a \text{ mod } b$  is even. The theorem is a consequence of (22).
- (27) Let us consider a non zero integer  $a$ , and an integer  $b$ . Then  $a \mid b$  if and only if  $a \mid b \text{ mod } a$ .
- PROOF: If  $a \mid b$ , then  $a \mid b \text{ mod } a$  by (6), [8, (12)]. If  $a \mid b \text{ mod } a$ , then  $a \mid b$  by [8, (12)], [1, (2)], [9, (6)], (6).  $\square$
- (28) Let us consider a non weightless integer  $a$ , and a non weightless, odd integer  $b$ . Suppose  $a$  and  $b$  are relatively prime. Then  $b + a \text{ mod } b \neq b - a \text{ mod } b$ . The theorem is a consequence of (1), (6), (27), and (26).

- (29) Let us consider an integer  $a$ , and an even integer  $b$ . Suppose  $b \nmid a$ . If  $a \bmod b$  is odd, then  $-a \bmod b$  is odd. The theorem is a consequence of (22).
- (30) Let us consider non zero integers  $a, b$ . Suppose  $b \bmod a = -b \bmod a$ . Then
- (i)  $a$  is even, or
  - (ii)  $a \mid b$ .
- The theorem is a consequence of (26).
- (31) Let us consider natural numbers  $a, b$ . Suppose  $a$  and  $b$  are relatively prime. Let us consider a non trivial natural number  $n$ . Then  $\max(a \bmod n, b \bmod n) > 0$ .
- (32) Let us consider square integer  $s$ . Then  $s \bmod 3$  is a trivial natural number.
- (33) Let us consider square natural numbers  $a, b$ . If  $\frac{a+b}{2}$  is a square, then  $a \bmod 3 = b \bmod 3$ . The theorem is a consequence of (32).
- (34) Let us consider odd natural numbers  $a, b$ . Suppose  $a$  and  $b$  are relatively prime. If  $\frac{a^2+b^2}{2}$  is a square, then  $3 \nmid a \cdot b$ . The theorem is a consequence of (33), (31), and (32).
- (35) Let us consider integers  $a, b$ . Then  $a \operatorname{div} b = -a \operatorname{div} -b$ .
- (36) Let us consider square natural numbers  $a, b$ . Suppose  $a$  and  $b$  are relatively prime. If  $\frac{a-b}{2}$  is a square, then  $b \bmod 3 = 1$ . The theorem is a consequence of (32) and (31).
- (37) Let us consider an odd natural number  $a$ . Then  $3 \mid 2^a + 1$ .
- (38) Let us consider integers  $a, b, c, d$ . If  $\gcd(a \cdot b, c \cdot d) = 1$ , then  $\gcd(a, c) = 1$ .
- (39) Let us consider integers  $a, b$ , and non zero natural numbers  $m, n$ . Then  $a$  and  $b$  are relatively prime if and only if  $a^m$  and  $b^n$  are relatively prime. PROOF: If  $a$  and  $b$  are relatively prime, then  $a^m$  and  $b^n$  are relatively prime by [3, (10)]. If  $a^m$  and  $b^n$  are relatively prime, then  $a$  and  $b$  are relatively prime by [7, (6)], (38).  $\square$
- (40) Let us consider square natural numbers  $a, b$ . If  $a$  and  $b$  are relatively prime, then  $3 \nmid a + b$ .
- (41) Let us consider odd, a square natural numbers  $a, b$ . If  $a$  and  $b$  are relatively prime, then  $3 \nmid \frac{a+b}{2}$ . The theorem is a consequence of (40).
- (42) Let us consider natural numbers  $a, b, c, d$ . Suppose  $a$  and  $c$  are relatively prime and  $b$  and  $d$  are relatively prime. If  $a \cdot b = c \cdot d$ , then  $a = d$  and  $b = c$ .
- (43) Let us consider natural numbers  $a, b, c$ . Suppose  $a$  and  $b$  are relatively prime. If  $c \mid a \cdot b$ , then  $(\gcd(a, c)) \cdot (\gcd(b, c)) = c$ .

- (44) Let us consider natural numbers  $a, b, c, d$ . Suppose  $a$  and  $b$  are relatively prime. If  $a \cdot b = c \cdot d$ , then  $a \cdot b = (\gcd(a, c)) \cdot (\gcd(b, c)) \cdot (\gcd(a, d)) \cdot (\gcd(b, d))$ . The theorem is a consequence of (43).
- (45) Let us consider positive real numbers  $a, b, c, d$ . If  $a \cdot b = c \cdot d$  and  $a \cdot c = b \cdot d$ , then  $a = d$ .
- (46) Let us consider integers  $a, b$ . If  $a$  and  $b$  are relatively prime, then  $\gcd((a - b) \cdot (a + b), a \cdot b) = 1$ .
- (47) Let us consider an odd integer  $a$ , and an even integer  $b$ . Suppose  $a$  and  $b$  are relatively prime. Then  $\gcd((a - b) \cdot (a + b), 2 \cdot a \cdot b) = 1$ . The theorem is a consequence of (46).
- (48) Let us consider an even integer  $a$ , and an integer  $b$ . If  $a$  and  $b$  are relatively prime, then  $a + b$  and  $a - b$  are relatively prime.
- (49) Let us consider an even integer  $a$ , an integer  $b$ , and a non zero natural number  $n$ . Suppose  $a$  and  $b$  are relatively prime. Then  $b^n + a^n$  and  $b^n - a^n$  are relatively prime. The theorem is a consequence of (48).
- (50) Let us consider natural numbers  $a, b$ , and non zero natural numbers  $c, d$ . Suppose  $a \bmod c \cdot d = b \bmod c \cdot d$ . Then  $a \bmod c = b \bmod c$ .

Let us consider non zero natural numbers  $a, b$ . Now we state the propositions:

- (51)  $a - b \bmod 2 \cdot b = a + b \bmod 2 \cdot b$ .
- (52) If  $a^2 - b^2 \in \mathbb{N}$ , then  $a^2 - b^2 \bmod 2 \cdot b = a^2 + b^2 \bmod 2 \cdot b$ . The theorem is a consequence of (51) and (50).
- (53)  $(a - b)^2 \bmod 4 \cdot a \cdot b = (a + b)^2 \bmod 4 \cdot a \cdot b$ .

Now we state the propositions:

- (54) Let us consider odd natural numbers  $a, b$ . Then  $(\frac{a-b}{2})^2 \bmod a \cdot b = (\frac{a+b}{2})^2 \bmod a \cdot b$ .
- (55) Let us consider natural numbers  $a, b, c$ . Suppose  $a^2 + b^2 = c^2$ . Then
- (i)  $b^2 \bmod a = c^2 \bmod a$ , and
  - (ii)  $a^2 \bmod b = c^2 \bmod b$ .
- (56) Let us consider a natural number  $a$ , a non trivial natural number  $b$ , and a non zero natural number  $c$ . If  $a \bmod b \cdot c = 1$ , then  $a \bmod b = 1$ .
- (57) Let us consider a natural number  $a$ , a non zero natural number  $b$ , and non zero natural numbers  $m, n$ . Suppose  $m \geq n$ . If  $a \bmod b^m = 1$ , then  $a \bmod b^n = 1$ . The theorem is a consequence of (56).

Let us consider an integer  $i$ . Now we state the propositions:

- (58) (i)  $i^2 \bmod 4 = 0$ , or
- (ii)  $i^2 \bmod 4 = 1$ .

$$(59) \quad (i) \ i^2 \bmod 8 = 0, \text{ or}$$

$$(ii) \ i^2 \bmod 8 = 1, \text{ or}$$

$$(iii) \ i^2 \bmod 8 = 4.$$

$$(60) \quad (i) \ i^4 \bmod 8 = 0, \text{ or}$$

$$(ii) \ i^4 \bmod 8 = 1.$$

The theorem is a consequence of (59).

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

$$(61) \quad (i) \ a + b \bmod 4 = 2, \text{ or}$$

$$(ii) \ a - b \bmod 4 = 2.$$

$$(62) \quad (i) \ a + b \bmod 4 = 0, \text{ or}$$

$$(ii) \ a - b \bmod 4 = 0.$$

The theorem is a consequence of (61) and (6).

$$(63) \quad \max(a + b \bmod 4, a - b \bmod 4) = 2. \text{ The theorem is a consequence of (61).}$$

$$(64) \quad \min(a + b \bmod 4, a - b \bmod 4) = 0. \text{ The theorem is a consequence of (62).}$$

Now we state the propositions:

$$(65) \quad \text{Let us consider natural numbers } a, b. \text{ Suppose } a \text{ and } b \text{ are relatively prime. Then}$$

$$(i) \ a^4 + b^4 \bmod 5 = 1, \text{ or}$$

$$(ii) \ a^4 + b^4 \bmod 5 = 2.$$

The theorem is a consequence of (9).

$$(66) \quad \text{Let us consider integers } a, b. \text{ Then } a \bmod b = b \cdot \left(\text{frac } \frac{a}{b}\right).$$

$$(67) \quad \text{Let us consider an integer } a, \text{ and a non zero integer } b. \text{ Then } \text{frac } b \cdot \left(\text{frac } \frac{a}{b}\right) = 0. \text{ The theorem is a consequence of (15).}$$

Let  $a$  be a heavy, positive real number. Note that  $\frac{1}{a}$  is light and positive.

Now we state the proposition:

$$(68) \quad \text{Let us consider positive natural numbers } b, c. \text{ Then } c \cdot \left(\text{frac } \frac{1}{b+c}\right) < 1.$$

Let  $a$  be an integer. Observe that  $a \div 1$  reduces to  $a$ .

Let  $a$  be a non zero integer. One can check that  $1 \cdot a \div a$  reduces to 1.

Let  $a$  be a heavy, positive integer. One can verify that  $1 \div a$  is zero.

Let  $b$  be an integer. One can verify that  $b \div a \cdot b$  is zero.

One can verify that  $b \bmod a \cdot b$  reduces to  $b$ .

Now we state the propositions:

$$(69) \quad \text{Let us consider integers } a, b, c. \text{ Then } a \cdot b \bmod a \cdot c = a \cdot (b \bmod c).$$



- (70) Let us consider non zero integers  $a$ ,  $b$ , and an integer  $c$ . Then  $(c \bmod a \cdot b) \bmod a = c \bmod a$ . The theorem is a consequence of (66) and (15).
- (71) Let us consider an integer  $a$ , a non zero integer  $b$ , and a non zero natural number  $n$ . Then  $(a \bmod b^n) \bmod b = a \bmod b$ . The theorem is a consequence of (70).

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

- (72) If  $b \bmod a < \lceil \frac{a}{2} \rceil$ , then  $\text{frac } \frac{b}{a} < \frac{1}{2}$ . The theorem is a consequence of (66).
- (73) If  $b \bmod a < \lceil \frac{a}{2} \rceil$ , then  $2 \cdot b \bmod a = 2 \cdot (b \bmod a)$ . The theorem is a consequence of (6), (66), (72), and (15).

Now we state the proposition:

- (74) Let us consider an odd, a square integer  $a$ . Then  $a \bmod 8 = 1$ .

Let  $a$  be square integer. Let us note that  $a \bmod 3$  is a square and  $a \bmod 4$  is a square and  $a \bmod 8$  is a square.

Now we state the propositions:

- (75) Let us consider an integer  $a$ . Then  $a^4 \bmod 8$  is a trivial natural number. The theorem is a consequence of (60).
- (76) Let us consider an odd integer  $a$ . Then  $a^4 \bmod 8 = 1$ . The theorem is a consequence of (60).
- (77) Let us consider an integer  $i$ . Then
- (i)  $i^4 \bmod 5 = 0$ , or
  - (ii)  $i^4 \bmod 5 = 1$ .
- (78) Let us consider odd natural numbers  $a$ ,  $b$ . Suppose  $a$  and  $b$  are relatively prime. Then
- (i)  $\frac{a^4+b^4}{2} \bmod 5 = 3$ , or
  - (ii)  $\frac{a^4+b^4}{2} \bmod 5 = 1$ .

The theorem is a consequence of (65).

- (79) Let us consider natural numbers  $a$ ,  $b$ . Suppose  $a$  and  $b$  are relatively prime. Then  $a^4 - b^4 \bmod 5$  is a square. The theorem is a consequence of (9).
- (80) Let us consider integers  $a$ ,  $b$ , and a natural number  $n$ . Then  $a^n \bmod b = (a \bmod b)^n \bmod b$ .
- (81) Let us consider an integer  $a$ , and a non zero integer  $b$ . Then  $a^2 \bmod b = (b - a)^2 \bmod b$ . The theorem is a consequence of (80).
- (82) Let us consider integers  $a$ ,  $b$ , and an odd integer  $c$ . If  $a + b \bmod c = a - b \bmod c$ , then  $c \mid b$ . The theorem is a consequence of (6).

- (83) Let us consider an integer  $k$ . Then there exist integers  $a, b$  such that  $a^2 - b^2 = k$  if and only if  $k \bmod 4 \neq 2$ .

PROOF: If there exist integers  $a, b$  such that  $a^2 - b^2 = k$ , then  $k \bmod 4 \neq 2$  by [14, (1)], [16, (53)], [15, (2)], [12, (62)]. If  $k \bmod 4 \neq 2$ , then there exist integers  $a, b$  such that  $a^2 - b^2 = k$  by [4, (11)], [12, (62)], [14, (1)].  $\square$

ACKNOWLEDGEMENT: Ad Maiorem Dei Gloriam

## REFERENCES

- [1] Marcin Acewicz and Karol Pąk. Pell's equation. *Formalized Mathematics*, 25(3):197–204, 2017. doi:10.1515/forma-2017-0019.
- [2] Marco B. Caminati and Giuseppe Rosolini. Custom automations in Mizar. *Journal of Automated Reasoning*, 50(2):147–160, 2013.
- [3] Andrzej Kondracki. The Chinese Remainder Theorem. *Formalized Mathematics*, 6(4):573–577, 1997.
- [4] Artur Korniłowicz. Elementary number theory problems. Part III. *Formalized Mathematics*, 30(2):135–158, 2022. doi:10.2478/forma-2022-0011.
- [5] Artur Korniłowicz. On rewriting rules in Mizar. *Journal of Automated Reasoning*, 50(2):203–210, 2013.
- [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] Xiquan Liang, Li Yan, and Junjie Zhao. Linear congruence relation and complete residue systems. *Formalized Mathematics*, 15(4):181–187, 2007. doi:10.2478/v10037-007-0022-7.
- [10] Adam Naumowicz. Elementary number theory problems. Part I. *Formalized Mathematics*, 28(1):115–120, 2020. doi:10.2478/forma-2020-0010.
- [11] Wacław Sierpiński. *250 Problems in Elementary Number Theory*. Elsevier, 1970. [https://www.isinj.com/mt-aime/250ProblemsinElementaryNumberTheory-Sierpinski\(1970\).pdf](https://www.isinj.com/mt-aime/250ProblemsinElementaryNumberTheory-Sierpinski(1970).pdf).
- [12] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(3):501–505, 1990.
- [13] Rafał Ziobro. Multiplication-related classes of complex numbers. *Formalized Mathematics*, 28(2):197–210, 2020. doi:10.2478/forma-2020-0017.
- [14] Rafał Ziobro. Some remarkable identities involving numbers. *Formalized Mathematics*, 22(3):205–208, 2014. doi:10.2478/forma-2014-0023.
- [15] 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.
- [16] Rafał Ziobro. Parity as a property of integers. *Formalized Mathematics*, 26(2):91–100, 2018. doi:10.2478/forma-2018-0008.

Received May 11, 2025