Zadanie 1. Szybka metoda obliczania $\mathrm{lcm}(m,n)$ dla $m,n \in \mathbb{N} \cup \{0\}$.

```
gcd(m,n):
    if a mod b == 0:
        return b:
    else:
        return gcd(b, a mod b)
```

```
lcm(m,n):
    if (a < 1) or (b < 1):
        return 0
    return a/gcd(m,n) * b
```

Aby otrzymać najmniejszą wspólną wielokrotność liczb $m,n \in \mathbb{N} \cup \{0\}$ możemy je przez siebie pomnożyć kompensując ze wzoru:

$$\mathrm{lcm}(m,n) = \frac{m \cdot n}{\gcd(m,n)},$$

jednak aby uniknąć wyjścia liczb poza zakres intów, przekształcamy go do postaci $\mathrm{lcm}(m,n) = \frac{m}{\gcd(m,n)} \cdot n$ (możemy bez straty ogólności założyć, że $m > n$, dzięki czemu nie musimy sprawdzać która liczba jest większa i powinna zostać podzielona).

Zadanie 2. Szybka metoda obliczania gcd oraz lcm liczb $\underbrace{m_1, m_2, \ldots, m_k}_{arr[]} \in \mathbb{N} \cup \{0\}$.

```
gcdarr(arr[], k):
    if k < 2: return error
    if k == 2: return gcd(arr[0], arr[1])
    result = arr[0]
    for (i = 1; i < k; i++)
        result = gcd(arr[i], result)
    return result.
```

```
lcmarr(arr[], k):
    if k < 2: return error
    if k == 2: return lcm(arr[0], arr[1])
    result = arr[0]
    for (i = 1, i < k; i++)
        result = lcm(arr[i], result)
    return result
```

Te algorytmy obliczają gcd / lcm tablicy arr[] poprzez obliczenie gcd / lcm pierwszych dwóch elementów (arr[0], arr[1]), a następnie poprzez powtarzanie obliczeń dla poprzedniego wyniku i następnego elementu z tablicy, aż do jej końca.

Zadanie 4. Opis algorytmu obliczającego gcd (a,b) z zależności:

- gcd (a,b) = gcd (a/2, b) : a parzyste, b nieparzyste
- gcd (a,b) = gcd (a-b, b) : a > b, a,b nieparzyste

gcd (a,b):

gcd (0,0) : error

gcd (a,0) : zwróć a

gcd (a,b) : a,b parzyste → zwróć 2 * gcd (a/2, b/2)

jeśli obie parzyste, to 2 jest wspólnym dzielnikiem

gcd (a,b) : a lub b parzyste : { a parzyste → zwróć gcd (a/2, b) ; b parzyste → zwróć gcd (a, b/2) }

gcd (a,b) : a i b nieparzyste : { a > b → zwróć gcd (a-b, b) ; b > a → zwróć gcd (b-a, a) }

Załóżmy, że pojedyncze przejście przez algorytm (sprawdzanie parzystości, dzielenie i odejmowanie) wykonuje się w czasie O(1), to złożoność algorytmu wynosi O(log₂ a + log₂ b), ponieważ w najgorszym przypadku będziemy dzielić a i b na zmiany przez 2.

Zadanie 8. Udowodnij zależności: (wskazówka: $a^n - b^n = (a-b)\left(\sum_i a^i b^{n-i-1}\right)$)

(a) jeśli $2^n - 1$ jest liczbą pierwszą, to n jest liczbą pierwszą:

Załóżmy nie wprost, że $2^n - 1$ jest liczbą pierwszą, ale n nie jest liczbą pierwszą. Niech $n = a \cdot b$ dla $a, b \in \mathbb{N}$, $a, b > 1$. Wtedy

$$2^n - 1 = 2^{ab} - 1 = (2^a)^b - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \ldots + 2^{a \cdot 0}),$$

zatem $2 \leq 2^a - 1 < 2^n - 1$, czyli $(2^a - 1)$ jest dzielnikiem $2^n - 1$. ■

(b) jeśli $a^n - 1$ jest liczbą pierwszą, to $a = 2$:

$$a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \ldots + a + 1) \Rightarrow (a-1) = 1, \text{ aby}$$

$a^n - 1$ było liczbą pierwszą, czyli $a - 1 = 1 \Rightarrow a = 2$ ■

(c) jeśli $2^n + 1$ jest liczbą pierwszą, to n jest potęgą liczby 2

Załóżmy nie wprost, że n nie jest potęgą 2. Weźmy więc $n = 2^{a}b$, wtedy $2^n + 1 = 2^{2^a b} + 1 = (2^{2^a})^b + 1$. Niech $x = 2^{2^a}$, wtedy $x^b + 1 = x^b - (-1) = (x+1)(x^{b-1} - x^{b-2} + \ldots - x + 1)$.

Skoro $x^b + 1$ możemy wyrazić jako iloczyn, to $2^n - 1$ nie jest liczbą pierwszą, gdy n nie jest potęgą 2. ■

Zadanie 9. Udowodnij, że jeśli p jest liczbą pierwszą, to p dzieli $((p-1)!+1)$. Wykaż najpierw, że $(p-2)! \equiv 1 \pmod p$.

WSKAZÓWKA:

$$(p-2)! \equiv 1 \pmod p \xRightarrow{\cdot(p-1)} (p-1)! \equiv (p-1) \pmod p \xRightarrow{+1} (p-1)!+1 \equiv p \pmod p \equiv 0$$

ROZWIĄZANIE:

Jeśli $x \in \{1, 2, \dots, p-1\}$, to istnieje $x^{-1} \pmod p$. Rozważmy:

$$x \equiv x^{-1} \pmod p \xRightarrow{\cdot x} x^2 \equiv 1 \pmod p \xRightarrow{-1} x^2 - 1 \equiv 0 \pmod p \Rightarrow$$

$$\Rightarrow (x-1)(x+1) \equiv 0 \pmod p \Rightarrow x = 1 \vee x = p-1.$$

Możemy podzielić pozostałe wyrazy $\{2, \dots, p-2\}$ w takie pary (a,b), że $ab \equiv 1 \pmod p$, a więc:

$$\underbrace{\prod_{i=1}^{p-1} i}_{(p-1)!} \equiv 1 \cdot (p-1) \cdot \prod_{i=2}^{p-2} i \equiv (p-1) \pmod p$$

■

Zadanie 12. Znajdź najmniejszy $x \in \mathbb{N}$ spełniający układ kongruencji

$$\begin{cases} x \equiv 11 \mod 27 \\ x \equiv 12 \mod 64 \\ x \equiv 13 \mod 25 \end{cases} \Rightarrow \begin{cases} b_1 = 11, n_1 = 27 \\ b_2 = 12, n_2 = 64 \\ b_3 = 13, n_3 = 25 \end{cases}$$

$NWD(27,64) = NWD(27,25) = NWD(64,25) = 1$, więc stosujemy chińskie twierdzenie o resztach. Obliczmy więc $N = n_1 n_2 n_3 = 43\,200$.

dane

b_i	N_i	x_i	$b_i N_i x_i$
11	$64 \cdot 25$	4	70 400
12	$27 \cdot 25$	11	89 100
13	$27 \cdot 64$	17	381 888

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

$$X = \sum_{i=1}^{3} b_i N_i x_i$$

x_i – odwrotność N_i

Obliczmy x_i i uzupełnijmy tabelę:

$64 \cdot 25 x_1 \equiv 1 \mod 27$

$7 x_1 \equiv 1 \mod 27$

$7 \cdot 4 \equiv 1 \mod 27$

$x_1 = 4$

$27 \cdot 25 x_2 \equiv 1 \mod 64$

$35 x_2 \equiv 1 \mod 64$

$35 \cdot 11 \equiv 1 \mod 64$

$x_2 = 11$

$27 \cdot 64 x_3 \equiv 1 \mod 25$

$3 x_3 \equiv 1 \mod 25$

$3 \cdot 17 \equiv 1 \mod 25$

$x_3 = 17$

$$X = \sum_{i=1}^{3} x_i N_i b_i = 70\,400 + 89\,100 + 381\,888 = 541\,388$$

$$X \equiv 541\,388 \mod N \equiv 541\,388 \mod 43200 = 22\,988$$

■

Zadanie 3. Rozszerzony algorytm Euklidesa dla $m_1, \dots, m_k$ liczb, $m_i \in \mathbb{N} \cup \{0\}$.

$$\gcd(\gcd(m_1, m_2, \dots, m_{k-1}), m_k) = y_1 m_k + y_2 \gcd(m_1, m_2, \dots, m_{k-1}) =$$

$$= y_1 m_k + y_2 (y_1 m_{k-1} + y_2 \gcd(m_1, \dots, m_{k-2})) =$$

$$= y_1 m_k + y_2 \cdot y_1 \cdot m_{k-1} + y_2 y_2 t \dots$$

Zadanie 5. Modyfikacja algorytmu binarnego gcd, aby $xa + yb = \gcd(a,b)$

1° $\gcd(0,b) = b$, czyli $x_1 = 0$, $y_1 = 1$

2° $\gcd(a,b) = 2 \cdot \gcd\left(\frac{a}{2}, \frac{b}{2}\right)$, $x_{n+1} = 2x_n$, $y_{n+1} = 2y_n$

3° $\gcd\left(\frac{a}{2}, b\right) \rightarrow x_{n+1} = x_n/2$, $y_{n+1} = y_n$

4° $\gcd\left(a, \frac{b}{2}\right) \rightarrow x_{n+1} = x_n$, $y_{n+1} = y_n/2$

5° $\gcd(a-b, b) \rightarrow x_{n+1} = x_n$, $y_{n+1} = y_n - x_n$

ad. 2° $2\gcd\left(\underbrace{a/2}_{a_{i+1}}, \underbrace{b/2}_{b_{i+1}}\right) = 2\left(x_{i+1} \cdot \underbrace{a/2}_{a_{i+1}} + y_{i+1} \underbrace{b/2}_{b_{i+1}}\right) =$

$$= x_{i+1} a_i + y_{i+1} b_i$$

ad. 3° $\gcd(a_i, b_i) = \gcd(a_i/2, b_i) = x_{i+1}(a_i/2) + y_{i+1} b_i$

ad. 5° $\gcd(a_i, b_i) = x_{i+1}(a_i - b_i) + y_{i+1} b_i = x_{i+1} a_i - x_{i+1} b_i + y_{i+1} b_i$

Zadanie 6. $(m_1, m_2, \dots)_p$, $(n_1, n_2, \dots)_p$

(a) $k = \gcd(m,n) \Leftrightarrow k_i = \min\{m_i, n_i\}$

($\Rightarrow$) $\exists k_j \neq \min\{m_j, n_j\}$

1° $k_j < \min\{m_j, n_j\}$ $k' = k \cdot p_j^{\min\{m_j,n_j\} - k_j}$, $k_j - n_j < 0$

$k' \mid m,n$, $k' > k$, $k \neq \gcd(m,n)$

2° $k_j > \min\{m_j, n_j\}$ $m_j > n_j$ $\frac{n}{k} = n' \frac{1}{p_j^{n_j - k_j}}$

($\Leftarrow$) $k \neq \gcd(m,n)$

1° $k \nmid m,n$

2° $\exists k'$ $k' > k \wedge k' \mid m,n$, $mn = \gcd(m,n) \cdot \operatorname{lcm}(m,n)$

$$p_1^{m_1+n_1} \cdot p_2^{m_2+n_2} \cdot \dots \cdot p_i^{m_i+n_i} = p_1^{(\min(m_1,n_1))} \cdot p_i^{(\min(m_i,n_i))} \cdot p_1^{(\max(m_1,n_1))} \cdot p_i^{(\max(m_i,n_i))}$$

L = P

Zadanie 7.

(a) $xz \equiv yz \pmod{mz} \iff x \equiv y \pmod{m}$, $z \neq 0$

$mz \mid xz - yz \Rightarrow mz \mid z(x-y) \Rightarrow m \mid (x-y) \Rightarrow x \equiv y \bmod m$

(b) $xz \equiv yz \pmod{m} \iff x \equiv y \pmod{\frac{m}{\gcd(z,m)}}$, $x, y, z, m \in \mathbb{Z}$

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

$x = k_1 \cdot \frac{m}{\gcd(m,z)} + r \qquad xz = m \cdot k_1 \frac{z}{\gcd(m,z)} + rz$

$y = k_2 \cdot \frac{m}{\gcd(m,z)} + r \qquad yz = m \cdot k_2 \underbrace{\frac{z}{\gcd(m,z)}}_{\in \mathbb{Z}} + rz$

($\Rightarrow$) $xz \equiv yz \pmod{m}$

$m \mid xz - yz \Rightarrow m \mid (x-y)z \quad \xrightarrow{\cdot \frac{1}{\gcd(m,z)}} \quad \underbrace{\frac{m}{\gcd(m,z)}}_{a} \mid (x-y)\underbrace{\frac{z}{\gcd(m,z)}}_{b}$

$\xrightarrow{a \perp b} \frac{m}{\gcd(m,z)} \mid x - y \Rightarrow xz \equiv yz \bmod m$

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

$\left.\begin{aligned} x &= (k_1 z)m + r \\ y &= (k_2 z)m + r \end{aligned}\right| \Rightarrow x \equiv y \pmod{m}$

Dlaczego $a^n - b^n = (a-b)\left(\sum_{i=0}^{n-1} a^i b^{n-i-1}\right)$?

$$(a-b)(a^{n-1}\cdot b^0 + a^{n-2}\cdot b^1 + \ldots + a^0 b^{n-1}) =$$

$$= a^n \underbrace{- a^{n-1}b^1 + a^{n-1}b^1}_{=0} \underbrace{- a^{n-2}b^2 + a^{n-2}b^2}_{=0} \underbrace{- a^{n-3}b^3 + a^{n-3}b^3}_{=0} + \underbrace{\ldots}_{=0} - a^0 b^n =$$

$$= a^n - b^n \blacksquare$$

Zadanie 10. Jaka jest liczba reszt modulo p^α spełniających równanie $x^2 \equiv 1 \pmod{p}$?

$$(x-1)(x+1) \equiv 0 \mod p^\alpha$$

1° $p > 2$: $p^\alpha \mid x-1$ lub $p^\alpha \mid x+1$

$x = 1$ $\qquad$ $x = p^\alpha - 1$

2° $p = 2$:

1° $\alpha = 1$: $x = 1$, więc 1 rozwiązanie

2° $\alpha = 2$: $x = 2^2 - 1$, $x = 2^2 + 1 \equiv 1 \mod 4$, więc 2 rozwiązania

3° $\alpha \geq 3$: $2^{\alpha-1} \mid (x-1) \Rightarrow 2 \mid (x+1)$ i $4 \nmid (x+1)$,

$x = 2^\alpha \pm 1 \vee x = 2^{\alpha-1} \pm 1$, więc 4 rozwiązania

Zadanie 11. Jak znajdę rozkład n wyznaczyć liczbę rozwiązań $x^2 \equiv 1 \mod n$?

$(x-1)(x+1) \equiv 0 \mod n$, [illegible] $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_k^{\alpha_k}$

$x^2 \equiv 1 \pmod{p_i^{\alpha_i}}$ ← dla każdego i $\iff x^2 \equiv 1 \pmod{n}$

...

zadanie do dokończenia (prawdopodobnie na 5. liście)

Zadanie 13. Najmniejsze $n \in \mathbb{N}$ takie, że $2^n \equiv 1 \mod 5 \cdot 7 \cdot 9 \cdot 11 \cdot 13$.

$$\begin{cases} 2^n \equiv 1 \mod 5 & n_1 = 4 \\ 2^n \equiv 1 \mod 7 & n_2 = 3 \\ 2^n \equiv 1 \mod 9 & n_3 = 6 \\ 2^n \equiv 1 \mod 11 & n_4 = 10 \\ 2^n \equiv 1 \mod 13 & n_5 = 12 \end{cases}$$

A więc liczymy lcm n_i, czyli:

lcm $(4,3,6,10,12) = 60$, co jest szukanym najmniejszym n. ■

Zadanie 14. Pokaż że istnieje nieskończenie wiele liczb pierwszych postaci:

(a) $3k+2$, $k \in \mathbb{N}$

Załóżmy, że istnieje skończona ilość liczb takiej postaci: $p_1, p_2, \dots, p_n$.

Niech $N = p_1 \cdot \dots \cdot p_n$, więc:

$3N+2$: w szczególności istnieje $p = 3k+2$

$p \mid 3N+2 \wedge p \mid N \Rightarrow p \mid 3N+2-3N \Rightarrow p \mid 2$

SPRZECZNOŚĆ ↯

Lemat: $\forall p \; \exists q \; (3p+1)^n = 3q+1$

$x \equiv 1 \pmod 3$

$x^n \equiv 1^n \pmod 3$

(b) $4k+3$ – analogicznie

$p \mid 4N+3 \wedge p \mid N \Rightarrow p \mid 4N+3-4N \Rightarrow p \mid 3$

SPRZECZNOŚĆ ↯

Zadanie 15. $d(k)$ – liczba dzielników k. Pokaż, że $\sum_{k=1}^{n} d(k) = n \ln n + O(n)$

$$\sum_{k=1}^{n} d(k) = n + \lfloor \tfrac{n}{2} \rfloor + \lfloor \tfrac{n}{3} \rfloor + \dots + \lfloor \tfrac{n}{n} \rfloor \leq$$

$$\leq n + \left(\tfrac{n}{2} + 1\right) + \left(\tfrac{n}{3} + 1\right) + \dots + \left(\tfrac{n}{n} + 1\right) =$$

$$= n \log n + O(n)$$ ■