Lista 4

Zadanie 1

```
gcd(x,y):
    If y = 0
        Return x
    Return gcd(y, x mod y)

lcm(x,y):
    If x=0 or y=0
        Return 0
    Return (x / gcd(x,y))*y     // wykonując dzielenie jako pierwsze
                                // nie przekroczymy zakresu
```

Zadanie 2

```
gcd_arr(x[],k):     // k - liczba elementów w tablicy x[]
    If k < 2
        Error
    res = x[0]
    For i in 1,2 ... k-1
        res = gcd(x[i], res)
    Return res

lcm_arr(x[], k):
    If k < 2
        Error
    res = x[0]
    For i in 1,2 ... k-1
        res = lcm(x[i], res)
    Return res
```

Metody korzystają z algorytmów przedstawionych w zadaniu 1 oraz własności

- $\gcd(m_1, m_2, ..., m_k) = \gcd(...\gcd(\gcd(m_1, m_2), m_3)..., m_k)$
- $\mathrm{lcm}(m_1, m_2, ..., m_k) = \mathrm{lcm}(...\mathrm{lcm}(\mathrm{lcm}(m_1, m_2), m_3)..., m_k)$

Zadanie 8

(a) **Załóżmy, że $2^n - 1$ jest liczbą pierwszą.**

Załóżmy nie wprost, że n jest liczbą złożoną. Przedstawmy ją jako iloczyn dwóch liczb naturalnych większych od 1: $n = ak$.

$2^n - 1 = 2^{ak} - 1 = (2^a)^k - 1^k = (2^a - 1)(\sum_{i=0}^{k-1}(2^a)^i)$
Ponieważ $3 \leq 2^a - 1 < 2^n - 1, k > 1$ oraz $(2^a - 1)\Big|(2^n - 1)$ to otrzymujemy, że $(2^n - 1)$ jest liczbą złożoną. Sprzeczność.

(b) **Załóżmy, że $a^n - 1$ jest liczbą pierwszą**

$a^n - 1^n = (a-1)(\sum_{i=0}^{n-1} a^i)$

Ponieważ $a^n - 1$ jest liczbą pierwszą to musi zachodzić:

- $a - 1 = 1 \wedge \sum_{i=0}^{n-1} a^i > 2$

Mamy zatem $a = 2$

- $a - 1 > 2 \wedge \sum_{i=0}^{n-1} a^i = 1$

Czyli musiałoby $a > 3 \wedge \sum_{i=0}^{n-1} a^i = 1$.
Własność zachodziłaby tylko dla $n = 1$, ale sprzeczność z np. $a = 16$.

(c) **Załóżmy, że $2^n + 1$ jest liczbą pierwszą**

Załóżmy nie wprost, że n nie jest potęgą liczby 2. Musi zatem mieć jakiś czynnik pierwszy $s > 2$ i można zapisać $n = rs$, gdzie $1 \leq r < n$.

Wiemy, że $(a - b)\Big|(a^m - b^m)$.

Niech $a = 2^r, b = -1, m = s$, wtedy:
$(2^r + 1)\Big|(2^{rs} - (-1)^s)$

Ponieważ s jest nieparzyste:
$(2^r + 1)\Big|(2^{rs} + 1)$

Zatem:
$(2^r + 1)\Big|(2^n + 1)$

A skoro $2 < 2^r + 1 < 2^k + 1$, to $2^n + 1$ nie jest liczbą pierwszą. Sprzeczność.

Zadanie 12

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

Ponieważ $27 \perp 64, 27 \perp 25, 64 \perp 25$ to korzystamy z chińskiego twierdzenia o resztach.

$N = n_1 n_2 n_3 = 27 \cdot 64 \cdot 25 = 43200$

$N_i = \frac{N}{n_i}$

no.	b_i	n_i	N_i	x_i	$N_i b_i x_i$
1	11	27	1600	4	70400
2	12	64	675	11	89100
3	13	25	1728	17	381888

Elementy odwrotne:
$64 \cdot 25 \cdot x_1 \equiv 1 \pmod{27}$
$7 \cdot x_1 \equiv 1 \pmod{27}$
$x_1 = 4$

$27 \cdot 25 \cdot x_2 \equiv 1 \pmod{64}$
$35 \cdot x_2 \equiv 1 \pmod{64}$
$x_2 = 11$

$27 \cdot 64 \cdot x_3 \equiv 1 \pmod{25}$
$3 \cdot x_3 \equiv 1 \pmod{25}$
$x_3 = 17$

Zatem

$x = 70400 + 89100 + 381888 = 541388$
$x \equiv 541388 \pmod{43200}$
$x \equiv 22988 \pmod{43200}$

Czyli najmniejszą taką liczbą naturalną spełniającą układ kongruencji jest 22988.

Zadanie 13

Znaleźć najmniejsze $n \in \mathbb{N}$, takie że $2^n \equiv 1 \pmod{5 \cdot 7 \cdot 9 \cdot 11 \cdot 179}$.

Musi zachodzić

$$\begin{cases} 2^n \equiv 1 \pmod{5} \\ 2^n \equiv 1 \pmod{7} \\ 2^n \equiv 1 \pmod{9} \\ 2^n \equiv 1 \pmod{11} \\ 2^n \equiv 1 \pmod{179} \end{cases}$$

Znajdźmy najmniejsze n spełniające poszczególne kongruencje.

$$\begin{cases} 2^{n_1} \equiv 1 \pmod{5} & n_1 = 4 \\ 2^{n_2} \equiv 1 \pmod{7} & n_2 = 3 \\ 2^{n_3} \equiv 1 \pmod{9} & n_3 = 6 \\ 2^{n_4} \equiv 1 \pmod{11} & n_4 = 10 \\ 2^{n_5} \equiv 1 \pmod{179} & n_5 = 178 \end{cases}$$

Wystarczy teraz znaleźć $\operatorname{lcm}(4, 3, 6, 10, 178) = 5340$.

---

tags: `mdm`