

Zadanie 1

Mamy wóz NWW(a, b) = $\frac{a \cdot b}{NWD(a, b)}$

NWD(a, b):

```
if (b == 0) return a;
return NWD(b, a mod b)
```

taka kolejność
dużym minimalizuje
wykro wyjścia poza zakres

NWW(a, b):

```
if (a == 0 and b == 0)
    return 0;
return  $\left(\frac{a}{NWD(a, b)}\right) \cdot b$ 
```

Zadanie 2 mamy dano funkcje NWD($a_1 \dots a_k$) z zad. 1

NWD($a_1 \dots a_k$):

```
if (k < 2) return -1 // error
```

nwd := a_1

for $i = 2 \dots k$

```
nwd := NWD(nwd,  $a_i$ )
```

return nwd

Analogicznie dla NWW($a_1 \dots a_k$):

NWW($a_1 \dots a_k$)

```
if (k < 2) return -1 // error
```

nww := a_1

for $i = 2 \dots k$

```
nww := NWW(nww,  $a_i$ )
```

return nww

Zadanie 6

$$m = p_1^{m_1} \cdot p_2^{m_2} \cdots \cdot p_i^{m_i} \cdots ; n = p_1^{n_1} \cdot p_2^{n_2} \cdots \cdot p_j^{n_j} \cdots$$

a) \Rightarrow niech $k = \gcd(m, n)$. Założymy, że $\exists_{i,j} : k_j \neq \min(m_j, n_j)$
 $k = p_1^{k_1} \cdot p_2^{k_2} \cdots \cdot p_i^{k_i} \cdots$

1° gdy $k_j > \min(m_j, n_j)$. Bez straty ogólności
Skoro $k = \gcd(m, n)$, to $k \mid m$ (1)

$$\frac{m}{k} = p_1^{m_1 - k_1} \cdot p_2^{m_2 - k_2} \cdots \cdot p_j^{m_j - k_j} \cdots$$

$\frac{m}{k}$ jest więc postaci $m' \cdot \frac{1}{p_j^{k_j - m_j}}$, gdzie m' , $p_j^{k_j - m_j}$
naturalne

Mamy więc spójność z (1). ↴

$$\text{oraz } \gcd(m', p_j^{k_j - m_j}) = 1$$

2° gdy $k_j < \min(m_j, n_j)$: Bez straty ogólności
niech $m_j < n_j$

Skoro $k = \gcd(m, n)$ to $\nexists k' : k' > k \wedge (k' \mid m \wedge k' \mid n)$

weźmy $k' = p_1^{k_1} \cdot p_2^{k_2} \cdots \cdot p_j^{k_j + (\min(m_j, n_j) - k_j)}$, oczywiście $k' > k$

mamy również $k' \mid m \wedge k' \mid n$, bo $p_j^{m_j} \mid p_j^{m_j}$ oraz $p_j^{m_j} \mid p_j^{n_j}$

Wobec tego $k \neq \gcd(m, n)$ ↴, czyli $k_j \neq \min(m_j, n_j)$

A więc z 1° i 2° mamy $k_j = \min(m_j, n_j)$ w spójne z (x)

Tak więc $\forall_{i,j} : k_j = \min(m_j, n_j)$

\Leftarrow niech $k = p_1^{k_1} \cdot p_2^{k_2} \cdots \cdot p_n^{k_n}$ i $\forall i : k_i = \min\{m_i, n_i\}$

oczywiście jest, że $\forall i : p_i^{k_i} \mid p_i^{m_i} \wedge p_i^{k_i} \mid p_i^{n_i}$, czyli
 $k \mid m \wedge k \mid n$. (**)

Weźmy dowolne k_i i oznaczmy $k'_i = k_i + a$; ($k = p_1^{k_1} \cdots p_i^{k'_i} \cdots p_n^{k_n}$)
założymy bez straty og., że $m_i < n_i$, mamy więc:

$$\frac{m}{k'} = p_1^{m_1 - k_1} \cdot \underbrace{p_i^{m_i - k'_i}}_{= p_i^{m_i - k_i - a}} \cdots \cdot p_n^{m_n - k_n}$$

$k' \mid m$, bo $\frac{m}{k'}$ jest postaci $m' \cdot \frac{1}{p^a}$ gdzie

$m', p \in \mathbb{N}$ oraz $\text{NWD}(m', p) = 1$. Taka z dowolności

wybioru k_i wynika, że nie istnieje $k' > k$ t.ż. $k' \mid m, n$.

Z tego i z (**) wynika, że $k = \gcd(m, n)$

b) \Rightarrow niech $k = \text{lcm}(m, n) = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$

1° zał. że $\exists i : k_i < \max\{m_i, n_i\}$. zst. że (bez straty ogólnosci) $m_i < n_i$ \Leftrightarrow

skoro $k = \text{lcm}(m, n)$, to $n \mid k$:

$$\frac{k}{n} = p_1^{k_1-n_1} \dots p_i^{k_i-n_i} \dots$$

$\frac{k}{n}$ jest więc postaci $k' \cdot \frac{1}{p_i^{n_i-k_i}}$, gdzie $k' , p_i^{n_i-k_i} \in \mathbb{N}$ oraz $\gcd(k', p_i^{n_i-k_i}) = 1$. Jest to sprzeczne z $n \mid k$ \Leftrightarrow

2° zał. że $\exists i : k_i > \max\{m_i, n_i\}$. zst. że (bez straty ogólnosci) $m_i \leq n_i$

! $\exists k' : k' < k \wedge m, n \mid k'$. (1)

weźmy $k' = p_1^{k_1} \dots p_i^{k_i - (\max\{m_i, n_i\})} \dots$, oznacza to $k' < k$

mamy także $m \mid k'$ oraz $n \mid k'$, ponieważ

z $p_i^{m_i} \mid p_i^{\max\{m_i, n_i\}}$ oraz $p_i^{n_i} \mid p_i^{\max\{m_i, n_i\}}$.

Jest to sprzeczne z (1) \Leftrightarrow , wobec tego

Tak więc z 1° i 2° wynika, że $\forall i \quad k_i = \max\{m_i, n_i\}$ ■

\Leftarrow niech $k = p_1^{k_1} \dots p_m^{k_m}$, gdzie $\forall i \quad k_i = \max\{m_i, n_i\}$

wówczas $\forall i \quad p_i^{m_i} \mid p_i^{k_i}$ oraz $p_i^{m_i} \mid p_i^{k_i}$, czyli
 $m, n \mid k$

~~$\text{Jednak } k' = p_1^{k_1} p_2^{k_2} \dots p_i^{k_i-a} \dots$~~ , oznacza to $k' < k$

zatem $k'_i = k_i - a$. Dla każdego i duchne t. że $k'_i = k_i - a$

wtedy $p_i^{m_i} \mid p_i^{k_i-a}$ lub $p_i^{m_i} \mid p_i^{k_i-a}$
wobec tego $m \mid k'$ lub $n \mid k'$.

Z dowolności wyboru k_i wynika, że nie istnieje
 $k' < k$ t. że $m, n \mid k'$, wobec czego $k = \text{lcm}(m, n)$

gdzie $\text{lcm}(m, n) = p_1^{\min(n_1, m_1)} p_2^{\min(n_2, m_2)} \dots p_n^{\min(n_n, m_n)}$

$$\text{gdzie } \text{lcm}(m, n) = p_1^{\min(n_1, m_1)} p_2^{\min(n_2, m_2)} \dots p_n^{\min(n_n, m_n)}.$$

 ~~$\text{lcm}(m, n) = p_1^{\max(n_1, m_1)} p_2^{\max(n_2, m_2)} \dots p_n^{\max(n_n, m_n)}$~~
$$= p_1^{\max(n_1, m_1)} p_2^{\max(n_2, m_2)} \dots p_n^{\max(n_n, m_n)} =$$

$$= p_1^{n_1+m_1} p_2^{n_2+m_2} \dots p_n^{n_n+m_n} = m \cdot n$$

zadanie 7

a) $xz \equiv yz \pmod{mz} \iff mz \mid (xz - yz) \iff mz \nmid z(x-y)$
 $\iff m \mid (x-y) \iff x \equiv y \pmod{m}$

b) \Rightarrow zai. ze $xz \equiv yz \pmod{m} \Rightarrow m \mid z(x-y)$

$$\Rightarrow \frac{m}{\gcd(m,z)} \mid \frac{z}{\gcd(m,z)}(x-y) . \text{ Ponieważ } \frac{m}{\gcd(m,z)} \perp \frac{z}{\gcd(m,z)}$$

to $\frac{m}{\gcd(m,z)} \mid x-y$, czyli $x \equiv y \pmod{\frac{m}{\gcd(z,m)}}$

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

$$x = k_1 \cdot \frac{m}{\gcd(m,z)} + r \quad ; \quad y = k_2 \cdot \frac{m}{\gcd(m,z)} + r \quad / \cdot z$$

$$xz = k_1 \cdot \frac{\text{lcm}}{\text{mam}}(m,z) + r_2 \quad ; \quad y = k_2 \cdot \frac{\text{lcm}}{\text{mam}}(m,z) + r_2 \cdot z$$

czyli, ponieważ $m \mid \text{lcm}(m,z)$, $xz \equiv yz \pmod{m}$

c) $x \equiv y \pmod{mz}$, $x = k_1 \cdot m \cdot z + r = (k_1 \cdot z) \cdot m + r$
 $y = k_2 \cdot m \cdot z + r = (k_2 \cdot z) \cdot m + r$
czyli $x \equiv y \pmod{m}$

Zadanie 8

a) niech $2^n - 1$ - pierwsza.

Założ. że n -złożona czyli

$$\exists_{\substack{1 < i < n \\ 1 < k < n}} : k \cdot i = n$$

Mamy więc $2^n - 1 = (2^i)^k - 1^k =$
 $= (2^i - 1) \left(\sum_{j=0}^{k-1} (2^i)^j \cdot 1 \right)$, czyli

$2^n - 1$ jest złożone ↴

Wobec tego n -pierwsze

b) $a^n - 1^n = (a-1)(a^{n-1} + a^{n-2} + \dots + 1)$

jeżeli $a \neq 2$, to $(a-1) | a^n - 1$

$a-1$ musi więc być równe 1:

$$a-1 = 1 \Leftrightarrow a=2$$

b) M.d.c) $2^n + 1$ - pierwsze

niech $n = 2^a \cdot b$, b -nieparzyste
(każda liczba nat. da się przedstawić
w takiej postaci)

Założ. że n nie jest potęgą 2, czyli $b > 1$

niech $x = 2^{2^a}$, mamy więc $x^b + 1$ - pierwsze

$$x^b + 1^b = x^b - (-1)^b = (x+1)(x^{b-1} - x^{b-2} + \dots - x+1)$$

Mamy więc $(x+1) | x^{b-1} + 1$
czyli $(2^{2^a} + 1) | 2^n + 1$ ↴

wobec tego $b=1$ czyli n musi
być potęgą 2.

Zadanie 9

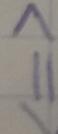
wykażmy, że $(p-2)! \equiv 1 \pmod{p}$

p jest pierwsze, więc mówimy ciało \mathbb{Z}_p

$(p-2)! = 2 \cdot 3 \cdot 4 \cdots (p-2)$ ← mówimy wszystkich elementów z \mathbb{Z}_p poza $(p-1) \cdot 1$.

Zauważmy, że wyniki ~~pośrodku~~ można pogrupować w pary postaci $\underbrace{a \cdot a^{-1} = 1}$. Wobec tego:

$$(p-2)! \equiv 1 \pmod{p}$$



$$(p-2)! = k \cdot p + 1, k \in \mathbb{N}$$

$$(p-1)! = (k \cdot p + 1)(p-1) = k \cdot p^2 + p(1-k) - 1$$

$$(p-1)! + 1 = p(k \cdot p + 1 - k)$$

wobec tego $p \mid (p-1)! + 1$ ■

Zadanie 12 27, 64, 25 sq wzgl. piensieć mieć konystancy z Ch. Tw. o resztach
 z (1) mamy: $x = 27 \cdot k_1 + 11$, $k_1 \in \mathbb{N}$

$$\left\{ \begin{array}{l} x \equiv 11 \pmod{27} \quad (1) \\ x \equiv 12 \pmod{64} \quad (2) \\ x \equiv 13 \pmod{25} \quad (3) \end{array} \right.$$

~~27 64 25 11 12 13~~

czyli $27k_1 \equiv 1 \pmod{64}$ (z (2))

można policzyć, że $18 \cdot 27 - 8 \cdot 64 = 1$, czyli $27^{-1} \equiv 13 \pmod{64}$

$$\text{wobei } \text{tego} \quad k_1 \equiv 19 \pmod{64} \Leftrightarrow k_1 = 64k_2 + 19.$$

$$x = 27(64k_2 + 19) = 1728k_2 + 524$$

$$1728k_2 + 524 \equiv 13 \pmod{25} \quad (2 \ (3))$$

$$1728 k_2 + 24 \equiv 13 \pmod{25}$$

$$1728 k_2 \equiv 14 \pmod{25}$$

~~17987,25~~ można policzyć, że $1 = 553 \cdot 25 - 8 \cdot 1728$

wobec tego $17 \cdot 28^{-1} \pmod{25} \equiv 17 \pmod{25}$, czyli

$$k_2 \equiv 13 \pmod{25} \iff k_2 = 25k_3 + 13, k_3 \in \mathbb{N}$$

$$x = 1728k_2 + 524 = 1728(25k_3 + 13) + 524 =$$

$= 27 \cdot 64 \cdot 25 k_3 + 524^{+22464}$ Tak więc najmniejsza

speñniajaca tñ ~~miem~~ ukad to $22464 + 524 = \underline{\underline{22988}}$