

Kryptografia z elementami algebry

notacja wielkie-O, arytmetyka w strukturach algebraicznych

W każdym zadaniu wykonaj oszacowania wykorzystując notację wielkie-O .

1. Oszacuj liczbę bitów potrzebnych do zapisania liczby $n \in \mathbb{Z}^+$.
2. Niech $a, b \in \mathbb{N}, a \leq b$. Oszacuj liczbę operacji elementarnych na bitach potrzebnych do obliczenia $a \pm b$.
3. Niech $a, b \in \mathbb{N}, a \leq b$. Oszacuj liczbę operacji elementarnych na bitach potrzebnych do obliczenia ab .
4. Niech $a, b \in \mathbb{N}, a \leq b$. Oszacuj liczbę operacji elementarnych na bitach potrzebnych do obliczenia q oraz r takiego, że $b = qa + r, 0 \leq r < a$.
5. Niech $a, b \in \mathbb{Z}_n^+, a \leq b < n$. Oszacuj liczbę operacji elementarnych na bitach potrzebnych do obliczenia $a \pm b$ w \mathbb{Z}_n^+ .
6. Niech $a, b \in \mathbb{Z}_n^*, a \leq b < n$. Oszacuj liczbę operacji elementarnych na bitach potrzebnych do obliczenia ab w \mathbb{Z}_n^* .
7. Niech $a \in \mathbb{Z}_n^*, k \in \mathbb{N}, k < n$. Oszacuj liczbę operacji elementarnych na bitach potrzebnych do obliczenia a^k w \mathbb{Z}_n^* za pomocą algorytmu iterowanego podnoszenia do kwadratu.
8. Niech $a \in \mathbb{Z}_p^*$, gdzie p jest liczbą pierwszą. Oszacuj liczbę operacji elementarnych na bitach potrzebnych do obliczenia a^{-1} w \mathbb{Z}_p^* . Do obliczania odwrotności wykorzystaj fakt, że $a^{p-2} = a^{-1}$ w \mathbb{Z}_p^* .
9. Niech $\Phi(n) = \{a \in \mathbb{Z}_n^*, (a, n) = 1\}$. Oszacuj liczbę operacji elementarnych na bitach potrzebnych do obliczenia a^{-1} w $\Phi(n)$. Do obliczania odwrotności wykorzystaj Rozszerzony Algorytm Euklidesa.
10. Które ze struktur algebraicznych wykorzystywanych na dzisiejszych ćwiczeniach są grupami?