

Równania wielomianowe

Sławomir Cynk

Instytut Matematyki Uniwersytetu Jagiellońskiego

20 marca 2009

Kraków

Równanie z jedną niewiadomą

Wielomian jednej zmiennej to wyrażenie postaci

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

gdzie *współczynniki* $a_0, a_1, \dots, a_n$ są elementami *pierścienia* (np. $\mathbb{Z}$) lub *ciała* (np. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$) współczynników.

Równanie z jedną niewiadomą

Wielomian jednej zmiennej to wyrażenie postaci

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

gdzie *współczynniki* $a_0, a_1, \dots, a_n$ są elementami *pierścienia* (np. $\mathbb{Z}$) lub *ciała* (np. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$) współczynników.

W teorii liczb często mamy do czynienia z wielomianami o współczynnikach z pierścienia lub ciała $\mathbb{Z}/n$ reszt z dzielenia przez n .

Równanie z jedną niewiadomą

Wielomian jednej zmiennej to wyrażenie postaci

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

gdzie *współczynniki* $a_0, a_1, \dots, a_n$ są elementami *pierścienia* (np. $\mathbb{Z}$) lub *ciała* (np. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$) współczynników.

W teorii liczb często mamy do czynienia z wielomianami o współczynnikach z pierścienia lub ciała $\mathbb{Z}/n$ reszt z dzielenia przez n .

Uwaga. Wtedy wielomian i funkcja wielomianowa nie są tym samym, np. wielomiany z i z^3 dają te same funkcje wielomianowe dla ciała współczynników $\mathbb{Z}/3$ ale są różnymi wielomianami (bo mają różne współczynniki).

Równanie z jedną niewiadomą

Wielomian jednej zmiennej to wyrażenie postaci

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

gdzie *współczynniki* $a_0, a_1, \dots, a_n$ są elementami *pierścienia* (np. $\mathbb{Z}$) lub *ciała* (np. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$) współczynników.

W teorii liczb często mamy do czynienia z wielomianami o współczynnikach z pierścienia lub ciała $\mathbb{Z}/n$ reszt z dzielenia przez n .

Uwaga. Wtedy wielomian i funkcja wielomianowa nie są tym samym, np. wielomiany z i z^3 dają te same funkcje wielomianowe dla ciała współczynników $\mathbb{Z}/3$ ale są różnymi wielomianami (bo mają różne współczynniki).

Jeśli $a_n \neq 0$, to liczbę n nazywamy stopniem $\deg P$ wielomianu, współczynnik a_n nazywa się wtedy (współczynnikiem wiodącym), natomiast a_0 – *współczynnikiem inicjującym*. Jeśli $a_n = 1$ to $P(x)$ nazywamy wielomianem *unormowanym*

Równania wielomianowe

Równania postaci $P(x) = 0$. Znajdowanie rozwiązań wymiernych (całkowitych) równań wielomianowych jednej zmiennej o współczynnikach wymiernych (całkowitych) jest łatwe. Jeśli $a_0, \dots, a_n \in \mathbb{Z}$, a liczba wymierna $\frac{p}{q}$ jest pierwiastkiem równania, $(p, q) = 1$, to $a_0 \mid p$, $a_n \mid q$.

Równania wielomianowe

Równania postaci $P(x) = 0$. Znajdowanie rozwiązań wymiernych (całkowitych) równań wielomianowych jednej zmiennej o współczynnikach wymiernych (całkowitych) jest łatwe. Jeśli $a_0, \dots, a_n \in \mathbb{Z}$, a liczba wymierna $\frac{p}{q}$ jest pierwiastkiem równania, $(p, q) = 1$, to $a_0 \mid p, a_n \mid q$.

Równanie liniowe: Bardzo proste. Ale jeśli rozwiązujemy w zbiorze reszt modulo n (czyli rozwiązujemy *kongruencje liniowe*), to wypisanie tabliczki dzielenia może być kłopotliwe. Kongruencja

$$ax \equiv b \pmod{n}$$

ma rozwiązanie wtedy i tylko wtedy gdy $(a, n) \mid b$.

Równania wielomianowe

Równania postaci $P(x) = 0$. Znajdowanie rozwiązań wymiernych (całkowitych) równań wielomianowych jednej zmiennej o współczynnikach wymiernych (całkowitych) jest łatwe. Jeśli $a_0, \dots, a_n \in \mathbb{Z}$, a liczba wymierna $\frac{p}{q}$ jest pierwiastkiem równania, $(p, q) = 1$, to $a_0 \mid p$, $a_n \mid q$.

Równanie liniowe: Bardzo proste. Ale jeśli rozwiązujemy w zbiorze reszt modulo n (czyli rozwiązujemy *kongruencje liniowe*), to wypisanie tabliczki dzielenia może być kłopotliwe. Kongruencja

$$ax \equiv b \pmod{n}$$

ma rozwiązanie wtedy i tylko wtedy gdy $(a, n) \mid b$. Istnieją wtedy liczby całkowite k, l takie, że $(a, n) = ka + ln$. Stąd $ak \equiv (a, n) \pmod{n}$, jeśli ponadto $b = d(a, n)$, to $a(kd) \equiv b \pmod{n}$.

Równanie kwadratowe

Potrafili je rozwiązać starożytni hinduscy i greccy matematycy. W starożytnym Babilonie rozwiązywano układ równań $x + y = p$, $xy = q$ geometrycznie, konstrukcja prowadziła się do

- 1 utworzenia $\frac{x+y}{2}$,
- 2 utworzenia $\left(\frac{x+y}{2}\right)^2$,
- 3 utworzenia $\left(\frac{x+y}{2}\right)^2 - xy$,
- 4 utworzenia $\sqrt{\left(\frac{x+y}{2}\right)^2 - xy} = \frac{x-y}{2}$,
- 5 wyznaczenia x i y

François Viète (1540-1603)



Jako pierwszy podał algebraiczną formułę na rozwiązanie równania kwadratowego. Wprowadził literowe oznaczenia stałych w równaniach. Podał zależności między pierwiastkami równania kwadratowego (zw. wzorami Viète'a)

$$x_1 + x_2 = -\frac{b}{a}, x_1 x_2 = \frac{c}{a}.$$

Wzory Viète'a zostały uogólnione na równania dowolnego stopnia.

$$\sum_{i_1 < i_2 < \dots < i_k} x_{i_1} \dots x_{i_k} = (-1)^k \frac{a_{n-k}}{a_n}$$

Aby rozwiązać równanie kwadratowe w danym zbiorze, musimy umieć znaleźć pierwiastek kwadratowy z wyróżnika. W zbiorze liczb rzeczywistych nie zawsze jest to wykonalne, dlatego właściwsze do rozwiązywania równań są liczby zespolone.

Kongruencje kwadratowe

Przy rozwiązywaniu kongruencji kwadratowych, musimy rozstrzygnąć, czy dana liczba jest resztą czy nieresztą kwadratową modulo n . Dla liczby pierwszej p połowa $(p-1)$ reszt modulo p jest resztą kwadratową, a połowa – nieresztą. Służy do tego symbol Legendre'a (Jacobiego).

$$\left(\frac{n}{p}\right) = 1 \text{ gdy } n \text{ jest resztą kwadratową (mod } n)$$

$$\left(\frac{n}{p}\right) = -1 \text{ gdy } n \text{ jest nieresztą kwadratową (mod } n)$$

Kongruencje kwadratowe

Przy rozwiązywaniu kongruencji kwadratowych, musimy rozstrzygnąć, czy dana liczba jest resztą czy nieresztą kwadratową modulo n . Dla liczby pierwszej p połowa $(p-1)$ reszt modulo p jest resztą kwadratową, a połowa – nieresztą. Służy do tego symbol Legendre'a (Jacobiego).

$$\left(\frac{n}{p}\right) = 1 \text{ gdy } n \text{ jest resztą kwadratową (mod } n)$$

$$\left(\frac{n}{p}\right) = -1 \text{ gdy } n \text{ jest nieresztą kwadratową (mod } n)$$

$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right) \left(\frac{b}{n}\right), \left(\frac{a}{nm}\right) = \left(\frac{a}{n}\right) \left(\frac{a}{m}\right)$$

$$\left(\frac{-1}{n}\right) = 1 \Leftrightarrow n \equiv 1 \pmod{4}$$

$$\left(\frac{2}{n}\right) = 1 \Leftrightarrow n \equiv 1 \pmod{8} \text{ lub } n \equiv 7 \pmod{8}$$

Kongruencje kwadratowe

Przy rozwiązywaniu kongruencji kwadratowych, musimy rozstrzygnąć, czy dana liczba jest resztą czy nieresztą kwadratową modulo n . Dla liczby pierwszej p połowa $(p-1)$ reszt modulo p jest resztą kwadratową, a połowa – nieresztą. Służy do tego symbol Legendre'a (Jacobiego).

$$\left(\frac{n}{p}\right) = 1 \text{ gdy } n \text{ jest resztą kwadratową (mod } n)$$

$$\left(\frac{n}{p}\right) = -1 \text{ gdy } n \text{ jest nieresztą kwadratową (mod } n)$$

$$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right) \left(\frac{b}{n}\right), \left(\frac{a}{nm}\right) = \left(\frac{a}{n}\right) \left(\frac{a}{m}\right)$$

$$\left(\frac{-1}{n}\right) = 1 \Leftrightarrow n \equiv 1 \pmod{4}$$

$$\left(\frac{2}{n}\right) = 1 \Leftrightarrow n \equiv 1 \pmod{8} \text{ lub } n \equiv 7 \pmod{8}$$

Do jego wyznaczania można wykorzystać prawo wzajemności Gaussa.

$$\left(\frac{n}{m}\right) = (-1)^{\frac{(n-1)(m-1)}{4}} \left(\frac{m}{n}\right)$$

Wzór Cardano dla równań trzeciego stopnia (najprawdopodobniej otrzymał od Tartaglii)



Gerolamo Cardano (1501-1576)



Niccolò Tartaglia (1499-1557)

Wzór Cardano dla równań trzeciego stopnia (najprawdopodobniej otrzymał od Tartaglii)



Gerolamo Cardano (1501-1576)

Cardano (inaczej Cardan), skonstruował przegub Cardana stosowany w wale Cardana (obecnie stosowany w motocyklach)



Niccolò Tartaglia (1499-1557)

Wzory Cardana

Rozwiązując równanie $ax^3 + bx^2 + cx + d = 0$, dokonujemy najpierw podstawienie $y = x + \frac{a}{3}$, pozbywając się współczynnika przy x^2 . Podobnie w równaniu stopnia n możemy się pozbyć współczynnika przy x^{n-1} .

Wzory Cardana

Rozwiązując równanie $ax^3 + bx^2 + cx + d = 0$, dokonujemy najpierw podstawienie $y = x + \frac{a}{3}$, pozbywając się współczynnika przy x^2 . Podobnie w równaniu stopnia n możemy się pozbyć współczynnika przy x^{n-1} . Rozważamy równanie

$$x^3 + px + q = 0.$$

Przyjmując $x = u - \frac{\lambda}{u}$, zauważamy, że dla $3\lambda = p$ otrzymamy równanie kwadratowe od u^3 , oznaczając $u^3 = z$ mamy

$$z^2 + qz - \frac{p^3}{27} = 0$$

Powyższe równanie nazywamy *równaniem rozwiązującym*, a jego wyróżnik $\Delta = \frac{q^2}{4} + \frac{p^3}{27}$ *wyróżnikiem równania stopnia 3*.

Równanie stopnia 3 ma pierwiastek wielokrotny (podwójny, potrójny) wtedy i tylko wtedy gdy $\Delta = 0$.

Równanie ma trzy pierwiastki rzeczywiste (liczone z krotnościami) wtedy i tylko wtedy gdy $\Delta < 0$.

Równanie stopnia 3 ma pierwiastek wielokrotny (podwójny, potrójny) wtedy i tylko wtedy gdy $\Delta = 0$.

Równanie ma trzy pierwiastki rzeczywiste (liczone z krotnościami) wtedy i tylko wtedy gdy $\Delta < 0$.

Rozwiązanie równania stopnia 3 sprowadza się do rozwiązania równania kwadratowego, oraz wyznaczenia pierwiastka stopnia 3. Operacje te są dla liczb zespolonych zawsze wykonalne.

Równanie stopnia 3 ma pierwiastek wielokrotny (podwójny, potrójny) wtedy i tylko wtedy gdy $\Delta = 0$.

Równanie ma trzy pierwiastki rzeczywiste (liczone z krotnościami) wtedy i tylko wtedy gdy $\Delta < 0$.

Rozwiązanie równania stopnia 3 sprowadza się do rozwiązania równania kwadratowego, oraz wyznaczenia pierwiastka stopnia 3. Operacje te są dla liczb zespolonych zawsze wykonalne. Jednak w przypadku równania stopnia 3 o współczynnikach rzeczywistych z $\Delta < 0$ do wyznaczenia pierwiastków równania konieczne może być wyznaczanie pierwiastków stopnia 3 liczb zespolonych. Jest to tzw. przypadek nieprzywiedlny (*casus irreducibilis*)

Wzory Ferrariego

Lodovico Ferrari (1522-1565)

Wzór Ferrariego dla równań czwartego stopnia również został opublikowany (ukradziony) przez Cardano w *"Ars Magna"*

Rozwiązujemy równanie postaci

$$x^4 + px^2 + qx + r = 0.$$

Przekształcamy dla dowolnego u do postaci

$$x^4 + ux^2 + \frac{u^2}{4} = (u - p)x^2 - qx + \left(\frac{u^2}{4} - r\right).$$

Następnie dobieramy u tak aby prawa strona była kwadratem, zachodzi to gdy

$$q^2 - 4(u - p)\left(\frac{u^2}{4} - r\right) = 0$$

czyli

$$u^3 - pu^2 - 4ru + (4pr - q^2) = 0.$$

Jest to tzw. równanie rozwiązujące.

Wzory Ferrariego

Równanie rozwiązujące jest stopnia 3, możemy je więc rozwiązać korzystając ze zworów Cardana.

Wzory Ferrariego

Równanie rozwiązujące jest stopnia 3, możemy je więc rozwiązać korzystając ze wzorów Cardana. Znajomość pierwiastka u_1 równania rozwiązującego pozwala nam zredukować równanie stopnia cztery do dwóch równań kwadratowych

$$x^2 + \frac{u_1}{2} = \sqrt{u_1 - p} \left(x - \frac{q}{2(u_1 - p)} \right)$$

$$x^2 + \frac{u_1}{2} = -\sqrt{u_1 - p} \left(x - \frac{q}{2(u_1 - p)} \right)$$

Wzory Ferrariego

Równanie rozwiązujące jest stopnia 3, możemy je więc rozwiązać korzystając ze wzorów Cardana. Znajomość pierwiastka u_1 równania rozwiązującego pozwala nam zredukować równanie stopnia cztery do dwóch równań kwadratowych

$$x^2 + \frac{u_1}{2} = \sqrt{u_1 - p} \left(x - \frac{q}{2(u_1 - p)} \right)$$

$$x^2 + \frac{u_1}{2} = -\sqrt{u_1 - p} \left(x - \frac{q}{2(u_1 - p)} \right)$$

Zauważmy, że liczby u_1, u_2, u_3 są równe

$$x_1x_2 + x_3x_4, x_1x_3 + x_2x_4, x_1x_4 + x_2x_3,$$

te ostatnie wyrażenia są niezmiennicze (jako zbiór trzech liczb) ze względu na permutacje zbioru $\{1, 2, 3, 4\}$.

Twierdzenie Bezoute'a



Étienne Bézout (1730—1783)

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

Inna postać:

liczba a jest pierwiastkiem wielomianu $P(x)$ wtedy i tylko wtedy gdy (x) dzieli się bez reszty przez $(x - a)$.

Znajomość jednego pierwiastka równania stopnia n , pozwala nam zredukować to równanie do równania stopnia $n - 1$.

Twierdzenie Bezoute'a



Étienne Bézout (1730—1783)

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

Inna postać:

liczba a jest pierwiastkiem wielomianu $P(x)$ wtedy i tylko wtedy gdy (x) dzieli się bez reszty przez $(x - a)$.

Znajomość jednego pierwiastka równania stopnia n , pozwala nam zredukować to równanie do równania stopnia $n - 1$.

Pierwiastkami największego wspólnego dzielnika Q wielomianów $P(x)$ i $P'(x)$ są wielokrotne pierwiastki wielomianu P ale z krotnością o jeden mniejszą, czyli wielomian P/Q ma te same pierwiastki co P , ale wyłącznie krotności 1.

Twierdzenie Bezoute'a



Étienne Bézout (1730—1783)

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

Inna postać:

liczba a jest pierwiastkiem wielomianu $P(x)$ wtedy i tylko wtedy gdy (x) dzieli się bez reszty przez $(x - a)$.

Znajomość jednego pierwiastka równania stopnia n , pozwala nam zredukować to równanie do równania stopnia $n - 1$.

Pierwiastkami największego wspólnego dzielnika Q wielomianów $P(x)$ i $P'(x)$ są wielokrotne pierwiastki wielomianu P ale z krotnością o jeden mniejszą, czyli wielomian P/Q ma te same pierwiastki co P , ale wyłącznie krotności 1. Korzystając z algorytmu euklidesa możemy sprowadzić równanie, do równania o tych samych pierwiastkach, ale wyłącznie pojedynczych.

Wielomiany parzyste, nieparzyste, symetryczne etc.

Równanie wielomianowe pochodzące od równania mającego dodatkowe własności, można zredukować do równania stopnia niższego.

Wielomian parzysty: Jeśli $P(x)$ jest wielomianem parzystym stopnia n , to można go zapisać w postaci $Q(x^2)$, gdzie Q jest wielomianem stopnia $\frac{n}{2}$.

Wielomiany parzyste, nieparzyste, symetryczne etc.

Równanie wielomianowe pochodzące od równania mającego dodatkowe własności, można zredukować do równania stopnia niższego.

Wielomian parzysty: Jeśli $P(x)$ jest wielomianem parzystym stopnia n , to można go zapisać w postaci $Q(x^2)$, gdzie Q jest wielomianem stopnia $\frac{n}{2}$.

Wielomian nieparzysty: Jeśli $P(x)$ jest wielomianem parzystym stopnia n , to można go zapisać w postaci $XQ(x^2)$, gdzie Q jest wielomianem stopnia $\frac{n-1}{2}$.

Wielomiany parzyste, nieparzyste, symetryczne etc.

Równanie wielomianowe pochodzące od równania mającego dodatkowe własności, można zredukować do równania stopnia niższego.

Wielomian parzysty: Jeśli $P(x)$ jest wielomianem parzystym stopnia n , to można go zapisać w postaci $Q(x^2)$, gdzie Q jest wielomianem stopnia $\frac{n}{2}$.

Wielomian nieparzysty: Jeśli $P(x)$ jest wielomianem parzystym stopnia n , to można go zapisać w postaci $XQ(x^2)$, gdzie Q jest wielomianem stopnia $\frac{n-1}{2}$.

Wielomian symetryczny: jest to taki wielomian, że $a_k = a_{n-k}$, czyli $P(x) = P(\frac{1}{x})x^n$. Wielomian symetryczny stopnia parzystego można zapisać w postaci $P(x) = Q(x + \frac{1}{x})x^{n/2}$, gdzie Q jest wielomianem stopnia $\frac{n}{2}$, natomiast wielomian symetryczny stopnia nieparzystego można zapisać w postaci $P(x) = (x - 1)Q(x + \frac{1}{x})x^{n-1/2}$, gdzie Q jest wielomianem stopnia $\frac{n-1}{2}$.

Zasadnicze Twierdzenie Algebry



Johann Carl Friedrich Gauss (1777—1855).

Dowolny wielomian (dodatniego stopnia) o współczynnikach zespolonych, ma pierwiastek zespolony. ^Z

Inna postać:

Wielomian o współczynnikach zespolonych stopnia n ma dokładnie n pierwiastków zespolonych liczonych z krotnościami.

zasadniczego twierdzenia algebry wynika, że dowolny wielomian o współczynnikach zespolonych rozkłada się na iloczyn wielomianów liniowych, natomiast wielomian o współczynnikach rzeczywistych, na iloczyn wielomianów liniowych i kwadratowych (o ujemnym wyróżniku).



Charles Sturm (1803-1855)

Podał metodę znajdowania liczby pierwiastków rzeczywistych równania wielomianowego znajdujących się w danym przedziale.



Charles Sturm (1803-1855)

Podał metodę znajdowania liczby pierwiastków rzeczywistych równania wielomianowego znajdujących się w danym przedziale.

Przyjmujemy $f_0 = P$, $f_1 = P'$ i definiujemy indukcyjnie f_{n+2} jako przeciwny do reszty z dzielenia f_n przez f_{n+1} .



Charles Sturm (1803-1855)

Podał metodę znajdowania liczby pierwiastków rzeczywistych równania wielomianowego znajdujących się w danym przedziale.

Przyjmujemy $f_0 = P$, $f_1 = P'$ i definiujemy indukcyjnie f_{n+2} jako przeciwny do reszty z dzielenia f_n przez f_{n+1} .

Następnie liczymy liczbę zmian znaku w ciągu f_i na końcu i na początku przedziału. Różnica jest liczbą pierwiastków w przedziale.

Ciąg Sturm



Charles Sturm (1803-1855)

Podał metodę znajdowania liczby pierwiastków rzeczywistych równania wielomianowego znajdujących się w danym przedziale.

Przyjmujemy $f_0 = P$, $f_1 = P'$ i definiujemy indukcyjnie f_{n+2} jako przeciwny do reszty z dzielenia f_n przez f_{n+1} .

Następnie liczymy liczbę zmian znaku w ciągu f_i na końcu i na początku przedziału. Różnica jest liczbą pierwiastków w przedziale.

Przykład:

$P = x^2 - x - 2$, ciąg Sturm ma postać $x^2 - x - 2, 2x - 1, \frac{7}{4}$.

Ciąg Sturm



Charles Sturm (1803-1855)

Podał metodę znajdowania liczby pierwiastków rzeczywistych równania wielomianowego znajdujących się w danym przedziale.

Przyjmujemy $f_0 = P$, $f_1 = P'$ i definiujemy indukcyjnie f_{n+2} jako przeciwny do reszty z dzielenia f_n przez f_{n+1} .

Następnie liczymy liczbę zmian znaku w ciągu f_i na końcu i na początku przedziału. Różnica jest liczbą pierwiastków w przedziale.

Przykład:

$P = x^2 - x - 2$, ciąg Sturm ma postać $x^2 - x - 2$, $2x - 1$, $\frac{7}{4}$.

Znaki: $(+ - +)$ dla $x < -1$, $(- - +)$ dla $x \in (-1, 1/2)$, $(- + +)$ dla $x \in (1/2, 2)$ oraz $(+ + +)$ dla $x > 2$,

Równania stopnia piątego i wyższego



Niels Henrik Abel (1802—1829) Évariste Galois (1811—1832).
Nie istnieją wzory na rozwiązywanie równań piątego i wyższych stopni: Twierdzenie Abela–Ruffiniego (dowiodł Abel w 1821 roku)