Lista 15

Sunday, 25 June 2023 22:03

lista15

Lista 15

Zadanie 1. Wykonaj poniższe obliczenia modulo 3, 5, 15. Oznaczenie 62^{-1} oznacza element odwrotny do 62 mod m w odpowiednim $\mathbb{Z}_m$.

- $-(125 \cdot 18 + 32 \cdot 49)^{-1} \cdot (75 \cdot 27 - 16 \cdot 7) + (77 \cdot 22^{-1} - 18 \cdot 255)$;
- $15^7 - 343^{12} \cdot 241^4 + 175 \cdot 123 - (176^{-1})^4 \cdot 121^2$.

Zadanie 2. Rozpatrz działanie algorytmu Euklidesa na dwóch kolejnych liczbach Fibonacciego. Jak wygląda para liczb trzymanych po k-tym kroku? Udowodnij, że dla pary liczb (F_{n+1}, F_{n+2}) algorytm wykonuje przynajmniej n kroków.

Pokaż, że algorytm Euklidesa (w którym zastępujemy a przez $a \bmod b$, a nie a przez $a - b$) wykonuje $\mathcal{O}(\log(a) + \log(b))$ kroków.

Wskazówka: Pokaż, że w jednym kroku którąś z liczb zmniejsza się o połowę.

Zadanie 3. Uogólnij algorytm Euklidesa dla większej liczby liczb $m_1, m_2, \ldots, m_k$. Pokaż, że $\text{nwd}(m_1, \ldots, m_k) = \sum_{i=1}^{k} x_i m_i$ dla pewnych liczb całkowitych x_i.

Wskazówka: Rozważ, co zwraca algorytm Euklidesa dla dwóch liczb m_1 oraz $m_2 m_3 \cdots m_k$. Rekurencyjnie postępuj dla $m_2 m_3 \cdots m_k$.

Zadanie 4. Pokaż, że dla dodatnich całkowitych liczb a, b istnieją dokładnie dwie pary liczb całkowitych (x, y), takich że:

- $xa + yb = \text{nwd}(a, b)$ oraz
- $|x| < \frac{b}{\text{nwd}(a,b)}$, $|y| < \frac{a}{\text{nwd}(a,b)}$.

Pokaż ponadto, że w jednej z tych par x jest dodatnie, a y niedodatnie, zaś w drugiej odwrotnie.

Wskazówka: Wydziel najpierw przez $\text{nwd}(a, b)$.

Zadanie 5. Pokaż, że dla liczb $m_1, \ldots, m_k$ istnieją $x_1, \ldots, x_k$ całkowite, takie że

$$\text{nwd}(m_1, \ldots, m_k) = \sum_{i=1}^{k} x_i m_i$$

$$\sum_{i=1}^{k} |x_i| = \mathcal{O}\left(\left(\sum_{i=1}^{k} m_i\right)^2\right).$$

Możesz w swoim rozwiązaniu skorzystać z Zadania 3, nawet jeśli nie umiesz go zrobić.

Wskazówka: Można na palcach, podobnie jak w Zadaniu 4. Można też przez dokładniejszą analizę algorytmu z Zadania 3.

Zadanie 6. Oblicz nwd dla następujących par liczb. Przedstaw je jako kombinację liniową (o współczynnikach całkowitych) tych liczb.

$$\{743, 342\}, \{3812, 71\}, \{1234, 321\}.$$

Zadanie 7. Pokaż, że jeśli n, m są względnie pierwsze, to $\varphi(nm) = \varphi(n) \cdot \varphi(m)$.

Ile wynosi $\varphi(p^k)$, gdzie p jest liczbą pierwszą a $k \geq 1$? Określ, ile wynosi $\varphi(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k})$ dla $p_1, p_2, \ldots, p_k$—różnych liczb pierwszych.

Wskazówka: Pierwsza część: najprościej z Chińskiego Tw. o resztach; da się też „na palcach", ale nie jest to takie łatwe.

Zadanie 8. Oblicz φ dla następujących liczb: 7, 9, 27, 77, 143, 105. Możesz skorzystać z Zadania 7.

Zadanie 9 (* Nie liczy się do podstawy). Przypomnijmy, że chińskie twierdzenie o resztach mówi, że gdy $m_1, m_2, \ldots, m_k$ są parami względnie pierwsze, to naturalny homomorfizm z $\mathbb{Z}_{m_1 \cdot m_2 \cdots m_k}$ w $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \cdots \times \mathbb{Z}_{m_k}$ jest izomorfizmem.

Pokaż, że obrazem $\mathbb{Z}^*_{m_1 \cdot m_2 \cdots m_k}$ (czyli elementów odwracalnych w $\mathbb{Z}_{m_1 \cdot m_2 \cdots m_k}$) tego izomorfizmu jest $\mathbb{Z}^*_{m_1} \times \mathbb{Z}^*_{m_2} \times \cdots \times \mathbb{Z}^*_{m_k}$.

Zadanie 10. Podaj dowolne rozwiązanie w liczbach naturalnych poniższych układów równań.

$$\begin{cases} x \bmod 7 &= 1 \\ x \bmod 5 &= 4 \end{cases} \quad \begin{cases} x \bmod 9 &= 8 \\ x \bmod 11 &= 3 \end{cases} \quad \begin{cases} x \bmod 13 &= 3 \\ x \bmod 17 &= 11 \end{cases}.$$

Zadanie 11. Wyznacz najmniejszą liczbę naturalną, która przy dzieleniu przez 2, 3, 5, 7, 11 daje odpowiednio reszty 1, 2, 4, 6 i 10.

$x = 1 \pmod 2$

$x = 2 \pmod 3$

$x = 4 \pmod 5$

$x = 6 \pmod 7$

$x = 10 \pmod{11}$

1 element odwr. później zrobić

Zadanie 1. Wykonaj poniższe obliczenia modulo 3, 5, 15. Oznaczenie 62^{-1} oznacza element odwrotny do 62 mod m w odpowiednim $\mathbb{Z}_m$.

- $-(125 \cdot 18 + 32 \cdot 49)^{-1} \cdot (75 \cdot 27 - 16 \cdot 7) + (77 \cdot 22^{-1} - 18 \cdot 255)$;
- $15^7 - 343^{12} \cdot 241^4 + 175 \cdot 123 - (176^{-1})^4 \cdot 121^2$.

a) $-(125 \cdot 18 + 32 \cdot 49)^{-1} \cdot (75 \cdot 27 - 16 \cdot 7) + (77 \cdot 22^{-1} - 18 \cdot 255)$ $\qquad 22^{-1} = 1^{-1} = 1$

$\frac{12}{1+5+6}$

mod 3: $-(125 \cdot 18 + \overset{1568}{32 \cdot 49})^{-1} \cdot (75 \cdot 27 - \overset{112}{16 \cdot 7}) + (77 \cdot 22^{-1} - 18 \cdot 255)$

1566

$0 \quad 2 \quad 0 \quad 1 \quad \underbrace{2 \quad 0}_{2}$

$-(2^{-1}) \cdot 1 \qquad \cdot (-1) = 2$

$2^{-1} = 2 \qquad -2 = 1 \qquad 1 \cdot 2$

ostatecznie mamy: $2 + 2 =_3 4 =_3 1$

– Chińskie twierdzenie o resztach:

1. $x = 1 \pmod 2$
2. $x = 4 \pmod 5$
3. $x = 4 \pmod 7$

r – poszczególne reszty w równaniach

M – pomnożone dzielniki modulo bez aktualnego dzielnika

M^{-1} – odwrotność danej liczby w konkretnym przystawaniu

$r_1 = 1 \quad M_1 = 5 \cdot 7 = 35 \quad M_1^{-1} = 35^{-1} = 1^{-1} = 1 \pmod 2$ ← aby znaleźć liczbę odwrotną modulo wystarczy potęgować daną liczbę operację modulo, a następnie zobaczyć ile razy trzeba przemnożyć daną liczbę, żeby dostać po operacji modulo wynik 1

$r_2 = 4 \quad M_2 = 2 \cdot 7 = 14 \quad M_2^{-1} = 14^{-1} = 4^{-1} = 4 \pmod 5$

$r_3 = 4 \quad M_3 = 2 \cdot 5 = 10 \quad M_3^{-1} = 10^{-1} = 3^{-1} = 5 \pmod 7$

5 razy 3 = 15

15 % 7 = 1

– szukamy x ostatecznie

– wzór ogólny: $x = r_1 \cdot M_1 \cdot M_1^{-1} + \ldots + r_i \cdot M_i \cdot M_i^{-1} \pmod{r_1 \cdot r_2 \cdot \ldots \cdot r_i}$

– rozw: $x = 1 \cdot 35 \cdot 1 + 4 \cdot 14 \cdot 4 + 4 \cdot 10 \cdot 5 = 459 = 39 \pmod{2 \cdot 5 \cdot 7}$

Zadanie 10. Podaj dowolne rozwiązanie w liczbach naturalnych poniższych układów równań.

$$\begin{cases} x \bmod 7 &= 1 \\ x \bmod 5 &= 4 \end{cases} \quad \begin{cases} x \bmod 9 &= 8 \\ x \bmod 11 &= 3 \end{cases} \quad \begin{cases} x \bmod 13 &= 3 \\ x \bmod 17 &= 11 \end{cases}.$$

a) $r_1 = 1 \quad M_1 = 5 \quad M_1^{-1} = 5^{-1} = 3 \pmod 7$

$r_2 = 4 \quad M_2 = 7 \quad M_2^{-1} = 7^{-1} = 2^{-1} = 3 \pmod 5$

$x = 15 + 28 \cdot 3 = 99 = 29 \pmod{7 \cdot 5}$

b) $r_1 = 8 \quad M_1 = 11 \quad M_1^{-1} = 11^{-1} = 2^{-1} = 5 \pmod 9$

$r_2 = 3 \quad M_2 = 9 \quad M_2^{-1} = 9^{-1} = 5 \pmod{11}$

$x = 8 \cdot 11 \cdot 5 + 3 \cdot 9 \cdot 5 = 440 + 135 = 575 = 80 \pmod{11 \cdot 9}$

: Pierwsza część: najprościej z Chińskiego Tw. o resztach; da się też „na palcach", ale nie jest to

Zadanie 8. Oblicz φ dla następujących liczb: 7, 9, 27, 77, 143, 105. Możesz skorzystać z Zadania 7.

Zadanie 9 (* Nie liczy się do podstawy). Przypomnijmy, że chińskie twierdzenie o resztach mówi

– dla liczby pierwszej:

$\varphi(p) = \{k \in \mathbb{N}_+ : k < p\}$

– dla liczby będącej potęgą jednej innej liczby

$\varphi(p^k) = p^k - p^{k-1}$ ← ilość liczb w zbiorze

$\varphi(7) = \{1\ 2\ 3\ 4\ 5\ 6\}$

$\varphi(9) = \{1, 2, 4, 5, 7, 8\}$, $9 = 3^2$

$3^2 - 3^1 = 6$

$\varphi(27) = \{1, 2, 4, 5, 7, 8, 10, 11, \ldots, 17\}$, $27 = 3^3$

$3^3 - 3^2 = 27 - 9 = 18$

$\varphi(77) = \{1, 2, 3, 4, 5, 6, 8, 9, \ldots\}$

Zadanie 6. Oblicz nwd dla następujących par liczb. Przedstaw je jako kombinację liniową (o współczynnikach całkowitych) tych liczb.

$$\{743, 342\}, \{3812, 71\}, \{1234, 321\}.$$

743 342

$743 = 2 \cdot 342 + 59$

$342 = 59 \cdot 5 + 47$

$59 = 47 \cdot 1 + 12$

$47 = 12 \cdot 3 + 11$

$12 = 11 \cdot 1 + 1$ NWD

$11 = 1 \cdot 11 + 0$

KOMBINACJA LINIOWA LICZB:

$1 = 12 - 1 \cdot 11 = 12 - 1 \cdot (47 - 12 \cdot 3) = 12 - (47 - 3 \cdot (59 - 47 \cdot 1)) =$

$= 12 - (47 - 3(59 - (342 - 59 \cdot 5))) =$

$= 12 - (47 - 3(59 - (342 - 5(743 - 2 \cdot 342)))) =$

$(59 - 47)$

$(743 - 2 \cdot 342) - (342 - 59 \cdot 5)$

$(743 - 2 \cdot 342) \cdot 5$

$47 = 342 - 5 \cdot 59 = 342 - 5(743 - 2 \cdot 342)$

$59 = 743 - 2 \cdot 342$

$= [(\overset{x}{743} - 2 \cdot \overset{y}{342}) - (342 - 5(743 - 2 \cdot 342))] - [(342 - 5(743 - 2 \cdot 342) - 3(743 - 2 \cdot 342 - (342 - 5(743 - 2 \cdot 342)))] =$

$= \underbrace{x - 2y - (y - 5(x - 2y))}_{x - 2y - y + 5x - 10y = 6x - 13y} - [(\overbrace{y - 5(x - 2y)}^{y - 5x + 10y = 11y - 5x}) - 3(\overbrace{x - 2y - (y - 5(x - 2y))}^{x - 2y - 11y + 5x = 6x - 13y})] =$

$\underbrace{\qquad}_{y - 5x + 10y}$

$-18x + 39y$

$-(11y - 5x - 18x + 39y) = -(-23x + 50y) = 23x - 50y$

$6x - 13y + 23x - 50y = 29x - 63y = 29 \cdot 743 - 63 \cdot 342$