Pierwiastki pierwotne, logarytmy dyskretne

Kongruencje – wykład 7

Definicja

Jeżeli rząd elementu a modulo n (dla n będącego liczba naturalną i całkowitego a, $a \perp n$) wynosi $\phi(n)$ to a nazywamy *pierwiastkiem pierwotnym* modulo n.

Przykład

Czy 7 jest pierwiastkiem pierwotnym modulo 45? Zachodzi $7 \perp 45$.
Mamy też $\phi(45) = \phi(3^2 \cdot 5) = 45(2/3)(4/5) = 24$.
Nasze pytanie – czy $\mathrm{ord}_{45}7 = 24$?
Liczymy modulo 45:
$7^1 \equiv 7;\ 7^2 \equiv 4;\ 7^3 \equiv 28;\ 7^4 \equiv 16;\ 7^5 \equiv 22;\ 7^6 \equiv 19;\ 7^7 \equiv -2;$
$7^8 \equiv -14;\ 7^9 \equiv -8;\ 7^{10} \equiv -11;\ 7^{11} \equiv -22;\ 7^{12} \equiv 1 \pmod{45}$.
Odpowiedź negatywna. Można sprawdzić, że 7 jest na przykład pierwiastkiem pierwotnym modulo 46.

Dla naszego ulubionego $p = 13$ pierwiastkami pierwotnymi są liczby: 2, 6, 7, 11. Ogólnie, dla modułu będącego liczbą złożoną m powinno („twierdzenie o dzielnikach") istnieć $l = \phi(\phi(m))$ pierwiastków pierwotnych. Dla $m = p$ będziemy mieć $l = \phi(p-1)$.
Rzeczywiście, $\phi(12) = 12(1/2)(2/3) = 4$.

Pierwiastki pierwotne . . .

. . . nie muszą istnieć dla każdego modułu. Na przykład, dla $m = 15$ mamy $\phi(15) = \phi(3 \cdot 5) = 8$, a każda reszta a, względnie pierwsza z 15, (a więc $\pm 1, \pm 2, \pm 4, \pm 7$), spełnia równanie $x^4 \equiv 1 \pmod{15}$.
To oczywiście konsekwencja . . .

. . . faktu, że często zachodzi $\lambda(m) < \phi(m)$.

Jeżeli prześledzić definicję λ to widać jasno, że nie mamy szans na pierwiastki pierwotne dla modułów, które *nie* mają postaci typu

$$m = 2, 4, p^\alpha \text{ i } 2p^\alpha,$$

bo tylko dla takich modułów zachodzi równość $\lambda(m) = \phi(m)$.
Dla $m = 2^\alpha$, $\alpha \geqslant 3$ albo dla $m = 2^\alpha {p_1}^{\alpha_1} \dots {p_k}^{\alpha_k}$, gdzie $\alpha \geqslant 2$ i $k \geqslant 2$ *nie istnieją pierwiastki pierwotne* modulo m.

Mimo, że potrafimy określić dla jakich liczb istnieją pierwiastki pierwotne nie są znane żadne efektywne metody ich szukania.

Pierwiastki pierwotne dla modułu p^2

$\phi(p^2) = p(p-1) \quad \rightarrow a^{p(p-1)} \equiv 1 \pmod{p^2}$ dla $a \perp p \ldots$
Przypuśćmy, że liczba r jest pierwiastkiem pierwotnym modulo p, a rząd r modulo p^2 wynosi d, czyli $r^d \equiv 1 \pmod{p^2}$, a więc musi zachodzić $d \mid p(p-1)$.
Mamy też $r^d \equiv 1 \pmod{p}$, a ponieważ r jest pierwiastkiem pierwotnym modulo p musi zachodzić $(p-1) \mid d$.
Daje to dwie możliwości: (a) $d = p-1$; (b) $d = p(p-1)$.
Ta druga oznacza, że *d jest pierwiastkiem pierwotnym modulo p^2*. A pierwsza?

$$r^{p-1} \equiv 1 \mod p^2 \tag{1}$$

Oznaczałoby to, że r *nie jest* p.p. modulo p^2. Gdyby jednak położyć

$$r_p = r + p; \qquad r_p \equiv r \pmod{p}$$

– a więc jest też p.p. modulo p. Ze wzoru dwumianowego mamy

$$r_p^{p-1} = r^{p-1} + \frac{p-1}{1} r^{p-2} p + \ldots,$$

gdzie wszystkie następne wyrazy zawierają już czynnik p^2, tak że

$$r_p^{p-1} \equiv r^{p-1} + p(p-1)r^{p-2} \pmod{p^2}.$$

Łącząc powyższe równanie z (1) dostajemy

$$r_p^{p-1} - 1 \equiv p(p-1)r^{p-2} \pmod{p^2}.$$

Z tego równania widać jasno, że r_p nie spełnia kongruencji (1), a więc jest pierwiastkiem pierwotnym modulo p^2. □.

Uwaga:

stosując metodę indukcji, łatwo wykazać, że takie r jest pierwiastkiem pierwotnym dla dowolnej potęgi modułu p.

Przykład:

Jaki jest pierwiastek pierwotny modulo $49 = 7^2$?
Dla $a = 3$ mamy $3^{\phi(7)} = 3^6 = 1 \pmod 7$, a więc p.p. modulo 7 jest 3.
Sprawdzamy kongruencję: $3^6 \not\equiv 1 \pmod{7^2}$, a więc 3 jest także p.p. modulo 7^2 (i wszystkich wyższych potęg siódemki).

Pierwiastki pierwotne tworzą układ reszt

Twierdzenie:

Dla $m \perp g$, gdzie g jest pierwiastkiem pierwotnym modulo m zbiór $\{g, g^2, g^3, \ldots, g^{\phi(m)}\}$ tworzy zredukowany układ reszt modulo m.

Dowód:

Te $\phi(m)$ liczby *nie mogą* przystawać do siebie parami modulo m. Rzeczywiście, jeżeli założyć dla $i > j$; $i \leqslant \phi(m)$
$g^i \equiv g^j \pmod{m}$ to – z uwagi na $g \perp m$ – możemy podzielić obie strony tej kongruencji przez r^j $g^{i-j} \equiv 1 \pmod{m}$, — co przeczy faktowi, że g jest pierwiastkiem pierwotnym (jego rząd wynosi $\phi(m)$).

Uwaga

Ponieważ $g^{\phi(m)} \equiv 1$ (tw. Eulera) to często podaje się układ zredukowanych reszt w równoważnej postaci $\{1, g, g^2, g^3, \ldots, g^{\phi(m)-1}\}$ – z jedynką przeniesioną z ostatniego miejsca na pierwsze.

Przykład: $m = 34$. Mamy $\phi(34) = \lambda(34) = \phi(2 \cdot 17) = 16$.
Zgodnie z poznanymi już twierdzeniami istnieje $\phi(\phi(34)) = 8$ pierwiastków pierwotnych. Sprawdźmy, że $g = 3$ jest takim pierwiastkiem:
$3^2 \equiv 9,\ 3^4 \equiv 13,\ 3^8 \equiv (-1),\ 3^{16} \equiv 1 \pmod{34}$;
w takim razie nasz zbiór to $\{g, g^2, \ldots, g^{\phi(m)}\} =$
$\{3, 3^2, 3^3, 3^4, 3^5, 3^6, 3^7, 3^8, 3^9, 3^{10}, 3^{11}, 3^{12}, 3^{13}, 3^{14}, 3^{15}, 3^{16}\}(\pmod{34})$
$= \{3, 9, 27, 81, 5, 15, 11, 33, 31, 25, 7, 21, 29, 19, 23, 1\}(\pmod{34})$ –
a po uporządkowaniu
$\{1, 3, 5, 7, 9, 11, 13, 15, 19, 21, 23, 25, 27, 29, 31, 33\}$.
Warto sprawdzić, jakie są pozostałe p.p. (5,7,11,23,27,29,31).
Dla ich kolejnych, szesnastu potęg, otrzymujemy też (ten sam) zredukowany układ reszt.

Indeksy – definicja

Ponieważ potęgi $\{g, g^2, g^3, \ldots, g^{\phi(m)}\}$ lub $\{1, g, g^2, g^3, \ldots, g^{\phi(m)-1}\}$ pierwiastków pierwotnych (N.B. – wybieramy tę druga konwencję) tworzą zredukowany układ reszt modulo m każda liczba a względnie pierwsza z m spełnia

$$a \equiv g^i \pmod{m}; \quad a \perp m; \quad 0 \leqslant i \leqslant \phi(m) - 1.$$

Wykładnik i dla którego spełniona jest ta kongruencja nazywamy *indeksem a przy podstawie g modulo m*, albo *logarytmem dyskretnym a przy podstawie g modulo m* i oznaczamy $\mathrm{ind}_g(a)$ (pomijamy zwykle moduł m, chociaż jest też w użyciu oznaczenie $\mathrm{ind}_{g,m}(a)$; innym oznaczeniem jest $\log_g a$).
Oczywiście zachodzi $a \equiv g^{\log_g a} \pmod{m}$
– ta właśnie kongruencja usprawiedliwia nazwę *logarytm dyskretny*.
Obliczanie indeksów jest problemem ciągle nie do końca rozwiązanym – tzn. istniejące algorytmy heurystyczne są nieefektywne – stąd zastosowania w kryptografii.

Indeksy – własności

Twierdzenie

Niech g będzie pierwiastkiem pierwotnym modulo m i niech a i b będą liczbami całkowitymi, względnie pierwszymi z m: $(a, m) = (b, m) = 1$. Wówczas zachodzi:

1. $\text{ind}_g(1) \equiv 0 \pmod{\phi(m)}$;
2. $\text{ind}_g(ab) \equiv \text{ind}_g(a) + \text{ind}_g(a) \pmod{\phi(m)}$;
3. $\text{ind}_g(a^k) \equiv k \cdot \text{ind}_g(a) \pmod{\phi(m)}$; k – liczba całkowita.
4. Dla *dowolnych* liczb całkowitych x, y $g^x \equiv g^y \pmod{m}$ wtedy i tylko wtedy gdy $x \equiv y \pmod{\phi(m)}$.

Prosty dowód: $x \equiv y \pmod{\phi(m)} \quad \rightarrow x = y + h\phi(m)$
stąd (rachunki $\pmod{m}$)

$$g^x \equiv g^{x=y+h\phi(m)} \equiv g^y \left(g^{\phi(m)}\right)^k \equiv g^y \pmod{m}.$$

Indeksy – pożytki

Indeksy mogą służyć na przykład do rozwiązywania kongruencji, *pod warunkiem*, że ... dysponujemy *tablicami indeksów modulo m*. Na przykład dla modułu $m = 9$ mamy $\phi(m) = 6$; a $g = 2$ jest pierwiastkiem pierwotnym. Kolejne potęgi g przystają modulo 9 do: $1,\ 2,\ 4,\ 8,\ 16 \equiv 7,\ 32 \equiv 5,\ 64 \equiv 1$. Stąd indeksy liczb a względnie pierwszych z 9 to

Liczba a	1	2	4	5	7	8
Indeks $\mathrm{ind}_2(a)$	0	1	2	5	4	3

Aby rozwiązać kongruencję $7x \equiv 2 \pmod 9$
„logarytmujemy” ją stronami; mamy
$\mathrm{ind}_2(x) = \mathrm{ind}_2(2) - \mathrm{ind}_2(7) \equiv 1 - 4 \equiv 3 \pmod 6$
i z tabeli odczytujemy, że $x \equiv 8 \pmod 9$.

Indeksy – pożytki, c.d.

Dla modułu $m = 23$ pierwiastkiem pierwotnym jest na przykład $g = 5$; rzeczywiście $5^{22} \equiv 5^2 \cdot 5^4 \cdot 5^{16} \equiv 2 \cdot 4 \cdot 3 \equiv 1 \pmod{23}$.
Tabela indeksów, zbudowana dla 22 potęg piątki

Liczba a	1	2	3	4	5	6	7	8	9	10	11
Indeks $\mathrm{ind}_5(a)$	0	2	16	4	1	18	19	6	10	3	9

Liczba a	12	13	14	15	16	17	18	19	20	21	22
Indeks $\mathrm{ind}_5(a)$	20	14	21	17	8	7	12	15	5	13	11

pozwoli rozwiązać kongruencje takie jak na przykład:

$$\begin{aligned} 3x^5 &\equiv 11 \pmod{23} \quad \text{jedno rozwiązanie} \\ 3x^{14} &\equiv 2 \pmod{23} \quad \text{dwa rozwiązania} \\ 13^x &\equiv 5 \pmod{23} \quad \text{brak rozwiązań} \end{aligned}$$

Indeksy – pożytki, c.d.

W końcu zauważmy, że zabawy z indeksami pozwalają określić natychmiast (pod warunkiem, że mamy pod ręką tablice indeksów[1]) rząd dowolnej liczby a modulo m.

Ponieważ rząd a to najmniejsze x, będące rozwiązaniem $a^x \equiv 1 \pmod{m}$ to $x \cdot \mathrm{ord}_m a \equiv 0 \pmod{\phi(m)}$.

Stąd $x = \dfrac{\phi(m)}{d}$, gdzie $d = (\phi(m), \mathrm{ord}_m a)$.

Na przykład: dla modułu 23 indeksem liczby 3 jest 16 (tabela); mamy też $(22, 16) = 2$, stąd $\mathrm{ord}_{23} 3 = 22/2 = 11$.

[1] Na przykład monumentalne dzieło Karola Gustava Jacobiego: *Canon Arithmeticus sive Tabulae quibus exhibentur pro Singulis Numeris Primis vel Primorum Potestatibus infra 1000 Numeri ad Datos Indices et Indices ad Datos Numeros pertinentes. Berlin, Typis Academicis, 1839.*