

Patryk Miciak 331542 Lista 4

Zad. 1.

$m, n \in \mathbb{N} \cup \{0\}$

$\text{lcm}(m, n) :$

jeśli $m < 1$ lub $n < 1$:

zwrócić 0

w.p.p. zwrócić $\left(\frac{m}{\text{gcd}(m, n)}\right) \cdot n$

Zad. 2.

$GCD(m[], i, k)$ \rightarrow tablica liczb m_1, \dots, m_n

jeśli $i = k$

zwrócić $m[i]$

w.p.p.

$$m[i+1] = \text{gcd}(m[i], m[i+1])$$

zwrócić $GCD(m, i+1, k)$

$LCM(m[], i, k)$

jeśli $i = k$

zwrócić $m[i]$

w.p.p.

$$m[i+1] = \text{lcm}(m[i], m[i+1])$$

zwrócić $LCM(m, i+1, k)$

Zad. 4.

$\text{gcd}(a, b)$:

jeśli $a = 0 \wedge b = 0$: bląd

jeśli $a = 0$: zwróci b

jeśli $b = 0$: zwróci a

jeśli $2 \mid a \wedge 2 \mid b$: zwróci $2 \cdot \text{gcd}\left(\frac{a}{2}, \frac{b}{2}\right)$

jeśli $2 \nmid a$: zwróci $\text{gcd}\left(\frac{a}{2}, b\right)$

jeśli $2 \nmid b$: zwróci $\text{gcd}\left(a, \frac{b}{2}\right)$

jeśli $a > b$: zwróci $\text{gcd}(a-b, b)$

w.p.p. zwróci $\text{gcd}(b-a, a)$

Złożoność: $O(\log_2 a + \log_2 b)$

(w najgorszym przypadku będziemy dzielić a i b na połówki)

Zad. 7.

$$a) xz \equiv yz \pmod{m_2} \quad (\Rightarrow x \equiv y \pmod{m}, z \neq 0)$$

\Rightarrow

$$xz \equiv yz \pmod{m_2}$$

$$xz - yz \equiv 0 \pmod{m_2}$$

$$z(x-y) \equiv 0 \pmod{m_2}$$

\Downarrow

$$\exists k \quad z(x-y) = km_2$$

$$x-y = km$$

\Downarrow

$$x-y \equiv 0 \pmod{m}$$

$$x \equiv y \pmod{m}$$

\Leftarrow

$$x \equiv y \pmod{m}$$

$$x-y \equiv 0 \pmod{m}$$

$$z(x-y) \equiv 0 \pmod{m_2}$$

$$xz \equiv yz \pmod{m_2}$$

$$b) x_2 \equiv y_2 \pmod{m} \Leftrightarrow x \equiv y \pmod{\frac{m}{\gcd(z, m)}}, \quad x, y, z, m \in \mathbb{Z}$$

$$\gcd(z, m) = az + bm$$

$$bm \equiv 0 \pmod{m} \Rightarrow x_2 \equiv \gcd(z, m) \pmod{m}$$

$$x_2 \equiv y_2 \pmod{m} \Leftrightarrow x_2 \equiv y_2 \pmod{m} \Leftrightarrow$$

$$\Leftrightarrow x \cdot \gcd(z, m) \equiv y \cdot \gcd(z, m) \pmod{m} \Leftrightarrow$$

$$\Leftrightarrow x \cdot \gcd(z, m) \equiv y \cdot \gcd(z, m) \pmod{m \cdot \gcd(z, m) \cdot \frac{1}{\gcd(z, m)}} \Leftrightarrow$$

$$\Leftrightarrow x \equiv y \pmod{\frac{m}{\gcd(z, m)}}$$

$$c) x \equiv y \pmod{m_2} \Rightarrow x \equiv y \pmod{m}$$

$$x - y \equiv 0 \pmod{m_2}$$

$$\exists k \quad x - y = km_2$$

||

$$m_2(x - y) \equiv 0 \pmod{m} \Rightarrow x \equiv y \pmod{m}$$

Zad. 12.

$$\gcd(27, 64) = \gcd(64, 25) = \gcd(27, 25) = 1$$

$$x_{\min} = ?$$

$$\begin{cases} x \equiv 11 \pmod{27} \\ x \equiv 12 \pmod{64} \\ x \equiv 13 \pmod{25} \end{cases}$$

$$M = 27 \cdot 64 \cdot 25$$

$$a_1 = 11$$

$$a_2 = 12$$

$$a_3 = 13$$

$$m_1 = 27 \cdot 25$$

$$m_2 = 64 \cdot 25$$

$$x = \sum_{i=1}^3 a_i c_i m_i$$

$$c_1 m_1 \equiv 1 \pmod{27}$$

$$c_1 \cdot 64 \cdot 25 \equiv 1 \pmod{27}$$

$$c_1 \cdot 7 \equiv 1 \pmod{27}$$

$$1 = 7 - 6 = 7 - (27 - 7 \cdot 3) = 27 + 7 \cdot 4$$

$$c_1 = 4 \quad (\text{nr. alg. Euklidova})$$

$$c_2 m_2 \equiv 1 \pmod{64}$$

$$675 \cdot c_2 \equiv 1 \pmod{64}$$

$$35 \cdot c_2 \equiv 1 \pmod{64}$$

$$c_2 = 11 \quad (\text{nr. alg. Euklidova})$$

64	35
35	29
29	6
6	5
5	1
1	0

$$1 = 6 - 5 = 6 - (29 - 4 \cdot 6) =$$

$$4 \cdot 29 - 10 \cdot 6 = -10 + 5(35 - 29) =$$

$$-6 \cdot 29 + 5 \cdot 35 = 5 \cdot 35 - 6(64 - 35) =$$
$$= 11 \cdot 35 + 6 \cdot 64$$

$$c_3 m_3 \equiv 1 \pmod{25}$$

$$1728 \cdot c_3 \equiv 1 \pmod{25}$$

$$c_3 \cdot 3 \cdot c_3 \equiv 1 \pmod{25}$$

$$c_3 = 17 \quad (\text{nr. alg. Euklidova})$$

$$1 = 25 - 3 \cdot 8$$

$$-8 \rightarrow 17$$

$$x = (11 \cdot 4 \cdot 64 \cdot 25 + 12 \cdot 11 \cdot 27 \cdot 25 + 13 \cdot 17 \cdot 64 \cdot 25) \pmod{M} =$$

$$= 547388 \pmod{43200} = \underline{\underline{22988}}$$

Patryk Maćay 331542 Lista 4

Zad. 14.

1) Zał. iż q_1, q_2, \dots, q_n to wszystkie liczby pierwsze postaci $3k+2$.

Zatem $q_1^2, q_2^2, \dots, q_n^2$ są postaci $3k+1$ ($bo (3k+1)^2 = 3(3k^2+6k+1)+1$).

Liczba $A = \left(\prod_{i=1}^n q_i^2\right) + 1$ jest postaci $3k+2$, ergo nie może mieć wszystkich dzielników pierwszych postaci $3k+1$, bo musiała by być postaci $3k+1$.

2 tego wynika, iż:

$$\exists q_i \in \{q_1, q_2, \dots, q_n\} \quad q_i = 3k+2 \quad | \quad q_i \mid A$$

Spóźnosc? Bo $q_i \neq 1$. Ergo liczba pierwszych postaci $3k+2$ jest niekoniecznie wiele.

2) Zał. iż q_1, q_2, \dots, q_n to wszystkie liczby pierwsze postaci $4k+3$.

Zatem $q_1^2, q_2^2, \dots, q_n^2$ są postaci $4k+1$ ($bo (4k+1)^2 = 4(4k^2+4k)+1$)

Liczba $A = \left(\prod_{i=1}^n q_i^2\right) + 2$ jest postaci $4k+3$.

Nie może mieć wszystkich dzielników pierwszych postaci $4k+1$, bo musiała by być postaci $4k+1$ oraz nie może znać wszystkich dzielników pierwszych postaci $4k+2$, bo nie jest parzysta.

2 tego wynika, iż:

$$\exists q_i \in \{q_1, q_2, \dots, q_n\} \quad q_i = 4k+3 \quad | \quad q_i \mid A$$

Spóźnosc? Bo $q_i \neq 2$. Ergo liczba pierwszych postaci $4k+3$ jest niekoniecznie wiele.