Logarytmy dyskretne: Od podstaw do zastosowań

Patryk Doniec

Politechnika Krakowska

11 maja 2024

Spis treści

Rząd

Definicja: Rząd

Jeśli a jest elementem $\mathbb{Z}_n^*$, to rzędem a nazywamy najmniejsze $k \in \mathbb{N} : k > 0$, takie że:

$$a^k \equiv 1 \pmod{n}$$

Rząd a modulo n jest zwykle oznaczany $\mathrm{ord}_n(a)$.

Przykład:

Weźmy $n = 5$. Elementy $\{1, 2, 3, 4\} \in \mathbb{Z}_n^*$. Ponieważ:

- Dla $k = 1$: $1^k \equiv 1 \pmod{5}$, to $\mathrm{ord}_5(1) = 1$
- Dla $k = 4$: $2^k \equiv 1 \pmod{5}$, to $\mathrm{ord}_5(2) = 4$
- Dla $k = 4$: $3^k \equiv 1 \pmod{5}$, to $\mathrm{ord}_5(3) = 4$
- Dla $k = 2$: $4^k \equiv 1 \pmod{5}$, to $\mathrm{ord}_5(4) = 2$

Funkcja Eulera

Definicja: Funkcja Eulera

Niech $\varphi : \mathbb{N} \to \mathbb{N}$ będzie funkcją przypisującą liczbie n liczbę $k \in \{1, \ldots, n\}$ liczb względnie pierwszych z n:

$$\varphi(n) = \#\{k \in \{1, \ldots, n\} : \mathrm{NWD}(k, n) = 1\}$$

Funkcję φ nazywamy funkcją Eulera.

Twierdzenie: Własności funkcji Eulera

Niech $p \in \mathbb{N}$ będzie liczbą pierwszą, oraz niech $m, n \in \mathbb{N}$ będą liczbami względnie pierwszymi, wtedy:

$$\varphi(p) = p - 1$$

$$\varphi(mn) = \varphi(m)\varphi(n)$$

Pierwiastek pierwotny

Definicja: Pierwiastek pierwotny

Jeśli g jest elementem $\mathbb{Z}_n^*$ i jest spełniona równość:

$$\mathrm{ord}_n(g) = \varphi(n)$$

to mówimy, że g jest pierwiastkiem pierwotnym z n.

Twierdzenie: Warunek konieczny i dostateczny istnienia

Pierwiastek pierwotny z n istnieje wtedy i tylko wtedy, gdy n jest jedną z następujących liczb:

- potęgą liczb pierwszych nieparzystych: $n = p^k$, $k \in \mathbb{N}$
- podwojoną potęgą liczb pierwszych nieparzystych: $n = 2p^k$, $k \in \mathbb{N}$
- liczbą 2 i 4.

Pierwiastek pierwotny

Twierdzenie:

Jeśli istnieje pierwiastek pierwotny modulo n, to istnieje dokładnie $\varphi(\varphi(n))$ pierwiastków pierwotnych modulo n.

Twierdzenie:

Element g jest pierwiastkiem pierwotnym modulo n wtedy i tylko wtedy, gdy każdy element $\mathbb{Z}_n^*$ jest odpowiednią potęgą elementu g.

Pierwiastek pierwotny

Przykład:

Elementy $\mathbb{Z}_5^*$ to 1,2,3,4 i są one przystające odpowiednio do:

- $2^4 \pmod 5 \equiv 1 \pmod 5$
- $2^1 \pmod 5 \equiv 2 \pmod 5$
- $2^3 \pmod 5 \equiv 3 \pmod 5$
- $2^2 \pmod 5 \equiv 4 \pmod 5$

Patrząc na pierwszą kongruencję mamy spełnioną równość:

$$\mathrm{ord}_5(2) = \varphi(5)$$

Zatem 2 jest pierwiastkiem pierwotnym z 5.
Podobnie możemy sprawdzić, że 3 również jest pierwiastkiem pierwotnym z 5.

Zagadnienie logarytmu dyskretnego

Definicja: Logarytm dyskretny

Niech $a, b \in \mathbb{Z}_n^*$. Zagadnienie logarytmu dyskretnego polega na znalezieniu takiego $x \in \mathbb{N} : 0 \leqslant x < \varphi(n)$, które spełnia kongruencję:

$$b^x \equiv a \pmod{n}$$

Wykładnik x nazywa się logarytmem dyskretnym a przy podstawie b modulo n i oznacza:

$$x = \log_b(a)$$

Aby mieć pewność że liczba a ma dobrze określony logarytm dyskretny, zakłada się że podstawa b jest pierwiastkiem pierwotnym z liczby n.

Zagadnienie logarytmu dyskretnego

Twierdzenie: Własności logarytmów dyskretnych

Niech $\mathrm{ord}_n(b) = k$. Wtedy dla dowolnego $r \in \mathbb{Z}$, oraz dowolnych klas reszt a, c, dla których określone są dyskretne logarytmy do podstawy b mamy:

- $\log_b(ac) \equiv \log_b(a) + \log_b(c) \pmod{k}$
- $\log_b(a^r) \equiv r \log_b(a) \pmod{k}$

Przykład:

Weźmy $n = 557$, $b = 2$, oraz $a = 7$.
Będziemy poszukiwać takiego $x \in \mathbb{N} : 0 \leqslant x < \varphi(n)$, że:
$x = \log_2(7) \pmod{557}$, lub inaczej

$$2^x \equiv 7 \pmod{557}$$

Zagadnienie logarytmu dyskretnego

Metoda przeliczania:

Metoda przeliczania polega ona na sprawdzaniu czy dla kolejnych liczb $x = 0, 1, 2 \dots$ zachodzi równość.

Przykład:

Dla wybranych przez nas liczb, możemy obliczyć że równość zachodzi dla $x = 458$:

$$2^{458} \equiv 7 \pmod{557}$$

Metoda przeliczania:

Ogólnie w metodzie przeliczania należy wykonać $x - 1$ mnożeń modulo n.

Protokół Diffiego-Hellmana

Wymiana klucza Diffiego-Hellmana:

1. Użytkownicy **A** i **B** uzgadniają dużą liczbę pierwszą p, oraz liczbę g, która jest pierwiastkiem pierwotnym modulo p. Liczby p, g są znane publicznie.
2. **A** wybiera tajną liczbę $a \in \mathbb{N}$, oraz przesyła **B** wartość:
$$x \equiv g^a \pmod{p}$$
3. **B** wybiera tajną liczbę $b \in \mathbb{N}$, oraz przesyła **A** wartość:
$$y \equiv g^b \pmod{p}$$
4. Wspólnym tajnym kluczem jest teraz:
$$K \equiv g^{ab} \pmod{p}$$

Protokół Diffiego-Hellmana

Wymiana klucza Diffiego-Hellmana:

Jeżeli użytkownik **C** podsłuchiwał konwersację i zna p, g, x, y, będzie chciał obliczyć K.

$$K \equiv g^{ab} \pmod p$$

Aby to zrobić, **C** musi obliczyć jeden z wykładników a lub b.

Ponieważ g jest pierwiastkiem pierwotnym, jest to równoważne z obliczeniem jednego z logarytmów dyskretnych:

$$a = \log_g(x) \pmod p \quad , \quad b = \log_g(y) \pmod p$$

$$a = \log_g(g^a) \pmod p \quad , \quad b = \log_g(g^b) \pmod p$$

System ElGamala

System wymaga aby użytkownik posiadał zarówno klucz **publiczny** jak i klucz **prywatny**.

Zaszyfrowane wiadomości są ogólnie dostępne, natomiast deszyfrowanie jest możliwe tylko przez powołane osoby, które posiadają klucz prywatny.

System ElGamala

Algorytm generowania klucza w systemie ElGamala:

1. Użytkownik **A** wybiera liczbę pierwszą p, oraz liczbę g, która jest pierwiastkiem pierwotnym modulo p.
2. **A** wybiera również liczbę $k \in \mathbb{N} : 0 \leqslant k < p - 1$, służącą za klucz prywatny. Obliczana jest liczba:

$$x \equiv g^k \pmod{p}$$

3. Trójka (p, g, x) jest kluczem publicznym użytkownika **A**. Jest on dostępny dla wszystkich innych użytkowników.

System ElGamala

Algorytm generowania klucza w systemie ElGamala:

Odkrycie liczby k na podstawie znajomości jawnych liczb p, g, x wymaga rozwiązania zagadnienia logarytmu dyskretnego.

Podobnie jak w przypadku metody Diffiego-Hellmana:

$$k = \log_g(x) \pmod{p}$$

$$k = \log_g(g^k) \pmod{p}$$

System ElGamala

Algorytm szyfrowania w systemie ElGamala:

Użytkownik **B** chce przesłać użytkownikowi **A** wiadmość którą przekształcił na odpowiednik liczbowy M.

1. Użytkownik **B** wybiera liczbę $j \in \mathbb{N} : 0 \leqslant j < p - 1$, oraz oblicza:

$$C_1 \equiv g^j \pmod{p} \quad , \quad C_2 \equiv Mx^j \pmod{p}$$

2. Szyfrogramem wiadomości M jest $C = (C_1, C_2)$.

Przypomnijmy:

- Klucz publiczny użytkownika **A**: (p, g, x)

System ElGamala

Algorytm deszyfrowania w systemie ElGamala:

Użytkownik **A** może odszyfrować otrzymaną wiadomość używając swojego klucza prywatnego k.

$$C_2 C_1^{-k} \equiv (Mx^j)(g^{-jk}) \equiv (Mg^{jk})(g^{-jk}) \equiv M \pmod{p}$$

Przypomnijmy:

- Klucz publiczny użytkownika **A**: (p, g, x)
- $x \equiv g^k \pmod{p}$
- $C_1 \equiv g^j \pmod{p}$
- $C_2 \equiv Mx^j \pmod{p}$

System ElGamala

Przykład:

Załóżmy że użytkownik **B** chce przesłać wiadomość SZYFR, osobie z kluczem publicznym $(p, g, x) = (43, 3, 22)$, oraz kluczem prywatnym $k = 15$.

1. Odpowiednikiem SZYFR jest $M = [18, 25, 24, 5, 17]$
2. **B** wybiera $j = 23$ i oblicza:

$$\begin{aligned} C_1 &= g^j = 3^{23} \equiv 34 \pmod{43} \\ C_2 &= Mx^j = M \cdot 22^{23} \equiv M \cdot 32 \pmod{43} \\ C_2 &= [17, 26, 37, 31, 28] \end{aligned}$$

3. Zaszyfrowana wiadomość ma postać:

$$(C_1, C_2) = (34, [17, 26, 37, 31, 28])$$

System ElGamala

Przykład:

Użytkownik **A** używa klucza prywatnego $k = 15$ otrzymując:

$$C_2 C_1^{-k} \equiv C_2 \cdot 34^{-15} \equiv C_2 \cdot 39 \pmod{43}$$

$$\begin{aligned} C_2 \cdot 39 \pmod{43} &\equiv [663, 1014, 1443, 1209, 1092] \pmod{43} \\ &\equiv [18, 25, 24, 5, 17] \pmod{43} \end{aligned}$$

Zatem użytkownik **A** otrzymał oryginalną wiadomość M, której odpowiednikiem jest wiadomość SZYFR.

Algorytm Pohliga-Hellmana

Algorytm Pohliga-Hellmana:

Algorytm Pohliga-Hellmana polega na zredukowaniu zagadnienia logarytmu dyskretnego do analogicznego problemu w mniejszych grupach cyklicznych.

1. Zakładamy że szukamy logarytmu $x : b^x \equiv a$, w grupie rzędu n, oraz że liczba n ma rozkład postaci:

$$n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$$

2. Dla każdej liczby p_i występującej w rozkładzie n obliczamy trzy liczby:

$$n_{p_i} = \frac{n}{p_i^{\alpha_i}}, \quad b_{p_i} = b^{n_{p_i}}, \quad a_{p_i} = a^{n_{p_i}}$$

Algorytm Pohliga-Hellmana

Twierdzenie:

Załóżmy że dla każdego czynnika pierwszego p rozkładu liczby n, liczba $x(p)$ jest rozwiązaniem logarytmu dyskretnego:

$$b_p^{x(p)} \equiv a_p$$

Niech x będzie rozwiązaniem układu kongruencji:

$$x \equiv x(p) \pmod{p^\alpha}$$

dla p przebiegającego zbiór wszystkich liczb pierwszych p w rozkładzie n.
Wówczas x jest rozwiązaniem zagadnienia logarytmu dyskretnego:

$$b^x \equiv a$$

Algorytm Pohliga-Hellmana:

3. Obliczamy ciąg logarytmów dyskretnych $x(p_i)$, związanych z kolejnymi czynnikami pierwszymi p_i liczby n.
4. Rozwiązujemy układ kongruencji postaci:

$$x \equiv x(p_1) \pmod{p_1^{\alpha_1}}$$
$$\vdots$$
$$x \equiv x(p_k) \pmod{p_k^{\alpha_k}}$$

5. Otrzymane rozwiązanie x jest rozwiązaniem zagadanienia

$$b^x = a$$

w grupie cyklicznej rzędu n.

Algorytm Pohliga-Hellmana

Przykład:

Spróbujmy znaleźć logarytm dyskretny $x : 2^x \equiv 7 \pmod{181}$.

1. Dla grupy $\mathbb{Z}^*_{181}$, której rząd wynosi 180, mamy rozkład:

$$180 = 2^2 \cdot 3^2 \cdot 5^1$$

2. Obliczamy kolejno:
   - Dla $p_1 = 2^2$: $n_{p_1} = 45$, $b_{p_1} = 2^{45}$, $a_{p_1} = 7^{45}$
   - Dla $p_2 = 3^2$: $n_{p_2} = 20$, $b_{p_2} = 2^{20}$, $a_{p_1} = 7^{20}$
   - Dla $p_3 = 5^1$: $n_{p_3} = 36$, $b_{p_3} = 2^{36}$, $a_{p_1} = 7^{36}$
3. Następnie liczymy:
   - $b_{p_1} \equiv 162 \pmod{181}$, $a_{p_1} \equiv 19 \pmod{181}$
   - $b_{p_2} \equiv 43 \pmod{181}$, $a_{p_2} \equiv 132 \pmod{181}$
   - $b_{p_3} \equiv 59 \pmod{181}$, $a_{p_3} \equiv 1 \pmod{181}$

Algorytm Pohliga-Hellmana

Przykład:

4. Wyznaczenie logarytmu dyskretnego $2^x \equiv 7 \pmod{181}$, możemy sprowadzić do rozwiązania trzech zagadnień:

$$162^{x(2)} \equiv 19 \pmod{181}$$
$$43^{x(3)} \equiv 132 \pmod{181}$$
$$59^{x(5)} \equiv 1 \pmod{181}$$

5. Możemy obliczyć że logarymami dyskretnymi są:

$$x(2) = 3$$
$$x(3) = 6$$
$$x(5) = 0$$

Algorytm Pohliga-Hellmana

Przykład:

6. Zgodnie z twierdzeniem, szukany logarytm dyskretny x jest rozwiązaniem układu kongruencji:

$$x \equiv 3 \pmod{2^2}$$
$$x \equiv 6 \pmod{3^2}$$
$$x \equiv 0 \pmod{5^1}$$

7. Rozwiązując układ w oparciu o chińskie twierdzenie o resztach, mamy: $x = 15$

Algorytm małych i wielkich kroków

Opis algorytmu:

1. Zaczynamy od obliczenia najmniejszego $m \in \mathbb{Z}$, nie mniejszego niż $\sqrt{n}$:
$$m = \lceil \sqrt{n} \rceil$$
2. Następnie zakładamy że znaleźliśmy logarytm x i dzielimy go przez m, z resztą r:
$$x = k \cdot m + r, \quad 0 \leqslant r < m, k \in \mathbb{Z}$$
3. Podstawiając nasze x do równania $b^x = a$, otrzymujemy:
$$b^{km+r} = a$$
$$b^{km} = ab^{-r}$$

Algorytm małych i wielkich kroków

Opis algorytmu:

4. Elementy po lewej stronie równości $b^{km} = ab^{-r}$ tworzą zbiór wielkich kroków:

$$\mathbb{G} = \{b^{km} : k = 1, 2, \ldots\}$$

5. Elementy po prawej stronie równości $b^{km} = ab^{-r}$, wraz z indeksami r tworzą natomiast zbiór małych kroków:

$$\mathbb{B} = \{(ab^{-r}, r) : 0 \leqslant r < m\}$$

6. Istotą metody jest znalezienie takiego elementu $b^{km} \in \mathbb{G}$, który jest poprzednikiem w pewnej parze $(ab^{-r}, r) \in \mathbb{B}$.
7. Jeśli znajdziemy takie k i r, to: $x = km + r$

Algorytm małych i wielkich kroków

Przykład:

Weźmy ponownie $n = 557$, $b = 2$, oraz $a = 7$.

1. W pierwszej kolejności obliczamy $m = \lceil\sqrt{557}\rceil = 24$
2. Teraz wypiszemy elementy zbioru $\mathbb{B} = \{(ab^{-r}, r) : 0 \leqslant r < m\}$, oraz $\mathbb{G} = \{b^{km} : k = 1, 2, \dots\}$:
$$\mathbb{B} = [[7, 0], [282, 1], [141, 2], \dots, [12, 21], [6, 22], [3, 23]]$$
$$\mathbb{G} = [376, 455, 81, \dots, 15, 70, 141]$$
3. Pierwszy element $\mathbb{G}$, który pokrył się z poprzednikiem pary zbioru $\mathbb{B}$, to 141, o numerze $k = 19$ i odpowiada małemu krokowi z indeksem $r = 2$.
4. Otrzymujemy $x = k \cdot m + r = 19 \cdot 24 + 2 = 458$