9 kwietnia 2024

Zadania z kryptografii, lista nr 5

1. Symbol Legendre'a określamy dla p pierwszego, nieparzystego i $a \in \mathbb{Z}$ następująco

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{gdy } p|a \\ 1 & \text{gdy istnieje } x : 0 \neq a = x^2 \bmod p \\ -1 & \text{gdy nie istnieje } x : a = x^2 \bmod p \end{cases}$$

   Pokaż, że $\left(\frac{a}{p}\right) = a^{(p-1)/2} \bmod p$.

2. Symbol Jacobiego określamy dla nieparzystego $n = p_1^{e_1} \dots p_k^{e_k}$ i $a \in \mathbb{Z}$ następująco

$$\left(\frac{a}{n}\right) = \prod \left(\frac{a}{p_i}\right)^{e_i}$$

   Pokaż, że

   (a) Jeżeli $m_1 \equiv m_2 \bmod n$, to $\left(\frac{m_1}{n}\right) = \left(\frac{m_2}{n}\right)$;

   (b) $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8} = \begin{cases} 1 & \text{gdy } n \equiv \pm 1 \bmod 8 \\ -1 & \text{gdy } n \equiv \pm 3 \bmod 8; \end{cases}$

   (c) $\left(\frac{m_1 m_2}{n}\right) = \left(\frac{m_1}{n}\right)\left(\frac{m_2}{n}\right)$;

   (d) Jeżeli m i n są nieparzyste, to $\left(\frac{m}{n}\right) = (-1)^{(m-1)(n-1)/4}\left(\frac{n}{m}\right) = \begin{cases} -\left(\frac{n}{m}\right) & \text{gdy } m \equiv n \equiv 3 \bmod 4 \\ \left(\frac{n}{m}\right) & \text{w przeciwnym przypadku.} \end{cases}$

3. Korzystając z powyższych wzorów oblicz:

$$\left(\frac{91}{167}\right), \left(\frac{11}{37}\right), \left(\frac{19}{31}\right), \left(\frac{97}{101}\right), \left(\frac{5}{160465489}\right), \left(\frac{3083}{3911}\right), \left(\frac{43691}{65537}\right).$$

4. Test pierwszości Solovaya-Strassena jest oparty na procedurze obliczającej symbol Jacobiego $\left(\frac{a}{n}\right)$. Może być on obliczony rekurencyjnie korzystając ze wzorów z poprzednich zadań. W teście tym sprawdzamy, czy n jest pierwsze w następujący sposób (test może być wykonany wiele razy)

   - jeśli $2|n$ to n ZŁOŻONE
   - losujemy $a \in \mathbb{Z}_n \setminus \{0\}$ i gdy $\gcd(a, n) > 1$, to n ZŁOŻONE
   - obliczamy $\left(\frac{a}{n}\right)$
   - jeśli $\left(\frac{a}{n}\right) \neq a^{(n-1)/2} \bmod n$, to n ZŁOŻONE

   (a) Pokaż, że $H = \{a \in \mathbb{Z}_n^*, \left(\frac{a}{n}\right) = a^{(n-1)/2} \bmod n\}$ jest podgrupą $\mathbb{Z}_n^*$.

   (b) Pokaż, że jeśli $n = pm$, gdzie p jest pierwsze i $m \perp p$, to istnieje a, że $a \bmod p$ nie jest resztą kwadratową w $\mathbb{Z}_p$ i $a \equiv 1(\bmod m)$ oraz

$$\left(\frac{a}{n}\right) = -1 \neq a^{(n-1)/2} \bmod n.$$

   (c) Pokaż, że jeśli $n = p^k m (k > 1)$, gdzie p jest pierwsze i $m \perp p$, to dla $a = 1 + p^{k-1}m$ mamy

$$\left(\frac{a}{n}\right) \neq a^{(n-1)/2} \bmod n.$$

   (d) Wywnioskuj z tego że $|H| \leq |\mathbb{Z}_n^*|/2 < (n-1)/2$ i w związku z tym przwdopodobieństwo wykrycia złożoności liczby n w jednym przebiegu testu Solovaya-Strassena przekracza $1/2$.