Podróże po Imperium Liczb

Część 06. Podzielność w Zbiorze Liczb Całkowitych

Rozdział 3

3. Liczby względnie pierwsze

Andrzej Nowicki 10 maja 2012, http://www.mat.uni.torun.pl/~anow

Spis treści

Wszystkie książki z serii "Podróże po Imperium Liczb" napisano w edytorze LaTeX. Spisy treści tych książek oraz pewne wybrane rozdziały moża znaleźć na internetowej stronie autora: http://www-users.mat.uni.torun.pl/~anow.

3 Liczby względnie pierwsze

3.1 Elementarne własności i przykłady

Dwie liczby całkowite a, b (z których co najmniej jedna jest różna od zera) są względnie pierwsze, jeśli ich największy wspólny dzielnik (a, b) jest równy 1. Jest to równoważne temu (patrz **??**), że istnieją liczby całkowite x, y takie, że $1 = xa + yb$. Przypomnijmy (patrz **??**), że jeśli $d = (a, b)$, to liczby całkowite $\frac{a}{d}$ i $\frac{b}{d}$ są względnie pierwsze. Innymi słowy:

$$\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1.$$

3.1.1. *Niech $d = (a, b)$ i niech x, y będą liczbami całkowitymi takimi, że $d = ax + by$. Wtedy liczby x i y są względnie pierwsze.*

W poniższych stwierdzenia i zadaniach a, b, c, d są liczbami całkowitymi.

3.1.2. *Jeśli $(a, b) = 1$ i $(a, c) = 1$, to $(a, bc) = 1$.*

D. Z **??** wiemy, że istnieją liczby całkowite x, y, u, v takie, że $1 = xa + yb$ oraz $1 = ua + vc$. Mnożąc te równości przez siebie stronami otrzymujemy równość $1 = (xua + xvc + ybu)a + (yv)bc$, z której (na mocy **??**) wynika, że $\mathrm{nwd}(a, bc) = 1$. ⊠

3.1.3. *Jeśli $(a, bc) = 1$, to $(a, b) = 1$ i $(a, c) = 1$.*

D. Istnieją liczby całkowite x, y takie, że $xa + y(bc) = 1$. Mamy więc równości $1 = xa + (yc)b$ oraz $1 = xa + (yb)c$, z których (na mocy **??**) wynika, że $(a, b) = (a, c) = 1$. ⊠

3.1.4. *Jeśli $(a, b) = 1$ i $n, m \in \mathbb{N}$, to $(a^n, b^m) = 1$.*

3.1.5. *Jeśli $(a, b) = 1$ i $a \mid bc$, to $a \mid c$.*

3.1.6. *Jeśli $(a, b) = 1$, $a \mid c$, $b \mid c$, to $ab \mid c$.*

3.1.7. *Jeśli $(a, b) = 1$, to $[a, b] = |ab|$.*

3.1.8. *Jeśli $(a, b) = 1$, to $(n, ab) = (n, a)(n, b)$.*

3.1.9. *Jeśli $(a, b, n) = 1$, to $(n, ab) = (n, a)(n, b)$.*

3.1.10. *Jeśli $(a, b, c) = 1$ i $(a, b, d) = 1$, to $(a, b, cd) = 1$.*

3.1.11. *Niech* $a_1, \ldots, a_s \in \mathbb{Z}$, $n_1, \ldots, n_s \in \mathbb{N}$. *Jeśli* $(a_1, \ldots, a_s) = 1$, *to* $(a_1^{n_1}, \ldots, a_s^{n_s}) = 1$.

3.1.12. *Jeżeli* $ad - bc = 1$, *to* $(a^2 + b^2, ac + bd) = 1$.

3.1.13. *Jeżeli* $(a, b) = 1$, *to* $(a^2 + b^2, a + b) = 1$ *lub* 2.

3.1.14. *Jeżeli* $(a, b) = 1$, *to* $(a + b, a^2 - ab + b^2) = 1$ *lub* 3. ([San2] 47).

3.1.15. *Jeżeli* $(a, b) = 1$, *to* $(a^2 + 2b, b^2) = 1$.

3.1.16. *Jeżeli* $(a, b) = 1$, *to* $(a^2 + 2b, a^4 + 4a^b + 3b^2) = 1$.

3.1.17. *Jeżeli* $(a, b) = 1$, *to* $(a^2 + b^2, a^3 + b^3) \mid a - b$. ([Grif] 18).

3.1.18. *Jeżeli* $(a, b) = 1$ *i* $a+b$ *jest liczbą parzystą, to* $24 \mid (a-b)ab(a+b)$. ([Mon] 22(1)(1915) 30).

3.1.19. *Niech* $n, m, a, b \in \mathbb{Z}$. *Jeśli* $(n, m) = 1$, $(a, n) = 1$ *i* $(b, m) = 1$, *to* $(am + bn, mn) = 1$.

D. Ponieważ $(m, n) = 1$ i $(a, n) = 1$, więc $(am, n) = 1$ i stąd $(am + bn, n) = 1$. Analogicznie $(am + bn, m) = 1$. Zatem $(am + bn, mn) = 1$. ⊠

3.1.20. *Niech* $m, n, u \in \mathbb{Z}$. *Niech* $(m, n) = 1$. *Jeśli* $(u, mn) = 1$, *to istnieją liczby całkowite* a, b *takie, że* $(a, n) = 1$, $(b, m) = 1$ *oraz* $u = am + bn$.

D. Niech $1 = mx + ny$, $x, y \in \mathbb{Z}$. Niech $a = xu$, $b = yu$. Wtedy $(a, n) = 1$, $(b, m) = 1$ oraz $u = u \cdot 1 = u \cdot (mx + ny) = am + bn$. ⊠

3.1.21. *Ułamek* $(12n + 1)/(30n + 2)$ *jest nieskracalny.*

3.1.22. *Ułamek* $(21n + 4)/(14n + 3)$ *jest nieskracalny.* ([IMO](1) 1959).

3.1.23. *Jeśli* $1 \leqslant i < j \leqslant n$, *to liczby* $i \cdot n! + 1$, $j \cdot n! + 1$ *są względnie pierwsze.* ([Ri97] 24).

3.1.24. *Niech* $a, b, c \in \mathbb{R}$. *Rozpatrzmy liczby* $\frac{1+ab}{a-b}$, $\frac{1+bc}{b-c}$, $\frac{1+ca}{c-a}$. *Jeśli liczby te są całkowite, to są parami względnie pierwsze.* ([OM] St Petersburg 1994).

3.2 Liczby względnie pierwsze oraz sumy, różnice i iloczyny

3.2.1. *Iloma sposobami można liczbę* 1000 *przedstawić w postaci sumy* $a + b$, *gdzie* a *i* b *są względnie pierwszymi liczbami naturalnymi? (Zakładamy, że przedstawienia* $a + b$ *i* $b + a$ *są identyczne*). Odp. 200. ([Berk] 1b/93).

3.2.2. *Każda liczba naturalna* > 6 *jest sumą dwóch liczb naturalnych większych od* 1 *i względnie pierwszych.* ([Wm] 7 31, [S64] 40).

3.2.3. *Jeśli $m \geqslant 2$ jest liczbą naturalną, to każda liczba naturalna n, większa od $2m+2$, jest sumą dwóch liczb naturalnych względnie pierwszych i większych od m.* ([Wm] 7 33).

3.2.4. *Każda liczba naturalna większa od* 17 *jest sumą trzech liczb naturalnych większych od* 1 *i parami względnie pierwszych.* ([Wm] 7 33, [S64] 41).

3.2.5. *Niech n, s będą takimi liczbami naturalnymi, że albo s jest nieparzyste, albo n i s są jednocześnie parzyste. Istnieją wtedy liczby całkowite a, b takie, że $n = a + b$ oraz $(a, s) = (b, s) = 1$.* ([Ibe] 2004).

3.2.6. *Niech $s \in \mathbb{N}$. Każdą liczbę naturalną $n > s$ można przedstawić w postaci $n = a + b$, gdzie $a, b \in \mathbb{N}$, $a \mid s$, $(b, s) = 1$.* ([Kw] 6/1977 48).

3.2.7. *Niech x i y będą liczbami całkowitymi względnie pierwszymi oraz niech $xy > 1$. Wykazać, że jeżeli n jest liczbą naturalną parzystą, to $x^n + y^n$ nie dzieli się przez $x + y$.* ([OM] Japonia 1992, [Pa97]).

3.2.8. *Znaleźć* 5 *parami różnych liczb naturalnych takich, że każde dwie są względnie pierwsze, a każda suma dowolnych kilku z nich jest liczbą złożoną.* ([WaJ] 449(87)).

O. 121, 241, 361, 481, 601. Dla dowolnego $n \in \mathbb{N}$ istnieje n takich liczb. Są to np. liczby $i \cdot n! + 1$ dla $i = 1, \ldots, n$. Uogólnieniem tego zadania jest 3.4.2. ☒

3.2.9. *Niech $a_1, \ldots a_n$ będą parami względnie pierwszymi liczbami naturalnymi takimi, że $(a_1 + \cdots + a_n, a_i) > 1$ dla wszystkich $i = 1, \ldots, n$. Znaleźć takie liczby dla następujących n.*

(1) $n = 3$. Odp. $3 + 5 + 22 = 30$ *lub* $5 + 7 + 58 = 70$. ([S59] 37).

(2) $n = 4$. Odp. $3 + 5 + 11 + 19 \cdot 164 = 19 \cdot 165 = 3 \cdot 5 \cdot 11 \cdot 19$.

(3) $n = 5$. Odp. $3 + 5 + 7 + 11 + 2284 = 2310 = 3 \cdot 5 \cdot 7 \cdot 11 \cdot 2$.

3.2.10. *Niech $n > 1$ będzie liczbą naturalną. Rozpatrzmy zbiór*

$$A_n = \{a \in \mathbb{N};\ (a, n) \neq 1\}.$$

Mówić będziemy, że n jest liczbą magiczną, jeśli zbiór A_n jest zamknięty ze względu na dodawanie.

(1) *Liczba* 67 *jest magiczna.*

(2) *Liczba* 2001 *nie jest magiczna.*

(3) *Liczba n jest magiczna wtedy i tylko wtedy, gdy jest potęgą liczby pierwszej.*

([MOc] 2000).

3.2.11. *Każda liczba parzysta jest dla każdej liczby naturalnej n różnicą dwóch liczb naturalnych względnie pierwszych z n.* ([S64] 42).

3.2.12. *Każda liczba naturalna jest na nieskończenie wiele sposobów różnicą dwóch liczb naturalnych względnie pierwszych.* ([Wm] 7 33).

3.2.13. *Dla każdej liczby naturalnej n istnieją parami względnie pierwsze liczby naturalne $a_0, a_1, \ldots, a_n$ takie, że liczba $a_0a_1 \cdots a_n - 1$ jest iloczynem dwóch kolejnych liczb naturalnych.* ([OM] USA 2008).

3.2.14. *Iloma sposobami można liczbę naturalną $n > 1$ przedstawić w postaci iloczynu ab, gdzie a i b są względnie pierwszymi liczbami naturalnymi? (Zakładamy, że przedstawienia ab i ba są identyczne).* ([S50] 67).

O. 2^{k-1}, gdzie k jest liczbą parami różnych liczb pierwszych dzielących n. ☒

3.3 Formy liniowe

3.3.1. *Niech $a, b, c \in \mathbb{N}$ i $(a, b) = 1$. Istnieje wtedy liczba naturalna x taka, że $a \mid xb + c$.* ([Kw] 2/1977 37).

3.3.2. *Niech $a, b, m \in \mathbb{N}$ i $(a, b) = 1$. Istnieją wtedy liczby naturalne x, y takie, że $(x, y) = 1$ oraz $m \mid ax + by$.* ([WaJ] 9(61)).

3.3.3. *Niech $a, b \in \mathbb{Z}$, $(a, b) = 1$. Dla każdej liczby naturalnej n istnieje liczba całkowita x taka, że $(ax + b, n) = 1$.* ([Mon] 72(8)(1965) E1730).

3.3.4. *Niech $a, b, 0 \neq c \in \mathbb{Z}$. Istnieją wtedy liczby $x, y \in \mathbb{Z}$ takie, że $(x, y) = 1$ oraz $c \mid ax+by$.* ([OM] ZSRR 1961).

D. Jeśli $c = a$ to przyjmujemy $x = 1$, $y = 0$. Załóżmy teraz, że $c \neq a$. Niech $d = (b, c-a)$, $x = b/d$, $y = (c - a)/d$. Wtedy $(x, y) = 1$ oraz $ax + by = xc$. ☒

3.3.5 (Thue)**.** *Niech $a, m \in \mathbb{N}$ i $(a, m) = 1$. Istnieją wtedy liczby naturalne $x, y \leqslant \sqrt{m}$ takie, że $m \mid ax + y$ lub $m \mid ax - y$.* ([S65] s.26).

3.3.6. *Niech $a, b, c, n \in \mathbb{N}$, $(a, b) = 1$. Jeśli $ab = c^n$, to istnieją liczby naturalne a_1, b_1 takie, że $a = a_1^n$, $b = b_1^n$.* ([S68] 125).

3.3.7. *Niech $a, b, d \in \mathbb{Z}$. Jeśli $(a, b) = 1$ i $d \mid a + b$, to $(d, a) = 1$ i $(d, b) = 1$.* ([S59] 37).

3.3.8. *Niech $a_1, a_2, b_1, b_2 \in \mathbb{N}$, $(a_1, a_2) = (b_1, b_2) = 1$. Niech*

$$A = \{a_1n + a_2;\ n \in \mathbb{N}\}, \quad B = \{b_1n + b_2;\ n \in \mathbb{N}\}.$$

Wtedy albo $A \cap B = \emptyset$, albo $A \cap B = \{c_1n + c_2;\ n \in \mathbb{N}\}$ dla pewnych względnie pierwszych liczb naturalnych c_1 i c_2. ([Maza] 28).

3.4 Liczby względnie pierwsze i ciągi arytmetyczne

3.4.1. *Niech $a, b, n \in \mathbb{N}$. Jeżeli żadna z liczb $a, a+b, a+2b, \ldots, a+(n-1)b$ nie jest podzielna przez n, to liczby n i b nie są względnie pierwsze.*

([Kw] 2/1977 37, [Mat] 1/1978 41, [Kw] 6/1991 38).

D. Istnieją liczby naturalne $i < j$ mniejsze od n takie, że reszty z dzielenia przez n liczb $a + ib$, $a + jb$ są jednakowe. Wtedy $n \mid (j-i)b = (a+jb) - (a+ib)$. Przypuśćmy, że $(b, n) = 1$. Wtedy $n \mid j - i$ i mamy sprzeczność (ponieważ $0 < j - i < n$). ⊠

3.4.2. *Dla każdej liczby naturalnej n istnieje ciąg arytmetyczny składający się z n parami względnie pierwszych liczb złożonych.* ([S64] 44, [B-zm] 66, [Bedn] 92).

3.4.3. *Nie istnieje nieskończony ciąg arytmetyczny rosnący o parami względnie pierwszych wyrazach naturalnych.* ([Bedn] 92).

3.4.4. *Niech $n \geqslant 7$ będzie taką liczbą naturalną, że zbiór*

$$\{a \in \mathbb{N};\ a < n, (a, n) = 1\}$$

tworzy ciąg arytmetyczny. Wykazać, że wtedy n jest albo liczbą pierwszą albo potęgą dwójki. ([WaG] 2-57).

3.4.5. *Jeśli a i b są względnie pierwszymi liczbami naturalnymi oraz m jest dowolną liczbą naturalną, to w ciągu arytmetycznym*

$$a,\ a+b,\ a+2b,\ a+3b, \ldots$$

istnieje nieskończenie wiele wyrazów względnie pierwszych z liczbą m. ([S88] 12).

3.5 Nieskończone ciągi liczb parami względnie pierwszych

3.5.1. *Niech $f(x) \in \mathbb{Z}[x]$, $f(0) = f(1) = 1$. Definiujemy ciąg (a_n) przyjmując za a_0 dowolną liczbę całkowitą oraz*

$$a_n = f(a_{n-1}), \quad \text{dla} \quad n \in \mathbb{N}.$$

Wtedy każde dwa wyrazy a_n i a_m, gdzie $n \neq m$, są względnie pierwsze. ([Mon] 75(10)(1968) E2025).

D. Istnieje $g(x) \in \mathbb{Z}[x]$ takie, że $f(x) = x(x-1)g(x) + 1$. Udowodnimy, metodą indukcji matematycznej, że $a_{n+1} \equiv 1 \pmod{a_0 a_1 \cdots a_n}$. Dla $n = 0$ jest to oczywiste. Załóżmy, że jest to prawdą dla pewnego n. Niech $a_{n+1} - 1 = k a_0 a_1 \cdots a_n$. Wtedy $a_{n+2} - 1 = f(a_{n+1}) - 1 = a_{n+1}(a_{n+1} - 1)g(a_{n+1}) + 1 - 1 = k a_0 a_1 \cdots a_n a_{n+1} g(a_{n+1})$, czyli $a_{n+2} \equiv 1 \pmod{a_0 a_1 \cdots a_{n+1}}$ i to kończy dowód. ⊠

3.5.2 (Sylvester)**.** *Niech (a_n) będzie ciągiem określonym wzorami:*

$$a_1 = 2, \quad a_{n+1} = a_n^2 - a_n + 1, \quad dla \;\; n \in \mathbb{N}.$$

Każde dwa różne wyrazy tego ciągu są względnie pierwsze. Dowód. *Jest to szczególny przypadek faktu* 3.5.1. ([Ca02]).

3.5.3. *Niech $b \in \mathbb{N}$ i niech (a_n) będzie ciągiem określonym wzorami:*

$$a_1 = b + 1, \quad a_{n+1} = a_n^2 - ba_n + b, \quad dla \;\; n \in \mathbb{N}.$$

Każde dwa różne wyrazy tego ciągu są względnie pierwsze. ([OM] Polska 2001/2002).

D. Dla $n \in \mathbb{N}$ zachodzi równość $a_{n+1} = a_1 a_2 \dots a_n + b$. ⊠

3.5.4. *Niech $f(x) = x^2 - x + 1$. Jeśli $n \in \mathbb{N}$, $n > 1$, to każde dwa różne wyrazy ciągu*

$$n, \;\; f(n), \;\; f(f(n)), \;\; f(f(f(n))), \dots$$

są względnie pierwsze. Dowód. *Jest to szczególny przypadek faktu* 3.5.1. ([WaJ] 258(77), [DoC] 78).

3.5.5. *Niech (a_n) będzie ciągiem o wyrazach naturalnych spełniających równość:*

$$a_{n+1} = a_n^3 - a_n + 1, \quad dla \;\; n \in \mathbb{N}.$$

Każde dwa różne wyrazy tego ciągu są względnie pierwsze. Dowód. *Jest to szczególny przypadek faktu* 3.5.1.

3.5.6. *Niech (a_n) będzie ciągiem określonym wzorami:*

$$a_1 = a, \quad a_2 = a_1 + b, \quad a_3 = a_1 a_2 + b, \quad a_4 = a_1 a_2 a_3 + b, \quad \dots,$$

gdzie a i b są względnie pierwszymi liczbami całkowitymi. Każde dwa różne wyrazy tego ciągu są względnie pierwsze. ([Ca02], [Ri97] 23).

3.5.7. *Niech a, b będą względnie pierwszymi liczbami naturalnymi takimi, że $b > a \geqslant 1$. Definiujemy ciąg (a_n) w następujący sposób:*

$$a_0 = b, \quad a_n = a_{n-1}(a_{n-1} - a) + a \quad dla \;\; n \in \mathbb{N}.$$

Wyrazy tego ciągu są parami względnie pierwsze. ([Ri97] 23).

3.5.8. *Jeśli f jest wielomianem o współczynnikach całkowitych różnym od stałej z dodatnim największym współczynnikiem, to wyrazy nieskończonego ciągu $f(1)$, $f(2)$, $f(3)$, ... nie mogą być wszystkie parami względnie pierwsze.* ([Wm] 7 35).

3.5.9. *Czy istnieją wielomian $f(x) \in \mathbb{Z}[x] \setminus \mathbb{Z}$ oraz liczba naturalna $k > 1$ takie, że wszystkie liczby $f(k^n)$, dla $n = 1, 2, \dots,$ są parami względnie pierwsze ?* Odp. *Nie.* ([Kw] 3/1999 M1664).

3.5.10. *Niech (a_n) będzie ciągiem zdefiniowanym następująco*

$$a_1 = 2, \quad a_{n+1} = 2^{a_n} - 1 \quad dla \quad n \in \mathbb{N}.$$

Każde dwa różne wyrazy tego ciągu są względnie pierwsze. ([MG] 495(1998) s.513).

3.5.11. *Ciągi (a_n) i (b_n) definiujemy następująco:*

$$\begin{cases} a_0 &= 0, \\ b_0 &= a_1 = b_1 = 1, \\ b_{n+1} &= a_n b_{n-1}, \\ a_{n+1} &= b_{n+1} + b_n. \end{cases}$$

Wtedy: $(a_n) = (0, 1, 2, 3, 5, 13, 49, 529, 21121, \dots)$, $(b_n) = (1, 1, 1, 2, 3, 10, 39, 490, 20631, \dots)$. *Każde dwie różne liczby ciągu (a_n) są względnie pierwsze.* (Somos-Haas).

3.5.12. *Istnieją takie nieskończone ciągi (a_n) i (b_n) liczb naturalnych, że wszystkie liczby postaci $a_n + b_m$, gdzie $n, m \in \mathbb{N}$, są parami względnie pierwsze.* ([Dlt] 11/1997).

3.5.13. *Niech $a > 1$ będzie liczbą naturalną i niech $A = \{a^n + a^{n-1} - 1;\ n \in \mathbb{N}\}$. Wykazać, że istnieje nieskończony podzbiór zbioru A składający się z liczb parami względnie pierwszych.* ([OM] Rumunia 1997).

3.5.14. *Istnieje nieskończony zbiór liczb naturalnych postaci $2^n - 3$, z których każde dwie są względnie pierwsze.* ([IMO] 1971).

3.5.15. *Każde dwie różne liczby postaci $1 + 3^{3^n} + 9^{3^n}$ są względnie pierwsze.* ([OM] Rosja 1995).

3.5.16. *Jeśli w danym zbiorze liczb naturalnych dla każdej liczby naturalnej n istnieje n parami względnie pierwszych liczb, to w zbiorze tym istnieje nieskończenie wiele liczb parami względnie pierwszych.* ([Mat] 2/1958 59).

★ A. W. F. Edwards, *Infinite coprime sequences*, [MG] 366(48)(1964) 416-422.
J. Lambek, L. Moser, *On relatively prime sequences*, [MG] 41(338)(1957) 287-288.
A. Lord, *A uniform construction of some infinite coprime sequences*, [MG] 92(523)(2008) 66-70.
K. Selucky, *Divisibility on infinite coprime sequences*, [Mon] 75(1)(1968) 43-44.
W. Sierpiński, *O ciągach liczb parami względnie pierwszych*, [Wm] 7 31-38.
M. Somos, R. Haas, *A linked pair of sequences implies the primes are infinite*, [Mon] 6/2003 539-540.
M. V. Subbarao, *On relatively prime sequences*, [Mon] 73(10)(1966) 1099-1102.

3.6 Ciągi a_1+n, ..., a_s+n

3.6.1. *Dla dowolnych dwóch różnych liczb całkowitych a, b istnieje nieskończenie wiele liczb naturalnych n takich, że $(a+n,\ b+n)=1$.* ([S59] 15, [S64] 37).

D. Załóżmy, że $a>b$ i niech k będzie dowolną liczbą naturalną większą od $(b-1)/(a-b)$. Wtedy $n=1-b+k(a-b)$ jest liczbą naturalną i liczby $a+n=1+(k+1)(a-b)$, $b+n=1+k(a-b)$ są względnie pierwsze. ⊠

3.6.2. *Jeśli a, b, c są różnymi liczbami całkowitymi, to istnieje nieskończenie wiele liczb naturalnych n takich, że liczby $a+n$, $b+n$ i $c+n$ są parami względnie pierwsze.* ([S64] 38).

3.6.3. *Niech $a_1, \ldots, a_s$ będą różnymi parami względnie pierwszymi liczbami naturalnymi. Istnieje wtedy nieskończenie wiele liczb naturalnych n takich, że liczby*

$$a_1+n,\ a_2+n,\ \ldots,\ a_s+n$$

są parami względnie pierwsze. ([Kw] 3/1987 24).

D. Niech $b=\left|\prod_{i<j}(a_i-a_j)\right|$ i niech $k\in\mathbb{N}$. Wtedy liczby $a_1+kb, \ldots, a_s+kb$ są parami względnie pierwsze. Istotnie, jeśli $d=(a_i+kb, a_j+kb)$, to $d \mid a_i-a_j$ więc $d \mid kb$, a zatem $d \mid (a_i, a_j)=1$. ⊠

3.6.4. *Niech $A\subseteq\mathbb{N}$. Jeśli $m\in\mathbb{N}$ oraz $i\in\{0,1,\ldots,m-1\}$, to przez $A(m,i)$ oznaczamy zbiór tych liczb ze zbioru A, których reszta z dzielenia przez m jest równa i. Następujące warunki są równoważne:*

(1) *Dla każdej liczby naturalnej $m>1$ istnieje $i\in\{0,1,\ldots,m-1\}$ takie, że $|A(m,i)|\leqslant 1$.*

(2) *Dla każdej liczby pierwszej p istnieje $i\in\{0,1,\ldots,p-1\}$ takie, że $|A(p,i)|\leqslant 1$.*

D. Implikacja (1) ⇒ (2) jest oczywista. Załóżmy, że zachodzi warunek (2) i niech $1<m\in\mathbb{N}$. Istnieje wtedy liczba pierwsza p dzieląca m i istnieje $i\in\{0,1,\ldots,p-1\}$ takie, że $|A(p,i)|\leqslant 1$. Niech $m=wp$, gdzie $w\in\mathbb{N}$. Wówczas $0\leqslant i<m$ i $|A(m,i)|\leqslant 1$. Przypuśćmy bowiem, że istnieją dwie różne liczby naturalne $a, b\in A$ takie, że $a=um+i$, $b=vm+i$, gdzie $u, v\in\mathbb{Z}$. Wtedy $a=uwp+i$, $b=vwp+i$, a zatem $a, b\in A(p,i)$ wbrew temu, że $|A(p,i)|\leqslant 1$. ⊠

3.6.5. *Niech $A\subseteq\mathbb{N}$. Jeśli $m\in\mathbb{N}$ oraz $i\in\{0,1,\ldots,m-1\}$, to przez $A(m,i)$ oznaczamy zbiór tych liczb ze zbioru A, których reszta z dzielenia przez m jest równa i.*

Jeśli istnieje liczba naturalna n taka, że wszystkie elementy zbioru $A+n=\{a+n;\ a\in A\}$ są parami względnie pierwsze, to dla każdej liczby pierwszej p istnieje $i\in\{0,1,\ldots,p-1\}$ takie, że $|A(p,i)|\leqslant 1$.

D. Załóżmy, że wszystkie elementy zbioru $A+n$ są parami względnie pierwsze i przypuśćmy, że istnieje liczba pierwsza p taka, że $|A(p,i)|\geqslant 2$ dla wszystkich $i=0,1,\ldots,p-1$. Niech r będzie resztą z dzielenia liczby n przez p. Jeśli $r=0$, to $p \mid n$, a zatem $p \mid (a+n, b+n)$ dla $a\neq b\in A(p,0)$ wbrew temu, że $(a+n, b+n)=1$. Jeśli $r>0$, to $p \mid (a+n, b+n)$ dla $a\neq b\in A(p,p-r)$; mamy więc również sprzeczność. ⊠

3.6.6. *Niech A będzie skończonym zbiorem parami różnych liczb naturalnych. Jeśli $m \in \mathbb{N}$ oraz $i \in \{0, 1, \ldots, m-1\}$, to przez $A(m, i)$ oznaczamy zbiór tych liczb ze zbioru A, których reszta z dzielenia przez m jest równa i. Następujące warunki są równoważne.*

(1) *Istnieje liczba naturalna n taka, że wszystkie liczby postaci $a + n$, gdzie $a \in A$, są parami względnie pierwsze.*

(2) *Dla każdej liczby naturalnej $m > 1$ istnieje $i \in \{0, 1, \ldots, m-1\}$ takie, że $|A(m, i)| \leqslant 1$.*

(3) *Dla każdej liczby pierwszej p istnieje $i \in \{0, 1, \ldots, p-1\}$ takie, że $|A(p, i)| \leqslant 1$.* ([Kw] 3/1987 24).

D. Równoważność (2) $\iff$ (3) wykazano w 3.6.4, a implikację (1) $\Rightarrow$ (3) w 3.6.5. Wystarczy wykazać implikację (3) $\Rightarrow$ (1). Załóżmy, że $a_1 < a_2 < \cdots < a_s$ są wszystkimi elementami zbioru A. Niech $w = a_s - a_1$ i niech Q będzie zbiorem wszystkich liczb pierwszych mniejszych od w. Dla każdej liczby pierwszej $q \in Q$ niech r_q będzie taką nieujemną liczbą całkowitą, że $|A(q, r_q)| \leqslant 1$. Niech

$$r'_q = \begin{cases} 0, & \text{gdy } r_q = 0, \\ q - r_q, & \text{gdy } r_q > 0. \end{cases}$$

Ponieważ wszystkie liczby należące do zbioru Q są parami względnie pierwsze, więc (na mocy twierdzenia chińskiego o resztach) istnieje liczba naturalna n taka, że

$$n \equiv r'_q \pmod{q} \quad \text{dla } q \in Q.$$

Wtedy liczby $a_1+n, \ldots, a_s+n$ są parami względnie pierwsze. Przypuśćmy bowiem, że $(a_i+n, a_j+n) = d > 1$ dla pewnych $i < j$. Istnieje wówczas liczba pierwsza q dzieląca d. Wtedy $q \mid (a_j+n)-(a_i+n) = a_j - a_i \leqslant a_s - a_1 = w$, a zatem $q \in Q$. Mamy wówczas

$$0 \equiv a_i + n \equiv a_i + r'_q \equiv a_i - r_q \pmod{q}, \quad 0 \equiv a_j + n \equiv a_j + r'_q \equiv a_j - r_q \pmod{q}.$$

Stą wynika, że $a_i, a_j \in A(q, r_q)$ wbrew temu, że $a_i \neq a_j$ oraz $|A(q, r_q)| \leqslant 1$. ⊠

U. Założenie o skończoności zbioru A jest tutaj istotne. Zbiór wszystkich liczb pierwszych spełnia warunek (3) i nie spełnia warunku (1). ⊠

3.6.7. *Niech $a_0, a_1, \ldots, a_s$ (gdzie $s \geqslant 1$) będą liczbami naturalnymi. Istnieje wtedy nieskończenie wiele liczb naturalnych n takich, że*

$$a_0 \mid n, \ (a_0 + a_1) \mid (a_1 + n), \ (a_0 + a_2) \mid (a_2 + n), \ \ldots, \ (a_0 + a_s) \mid (a_s + n).$$

Każda taka liczba naturalna n jest postaci $m \cdot \mathrm{nww}(a_0, a_0 + a_1, a_0 + a_2, \ldots, a_0 + a_s)$, gdzie $m \in \mathbb{N}$. ([IMO] Longlist 1968, [Djmp] 54(365)).

3.7 Istnienie lub nieistnienie pewnych liczb względnie pierwszych

3.7.1. *Dane są trzy liczby naturalne mniejsze od* 1 000 000. *Wykazać, że istnieje liczba naturalna mniejsza od* 100, *względnie pierwsza z każdą z tych liczb.* ([GaT] 3/68).

3.7.2. *Jeśli $n = 100$, to istnieje bijekcja $f : \{1, 2, \ldots, n\} \to \{n+1, n+2, \ldots, 2n\}$ taka, że $(k, f(k)) = 1$ dla $k = 1, 2, \ldots, n$.* ([Mat] 3/1967 140).

D. Definiujemy f przyjmując $f(n) = n+1$ oraz $f(k) = n+1+k$ dla $k = 1, 2, \ldots, n-1$.

Uwaga. Udowodniono, że taka bijekcja istnieje dla każdej liczby naturalnej n. Jeśli $n+1$ jest liczbą pierwszą, to funkcję f można zdefiniować dokładnie tak, jak powyżej. ⊠

3.7.3. *Dla każdej liczby naturalnej n istnieje co najmniej n^2 par (a, b) takich, że*

(1) $a, b \in \{1, 2, \ldots, 2n\}$ *oraz*

(2) $\mathrm{nwd}(a, b) = 1$. ([Kw] 5/1997 54).

3.7.4. *Niech $w(x) \in \mathbb{Z}[x]$. Jeśli istnieją dwie różne liczby całkowite a i b takie, że $\mathrm{nwd}(w(a), w(b)) = 1$, to istnieje nieskończony zbiór $A \subseteq \mathbb{Z}$ taki, że $\mathrm{nwd}(w(u), w(v)) = 1$ dla wszystkich $u, v \in A$, $u \neq v$.* ([OM] Polska 2004).

3.7.5. *Spośród 6 czerocyfrowych liczb naturalnych, których największy wspólny dzielnik jest równy 1, można wybrać 5 takich, których największy wspólny dzielnik również jest równy 1.* ([OM] Rosja 2003).

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

3.8 Liczba 24

oooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooooo

Doba ma 24 godziny. Liczba naturalna dzieli się przez 24 wtedy i tylko wtedy, gdy jej suma cyfr dzieli się przez 3 oraz liczba utworzona z trzech jej ostatnich cyfr jest podzielna przez 8. Z równości $1^2 + 2^2 + \cdots + 24^2 = 70^2$ wynika, że suma 24 początkowych liczb kwadratowych jest liczbą kwadratową. 24 to 4!. Liczba 100! ma na końcu 24 zera. $(24!)^2 + 1$ jest liczbą pierwszą. W przedziale $1, 5000]$ istnieją dokładnie 24 pary liczb pierwszych bliźniaczych. Liczba 24 ma jeszcze inne ciekawe własności. Jeśli p jest liczbą pierwszą większą od 3 to liczba $p^2 - 1$ jest podzielna przez 24.

To ostatnie zdanie można wysłowić inaczej: kwadrat każdej liczby pierwszej, względnie pierwszej z liczbą 24, przystaje do jedynki modulo 24. Zanotujmy jeszcze raz:

3.8.1. *Jeśli $p \in \mathbb{P}$ oraz $(p, 24) = 1$, to $p^2 \equiv 1 \pmod{24}$.*

Założyliśmy, że p jest liczbą pierwszą. Okazuje się, że to założenie nie jest potrzebne.

3.8.2. *Jeśli a jest liczbą całkowitą względnie pierwszą z liczbą 24, to $a^2 \equiv 1 \pmod{24}$.*

D. Niech a będzie liczbą całkowitą względnie pierwszą z liczbą 24 i niech r będzie resztą z dzielenia a przez 24. Reszta r jest oczywiście liczbą naturalną mniejszą od 24 i względnie pierwszą z 24. Liczba r jest więc jedną z liczb: $1, 5, 7, 11, 13, 17, 19, 23$. Bez trudu sprawdzamy, że kwadrat każdej z tych liczb przystaje do jedynki modulo 24. Zatem $a^2 \equiv r^2 \equiv 1 \pmod{24}$. ⊠

Istnieją również inne liczby naturalne (większe od 1) mające tę samą własność co liczba 24. Łatwo sprawdzić:

3.8.3. *Niech $m \in \{2, 3, 4, 6, 8, 12, 24\}$. Jeśli a jest liczbą całkowitą względnie pierwszą z liczbą m, to $a^2 \equiv 1 \pmod{m}$.*

Czy oprócz podanych powyżej liczb m są jeszcze inne liczby naturalne mające omawianą własność? Udowodnimy, że innych nie ma. Liczba 24 jest największą liczbą naturalną o tej własności.

W dowodzie tego faktu wykorzystamy następujący lemat, w którym przez $U(b)$ oznaczamy zbiór wszystkich liczb całkowitych względnie pierwszych z daną liczbą naturalną b.

3.8.4. *Załóżmy, że $m \geqslant 2$ jest taką liczbą naturalną, że dla każdej liczby całkowitej a, należącej do zbioru $U(m)$, zachodzi kongruencja $a^2 \equiv 1 \pmod m$. Niech $m = p_1^{\alpha_1} \cdots ps^{\alpha_s}$ będzie rozkładem kanonicznym liczby m. Wówczas dla każdej liczby pierwszej p_i (występującej w tym rozkładzie kanonicznym), każda liczba całkowita u, należąca do zbioru $U(p_i)$, spełnia kongruencję $u^2 \equiv 1 \pmod{p_i^{\alpha_i}}$.* ([Crux] 2005 s.291).

D. ([Crux] 2005 s.291). Wystarczy to udowodnić dla liczby pierwszej p_1. Niech $u \in U(p_1)$. Załóżmy, że liczba u jest podzielna przez liczby pierwsze $p_2, p_3, \ldots, p_k$ oraz nie jest podzielna przez żadną z liczb pierwszych $p_{k+1}, \ldots, p_s$. Rozpatrzmy liczbę całkowitą

$$a = u + p_1^{\alpha_1} p_{k+1} p_{k+2} \cdots p_s$$

i zauważmy (co jest oczywiste), że liczba ta jest względnie pierwsza z liczbą m. Ponieważ a należy do zbioru $U(m)$, więc $a^2 \equiv 1 \pmod m$ i tym bardziej $a^2 \equiv 1 \pmod{p_1^{\alpha_1}}$. Ale $a^2 \equiv u^2 \pmod{p_1^{\alpha_1}}$. Zatem $u^2 \equiv 1 \pmod{p_i^{\alpha_i}}$. ⊠

Teraz możemy udowodnić zapowiedziane wcześniej twierdzenie.

3.8.5. *Jeśli $m \geqslant 2$ jest taką liczbą naturalną, że dla każdej liczby całkowitej a, względnie pierwszej z m, zachodzi kongruencja $a^2 \equiv 1 \pmod m$, to m jest jedną z liczb:* 2, 3, 4, 6, 8, 12, 24. ([IMO] Shortlist 2000, [MG] 499(2000) s.96, [Crux] 2005 s.291).

D. ([Crux] 2005 s.291). Niech $m = p_1^{\alpha_1} \cdots ps^{\alpha_s}$ będzie rozkładem kanonicznym liczby m. Załóżmy najpierw, że któraś z liczb pierwszych $p_1, \ldots, p_s$, jest równa 2. Dla ustalenia uwagi niech $p_1 = 2$. Ponieważ $\operatorname{nwd}(3, 2) = 1$, więc (na mocy lematu 3.8.4) mamy kongruencję $3^2 \equiv 1 \pmod{2^{\alpha_1}}$; więc 8 jest podzielne przez 2^{α_1} i stąd $\alpha_1 \leqslant 3$. Jeśli więc w rozkładzie kanonicznym liczby m występuje liczba pierwsza 2, to może ona występować z wykładnikiem co najwyżej równym 3.

Załóżmy teraz, że wśrod liczb pierwszych $p_1, \ldots, p_s$ występuje liczba nieparzysta; niech to będzie p_i. Wtedy liczba 2 jest względnie pierwsza z p_i. Z lematu 3.8.4 wynika, że $2^2 \equiv 1 \pmod{p_i^{\alpha_i}}$. To jest możliwe tylko wtedy, gdy $p_i = 3$ oraz $\alpha_i = 1$. Wykazaliśmy, że $m = 2^i 3^j$, gdzie $0 \leqslant i \leqslant 3$ oraz $0 \leqslant j \leqslant 1$. Zatem $m \in \{2, 3, 4, 6, 8, 12, 24\}$. ⊠

Udowodniliśmy:

3.8.6. *Liczba* 24 *jest największą taką liczbą naturalną m, że dla każdej liczby całkowitej a, względnie pierwszej z m, zachodzi kongruencja $a^2 \equiv 1 \pmod m$.*

Opisaną własność liczby 24 moża równoważnie przedstawiać w trochę innych postaciach. Spójrzmy na kilka tego typu przykładów.

3.8.7. *Niech a, b będą liczbami całkowitymi względnie pierwszymi z liczbą* 24. *Wówczas*

$$a \equiv b \pmod{24} \iff ab \equiv 1 \pmod{24}.$$

Ponadto, 24 *jest największą liczbą naturalną posiadającą powyższą własność.*

D. Niech $a \equiv b \,(\mathrm{mod}\ 24)$. Wtedy (patrz 3.8.1) $ab \equiv b^2 \equiv 1 \,(\mathrm{mod}\ 24)$. Załó.zmy teraz odwrotnie, że $ab \equiv 1 \,(\mathrm{mod}\ 24)$. Ponieważ $a \overset{=}{} 1 \,(\mathrm{mod}\ 24)$, więc $a = a \cdot 1 \equiv a \cdot ab = a^2 b \equiv 1 \cdot b = b \,(\mathrm{mod}\ 24)$. Wykazaliśmy zatem równoważność $a \equiv b \,(\mathrm{mod}\ 24) \iff ab \equiv 1 \,(\mathrm{mod}\ 24)$.

Niech $m \geqslant 2$ będzie taką liczbą naturalną, że dla dowolnych liczb całkowitych a, b, względnie pierwszych z m, zachodzi równoważność $a \equiv b \,(\mathrm{mod}\ m) \iff ab \equiv 1 \,(\mathrm{mod}\ m)$. Wtedy dla każdej liczby całkowitej a, względnie pierwszej z m, mamy $a^2 \equiv 1 \,(\mathrm{mod}\ m)$, a zatem teza wynika z twierdzenia 3.8.6. ⊠

3.8.8. *Niech $a, b \in \mathbb{Z}$. Jeżeli $ab + 1$ jest podzielne przez 24, to $a + b$ również jest podzielne przez 24.* ([Mon] E2510, [OM] Słowenia 1994, [Pa97]).

D. Załóżmy, że $24 \mid ab + 1$. Wtedy $a(-b) \equiv 1 \,(\mathrm{mod}\ 24)$. Zatem, liczby a, b są względnie pierwsze z liczbą 24 oraz, na mocy 3.8.7, $a \equiv -b \,(\mathrm{mod}\ 24)$, czyli $24 \mid a + b$. ⊠

3.9 Różne fakty i zadania o liczbach względnie pierwszych

3.9.1. *Ciąg (a_n) określamy następująco:*

$$a_1 = 5,\ a_2 = 7,\ a_{n+1} = 1980 a_n + a_{n-1},\ n > 2.$$

Wykazać, że każde dwa kolejne wyrazy są względnie pierwsze. ([Dlt] 2/1980).

3.9.2. *Jeśli a i b są względnie pierwszymi liczbami naturalnymi większymi od 1, to liczba $a/b + b/a$ nie jest całkowita.*

3.9.3. *Niech $a, b, k \in \mathbb{N}$, $(a, b) = 1$, $k \geqslant 2$. Załóżmy, że $ab \mid a^k + b^k + 1$. Wtedy:*

(1) $a \mid b^k + 1$; *oznaczmy* $c = (b^k + 1)/a$;

(2) $bc \mid b^k + c^k + 1$;

(3) $(b, c) = 1$. ([Crux] 1997 s.124).

3.9.4. *Na końcach danego odcinka wpisano dwie jedynki. W środku wpisano ich sumę; liczbę 2. W następnych krokach pomiędzy każdymi liczbami wpisano ich sumę. Ile razy pojawi się liczba 1973?* Odp. 1972 *razy.* ([Kw] 7/1974 39).

3.9.5 (Ernesto Cesaro)**.** *Prawdopodobieństwo tego, że dwie losowo wybrane liczby całkowite są względnie pierwsze wynosi $6/\pi^2 \approx 0,608$.* ([Ca04]).

3.9.6. *Danych jest 15 liczb naturalnych mniejszych od 1998, z których każde dwie są względnie pierwsze. Wykazać, że wśród tych liczb jest co najmniej jedna liczba pierwsza.* ([OM] Brazylia 1998).

3.9.7. *Niech $a_1 = 1$, $a_2 = 2$ i niech a_{n+1} będzie najmniejszą liczbą naturalną taką, że $a_{n+1} \notin \{a_1, \ldots, a_n\}$ i $\mathrm{nwd}(a_n, a_{n+1}) > 1$. (Początkowe wyrazy: $1, 2, 4, 6, 3, 9, 12, 8, 10, 5$). Wykazać, że każda liczba naturalna występuje w ciągu (a_n).* ([TTsa] 2002).

3.9.8. *Niech $A \subseteq \mathbb{N}$. Mówić będziemy, że podzbiór A jest* konspiracyjny*, jeśli żadne trzy jego elementy nie są parami względnie pierwsze. Znaleźć maksymalnej długości konspiracyjny podzbiór zbioru $\{1, 2, 3, \ldots, 16\}$.* Odp. $A = \{2, 3, 4, 6, 8, 9, 10, 12, 14, 15, 16\}$, *długość* $= 11$. ([Putn] 1980).

Literatura

[B-zm] V. I. Bernik, I. K. Żuk, O. W. Melnikow, *Zbiór Zadań Olimpijskich z Matematyki* (po rosyjsku), Narodnaja Aswieta, Minsk, 1980.

[Bedn] W. Bednarek, *Zbiór Zadań dla Uczniów Lubiących Matematykę*, Gdańskie Wydawnictwo Oświatowe, Gdańsk, 1995.

[Berk] V. I. Bernik, *Byelorussian Mathematical Olympiads*, 1992-1993, Minsk, 1993.

[Ca02] Ch. K. Caldwell, *Goldbach's proof of the infinitude of primes*, 1996, `http://www.utm.edu/research/primes/goldbach.html`.

[Ca04] Ch. K. Caldwell, *What is the probability that gcd(n,m)=1?*, 1996, `http://www.utm.edu/research/primes`.

[Crux] Crux Mathematicorum, Canadian Mathematical Society, popolarne matematyczne czasopismo kanadyjskie.

[Djmp] D. Djukić, V. Janković, I. Matić, N. Petrović, *The IMO Compendium. A Collection of Problems Suggested for the International Mathematical Olympiads: 1959-2004*, Problem Books in Mathematics, Springer, 2006.

[Dlt] Delta, popularny polski miesięcznik matematyczno-fizyczno-astronomiczny.

[DoC] S. Doduniekow, K. Czakyrjan, *Zadania z Teorii Liczb* (po rosyjsku), Narodna Poswieta, Sofia, 1985.

[GaT] G. A. Galpierin, A. K. Tołpygo, *Moskiewskie Olimpiady Matematyczne* (po rosyjsku), 1935-1985, Moskwa, 1986.

[Grif] H. Griffin, *Elementary Theory of Numbers*, McGraw-Hill Book Company, Inc., New York, Toronto, London, 1954.

[Ibe] Iberoamerican Mathematical Olympiad.

[IMO] Międzynarodowa Olimpiada Matematyczna.

[Kw] Kwant, popularne czasopismo rosyjskie.

[Mat] Matematyka, polskie czasopismo dla nauczycieli.

[Maza] W. Marzantowicz, P. Zarzycki, *Elementarna Teoria Liczb*, Wydawnictwo Naukowe PWN, Warszawa, 2006.

[MG] The Mathematical Gazette, angielskie popularne czasopismo matematyczne.

[MOc] Mathematical Olympiads' Correspondence Program, Canada, 1997-2012.

[Mon] The American Mathematical Monthly, Mathematical Association of America.

[OM] Olimpiada Matematyczna.

[Pa97] H. Pawłowski, *Zadania z Olimpiad Matematycznych z Całego Świata*, Tutor, Toruń, 1997.

[Putn] Putnam (William Lowell) Mathematical Competition.

[Ri97] P. Ribenboim, *Mała Księga Wielkich Liczb Pierwszych*, WNT, Warszawa, 1997.

[S50] W. Sierpiński, *Teoria Liczb*, Warszawa - Wrocław, 1950.

[S59] W. Sierpiński, *Teoria Liczb* II, PWN, Warszawa, 1959.

[S64] W. Sierpiński, *200 Zadań z Elementarnej Teorii Liczb*, Biblioteczka Matematyczna 17, PZWS, Warszawa, 1964.

[S65] W. Sierpiński, *Wstęp do Teorii Liczb*, (wydanie 2), Biblioteczka Matematyczna 25, PZWS, Warszawa, 1965.

[S68] W. Sierpiński, *Arytmetyka Teoretyczna*, (wydanie 4), Biblioteka Matematyczna 7, PWN, Warszawa, 1968.

[S88] W. Sierpiński, *Elementary Theory of Numbers*, Editor: A. Schinzel, North-Holland Mathematical Library, Vol. 31, 1988.

[San2] D. A. Santos, *Elementary Number Theory Notes*, Preprint, Internet 2002.

[TTsa] Tournament of the Towns, Senior, Autumn.

[WaG] N. B. Wasilev, W. L. Gutenmacher, Z. M. Rabbot, A. L. Toom, *Zaoczne Matematyczne Olimpiady* (po rosyjsku), Moskwa, Nauka, 1987.

[WaJ] N. B. Wasilev, A. A. Jegorow, *Zadania Olimpiad Matematycznych Związku Radzieckiego* (po rosyjsku), 1961-1987, Moskwa, Nauka, 1988.

[Wm] Wiadomości Matematyczne, Roczniki Polskiego Towarzystwa Matematycznego, 1956-2012.