Kongruencje kwadratowe – symbole Legendre'a i Jacobiego

Kongruencje – Wykład 4

Definicja 1

Kongruencję w postaci $x^2 \equiv a \pmod{m}$, gdzie $a \perp m$, nazywamy *kongruencją kwadratową;* jej bardziej ogólna postać $ax^2 + bx + c$ może zostać zredukowana do tej prostszej jeżeli: $a \perp m$ i b jest liczbą nieparzystą, albo dla nieparzystego m.

Stwierdzenie

Dla modułu złożonego $m = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \dots {p_r}^{\alpha_r}$ kongruencja $x^2 \equiv a \pmod{m}$ jest równoważna układowi kongruencji

$$x^2 \equiv a \pmod{p_i^{\alpha_i}} \qquad i = 1, 2, \dots, r.$$

Definicja 2

Jeżeli kongruencja $x^2 \equiv a \pmod{m}$, $a \perp m$ ma rozwiązanie,
to liczbę a nazywamy *resztą kwadratową modulo* m;
jeżeli kongruencja rozwiązania nie ma,
to liczbę a nazywamy *niereszta kwadratową modulo* m.
(określenie reszta kwadratowa można w sposób naturalny rozszerzyć na „reszty stopnia k-tego” – dla kongruencji $x^k \equiv a \pmod{m}$)

Kongruencje kwadratowe dla modułu p

Twierdzenie

Dla modułu będącego nieparzystą liczbą pierwszą p i dla $a \perp m$ kongruencja

$$x^2 \equiv a \pmod{p}$$

ma dwa rozwiązania modulo p albo w ogóle nie ma rozwiązań.

Dowód: jeżeli x i y są dwoma rozwiązaniami naszej kongruencji to $x^2 \equiv y^2 \pmod{p} \quad \rightarrow \quad p \mid (x+y)(x-y)$.
Oznacza to, że $p \mid (x+y)$ lub $p \mid (x-y)$, a stąd $x \equiv \pm y \pmod{p}$.
Jeżeli kongruencja ma rozwiązania, to są to dwa rozwiązania, różniące się znakiem.

Reszty i niereszty kwadratowe dla modułów p

dla modułu $p = 5 \ldots$

$\ldots$ resztami kwadratowymi są liczby 1 i 4; niereszty to liczby 2 i 3:
$1^2 \equiv 4^2 \equiv \boxed{1} \pmod 5$, $2^2 \equiv 3^2 \equiv \boxed{4} \pmod 5$.

dla modułu $p = 7 \ldots$

$\ldots$ resztami kwadratowymi są liczby 1, 2 i 4; niereszty to 3, 5 i 6:
$1^2 \equiv 6^2 \equiv \boxed{1} \pmod 7$, $2^2 \equiv 5^2 \equiv \boxed{4} \pmod 7$, $3^2 \equiv 4^2 \equiv \boxed{2} \pmod 7$ $\ldots$

$\ldots$ dla modułu $p = 11$ kwadratowymi $\ldots$

$\ldots$ resztami są liczby 1, 3, 4, 5 i 9; niereszty to liczby 2, 6, 7, 8 i 10:
$1^2 \equiv 10^2 \equiv 1 \pmod{11}$, $2^2 \equiv 9^2 \equiv 4 \pmod{11}$, $3^2 \equiv 8^2 \equiv 9 \pmod{11}$, $4^2 \equiv 7^2 \equiv 5 \pmod{11}$, $5^2 \equiv 6^2 \equiv 3 \pmod{11}$

$\ldots$ i wreszcie dla modułu $p = 23$ kwadratowymi $\ldots$

$\ldots$ resztami są liczby 1, 2, 3, 4, 6, 8, 9, 12, 13, 16 i 18; pozostałe liczby(z zakresu 5–22) są niereszta mi.
(sprawdź wszystkie kongruencje modulo 23!)

Reszty i niereszty kwadratowe dla modułu złożonego

Dla złożonego modułu, na przykład dla $m = 15$, kongruencje kwadratowe mają postacie

$$1^2 \equiv 4^2 \equiv 11^2 \equiv 14^2 \equiv 1 \pmod{15}$$

$$2^2 \equiv 7^2 \equiv 8^2 \equiv 13^2 \equiv 4 \pmod{15}$$

Tak więc resztami kwadratowymi są tylko liczby 1 i 4!
Wszystkie pozostałe reszty z przedziału 2–13 są nieresztami kwadratowymi.

Reszty i niereszty kwadratowe – ile ich jest?

. . . twierdzenie

Kongruencja kwadratowa z modułem $p > 2$ ma dokładnie $\frac{p-1}{2}$ reszt kwadratowych i taką samą liczbę niereszt kwadratowych.

dowód: wystarczy rozważyć $p-1$ kongruencji:
$x^2 \equiv 1 \pmod{p}$, $x^2 \equiv 2 \pmod{p}$, $\ldots$, $x^2 \equiv p-1 \pmod{p}$.
Każda z nich albo nie ma rozwiązania, albo ma dwa rozwiązania:
są to liczby $1^2 \pmod{p}$, $2^2 \pmod{p}$, $\ldots$, $\left(\frac{p-1}{2}\right)^2 \pmod{p}$. $\square$.

. . . i jeszcze jedno twierdzenie

Kongruencja kwadratowa z modułem $p > 2$ ma $N(p)$ *par (kolejnych liczb)* będących resztami kwadratowymi.

$$N(p) = \frac{1}{4}\left(p - 4 - (-1)^{(p-1)/2}\right).$$

Reszty i niereszty kwadratowe – weryfikacja

dla modułu $p = 23$ kwadratowymi . . .

. . . resztami są liczby 1, 2, 3, 4, 6, 8, 9, 12, 13, 16 i 18; pozostałe liczby 5, 7, 10, 11, 14, 15, 17, 19, 20, 21 i 22 są nieresztami. Jednych i drugich jest $(23 - 1)/2 = 11$.
Wartość $N(23) = 5$; te 5 kolejnych reszt kwadratowych to dwójki: (1,2), (2,3), (3,4), (8,9) i (12,13).

Kryterium Eulera

Dla $p > 2$ liczba $a \perp p$ jest resztą kwadratową modulo p wtedy i tylko wtedy gdy

$$\boxed{a^{(p-1)/2} \equiv 1 \pmod{p}.}$$

(Dowód podamy przy małym twierdzeniu Fermata.)

Symbol Legendre'a i symbol Jacobiego

definicja – Legendre

Dla p będącego liczbą pierwszą nieparzystą i $a \in \mathbb{Z}$, $a \perp p$ wprowadzamy symbol Legendre'a:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{gdy } a \text{ jest resztą kwadratową modulo } p, \\ -1, & \text{gdy } a \text{ jest nieresztą kwadratową modulo } p. \end{cases}$$

(Używa się też notacji $a \in Q_p$ – reszta; $a \in \overline{Q_p}$ – niereszta.)

przykład – Legendre

Dla $p = 11$ resztami kwadratowymi są liczby 1, 3, 4, 5, 9; nieresztami – 2, 6, 7, 8, 10. Dlatego

$$\left(\frac{1}{11}\right) = \left(\frac{3}{11}\right) = \left(\frac{4}{11}\right) = \left(\frac{5}{11}\right) = \left(\frac{9}{11}\right) = 1$$

$$\left(\frac{2}{11}\right) = \left(\frac{6}{11}\right) = \left(\frac{7}{11}\right) = \left(\frac{8}{11}\right) = \left(\frac{10}{11}\right) = -1$$

Własności symbolu Legendre'a

Dla p będącego liczbą pierwszą nieparzystą oraz $a, b \in \mathbb{Z}$, $a, b \perp p$ zachodzi

1. $$a \equiv b \pmod{p} \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right).$$
2. $$\left(\frac{a^2}{p}\right) = 1 \quad \text{na przykład} \quad \left(\frac{1}{p}\right) = 1.$$
3. $$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p} \quad \text{(kryterium Eulera)}.$$
4. $$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right).$$
5. $$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}.$$

Własności symbolu Legendre'a, c.d.

Pierwsze trzy własności są oczywiste i bardzo łatwe do wykazania. Piąta również – jest to kryterium Eulera dla $a = -1$. Dla udowodnienia własności (4) też korzystamy z kryterium Eulera:

$$\left(\frac{ab}{p}\right) \equiv (ab)^{(p-1)/2} (\mathrm{mod}\ p) \equiv a^{(p-1)/2} b^{(p-1)/2} (\mathrm{mod}\ p) \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) (\mathrm{mod}\ p).$$

Wartości wszystkich symbolów to ± 1, stąd z kongruencji wynika zwykła równość.

Z własności tych wynika ważny praktyczny ...

... wniosek:

Dla p będącego liczbą pierwszą nieparzystą zachodzi

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{gdy } p \equiv 1 \pmod 4, \\ -1, & \text{gdy } p \equiv 3 \pmod 4. \end{cases}$$

Dowód korzysta znowu z kryterium Eulera. Na przykład, pierwsza część alternatywy: $p = 4n + 1 \quad \rightarrow \quad (-1)^{(p-1)/2} = (-1)^{2n} = 1$ i analogicznie dla $p = 4n + 3$.

Obliczanie symbolu Legendre'a

na przykład – czy kongruencja $x^2 \equiv 63 \pmod{11}$ ma rozwiązanie?

Obliczamy: $\left(\frac{63}{11}\right) \overset{(1)}{=} \left(\frac{8}{11}\right) \overset{(4)}{=} \left(\frac{2}{11}\right)\left(\frac{2^2}{11}\right) \overset{(2)}{=} \left(\frac{2}{11}\right) \cdot 1 = -1$, gdzie ostatnie przejście wymaga przeanalizowania układu reszt modulo 11. Kongruencja nie ma rozwiązania.

Metoda (lemat) Gaussa obliczania symbolu Legendre'a

Dla p będącego liczbą pierwszą nieparzystą i liczby a, $a \perp p$ tworzymy zbiór $\left\{a, 2a, \ldots, \frac{p-1}{2}a\right\}$

i sprawdzamy dla ilu z tych liczb najmniejsza (co do wartości bezwzględnej) reszta z dzielenia przez p jest ujemna.
Liczbę tych ujemnych reszt oznaczamy ω. Mamy:

$$\left(\frac{a}{p}\right) = (-1)^{\omega}.$$

Dowód pozostawiamy jako zadanie do rozwiązanie (por.Yan).

Obliczanie symbolu Legendre'a

przykład – jeszcze raz kongruencja $x^2 \equiv 63 \pmod{11}$.

Dla obliczenia symbolu $\left(\frac{63}{11}\right) \overset{(1)}{=} \left(\frac{8}{11}\right)$ tworzymy układ reszt modulo 11

– układ pięciu $((p-1)/2 = 5)$ liczb: $\{1 \cdot 8, 2 \cdot 8, 3 \cdot 8, 4 \cdot 8, 5 \cdot 8\}$.
Obliczamy te i przekształcamy je w reszty najmniejsze, tzn. reszty kongruentne do nich modulo 11, ale zawarte w przedziale $[-5, +5]$.
mamy:

$\{8, 16, 24, 32, 40\} \pmod{11} \equiv \{8, 5, 2, 10, 7\}$
$\pmod{11} \equiv \{-3, 5, 2, -1, -4\} \pmod{11}$.

$\omega = 3$ — a więc jeszcze raz wykazaliśmy, że $\left(\frac{63}{11}\right) = -1$

– kwadratowa kongruencja nie ma rozwiązań.

Symbol Legendre'a dla $a = 2$

Z lematu Gaussa wynika kolejne ...

... twierdzenie:

Dla p będącego liczbą pierwszą nieparzystą

$$\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8} \begin{cases} 1, & \text{gdy } p \equiv \pm 1 \pmod 8, \\ -1, & \text{gdy } p \equiv \pm 3 \pmod 8. \end{cases}$$

Dowód pozostawiamy jako zadanie do rozwiązanie (por.Yan).

przykład – czy kongruencja $x^2 \equiv 2 \pmod 7$ ma rozwiązanie?

wystarczy obliczyć $\left(\frac{2}{7}\right)$. Ponieważ $7 \equiv -1 \pmod 8$ to $\left(\frac{2}{7}\right) = 1$ – kongruencja ma rozwiązanie – zresztą widać go jak na dłoni - ± 3.

Prawo wzajemności reszt kwadratowych

„Matematyka to królowa nauk,
a teoria liczb to królowa Matematyki".
Osiągnięciem, z którego Gauss był najbardziej dumny jest właśnie ...

... twierdzenie o wzajemności reszt kwadratowych

Dla p i q będących różnymi nieparzystymi liczbami pierwszymi zachodzi alternatywa

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right) \quad \text{jeżeli } p \equiv 1 \pmod 4 \quad \text{lub} \quad q \equiv 1 \pmod 4;$$
$$\left(\frac{p}{q}\right) = -\left(\frac{q}{p}\right) \quad \text{jeżeli } p \equiv 3 \pmod 4 \quad \text{i} \quad q \equiv 3 \pmod 4.$$

Alternatywne – bardziej kompaktne – sformułowanie to:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}.$$

Prawo to pozwala szybko obliczać wartości symbolu Legendre'a – oczywiście dla modułów p będących liczbami pierwszymi...

Symbol Jacobiego

definicja – Jacobi

Dla n będącego liczbą *złożoną i nieparzystą* o rozkładzie kanonicznym

$$n = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \dots {p_r}^{\alpha_r}$$

oraz liczby $a \in \mathbb{Z}$ wprowadzamy symbol Jacobiego:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \left(\frac{a}{p_2}\right)^{\alpha_2} \dots \left(\frac{a}{p_r}\right)^{\alpha_r},$$

gdzie $\left(\frac{a}{p_i}\right)$ oznacza symbol Legendre'a.

Symbol Jacobiego jest rozszerzeniem symbolu Legendre'a na przypadek modułów złożonych;
oczywiście dla $n = p$ symbol J to nic innego jak symbol L.

Własności symbolu Jacobiego

Dla m i n będących nieparzystymi liczbami całkowitymi oraz $a, b \in \mathbb{Z}$, $a, b \perp n$ zachodzi

1. $$a \equiv b \pmod{n} \implies \left(\frac{a}{n}\right) = \left(\frac{b}{n}\right).$$
2. $$\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right).$$
3. $$\text{dla } m \perp n \quad \left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$$
4. $$\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}.$$

Własności symbolu Jacobiego – ciąg dalszy

Dla m i n będących nieparzystymi liczbami całkowitymi oraz $a, b \in \mathbb{Z}$, $a, b \perp n$ zachodzi

5. $$\left(\frac{1}{n}\right) = 1.$$

6. $$\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}.$$

7. $$\text{dla } \; m \perp n \quad \left(\frac{m}{n}\right) = (-1)^{(m-1)(n-1)/4}\left(\frac{n}{m}\right).$$

8. $$\left(\frac{a_1 a_2 \dots a_r}{n}\right) = \left(\frac{a_1}{n}\right)\left(\frac{a_2}{n}\right)\dots\left(\frac{a_r}{n}\right)$$

9. $$\left(\frac{ab^2}{n}\right) = \left(\frac{a}{n}\right); \qquad \text{dla } \; a, b \perp n\,!$$

Własności symbolu Jacobiego

Przykład

$$\left(\frac{6}{35}\right) = \left(\frac{6}{5}\right)\left(\frac{6}{7}\right) = \left(\frac{1}{5}\right)\left(\frac{-1}{7}\right) = -1$$

— liczba 6 jest nieresztą kwadratową modulo 6

mieliśmy — Legendre

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{gdy } a \text{ jest resztą kwadatową modulo } p, \\ -1, & \text{gdy } a \text{ jest nieresztą kwadatową modulo } p. \end{cases}$$

Mamy – Jacobi

$$\left(\frac{a}{n}\right) = \begin{cases} 1, & \text{gdy } a \text{ jest } \textit{lub nie jest} \text{ resztą kwadatową modulo } n, \\ -1, & \text{gdy } a \text{ jest nieresztą kwadatową modulo } n. \end{cases}$$

Własności symbolu Jacobiego

A więc symbol Jacobiego, obliczany podobnie jak symbol Legendre'a dostarcza jednoznacznej informacji o *niemożności* rozwiązania kwadratowej kongruencji $x^2 \equiv a \pmod{n}$ – kiedy jego wartość jest równa -1;
natomiast dla wartości równej $+1$ sprawa pozostaje otwarta ...

... na przykład

$$\left(\frac{1009}{2307}\right) \overset{(J7)}{=} \left(\frac{2307}{1009}\right) \overset{(J1)}{=} \left(\frac{289}{1009}\right) \overset{(J2)}{=} \left(\frac{17^2}{1009}\right) \overset{(J9)}{=} 1.$$

w praktyce symbol J jest wykorzystywany do obliczeń („na skróty") symbolu L:

$$\left(\frac{335}{2999}\right) \overset{(J7)}{=} -\left(\frac{2999}{335}\right) \overset{(J1)}{=} -\left(\frac{-16}{335}\right) \overset{(J2)}{=} -\left(\frac{-1 \cdot 4^2}{335}\right) \overset{(J9)}{=} -\left(\frac{-1}{335}\right) = 1.$$

Ponieważ moduł (wyjściowy !) był liczbą pierwszą obliczona wartość (według reguł dla s. J.) pokrywa się z wartością symbolu L.)