Zadanie 3.7. Mnożenie liczb a, b (n-cyfrowych) poprzez rozbicie ich na części.

$T(n) \leq 5T\left(\frac{n}{3}\right) + O(n) \Rightarrow T(n) = O(n^{\log_3 5})$

$a(x) = a_0 + a_1 x + a_2 x^2$

$a = a_2 a_1 a_0$ (każdy blok długości $\frac{n}{3}$)

$a(x) = a = a_0 + a_1 \cdot 2^{\frac{n}{3}} + a_2 \cdot 2^{\frac{2n}{3}}$ ($x \to 2^{\frac{n}{3}}$, $x^2 \to 2^{\frac{2n}{3}}$)

$b(x) = b = b_0 + b_1 \cdot 2^{\frac{n}{3}} + b_2 \cdot 2^{\frac{2n}{3}}$

interesuje nas $a\left(2^{\frac{n}{3}}\right) \cdot b\left(2^{\frac{n}{3}}\right)$ ($w(x) = a(x) \cdot b(x)$)

INTERPOLACJA WIELOMIANU:

Dla dowolnych n par $(x_1, y_1), \ldots, (x_n, y_n) \in \mathbb{R}^2$ (dla takich $x_i = x_j \Rightarrow i = j$), istnieje dokładnie jeden wielomian P stopnia $\leq n$, taki że $P(x_i) = y_i$ dla każdego i.

$m_0 = a_0 b_0 = a(0) \cdot b(0)$

$m_1 = a_2 b_2 = \lim_{x \to \infty} \frac{a(x) b(x)}{x^4}$

$m_2 = (a_0 + a_1 + a_2)(b_0 + b_1 + b_2) = a(1) \cdot b(1)$

$m_3 = \ldots$

$m_4 = \ldots$

$w(x) = w_0 + w_1 x + w_2 x^2 + w_3 x^3 + w_4 x^4$

$$\underbrace{\begin{bmatrix} m_0 \\ m_1 \\ m_2 \\ m_3 \\ m_4 \end{bmatrix}}_{m} = \underbrace{\begin{bmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 1 & 1 \\ 1 & -1 & 1 & -1 & 1 \\ 1 & 2 & 4 & 8 & 16 \end{bmatrix}}_{A} \underbrace{\begin{bmatrix} w_0 \\ w_1 \\ w_2 \\ w_3 \\ w_4 \end{bmatrix}}_{w} \Rightarrow w = A^{-1} \cdot m$$

(A^{-1} istnieje dzięki interpolacji)

$T(n) \leq (2k-1) \cdot T\left(\frac{n}{k}\right) + O(n) \Rightarrow T(n) \leq O\left(n^{\log_k(2k-1)}\right)$

Zadanie 4.4.

$\gcd(a,b) = \gcd\left(\frac{a}{2}, b\right)$ gdy $2 \mid a$ i $2 \nmid b$.

$\gcd(a,b) = \gcd(a-b, b)$ gdy $a > b$ i $2 \nmid a$, $2 \nmid b$

Gdy liczby są parzyste, to dzielimy je na 2 dopóki jedna z nich nie będzie nieparzysta, wtedy działamy z zasadami powyższymi.

Zadanie 4.9 Twierdzenie Wilsona: $p \mid (p-1)! + 1$

$$(p-2)! \equiv_p 1 \xrightarrow{\cdot(p-1)} (p-1)! \equiv_p p-1 \xRightarrow{+1} (p-1)! + 1 \equiv_p p \equiv_p 0$$

Jeśli $x \in \{1, 2, \dots, p-1\}$ to istnieje $x^{-1} \bmod p$, rozważmy więc:

$x \equiv_p x^{-1}$, $x^2 \equiv_p 1$, wtedy $(x-1)(x+1) \equiv_p 0$, więc $x = 1 \vee x = p-1$.

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

Łączymy w pary i z $i^{-1} \pmod p$

$$\forall i \in \{2, \dots, p-2\}\ \exists j \in \{2, \dots, p-2\}\quad ij \equiv 1 \pmod p$$

Zadanie 4.10.

$x^2 \equiv 1 \pmod{p^\alpha}$

$(x-1)(x+1) \equiv 0 \pmod{p^\alpha}$

$p > 2$, więc nie może dzielić dwóch czynników jednocześnie, tzn. $x = 1 \vee x = p^\alpha - 1$

$p = 2$: $2^{\alpha-1} \mid x-1 \Rightarrow 2 \mid x+1$, ale $2^2 \nmid x+1$
$(\alpha \geq 3)$

$\alpha = 1 \Rightarrow x = 1$

$\alpha = 2 \Rightarrow x \equiv 2^2 - 1 \vee x \equiv 2^2 + 1 \Rightarrow x = 1 \vee x = 3$

$\alpha = 3 \Rightarrow x = 2^{\alpha-1} \pm 1 \Rightarrow x = 2^\alpha \pm 1 \Rightarrow$

$\Rightarrow x = 1 \vee x = 2^\alpha - 1 \vee x = 2^{\alpha-1} - 1 \vee x = 2^{\alpha-1} + 1$

Zadanie 4.8.a

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 $2 \leq 2^a - 1 < 2^n - 1$ jest dzielnikiem $2^n - 1$, czyli sprzeczność. ↯

Zadanie 4.1

Należy skorzystać z algorytmu Euklidesa (lżejszy jest „szybki"), a następnie wykorzystać własność $\operatorname{lcm}(m,n) = \frac{m \cdot n}{\gcd(m,n)} = \frac{m}{\gcd(m,n)} \cdot n$, aby uniknąć wyjścia poza zakres (np. int w C).

Zadanie 4.2.

$\operatorname{lcm}(a,b,c) = \frac{a \cdot \operatorname{lcm}(b,c)}{\gcd(a, \operatorname{lcm}(b,c))}$, więc algorytm z poprzedniego zadania nie jest za bardzo optymalny, jednak musimy go wykorzystać.