Kryptografia

1. (1pkt) Udowodnij, że jeśli liczba nieparzysta złożona n nie jest liczbą Carmichaela, to pierwszy z podanych na wykładzie testów (tj. dla losowego b: $b^{(n-1)/2} \equiv 1 \bmod n$) nie przechodzi dla co najmniej połowy baz z Z_n^*.

2. (2pkt) Udowodnij następujące własności symbolu Jacoby'ego (n oznacza nieparzystą liczbę całkowitą):
   - $\left(\frac{m_1}{n}\right) = \left(\frac{m_2}{n}\right)$, gdy $m_1 \equiv m_2 \bmod n$.
   - $\left(\frac{2}{n}\right) = \begin{cases} 1, & \text{gdy } n \equiv \pm 1 (\bmod 8) \\ -1, & \text{gdy } n \equiv \pm 3 (\bmod 8) \end{cases}$
   - $\left(\frac{m_1 m_2}{n}\right) = \left(\frac{m_1}{n}\right)\left(\frac{m_2}{n}\right)$
   - $\left(\frac{m}{n}\right) = \begin{cases} -\left(\frac{n}{m}\right), & \text{gdy } m \equiv n \equiv 3 (\bmod 4) \\ \left(\frac{n}{m}\right), & \text{w przeciwnym przypadku.} \end{cases}$

3. (0,5pkt) 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. (1pkt) W jakim czasie można okrełić, czy dana liczba jest resztą kwadratową w Z_p^* (p jest liczbą pierwszą)?

5. (1pkt) Udowodnij, że żadna reszta kwadratowa nie jest generatorem Z_p^*.

6. (2pkt) (Prawdopodobieństwo błędu w teście Solovay'a-Strassena.)
   (a) Niech $G(n) = \{a \ : \ a \in Z_n^*, \ \left(\frac{m}{n}\right) \equiv a^{(n-1)/2} (\bmod n)$. Wykaź, że $G(n)$ jest podgrupą grupy Z_n i wywnioskuj stąd, że $|G(n)| \leq (n-1)/2$.
   (b) Załóźmy, że $n = p^k q$, gdzie p i q są liczbami nieparzystymi, p jest pierwsza, $k \geq 2$ oraz $NWD(p,q) = 1$. Niech $a = 1 + p^{k-1}q$. Udowodnij, że
   $$\left(\frac{a}{n}\right) \not\equiv a^{(n-1)/2} (\bmod n)$$
   (c) Niech $n = p_1 p_2 \dots p_k$, gdzie p_i są różnymi liczbami pierwszymi. Niech $a \equiv u \bmod p_1$ oraz $a \equiv 1 \bmod p_2 \dots p_k$, gdzie u jest nieresztą kwadratową modul p_1 (zauważ, że takie a istnieje na mocy chińskiego twierdzenia o resztach). Wykaź, że
   $\left(\frac{a}{n}\right) \equiv -1 (\bmod n)$ lecz $a^{(n-1)/2} \equiv 1 (\bmod n)$, a zatem $a^{(n-1)/2} \not\equiv -1 (\bmod n)$.
   (d) Wykaź, że jeśli n jest liczbą nieparzystą i złożoną, to $|G(n)| \leq (n-1)/2$.
   (b) Wywnioskuj z powyższych faktów, że prawdopodobieństwo błędu w teście Solovay'a-Strassena nie przekracza $1/2$.

7. (2pkt) Wykaź, że liczby pierwsze przechodzą test Rabina-Milera przy każdej bazie.