25 marca 2024

Zadania z kryptografii, lista nr 4

1. *Resztą kwadratową* modulo n nazywamy takie $a \in \mathbb{Z}_n$, że dla pewnego $b \in \mathbb{Z}_n$ mamy $b^2 \bmod n = a$.
   (a) Wykaż, że reszty kwadratowe tworzą podgrupę $\mathbb{Z}_n^*$.
   (b) Pokaż, że jeśli g jest generatorem $\mathbb{Z}_p^*$, dla p-pierwszego to zbiór reszt kwadratowych pokrywa się ze zbiorem elementów w postaci g^{2k}.
   (c) Pokaż, że jeśli $p = 4k+3$ (p – liczba pierwsza) to w $\mathbb{Z}_p$ dokładnie jeden z elementów $a, -a \in \mathbb{Z}_p^*$ jest resztą kwadratową modulo p.
   (d) Pokaż, że jeśli $p = 4k+1$ (p – liczba pierwsza) to w $\mathbb{Z}_p$ albo oba elementy $a, -a$ albo żaden nie jest resztą kwadratową modulo p.

2. Pokaż, że jeśli $p = 4k+3$ (p – liczba pierwsza) i a jest resztą kwadratową modulo p, to dla $b = a^{(p+1)/4} \bmod p$ zachodzi $b^2 \bmod p = a$. Czemu równy jest kwadrat tak zdefiniowanego b, jeśli a nie jest resztą kwadratową?

3. Niech $y = x^2 \bmod p$ gdzie p jest liczbą pierwszą i znamy y. W poprzednim zadaniu podany jest prosty wzór pozwalający znaleźć x jeśli $p \equiv 3 \bmod 4$. Przypuśćmy, że jednak $p \equiv 1 \bmod 4$.
   (a) W jaki sposób można sprawdzić, czy y jest resztą kwadratową?
   (b) Pokaż, że losując u z Z_p^* mamy 50% szans na to, że $u^{(p-1)/2} \not\equiv 1 \bmod p$. Niech $p-1 = 2^s t$, gdzie t jest liczbą nieparzystą. Pokaż, że $v = u^t \bmod p$ ma rząd 2^s w Z_p^*, czyli v jest pierwiastkiem pierwotnym stopnia 2^s z 1 modulo p.
   (c) Można wyliczyć $z = y^{(t+1)/2} \bmod p$ i $q = yz^{-2} \bmod p$. Pokaż, że $q^{2^{s-1}} \equiv 1 \bmod p$. Wprowadźmy oznaczenie $r = xz^{-1} \bmod p$. Pokaż, że $q = r^2 \bmod p$ i $r^{2^s} \equiv 1 \bmod p$. Pokaż też, że istnieje l takie, że $r = v^l \bmod p$.
   (d) Niech $l = l_0 + l_1 \cdot 2 + l_2 \cdot 2^2 + \cdots + l_{s-1} \cdot 2^{s-1}$. Pokaż, jak wyznaczyć $l_0, l_1, \ldots, l_{s-2}$ dysponując resztami y, q, v. (Wsk.: $l_0 = 0 \Leftrightarrow q^{2^{s-2}} \equiv 1 \bmod p$).
   (e) Pokaż, że x można wyliczyć ze wzoru $x = z \cdot r \bmod p = z \cdot v^l \bmod p$.

4. W jaki sposób znając dwie reszty b, c modulo n takie $b \neq \pm c \bmod n$ i $b^2 = c^2 \bmod n$ można znaleźć rozkład n na dwa czynniki.

5. Pokaż jak można rozłożyć na dwa czynniki liczbę złożoną n, która w teście Millera-Rabina okazała się złożona, ponieważ dla pewnego a wyliczyliśmy $a^{2^k r} \not\equiv \pm 1$, $a^{2^{k+1} r} \equiv 1$ modulo n.

6. Pokaż, że liczb naturalnych pomiędzy 1 i n, które rozkładają się na czynniki pierwsze nie większe, niż B jest co najmniej
$$\binom{\pi(B)}{\log_B n},$$
gdzie $\pi(B)$ jest ilością liczb pierwszych w przedziale $[1, B]$. Niech $B = e^{\sqrt{\ln n \ln \ln n}}$.
   (a) Pokaż, że prawdopodobieństwo, że losowa reszta modulo n ma rozkład na czynniki niewiększe niż B jest co najmniej $1/B$. Skorzystaj z zależności $\pi(B) \sim B/\ln B$.
   (b) Oszacuj oczekiwaną liczbę operacji wykonywanych przez algorytm Dixona potrzebną do faktoryzacji n.