Przemysław Pawełczyk

Twierdzenia matematyczne

Spis treści

1. Oznaczenia

Oznaczenie	Znaczenie
$\mathbb{R}_{0+}$	$\mathbb{R} \setminus \mathbb{R}_{-}$
$\mathbb{P}$	zbiór liczb pierwszych
$\Theta(n)$	liczba dzielników n
$\varphi(n)$	liczba dzielników mniejszych od n i względnie pierwszych z n
$\sigma(n)$	suma dzielników n
$[x]$	część całkowita liczby x
$a \equiv b \pmod d$[a]	$d \mid a - b$
$\sum x_{i_1} \ldots x_{i_k}$[b]	$\sum\limits_{1 \leqslant i_1 < \ldots < i_k \leqslant n} x_{i_1} \ldots x_{i_k}$
$a_n{}^{\nearrow}$	$a_1 < a_2 < \ldots < a_n$
$a_n{}^{\not\searrow}$	$a_1 \leqslant a_2 \leqslant \ldots \leqslant a_n$
$a_n{}^{\searrow}$	$a_1 > a_2 > \ldots > a_n$
$a_n{}^{\not\nearrow}$	$a_1 \geqslant a_2 \geqslant \ldots \geqslant a_n$
$a_n{}^{\rightarrow}$	$a_1 = a_2 = \ldots = a_n$
$a \perp p$	$\mathrm{NWD}(a, p) = 1$
$f^{(n)}(x)$	n-ta pochodna funkcji $f(x)$
$\left(\frac{a}{p}\right)$[c]	$= \begin{cases} -1 & \bigvee\limits_{m \in \mathbb{N}} m^2 \equiv a \pmod p \\ 1 & \bigwedge\limits_{m \in \mathbb{N}} m^2 \not\equiv a \pmod p \end{cases}$
$(a_1, a_2, \ldots, a_n) \succ (b_1, b_2, \ldots, b_n)$[d]	$\begin{cases} a_i, b_i \in \mathbb{R}, \\ a_n{}^{\not\nearrow},\ b_n{}^{\not\nearrow}, \\ \bigwedge\limits_{i \in \{1, \ldots, n-1\}} \sum\limits_{k=1}^{i} a_k \geqslant \sum\limits_{k=1}^{i} b_k, \\ \sum\limits_{k=1}^{n} a_k = \sum\limits_{k=1}^{n} b_k \end{cases}$

[a] Jest to tzw. *kongruencja*. Mówimy, że a *przystaje* do b *modulo* d.
[b] Jest to tzw. k-ty elementarny wielomian symetryczny n zmiennych (zwany też k-tą *formą symetryczną*).
[c] Jest to tzw. *symbol Legendre'a*.
[d] Mówimy, że ciąg/wektor $(a_1, a_2, \ldots, a_n)$ *majoryzuje* ciąg/wektor $(b_1, b_2, \ldots, b_n)$.

2. Nierówności funkcyjne

2.1. Nierówność Jensena

$f\colon X \to \mathbb{R},\ x_i \in X,\ p_i \in \mathbb{R}_{0+},\ \sum_{i=1}^{n} p_i = 1$

$$f(\sum_{i=1}^{n} p_i x_i) \leqslant \sum_{i=1}^{n} p_i f(x_i) \qquad f \text{ - wypukła}$$

$$f(\sum_{i=1}^{n} p_i x_i) \geqslant \sum_{i=1}^{n} p_i f(x_i) \qquad f \text{ - wklęsła}$$

Dowód: [5] str. 90

2.2. Uogólniona nierówność Jensena

$f\colon \mathbb{R}^d \to \mathbb{R},\ X_i \in \mathbb{R}^d,\ p_i \in \mathbb{R}_{0+},\ \sum_{i=1}^{n} p_i = 1$

$$f(\sum_{i=1}^{n} p_i X_i) \leqslant \sum_{i=1}^{n} p_i f(X_i) \qquad f \text{ - wypukła}$$

$$f(\sum_{i=1}^{n} p_i X_i) \geqslant \sum_{i=1}^{n} p_i f(X_i) \qquad f \text{ - wklęsła}$$

Dowód: [5] str. 101

2.3. Nierówność Hardy'ego-Littlewooda-Pólya'i

$f\colon \mathbb{R} \to \mathbb{R}$ wypukła, $(a_1, a_2, \ldots, a_n) \succ (b_1, b_2, \ldots, b_n)$

$$\sum_{i=1}^{n} f(a_i) \geqslant \sum_{i=1}^{n} f(b_i)$$

Dowód: [6] rozdział 2.24, twierdzenia 1 i 2

3. Nierówności klasyczne

3.1. Nierówność Bernoulliego

$n, x \in \mathbb{R},\ x > -1,\ x \neq 0,\ n \neq 0,\ n \neq 1$

$$(1+x)^n < 1 + nx \qquad n \in (0,1)$$

$$(1+x)^n > 1 + nx \qquad n \in (-\infty, 0) \cup (1, +\infty)$$

Dowód: z nierówności Jensena ($f(x) = -\ln x$, $x_1 = 1 + xn$, $x_2 = 1$, $p_1 = \frac{1}{n}$, $p_2 = 1 - \frac{1}{n}$)

3.2. Nierówność Cauchy'ego

$a_i \in \mathbb{R}_{0+}$

$$\sum_{i=1}^{n} \frac{a_i}{n} \geqslant \sqrt[n]{\prod_{i=1}^{n} a_i}$$

$= \quad \Leftrightarrow \quad a_n{}^{\rightarrow}$

Dowód: z nierówności Jensena ($f(x) = e^x$, $x_i = \ln a_i$, $p_i = \frac{1}{n}$)

3.3. Nierówność Cauchy'ego-Schwarza

$a_i, b_i \in \mathbb{R}$

$$\sum_{i=1}^{n} a_i b_i \leqslant \sqrt{\sum_{i=1}^{n} a_i^2} \sqrt{\sum_{i=1}^{n} b_i^2}$$

$= \quad \Leftrightarrow \quad \bigvee_{t\in\mathbb{R}} \bigwedge_{i\in\{1,\ldots,n\}} a_i = tb_i$

Dowód: z nierówności Jensena ($f(x) = x^2$, $x_i = \frac{a_i}{b_i}$, $p_i = \frac{b_i^2}{\sum\limits_{k=1}^{n} b_k^2}$)

3.4. Nierówności Czebyszewa

$a_i, b_i \in \mathbb{R}$

$$\left(\sum_{i=1}^{n} \frac{a_i}{n}\right)\left(\sum_{i=1}^{n} \frac{b_i}{n}\right) \leqslant \sum_{i=1}^{n} \frac{a_i b_i}{n} \qquad a_n{}^{\searrow} \wedge b_n{}^{\searrow} \ \vee \ a_n{}^{\nearrow} \wedge b_n{}^{\nearrow}$$

$$\left(\sum_{i=1}^{n} \frac{a_i}{n}\right)\left(\sum_{i=1}^{n} \frac{b_i}{n}\right) \geqslant \sum_{i=1}^{n} \frac{a_i b_i}{n} \qquad a_n{}^{\searrow} \wedge b_n{}^{\nearrow} \ \vee \ a_n{}^{\nearrow} \wedge b_n{}^{\searrow}$$

$= \quad \Leftrightarrow \quad a_n{}^{\rightarrow} \vee b_n{}^{\rightarrow}$

3.5. Uogólnione nierówności Czebyszewa

$a_i, b_i \in \mathbb{R}_+,\ k \in \mathbb{N}$

$$\sqrt[k]{\sum_{i=1}^{n} \frac{a_i^k}{n}} \sqrt[k]{\sum_{i=1}^{n} \frac{b_i^k}{n}} \leqslant \sqrt[k]{\sum_{i=1}^{n} \frac{(a_i b_i)^k}{n}} \qquad a_n{}^{\searrow} \wedge b_n{}^{\searrow} \ \vee \ a_n{}^{\nearrow} \wedge b_n{}^{\nearrow}$$

$$\sqrt[k]{\sum_{i=1}^{n} \frac{a_i^k}{n}} \sqrt[k]{\sum_{i=1}^{n} \frac{b_i^k}{n}} \geqslant \sqrt[k]{\sum_{i=1}^{n} \frac{(a_i b_i)^k}{n}} \qquad a_n{}^{\searrow} \wedge b_n{}^{\nearrow} \ \vee \ a_n{}^{\nearrow} \wedge b_n{}^{\searrow}$$

$= \quad \Leftrightarrow \quad a_n{}^{\rightarrow} \vee b_n{}^{\rightarrow}$

3.6. Nierówność Höldera

$a_i, b_i \in \mathbb{R}_+,\ p, q > 1,\ \frac{1}{p} + \frac{1}{q} = 1$

$$\sum_{i=1}^{n} a_i b_i \leqslant \sqrt[p]{\sum_{i=1}^{n} a_i^p} \cdot \sqrt[q]{\sum_{i=1}^{n} b_i^q}$$

Dowód: z nierówności Jensena ($f(x) = x^p$, $x_i = a_i b_i^{1-q}$, $p_i = \frac{b_i^q}{\sum\limits_{k=1}^{n} b_k^q}$)

3.7. Nierówność Maclaurina

$x_i \in \mathbb{R}_{0+}$

$$m_k(x_1, \ldots, x_n) = \sqrt[k]{\binom{n}{k}^{-1} \sum x_{i_1} \ldots x_{i_k}}$$

$$m_1(x_1, \ldots, x_n) \geqslant m_2(x_1, \ldots, x_n) \geqslant \ldots \geqslant m_n(x_1, \ldots, x_n)$$

$= \quad \Leftrightarrow \quad a_n{}^{\rightarrow}$

Dowód: [5] str. 97

3.8. Nierówność Minkowskiego

$a_i, b_i \in \mathbb{R}_+,\ k \in \mathbb{N} \setminus \{1\}$

$$\sqrt[k]{\sum_{i=1}^{n}(a_i+b_i)^k} \leqslant \sqrt[k]{\sum_{i=1}^{n} a_i^k} + \sqrt[k]{\sum_{i=1}^{n} b_i^k}$$

Dowód: z nierówności Jensena ($f(x) = \ln(1+e^x)$, $x_i = \ln \frac{a_i}{b_i}$, $p_i =?$)

3.9. Nierówność Radona

$a_i, b_i, p \in \mathbb{R}_+$

$$\sum_{i=1}^{n} \frac{a_i^{p+1}}{b_i^p} \geqslant \frac{\left(\sum_{i=1}^{n} a_i\right)^{p+1}}{\left(\sum_{i=1}^{n} b_i\right)^{p}}$$

4. Tożsamości dla ciągów

4.1. Tożsamość Abela

$a_i, b_i \in \mathbb{R}$

$$\sum_{i=1}^{n} a_i b_i = \sum_{i=1}^{n-1}\left((a_i - a_{i+1})\sum_{k=1}^{i} b_k\right) + a_n \sum_{i=1}^{n} b_i$$

4.2. Tożsamość Czebyszewa

$a_i, b_i \in \mathbb{R}$

$$\left(\sum_{i=1}^{n} a_i\right)\left(\sum_{i=1}^{n} b_i\right) = n\sum_{i=1}^{n-1} a_i b_i - \sum_{1\leqslant i<j\leqslant n}(a_i - a_j)(b_i - b_j)$$

4.3. Tożsamość Lagrange'a

$a_i, b_i \in \mathbb{R}$

$$\left(\sum_{i=1}^{n-1} a_i b_i\right)^2 = \left(\sum_{i=1}^{n} a_i^2\right)\left(\sum_{i=1}^{n} b_i^2\right) - \sum_{1\leqslant i<j\leqslant n}(a_i b_j - a_j b_j)^2$$

5. Tożsamości teorioliczbowe

5.1. Tożsamość Hermite'a

$m \in \mathbb{N},\ x \in \mathbb{R}$

$$\sum_{k=1}^{m-1}\left[x + \frac{k}{m}\right] = [mx]$$

Dowód: [9] str. 134

5.2. Wzór Dirichleta

$x \in \mathbb{R}_+ \setminus (0,1)$

$$\sum_{i=1}^{[x]} \Theta(i) = 2\sum_{n=1}^{[\sqrt{x}]}\left[\frac{x}{n}\right] - \left[\sqrt{x}\right]^2$$

Dowód: [9] str. 126

5.3. Wzór sumacyjny na sumę dzielników liczby naturalnej

$x \in \mathbb{R}_+ \setminus (0,1)$

$$\sum_{i=1}^{[x]} \sigma(i) = \frac{1}{2}\left(\sum_{n=1}^{[\sqrt{x}]} \left[\frac{x}{n}\right]\left(\left[\frac{x}{n}\right] + 2n + 1\right) - \left[\sqrt{x}\right]^2\left(\left[\sqrt{x}\right] + 1\right)\right)$$

6. Twierdzenia dotyczące ciągów i funkcji

6.1. Twierdzenie (o dzieleniu z resztą)

Dla dowolnych wielomianów $P(x)$ i $W(x)$, gdzie $W(x) \neq 0$, istnieje dokładnie jedna para wielomianów $Q(x)$ i $R(x)$ takich, że

$$P(x) \equiv Q(x)W(x) + R(x) \qquad \wedge \qquad \operatorname{st} R(x) < \operatorname{st} W(x) \ \vee \ \operatorname{st} R(x) \equiv 0$$

6.2. Twierdzenie (o krotności pierwiastka)

Liczba a jest n-krotnym pierwiastkiem wielomianu $P(x)$ wtedy i tylko wtedy gdy

$$\bigwedge_{k \in \{0,1,\ldots,n-1\}} P^{(k)}(a) = 0 \qquad \wedge \qquad P^{(n)}(a) \neq 0$$

Dowód: [8] str. 149

6.3. Twierdzenie Bèzouta

Reszta z dzielenia wielomianu $P(x)$ przez dwumian $x - a$ wynosi $P(a)$.

6.4. Kryterium Eisensteina nierozkładalności wielomianów

Jeżeli współczynniki wielomianu

$$P(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$$

są całkowite i jeżeli istnieje taka liczba pierwsza p, że współczynniki $a_0, a_1, \ldots, a_{n-1}$ są podzielne przez p, a_n nie jest podzielne przez p oraz a_0 nie jest podzielne przez p^2, to wielomian $P(x)$ jest nierozkładalny w zbiorze liczb wymiernych.

6.5. Wzory Viète'a

Liczby $x_1, x_2, \ldots, x_n$ są pierwiastkami wielomianu $a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ (gdzie $a_n \neq 0$), wtedy i tylko wtedy, gdy spełnione są równości:

$$\begin{array}{rcr} \sum_{i=1}^{n} x_i & = & -\frac{a_{n-1}}{a_n} \\ \sum x_i x_j & = & \frac{a_{n-2}}{a_n} \\ & \vdots & \\ \sum x_{i_1} x_{i_2} \ldots x_{i_k} & = & (-1)^k \cdot \frac{a_{n-k}}{a_n} \\ & \vdots & \\ \prod_{i=1}^{n} x_i & = & (-1)^n \cdot \frac{a_0}{a_n} \end{array}$$

6.6. Zadadnicze twierdzenie algebry

Każdy wielomian dodatniego stopnia ma pierwiastek zespolony.

6.7. Twierdzenie Stolza

Jeżeli $x_n \to \infty$, $y_n \to +\infty$ i $\bigvee_{N} \bigwedge_{n>N} y_{n+1} > y_n$ to

$$\lim_{n\to\infty} \frac{x_n}{y_n} = \lim_{n\to\infty} \frac{x_n - x_{n-1}}{y_n - y_{n-1}}$$

o ile istnieje granica po prawej stronie (skończona lub nieskończona).

Dowód: [2] str. 55

6.8. Twierdzenie Bolzano-Cauchy'ego

Jeżeli funkcja $f\colon [a,b] \to \mathbb{R}$ jest ciągła oraz $f(a) \cdot f(b) < 0$, to

$$\bigvee_{c\in(a,b)} f(c) = 0$$

Dowód: [2] str. 142

6.9. Twierdzenie Cantora

Jeżeli funkcja $f\colon [a,b] \to \mathbb{R}$ jest ciągła, to jest również jednostajnie ciągła w $[a,b]$.

Dowód: [2] str. 152

6.10. Twierdzenie Weierstrassa

Jeżeli funkcja $f\colon [a,b] \to \mathbb{R}$ jest ciągła, to jest ograniczona na przedziale $[a,b]$ oraz

$$\bigvee_{x_1,x_2\in[a,b]} f(x_1) = \inf\{f(x); x \in [a,b]\} \ \wedge \ f(x_2) = \sup\{f(x); x \in [a,b]\}$$

Dowód: [2] str. 148-149

6.11. Twierdzenie Fermata

Jeżeli funkcja $f\colon X \to \mathbb{R}$, gdzie $X \subset \mathbb{R}$ jest przedziałem, osiąga w pewnym punkcie wewnętrznym x_0 tego przedziału wartość największą lub wartość najmniejszą oraz istnieje $f'(x_0)$, to

$$f'(x_0) = 0$$

Dowód: [2] str. 193

6.12. Twierdzenie Darboux I

Jeżeli funkcja $f\colon [a,b] \to \mathbb{R}$ jest ciągła oraz $f(a) \neq f(b)$, to

$$\bigwedge_{y\in(f(a),f(b))} \bigvee_{c\in(a,b)} f(c) = y$$

6.13. Twierdzenie Darboux II

Jeżeli funkcja $f\colon [a,b] \to \mathbb{R}$ jest różniczkowalna oraz $f'(a) \neq f'(b)$, to

$$\bigwedge_{y\in(f'(a),f'(b))} \bigvee_{c\in(a,b)} f'(c) = y$$

Dowód: [2] str. 194

6.14. Twierdzenie Rolle'a

Jeżeli funkcja $f\colon [a,b] \to \mathbb{R}$ jest ciągła oraz różniczkowalna (co najmniej w przedziale otwartym (a,b)) i $f(a) = f(b)$, to

$$\bigvee_{c\in(a,b)} f'(c) = 0$$

Dowód: [2] str. 195

6.15. Twierdzenie Lagrange'a (twierdzenie o wartości średniej)

Jeżeli funkcja $f\colon [a,b] \to \mathbb{R}$ jest ciągła oraz różniczkowalna (co najmniej w przedziale otwartym (a,b)), to

$$\bigvee_{c\in(a,b)} f'(c) = \frac{f(b)-f(a)}{b-a}$$

Dowód: [2] str. 196

6.16. Twierdzenie Cauchy'ego (uogólnione twierdzenie o wartości średniej)

Jeżeli funkcje $f\colon [a,b] \to \mathbb{R}$, $g\colon [a,b] \to \mathbb{R}$ są ciągłe oraz różniczkowalne (co najmniej w przedziale otwartym (a,b)) i $g'(x) \neq 0$ w przedziale (a,b), to

$$\bigvee_{c\in(a,b)} \frac{f'(c)}{g'(c)} = \frac{f(b)-f(a)}{g(b)-g(a)}$$

Dowód: [2] str. 199

7. Twierdzenia geometryczne

7.1. Czwarta cecha przystawania trójkątów

Jeżeli dwa boki jednego trójkąta są odpowiednio równe dwóm bokom drugiego trójkąta i jeżeli kąty trójkątów leżące naprzeciw większych z owych boków są równe, to trójkąty są przystające.

Dowód: [10] str. 30

7.2. Twierdzenia Carnota

1. Jeżeli prosta przecina boki $A_1A_2, A_2A_3, \ldots, A_nA_1$ wielokąta płaskiego $A_1A_2\ldots A_n$ lub ich przedłużenia odpowiednio w punktach $M_1, M_2, \ldots, M_n$, to:
2. Jeżeli płaszczyzna przecina boki $A_1A_2, A_2A_3, \ldots, A_nA_1$ wieloboku przestrzennego $A_1A_2\ldots A_n$ lub ich przedłużenia odpowiednio w punktach $M_1, M_2, \ldots, M_n$, to:

$$\frac{A_1M_1}{M_1A_2}\cdot\frac{A_2M_2}{M_2A_3}\cdot\ldots\cdot\frac{A_nM_n}{M_nA_1} = 1$$

7.3. Twierdzenie Cevy

Jeżeli proste AS, BS, CS przecinają odpowiednio boki BC, CA, AB trójkąta ABC lub ich przedłużenia w punktach N, P, M, przy czym punkt S nie leży na żadnej z prostych AB, BC, CA, to

$$\frac{AM}{MB}\cdot\frac{BN}{NC}\cdot\frac{CP}{PA} = 1$$

7.4. Twierdzenie Cevy - wersja trygonometryczna

Jeżeli proste AS, BS, CS przecinają odpowiednio boki BC, CA, AB trójkąta ABC lub ich przedłużenia w punktach M, N, P, przy czym punkt S nie leży na żadnej z prostych AB, BC, CA, to

$$\frac{\sin\measuredangle MAB}{\sin\measuredangle CAM} \cdot \frac{\sin\measuredangle NBC}{\sin\measuredangle ABC} \cdot \frac{\sin\measuredangle PCA}{\sin\measuredangle BCP} = 1$$

7.5. Twierdzenie Cramera

Spośród wszystkich wielokątów o danych bokach $a_1, a_2, \ldots, a_n$ (gdzie $n \geqslant 3$) największe pole ma wielokąt wpisany w koło.

7.6. Twierdzenie Eulera (o wielościanie)

Jeżeli wielościan jest wypukły, lub można go w sposób ciągły przekształcić na wypukły, to

$$w + s = k + 2$$

gdzie w to liczba wierzchołków wielościanu, s - liczba ścian, k - liczba krawędzi.

Dowód: [12] str. 338

7.7. Uogólnione twierdzenie Eulera (o n-wymiarowym wielościanie) Schläfliego

Jeżeli przez N_k oznaczymy liczbę komórek k-wymiarowych w n-wymiarowym wielościanie ($k < n$) to:

$$\sum_{i=0}^{n-1} (-1)^i N_i = 1 - (-1)^n$$

7.8. Twierdzenie Helly'ego

Jeżeli na płaszczyźnie dana jest pewna niepusta rodzina zbiorów wypukłych taka, że każde trzy zbiory tej rodziny mają punkt wspólny, to istnieje punkt należący do wszystkich zbiorów tej rodziny.

Dowód: [4] str. 131

7.9. Twierdzenie Helly'ego-Radona

Jeżeli figury wypukłe $F_1, F_2, \ldots, F_n$ ($n \geqslant k + 1$) są położone w przestrzeni k-wymiarowej w taki sposób, że każde $k + 1$ z nich mają (co najmiej jeden) punkt wspólny, to wszystkie figury mają (co najmniej jeden) punkt wspólny.

7.10. Twierdzenie Newtona

W czworokącie opisanym na kole odcinki łączące punkty styczności boków przeciwległych z kołem przechodzą przez punkt przecięcia przekątnych czworokąta.

Dowód: [10] str. 94

7.11. Twierdzenia Simsona

Czworokąt wypukły $ABCD$ można wpisać w okrąg wtedy i tylko wtedy, gdy rzuty prostokątne wierzchołka D na proste AB, BC, CA leżą na jednej prostej.

7.12. Twierdzenia Stewarta

Jeżeli punkt D należy do boku AB trójkąta ABC, to

$$\frac{CD}{AD} \cdot \frac{CD}{BD} = \frac{AC}{AB} \cdot \frac{AC}{AD} + \frac{BC}{AB} \cdot \frac{BC}{BD} - 1$$

7.13. Twierdzenia Van Aubela

Jeżeli proste AS, BS, CS przecinają odpowiednio boki BC, CA, AB trójkąta ABC lub ich przedłużenia w punktach P, Q, R, przy czym punkt S nie leży na żadnej z prostych AB, BC, CA, to

$$\frac{AS}{SP} = \frac{AR}{RB} + \frac{AQ}{QC}$$

8. Twierdzenia teorioliczbowe

8.1. Twierdzenie (zależność między NWD a NWW)

Jeżeli $a, b \in \mathbb{N}$ to

$$a \cdot b = \mathrm{NWD}(a, b) \cdot \mathrm{NWW}(a, b)$$

Dowód: [9] str. 4

8.2. Zasadnicze twierdzenie arytmetyki

Liczba dzieląca iloczyn dwóch liczb i pierwsza względem jednego z czynników jest dzielnikiem drugiego czynnika.
Dowód: [9] str. 6

8.3. Twierdzenie (o przedstawieniu liczby w postaci iloczynu liczb pierwszych)

Każda liczba całkowita $n > 1$, która nie jest liczbą pierwszą, daje się przedstawić jako iloczyn samych tylko czynników pierwszych i to tylko w jeden sposób.
Dowód: [9] str. 8

8.4. Twierdzenie (o istnieniu formy liniowej dla NWD)

$$\bigwedge_{\substack{a,b \in \mathbb{Z} \\ a \neq 0 \vee b \neq 0}} \bigvee_{\xi, \eta \in \mathbb{Z}} \mathrm{NWD}(a, b) = a\xi + b\eta$$

Dowód: [9] str. 27

8.5. Twierdzenie (o implikacji kongruencji)

Jeśli $P(x)$ jest wielomianem całkowitym o współczynnikach całkowitych oraz zachodzi kongruencja $a \equiv b \pmod{m}$ to implikuje ona kongruencję

$$P(a) \equiv P(b) \pmod{m}$$

Dowód: [9] str. 47

8.6. Twierdzenie (o liczbie dzielników)

Jeżeli n przedstawimy jako $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ gdzie $p_i \in \mathbb{P}$, a $\alpha_i \in \mathbb{N}_0$ to

$$\Theta(n) = \prod_{i=1}^{k} (\alpha_i + 1)$$

Dowód: [9] str. 113

8.7. Twierdzenie (o sumie dzielników)

Jeżeli n przedstawimy jako $p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ gdzie $p_i \in \mathbb{P}$, a $\alpha_i \in \mathbb{N}_0$ to

$$\sigma(n) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}$$

Dowód: [9] str. 115

8.8. Twierdzenie (o liczbie dzielników względnie pierwszych z n)

Jeżeli $n > 1$ jest liczbą naturalną oraz $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ jest jej przedstawieniem w postaci iloczynu różnych potęg liczb pierwszych, to

$$\varphi(n) = n \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right)$$

8.9. Twierdzenie Eulera I

Jeżeli $a \in \mathbb{Z}, p \in \mathbb{P}$ i $p \nmid a$ to

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$$

8.10. Twierdzenie Eulera II

Jeżeli $a, n \in \mathbb{N}$ i $a \perp n$ to

$$n \mid a^{\varphi(n)} - 1$$

8.11. Małe twierdzenie Fermata

Jeżeli $a \in \mathbb{Z}, p \in \mathbb{P}$ i $p \nmid a$ to

$$a^{p-1} \equiv 1 \pmod{p}$$

8.12. Twierdzenie Lagrange'a

Liczba pierwsza p występuje w rozkładzie liczby $n!$ na czynniki pierwsze w potędze o wykładniku

$$\alpha = \sum_{i=1}^{m} \left[\frac{n}{p^i}\right] \qquad\qquad p^m \leqslant n < p^{m+1}$$

Dowód: [5] str. 35

8.13. Twierdzenie Leibniza

Na to, by liczba $p > 1$ była pierwsza, potrzeba i wystarcza, żeby zachodziła kongruencja

$$(p-2)! \equiv 1 \pmod{p}$$

8.14. Twierdzenie Wilsona

Jeżeli $p \in \mathbb{P}$, to

$$p \nmid (p-1)! + 1$$

Dowód: [9] str. 57

8.15. Uogólnienie twierdzeń Leibniza i Wilsona

Na to, by liczba całkowita $p > 1$ była pierwsza, potrzeba i wystarcza, żeby

$$\bigwedge_{n \in \{0,1,\ldots,p-1\}} (p-1-n)!\, n! + (-1)^n \equiv 0 \pmod p$$

Literatura

[1] J. Browkin, J. Rempała, S. Straszewicz, *25 lat olimpiady matematycznej*, WSiP, Warszawa 1975
[2] G. M. Fichtenholz, *Rachunek różniczkowy i całkowy*, Tom I, PWN, Warszawa 1976
[3] J. Górnicki, *Okruchy matematyki*, PWN, Warszawa 1995
[4] I. M. Jagłom, W. G. Boltański, *Figury wypukłe*, PWN, 1955
[5] M. E. Kuczma, *Olimpiady matematyczne*, Tom VIII, WSiP, Warszawa 2000
[6] D. S. Mintrović, *Analytic inequalities*, Berlin-Heidelberg-New York, 1970
[7] H. Pawłowski, *Kółko matematyczne dla olimpijczyków*, Turpress, Toruń 1994
[8] H. Pawłowski, *Zadania z olimpiad matematycznych z całego świata*, Tutor, Toruń 1997
[9] W. Sierpiński, *Teoria Liczb*, PWN, Warszawa-Wrocław 1950
[10] Sprawozdanie Komitetu Głównego, *V Olimpiada Matematyczna*, Olimpiada Matematyczna, Warszawa 1955
[11] Sprawozdanie Komitetu Głównego, *LII Olimpiada Matematyczna*, Olimpiada Matematyczna, Warszawa 2002
[12] J. Zydler, *Geometria*, Prószyński i S-ka, Warszawa 1997