## Zadania z matematyki dyskretnej, lista nr 4

- 1. Zaproponuj szybką metodę obliczania lcm(m,n), gdzie  $m,n \in \mathbb{N} \cup \{0\}$ , która wyznacza poprawną wartość w każdym przypadku, gdy tylko liczba lcm(m,n) mieści się w określonym zakresie liczb całkowitych (np. integer w Pascalu).
- 2. Opisz szybką metodę obliczania  $\gcd(m_1, m_2, \cdots, m_k)$ , gdzie  $m_1, m_2, \dots, m_k \in \mathbb{N} \cup \{0\}$  i analogiczną dla lcm.
- 3. Zaproponuj szybką metodę obliczania dla danych liczb całkowitych  $m_1, m_2, \ldots, m_k$  takich współczynników całkowitych  $x_1, x_2, \ldots, x_k$ , że

$$x_1m_1 + x_2m_2 + \dots + x_km_k = \gcd(m_1, m_2, \dots, m_k).$$

- 4. (Binarny algorytm gcd) Opisz algorytm obliczający gcd(a, b) z zależności:
  - gcd(a,b) = gcd(a/2,b) gdy a parzyste i b nieparzyste,
  - gcd(a, b) = gcd(a b, b) gdy a > b i obie nieparzyste.

Co powinien zrobić algorytm, gdy na początku a i b są parzyste? Jaka jest złożoność tego algorytmu?

5. Pokaż jak zmodyfikować algorytm z poprzedniego zadania, żeby wyliczał również x,y, takie że  $xa+yb=\gcd(a,b)$ .

Wsk.: Skorzystaj z równości xa + yb = (x - b)a + (y + a)b.

- 6. Udowodnij, że jeśli  $(m_1, m_2, ...)_p$  i  $(n_1, n_2, ...)_p$  są reprezentacjami liczb naturalnych m i n względem układu kolejnych liczb pierwszych, to:
  - (a)  $k = \gcd(m, n) \Leftrightarrow k_i = \min\{m_i, n_i\}$  dla każdego i = 1, 2, ...
  - (b)  $k = \text{lcm}(m, n) \Leftrightarrow k_i = \max\{m_i, n_i\}$  dla każdego  $i = 1, 2, \dots$

gdzie  $(k_1,k_2,\ldots)_p$  jest rozkładem liczby k. Korzystając z powyższych równości pokaż, że  $mn=\gcd(m,n) \mathrm{lcm}(m,n)$ 

- 7. Wykaż zależności:
  - (a)  $xz \equiv yz \pmod{mz} \Leftrightarrow x \equiv y \pmod{m}$ , dla  $z \neq 0$
  - (b)  $xz \equiv yz \pmod{m} \Leftrightarrow x \equiv y \pmod{\frac{m}{\gcd(z,m)}}, x, y, z, m \in \mathbb{Z}$
  - (c)  $x \equiv y \pmod{mz} \Rightarrow x \equiv y \pmod{m}$
- 8. Udowodnij, że
  - (a) jeśli  $2^n 1$  jest liczbą pierwszą, to n jest liczbą pierwszą.
  - (b) jeśli  $a^n 1$  jest liczbą pierwszą, to a = 2.
  - (c) jeśli  $2^n + 1$  jest liczbą pierwszą, to n jest potęgą liczby 2.

Wsk.: Skorzystaj z wzoru:  $a^n - b^n = (a - b)(\sum a^i b^{n-i-1})$ .

- 9. (Twierdzenie Wilsona) Udowodnij, że jeśli p jest liczbą pierwszą, to p dzieli ((p-1)!+1). Wsk.: Wykaż najpierw, że  $(p-2)! \equiv 1 \pmod{p}$ .
- 10. Jaka jest liczba reszt modulo  $p^{\alpha}$  spełniających równanie:  $x^{2}\equiv 1 \bmod p^{\alpha}?$

Wsk.: Jake muszą być x-1 i x+1, żeby  $p^{\alpha}|(x+1)(x-1)$ ? Osobno rozważ przypadek p=2.

- 11. Jak znając rozkład n można wyznaczyć liczbę rozwiązań równania  $x^2 \equiv 1 \mod n$ ?
- 12. Znajdź najmniejsza liczbę naturalną x, dla której

$$\begin{cases} x \equiv 11 \mod 27, \\ x \equiv 12 \mod 64, \\ x \equiv 13 \mod 25. \end{cases}$$

- 13. Ile wynosi najmniejsze takie  $n \in \mathbb{N}$ , że  $2^n \equiv 1 \mod 5 \cdot 7 \cdot 9 \cdot 11 \cdot 127$ .
- 14. Powtarzając dowód Euklidesa pokaż, że istnieje nieskończenie wiele liczb pierwszych w postaci 3k+2 i 4k+3.
- 15. Niech d(k) będzie liczbą dzielników k. Pokaż, że  $\sum_{k=1}^{n} d(k) = n \ln n + O(n)$ .