AiSD – ćwiczenia 02

Niech $\gcd(x, y)$ to największy wspólny dzielnik x i y; $\mathrm{lcm}(x, y)$ to najmniejsza wspólna wielokrotność.

1. Udowodnij, że dla dowolnych $x, y \in \mathbb{N}$, jeśli $1 \leqslant x < y$, to $\gcd(x, y) = \gcd(y, y - x)$.

2. Udowodnij, że dla dowolnych $x, y \in \mathbb{N}$, jeśli $1 < x < y$ i x nie dzieli y, to $\gcd(x, y) = \gcd(x, y \bmod x)$.

3. Zapisz algorytm Euklidesa w wersji używającej odejmowania i w drugiej wersji używającej reszt modulo. Zaanalizuj czas działania obu wersji. Pamiętaj o różnicy pomiędzy wartością liczby a długością jej zapisu.

4. Zapisz algorytm szybkiego potęgowania, korzystając z zależności: dla $x, y \in \mathbb{N}$

   $$x^y = (x^2)^{\lfloor y/2 \rfloor} * x^{y \bmod 2}.$$

   (*) Zanalizuj czas działania tego algorytmu przyjmując koszt wykonania mnożenia dwóch n bitowych liczb jako (1) $O(n^2)$, (2) $O(n^a)$, dla pewnej stałej $1 < a < 2$. Pamiętaj, że wynik mnożenia dwóch liczb n-bitowych ma długość ograniczoną przez $2n$.

5. Przeprowadź analizę czasu działania algorytmu z poprzedniego zadania dla działań w ciele $\mathbb{Z}_p$, dla pewnej liczby pierwszej p. Uwaga, x, y wciąż mogą być dowolnymi liczbami naturalnymi.

6. Skonstruuj efektywny algorytm dla obliczenia $a^{b^c} \bmod p$, dla pewnej ustalonej liczby pierwszej p. Skorzystaj z małego twierdzenia Fermata: dla dowolnej liczby pierwszej p i a takiego, że $1 \leqslant a < p$, $a^{p-1} \equiv 1 \pmod p$.

7. Zaimplentuj schemat Hornera obliczania wartości wielomianu. Schemat Hornera opiera się na przedstawieniu wielomianu $W(x) = a_0 + a_1 * x + a_2 * x^2 + \cdots + a_n * x^n$ jako $W(x) = a_0 + x * (a_1 + x * (a_2 + \cdots + x * a_n) \dots)$.