Definicja

Liczbę $p \in \mathbb{N}$ nazywamy pierwszą, jeśli spełnia następujące warunki:

- $p \neq 1$,
- jeśli $a \in \mathbb{N}$ dzieli p, to $a = 1$ lub $a = p$.

Sito Eratostenesa

- Dane: $n > 1$.
- Wynik: Liczby pierwsze nie większe niż n.
- Algorytm:
    1. Wypisujemy liczby całkowite od 2 do n.
    2. Dla każdej nieskreślonej liczby od 2 do $\lfloor \sqrt{n} \rfloor$ (w tej kolejności) skreślamy wszystkie jej wielokrotności z wyjątkiem jej samej.
    3. Nieskreślone liczby są poszukiwanymi liczbami pierwszymi.

Przykład

Wyznaczymy liczby pierwsze nie większe niż 100.

	$\boxed{2}$	$\boxed{3}$	~~4~~	$\boxed{5}$	~~6~~	$\boxed{7}$	~~8~~	~~9~~	~~10~~
$\boxed{11}$	~~12~~	$\boxed{13}$	~~14~~	~~15~~	~~16~~	$\boxed{17}$	~~18~~	$\boxed{19}$	~~20~~
~~21~~	~~22~~	$\boxed{23}$	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	$\boxed{29}$	~~30~~
$\boxed{31}$	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	$\boxed{37}$	~~38~~	~~39~~	~~40~~
$\boxed{41}$	~~42~~	$\boxed{43}$	~~44~~	~~45~~	~~46~~	$\boxed{47}$	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	$\boxed{53}$	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	$\boxed{59}$	~~60~~
$\boxed{61}$	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	$\boxed{67}$	~~68~~	~~69~~	~~70~~
$\boxed{71}$	~~72~~	$\boxed{73}$	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	$\boxed{79}$	~~80~~
~~81~~	~~82~~	$\boxed{83}$	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	$\boxed{89}$	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	$\boxed{97}$	~~98~~	~~99~~	~~100~~

Wśród liczb od 1 do 100 jest 25 liczb pierwszych.

Definicja

Niech $n > 1$.
Niech $a_k, \dots, a_0 \in [0, n-1]$ oraz $k = 0$ lub $a_k > 0$.
Jeśli

$$a_k n^k + a_{k-1} n^{k-1} + \cdots + a_1 n + a_0 = m,$$

to piszemy

$$m = (a_k a_{k-1} \cdots a_1 a_0)_n$$

(mówimy, że $(a_k a_{k-1} \cdots a_1 a_0)_n$ jest przedstawieniem liczby m w systemie o podstawie n).

Przykłady

- $(10110011)_2 = 2^7 + 2^5 + 2^4 + 2 + 1 = 179$.
- $(375)_{10} = 375$.
- $(AF9)_{16} = 10 \cdot 16^2 + 15 \cdot 16 + 9 = 2809$.

Zamiana z systemu dziesiętnego

Algorytm

- Dane: $n > 1$ (podstawa systemu), $m \in \mathbb{N}_+$ (liczba w systemie dziesiętnym).
- Wynik: Liczby $a_k, \ldots, a_0 \in [0, n-1]$ takie, że $m = (a_k \cdots a_0)_n$.
- Algorytm:
  1. Definiujemy $q_0 := m$.
  2. Dopóki $q_i > 0$, definiujemy $a_i := q_i \bmod n$ oraz $q_{i+1} := q_i \operatorname{div} n$.

Przykład

Dla $n = 4$ i $m = 2021$ mamy:

$$\begin{array}{r|l} 2021 & 1 \\ 505 & 1 \\ 126 & 2 \\ 31 & 3 \\ 7 & 3 \\ 1 & 1 \\ 0 & \end{array}$$

Zatem

$$2021 = (133211)_4.$$

Wskazówki do zadań 6–8

Wskazówki

- Liczba zer kończących rozwinięcie liczby m w systemie podstawie n to maksymalna potęgą liczby n dzieląca liczbę m. [Oznaczamy tę wielkość $\nu_n(m)$.]
- Jeśli $n = p_1^{l_1} \cdots p_k^{l_k}$, gdzie $p_1, \ldots, p_k$ są parami różnymi liczbami pierwszymi, to
$$\nu_n(m) = \min \left\{ \nu_{p_1^{l_1}}(m), \ldots, \nu_{p_k^{l_k}}(m) \right\}.$$
- Jeśli p jest liczbą pierwszą, to $\nu_{p^l}(m) = \lfloor \frac{\nu_p(m)}{l} \rfloor$.
- Jeśli p jest liczbą pierwszą, to
$$\nu_p(k!) = \lfloor \tfrac{k}{p} \rfloor + \lfloor \tfrac{k}{p^2} \rfloor + \cdots .$$

Przykład

Ioma zerami kończy się rozwinięcie liczby 100! w systemie o podstawie 12?

Mamy $12 = 2^2 \cdot 3$.

Ponadto
$$\nu_2(100!) = \lfloor \tfrac{100}{2} \rfloor + \lfloor \tfrac{100}{2^2} \rfloor + \cdots = 50 + 25 + 12 + 6 + 3 + 1 = 97,$$
oraz
$$\nu_3(100!) = \lfloor \tfrac{100}{3} \rfloor + \lfloor \tfrac{100}{3^2} \rfloor + \cdots = 33 + 11 + 3 + 1 = 48.$$
Zatem
$$\nu_{12}(100!) = \min\{\nu_4(100!), \nu_3(100!)\} = \min \left\{ \lfloor \tfrac{\nu_2(100!)}{2} \rfloor, \nu_3(100!) \right\} = \min \left\{ \lfloor \tfrac{97}{2} \rfloor, 48 \right\} = 48.$$