Algebra i Teoria Liczb

Autor:
Hai An Mai

W tej książce przedstawię Wam najważniejsze i mniej ważne twierdzenia, lematy, własności, tożsamości, które są związane z Algebrą, a także z Teorią Liczb.

1 Podstawowe własności

Twierdzenie 1.1. *NWD (+ trochę NWW)*

- (a, b) - $NWD(a, b)$, $[a, b]$ - $NWW(a, b)$
- $(a, b)[a, b] = ab$
- $((a, b), c) = (a, b, c) = (a, (b, c))$, $[[a, b], c] = [a, b, c] = [a, [b, c]]$
- *Algorytm Euklidesa:* $(a, b) = (|a - b|, b) = (a, |a - b|)$
- *Wniosek 1:* $\forall a, b \in \mathbb{Z}\ \exists x, y \in \mathbb{Z}\ ax + by = (a, b)$
- *Wniosek 2:* $a, m, n \in \mathbb{Z}$, $a > 1$ $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$

Definicja 1.2. *Wykładniki p-adyczne.*
*Jeżeli $p \in \mathbb{P}$ i $a \neq 0$ - całkowite to symbol $v_p(a)$ oznacza największą liczbę całkowitą k, dla której $p^k|a$. Nazywamy tą liczbą **wykładnikiem** p-**adycznym** a.*
Definicję możemy rozszerzyć na liczby wymierne:

$$v_p(\frac{a}{b}) = v_p(a) - v_p(b)$$

Kilka własności:

- $v_p(ab) = v_p(a) + v_p(b)$
- $a|b \Leftrightarrow v_p(a) \leqslant v_p(b)$
- $v_p((a, b)) = min\{v_p(a), v_p(b)\}$, $v_p([a, b]) = max\{v_p(a), v_p(b)\}$
- $v_p(a + b) \geqslant min\{v_p(a), v_p(b)\}$ *(przy czym, gdy $v_p(a) \neq v_p(b)$ to zachodzi równość)*

Twierdzenie 1.3. *Twierdzenie Legendre'a.*

$$v_p(n!) = \sum_{i=1}^{k} = \lfloor \frac{n}{p^i} \rfloor$$

gdzie k to taka liczba całkowita, że $p^k \leqslant n < p^{k+1}$.
W dodatku można ten wykładnik przedstawić jako:

$$v_p(n!) = \frac{1}{p-1}(n - s_p(n))$$

gdzie $s_p(n)$ oznaczna sumę cyfr n w systemie p.

Twierdzenie 1.4. *LTE - Lemat o Zwiększaniu Wykładniku. Niech $x, y \in \mathbb{Z}, k \in \mathbb{N}$ i $p \in \mathbb{P}$. Wówczas, jeżeli spełnione są warunki $v_p(xy) = 0$ i $v_p(x - y) \geqslant \frac{3}{p}$*

$$v_p(x^k - y^k) = v_p(x - y) + v_p(k)$$

Wniosek 1.4.1. *LTE*
Są kilka różnych wersji tego twierdzenia, podam kilka: (tu $p \in \mathbb{P}$, $x, y \in \mathbb{Z}$, $k \in \mathbb{N}$, $v_p(xy) = 0$)

- $p > 2$, $v_p(x - y) \geqslant 1$, $v_p(x^k - y^k) = v_p(x - y) + v_p(k)$
- $p > 2$, $v_p(x + y) \geqslant 1$, $2 \nmid k$, $v_p(x^k + y^k) = v_p(x + y) + v_p(k)$
- $p = 2$, $v_p(x - y) \geqslant 1$, $2|k$, $v_p(x^k - y^k) = v_p(x - y) + v_p(x + y) + v_p(k) - 1$
- $p = 2$, $v_p(x - y) \geqslant 2$, $v_p(x^k - y^k) = v_p(x - y) + v_p(k)$ *(Gdy $2 \nmid k$ to można dać plusa)*
- $p > 2$, $v_p(x - 1) = \alpha$, *dla dowolnego* $\beta \geqslant 0$, $p^{\alpha+\beta}|x^k - 1 \Leftrightarrow p^\beta|k$
- $p = 2$, $v_2(x^2 - 1) = \alpha$, *dla dowolnego* $\beta \geqslant 0$, $2^{\alpha+\beta}|x^k - 1 \Leftrightarrow 2^{\beta+1}|k$

Dodałem ostatnie dwa fakty, bo pojawiły się kiedyś na IMO, a dowody wychodzą prosto z LTE.

2 Kongruencje

Twierdzenie 2.1. *Twierdzenie Eulera Jeżeli $(a, m) = 1$, to $a^{\varphi(m)} \equiv 1 \pmod m$, gdzie $\varphi(m)$ - to funkcja Eulera/tocjent (Więcej o tej funkcji później)*

Twierdzenie 2.2. *Wniosek: Twierdzenie Fermata Jeżeli $p \in \mathbb{P}$ i $a \perp p$ to $a^{p-1} \equiv 1 \pmod p \Leftrightarrow$ (można bez $a \perp p$) $a^p \equiv a \pmod p$.*

Twierdzenie 2.3. *Twierdzenie Wilsona Dla każdej $p \in \mathbb{P}$ zachodzi $(p-1)! \equiv -1 \pmod p$. Bonus: Dla $n \in \mathbb{Z}_{\geqslant 6}$ $(n-1)! \equiv 0 \pmod n$*

Twierdzenie 2.4. *Uogólnienie Twierdzenia Wilsona*
Dany jest liczba $m \in \mathbb{Z}_+$. Niech $P(m)$ oznacza iloczyn wszystkich liczb mniejszych m i względnie pierwszych z m, to:

$$P(m) \equiv_m \begin{cases} -1 & \text{gdy } m = 2, 4, p^t, 2p^t \\ 1 & \text{w przeciwnym przypadku} \end{cases}$$

Twierdzenie 2.5. *Chińskie twierdzenie o resztach Jeżeli $m_1, m_2, \ldots, m_r \geqslant 2$ są parami względnie pierwszymi liczbami naturalnymi, $a_1, a_2, \ldots, a_r$ są dowolnymi liczbami całkowitymi i spełniają układ kongruencji:*

$$\begin{cases} x \equiv a_1 & \pmod{m_1} \\ x \equiv a_2 & \pmod{m_2} \\ \vdots \\ x \equiv a_r & \pmod{m_r} \end{cases}$$

To istnieje dokładnie jedno rozwiązanie x, gdzie $0 \leqslant x < M = m_1 \cdot \ldots \cdot m_r$.

Definicja 2.6. *Rzędy.*
Rzędem *a modulo n dla liczb $a \perp n \in \mathbb{Z}_+$, nazywamy najmniejszą liczbę całkowitą dodatnią k taką, że $a^k \equiv 1 \pmod n$, oznaczamy $k = ord_n(a)$. Ważne własności:*

- *$a^x \equiv 1 \pmod n \iff ord_n(a)|x$, w szczególności $ord_n(a)|\varphi(n)$*
- *Jeśli $t = ord_n(a)$ to liczby $1, a, a^2, \ldots, a^{t-1}$ dają parami różne reszty modulo n.*

Wniosek 2.6.1. *Rzędy*
Tu są kilka wniosków, które warto znać o rzędach.

- *Jeżeli $(ord_n(a), ord_n(b)) = 1$, to $ord_n(ab) = ord_n(a) \cdot ord_n(b)$*
- *$ord_n(a^k) = ord_n(a)/(k, ord_n(a))$*
- *$ord_n(a) = ord_n(a^{-1})$ (Tu a^{-1} oznaczna odwrotność a modulo n)*
- *$n|\varphi(a^n - 1)$*

Definicja 2.7. *Pierwiastki pierwotne (Generator).*
Liczba całkowita g nazywamy ***pierwiastkiem pierwotnym modulo*** *m, gdy $(g, m) = 1$ i $ord_m(g) = \varphi(m)$.*

Twierdzenie 2.8. *Pierwiastek pierwotny modulo m istnieje wtedy i tylko wtedy, gdy $m = p^t$, $m = 2p^t$, $m = 2$ lub $m = 4$, gdzie $p \in \mathbb{P}$ - nieparzyste i t - dowolna liczba naturalna.*

Lemat 2.9. *Wnioski*
Proste i nieproste wnioski o pierwiastkach pierwotnych.

- *Jeśli istnieje pierwiastek modulo m, to ich jest $\varphi(\varphi(m))$ (różnych $\pmod m$)*
- *Iloczyn wszystkich (różnych $\pmod p$) pierwiastków pierwotnych modulo p przystaje do $(-1)^{\varphi(p-1)}$ modulo p*
- *Jeżeli $p = 4k+1 \in \mathbb{P}$, dla pewnego $k \in \mathbb{Z}_+$, to g jest generatorem $\Leftrightarrow$ $-g$ jest generatorem.*
- *Jeżeli $p = 4k+3 \in \mathbb{P}$, dla pewnego $k \in \mathbb{Z}_+$, to g jest generatorem $\Leftrightarrow$ $ord_p(-g) = (p-1)/2$*

Twierdzenie 2.10. *Liczba Carmichaela*
Liczba złożona $m \in N$ spełnia kongruencje $a^{m-1} \equiv 1 \ (mod\ m)$, dla każdego $m \perp a \in \mathbb{Z}$ (jest to tzn. liczba Carmichaela), wtedy i tylko wtedy gdy spełnia te dwa warunki:

- *m jest liczbą bezkwadratową (czyli $v_p(m) \leqslant 1$ dla każdego $p \in \mathbb{P}$)*
- *$p|m \Rightarrow p-1|m-1$*

Łatwo wywnioskować, że liczba Carmichaela ma co najmniej trzy różne dzielniki pierwsze. Także udowodniono, że istnieje nieskończenie wiele liczb Carmichaela.

Definicja 2.11. *Reszty kwadratowe.*
Liczba a jest **resztą kwadratową** *modulo p. jeżeli kongruencja $x^2 \equiv a \ (mod\ p)$ ma rozwiązanie w liczbach całkowitych.*

Definicja 2.12. *Symbol Legendre'a. Niech p będzie nieparzystą liczbą pierwszą. Dla $a \in \mathbb{Z}$:*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & p|a \\ +1 & \text{jeśli } a \text{ jest resztą kwadratową modulo } p \\ -1 & \text{w przeciwnym przypadku} \end{cases}$$

Twierdzenie 2.13. *Kryterium Gaussa*
Jeżeli p jest nieparzystą liczbą pierwszą, to dla dowolnego $a \in \mathbb{Z}$ zachodzi:

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

Twierdzenie 2.14. *Prawo wzajemności reszt kwadratowych*
Jeżeli p, q są nieparzystymi liczbami pierwszymi, to zachodzi:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Twierdzenie 2.15. *Dwa uzupełnienia praw wzajemności reszt kwadratowych*

$$\left(\frac{-1}{p}\right) = \begin{cases} +1 & p \equiv 1 \ (mod\ 4) \\ -1 & p \equiv 3 \ (mod\ 4) \end{cases}$$

$$\left(\frac{2}{p}\right) = \begin{cases} +1 & p \equiv \pm 1 \ (mod\ 8) \\ -1 & p \equiv \pm 3 \ (mod\ 8) \end{cases}$$

3 Wielomiany

Definicja 3.1. *Wielomian stopnia n o współczynnikach $a_0, a_1, \ldots, a_n \in \mathbb{A}$ i $a_n \neq 0$ ($\mathbb{A}$ to dowolny pierścień) nazywamy funkcję $f : \mathbb{A} \to \mathbb{A}$*

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = \sum_{k=0}^{n} a_k x^k$$

a_n nazywamy współczynnikiem wiodący i a_0 współczynnik wolny.
Gdy $a_n = 1$ to nazywamy ten wielomian unormowanym.
$\mathbb{A}[x]$ oznaczamy ciałem wielomianów o współczynnikach w $\mathbb{A}$
Stopień wielomianu oznaczamy deg f, a pierwiastkiem wielomianu nazywamy taką liczbą λ, że $f(\lambda) = 0$.

Twierdzenie 3.2. *Bézout*
Dany jest wielomian $f(x) \in \mathbb{A}[x]$ stopnia n i $a \in \mathbb{R}$, to istnieje taki wielomian $g(x) \in \mathbb{A}[x]$, że zachodzi równość:

$$f(x) = (x-a)g(x) + f(a)$$

Także wiemy, że deg $g(x) = n-1$ i $f(x)$, $g(x)$ mają ten sam współczynnik wiodący.

Wniosek 3.2.1. *Bézout*
Kilka prostych wniosków z twierdzenie powyżej:

- *Gdy a jest pierwiastkiem wielomiany $f(x)$ to mamy: $f(x) = (x-a)g(x)$*
- *Gdy $f(x) \in \mathbb{Z}[x]$, to dla różnych $a, b \in \mathbb{Z}$: $a - b | f(a) - f(b)$*
- *$f(x) = (x-\alpha_1)(x-\alpha_2)\dots(x-\alpha_s)h(x)$, gdzie α_k dla $k = 1, 2, \dots, s$ to pierwiastki wielomianu $f(x)$, deg $h(x) =$ deg $f(x) - s$ i $f(x)$, $h(x)$ mają ten sam współczynnik wiodący.*

Definicja 3.3. *Wielomiany nierozkładalne*
Wielomian $f(x) \in \mathbb{A}[x]$ jest nierozkładalny nad $\mathbb{A}$, gdy ma stopień co najmniej jeden i jeżeli $f(x) = a(x)b(x)$, $a(x)$ i $b(x) \in \mathbb{A}[x]$ to deg $a = 0$ lub deg $b = 0$.

Twierdzenie 3.4. *Kryterium Eisensteina*
Dany jest wielomian $f(x) \in \mathbb{Z}[x]$, że $f(x) = \sum_{k=0}^{n} a_k x^k$ i $a_n \neq 0$ i istnieje liczba pierwsza p, że:

$$p \nmid a_n \quad p | a_k \ \ \text{dla} \ \ k = 0, 1, \dots, n-1 \ \ \text{i} \ \ p^2 \nmid a_0$$

To wielomian $f(x)$ jest nierozkładalny.

Twierdzenie 3.5. *Zasadnicze twierdzenie algebry*
Każda niezerowy wielomian $f(x) \in \mathbb{C}[x]$ ma pierwiastek zespolony. Co więcej, wielomian można przedstawić jako: (deg $f(x) = n$, a_n - współczynnik wiodący)

$$f(x) = a_n(x-x_1)(x-x_2)\dots(x-x_n)$$

gdzie $x_1, x_2, \dots, x_n$ są to pierwiastki wielomiany $f(x)$.
Można z tego wywnioskować, że każdy wielomian $g(x) \in \mathbb{A}[x]$ stopnia n ma co najwyżej n pierwiastków w $\mathbb{A}$.

Twierdzenie 3.6. *Dany jest wielomian $f(x) \in \mathbb{Z}[x]$. Jeśli ma pierwiastek wymierny $\frac{k}{m}$, gdzie $k \perp m$, to $k | a_0$ i $m | a_n$.*
Ważny wniosek jest taki, że każdy unormowany wielomian ma pierwiastki całkowite lub niewymierne.

Twierdzenie 3.7. *Wzory Viete'a*
Jeśli $x_1, x_2, \dots, x_n$ są pierwiastkami wielomianu $f(x) = \sum_{k=0}^{n} a_k x^k$, to zachodzą wzory:

$$\begin{cases} x_1 + x_2 + \ldots + x_n = -a_{n-1}/a_n \\ \sum_{i>j} x_i x_j = a_{n-2}/a_n \\ \sum_{i>j>k} x_i x_j x_k = -a_{n-3}/a_n \\ \vdots \\ x_1 x_2 \dots x_n = (-1)^n \cdot a_0/a_n \end{cases}$$

Definicja 3.8. *Wielomian cyklotomiczny*
Dany jest $n \in \mathbb{N}$ to wielomian cyklomotomiczny definiujemy tak:

$$\Phi_n(x) = \prod_{k \perp n} (x - \omega^k)$$

Gdzie $\omega = \omega_n$ to jest pierwiastek wielomianu $x^n - 1$ i ma postać:

$$\cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}$$

(i jednostka urojona ma własność $i^2 = -1$)

Wniosek 3.8.1. *Własności wielomianów cyklotomicznych*

- *deg $\Phi_n = \varphi(n)$, $\Phi_n(x) \in \mathbb{Z}$*
- *$\Phi_n(x)$ jest nierozkładalny nad ciałem liczb wymiernych.*
- *$x^n - 1 = \prod_{d|n} \Phi_d(x)$*

Twierdzenie 3.9. *Lemat Hensela*
Dany jest wielomian $f(x) \in \mathbb{Z}[x]$ i $p \in \mathbb{P}$. Załóżmy, że istnieje taka liczba całkowita a, że $f(a) \equiv 0 \pmod{p^n}$ i $f'(a) \not\equiv 0 \pmod{p}$. Wówczas istnieje dokładnie jedno takie $b \in \mathbb{Z}$, że:

$$f(b) \equiv 0 \pmod{p^{n+1}} \ \text{i} \ b \equiv a \pmod{p^n}$$

4 Funkcje arytmetyczne

Definicja 4.1. *Funkcję arytmetyczną nazywamy dowolną funkcję $f : \mathbb{N} \longrightarrow \mathbb{C}$.*

Definicja 4.2. *Funkcję arytmetyczną nazywamy multiplikatywną, gdy dla wszystkich liczb względnie pierwszych $m, n \in \mathbb{N}$ zachodzi: $f(mn) = f(m)f(n)$.*

Twierdzenie 4.3. *Suma k-tych potęg dzielników oznaczamy:*

$$\sigma_k(n) = \sum_{d|n} d^k$$

W szczególności mamy: $\sigma_0 = \tau$ - liczba dzielników, $\sigma_1 = \sigma$ - suma dzielników. Ta funkcja jest multiplikatywna
Gdy $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$, wtedy:

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \cdot \ldots \cdot (\alpha_s + 1),\ \sigma(n) = \frac{p_1^{\alpha_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{\alpha_2+1} - 1}{p_2 - 1} \cdot \ldots \cdot \frac{p_s^{\alpha_s+1} - 1}{p_s - 1}$$

Trochę własności:

$$\sum_{i=1}^{n} \tau(i) = \sum_{i=0}^{n} \left\lfloor \frac{n}{i} \right\rfloor,\ \sum_{i=1}^{n} \sigma(i) = \sum_{i=1}^{n} i \left\lfloor \frac{n}{i} \right\rfloor$$

Uogólniając dla σ_k:

$$\sum_{i=1}^{n} \sigma_k(i) = \sum_{i=1}^{n} i^k \left\lfloor \frac{n}{i} \right\rfloor$$

Twierdzenie 4.4. *Funkcja Eulera φ (tocjent):*
$\varphi(n)$ to ilość liczb naturalnych mniejszych (równych) od n i względnie pierwszych z n. Jest to funkcja multiplikatywna. Spełnia:

$$\varphi(p^k) = p^k - p^{k-1} = p^k \left(1 - \frac{1}{p}\right)$$

Więc jasne jest, że działa ten wzór, dla $n = n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdot \ldots \cdot \left(1 - \frac{1}{p_s}\right)$$

Kilka własności:

$$n = \sum_{d|n} \varphi(d),\ \sum_{i=1}^{n} \varphi(i) \left\lfloor \frac{n}{i} \right\rfloor = \frac{n(n-1)}{2}$$

Definicja 4.5. *Zdefiniujemy kilka funkcji arytmetycznych, przydatnych później.*

- *$\omega(n)$ jest to liczba dzielników pierwszych n.*
- *Funkcja Möbiusa μ, którą definiujemy tak:*

$$\mu(n) = \begin{cases} (-1)^{\omega(n)}, & \text{gdy } n \text{ jest bezkwadratowe} \\ 0, & \text{w przeciwnym przypadku} \end{cases}$$

- *Funkcja jednostkowa $e(n)$:*

$$e(n) = \begin{cases} 1, & \text{gdy } n = 1 \\ 0, & \text{gdy } n > 1 \end{cases}$$

- *Identyczność: $id(n) = n$*
- *Funkcja stale równa $\boldsymbol{1} : \boldsymbol{1}(n) = 1$*

Każda funkcja powyżej jest mutliplikatywna, ostatnie 3 funkcje są całkowicie multiplikatywna (nie potrzeba warunku $a \perp b$). Poniżej mamy przydatną własność:

$$\sum_{d|n} \mu(d) = e(n)$$

Definicja 4.6. *Splot Dirichleta*
Niech dane są dwie funkcje arytmetyczne f i g. Splotem Dirichleta tych funkcji nazywamy $f * g$ i jest równa:

$$(f * g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right)$$

Twierdzenie 4.7. *Klika własności splotu*

- *Splot jest przemienny i łączny.*
- *Ma element neutralny e.*
- *Jeśli $f(1) \neq 0$ to f jest odwracalny (splotowo): istnieje g takie, że $f * g = e$*
- *Splot dwóch funkcji multiplikatywnych jest funkcją multiplikatywną.*

Kilka splotów znanych funkcji:

- $\mu * \mathbf{1} = e$
- $\mathbf{1} * \mathbf{1} = \tau$
- $\varphi * \mathbf{1} = id$
- $\mu * id = \varphi$
- $id * \mathbf{1} = \sigma$

Twierdzenie 4.8. *Twierdzenie inwersyjne Möbiusa*
Jeżeli dane są dwie funkcje arytmetyczne f i g oraz:

$$g(n) = \sum_{d|n} f(d)$$

Wtedy jest to równoważne z:

$$f(n) = \sum_{d|n} \mu(d) g\left(\frac{n}{d}\right)$$

5 Ciągi rekurencyjne

Definicja 5.1. *Wielomian charakterystyczny ciągu*
Jeżeli ciąg a_n spełnia rekurencję $a_n = Pa_{n-1} + Qa_{n-2}$ to wielomian charakterystyczny nazywamy $W(x) = x^2 - Px - Q$. (Będziemy bardziej rozważać ich pierwiastki, można analogicznie definiować dla większego stopnia rekurencji).

Twierdzenie 5.2. *Metoda Eulera*
Dany jest ciąg a_n, jeżeli α i β są pierwiastkami wielomianu charakterystycznego tego ciągu, to:

- *Jeżeli $\alpha \neq \beta$ to istnieją takie stałe A, B, że:*

$$a_n = A \cdot \alpha^n + B \cdot \beta^n$$

- *Jeżeli $\alpha = \beta$ to istnieją takie stałe C i D, że:*

$$a_n = C \cdot \alpha^n + D \cdot n\alpha^{n-1}$$

Stałe te są jednoznacznie wyznaczone przez pierwsze dwa wyrazy ciągu.

Definicja 5.3. *Funkcja tworząca*
Funkcją tworzącą ciągu a_n definiujemy tak:

$$\sum_{k=0}^{\infty} a_k x^k = a_0 + a_1 x + a_2 x^2 + \dots$$

6 Ciekawe tożsamości algebraiczne

Jeżeli $x+y+z=0$, to:

- $2(x^4+y^4+z^4)=(x^2+y^2+z^2)^2$
- $\dfrac{x^5+y^5+z^5}{5}=\dfrac{x^2+y^2+z^2}{2}\cdot\dfrac{x^3+y^3+z^3}{3}$
- $\dfrac{x^7+y^7+z^7}{7}=\dfrac{x^2+y^2+z^2}{2}\cdot\dfrac{x^5+y^5+z^5}{5}$

- $4x^4+y^4=(2x^2+2xy+y^2)(2x^2-2xy+y^2)$ **Tożsamość Sophie Germain**

- $x^3+y^3+z^3-3xyz=(x+y+z)(x^2+y^2+z^2-xy-yz-zx)$
- $(x+y+z)^3-x^3-y^3-z^3=(x+y)(y+z)(z+x)$
- $x^3+y^3+z^3+(x+y)^3+(y+z)^3+(z+x)^3=(x+y+z)(x^2+y^2+z^2)$

- $(ab+bc+ca)(a+b+c)=(a+b)(b+c)(c+a)+abc$
- $(a+b+c)(a+b-c)(a-b+c)(-a+b+c)=2(a^2b^2+b^2c^2+c^2a^2)-(a^4+b^4+c^4)$
- $(a+b+c)^3-(a+b-c)^3-(a-b+c)^3-(-a+b+c)^3=24abc$

- $(x+y)(y+z)(z+x)=x^2(y+z)+y^2(z+x)+z^2(x+y)+2xyz$
- $(x-y)(y-z)(z-x)=-xy(x-y)-yz(y-z)-zx(z-x)$
- $3(x-y)(y-z)(z-x)=(x-y)^3+(y-z)^3+(z-x)^3$

- $\dfrac{b-c}{(a-b)(a-c)}+\dfrac{c-a}{(b-c)(b-a)}+\dfrac{a-b}{(c-a)(c-b)}=\dfrac{2}{a-b}+\dfrac{2}{b-c}+\dfrac{2}{c-a}$ a,b,c - różne
- $\dfrac{(b+c)^2}{(a-b)(a-c)}+\dfrac{(c+a)^2}{(b-c)(b-a)}+\dfrac{(a+b)^2}{(c-a)(c-b)}=1$ a,b,c - różne
- $\dfrac{bc}{(a-b)(a-c)}+\dfrac{ca}{(b-c)(b-a)}+\dfrac{ab}{(c-a)(c-b)}=1$ a,b,c - różne
- $\dfrac{(a+b)(a+c)}{(a-b)(a-c)}+\dfrac{(b+c)(b+a)}{(b-c)(b-a)}+\dfrac{(c+a)(c+b)}{(c-a)(c-b)}=1$ a,b,c - różne
- $\dfrac{(1-ab)(1-ac)}{(a-b)(a-c)}+\dfrac{(1-bc)(1-ba)}{(b-c)(b-a)}+\dfrac{(1-ca)(1-cb)}{(c-a)(c-b)}=1$ a,b,c - różne

---

- $\dfrac{(a+b)}{(a-b)}+\dfrac{(b+c)}{(b-c)}+\dfrac{(c+a)}{(c-a)}=\dfrac{a(b-c)^2+b(c-a)^2+c(a-b)^2}{(a-b)(b-c)(c-a)}$ a,b,c - różne
- $\dfrac{(a-b)}{(a+b)}+\dfrac{(b-c)}{(b+c)}+\dfrac{(c-a)}{(c+a)}=\dfrac{(a-b)(b-c)(c-a)}{(a+b)(b+c)(c+a)}$
- $(x^2-yz)(y+z)+(y^2-zx)(z+x)+(x^2-yz)(y+z)=0$
- $x^2+y^2+z^2+3(xy+yz+zx)=(x+y)(y+z)+(y+z)(z+x)+(z+x)(x+y)$