# 1. Luki z wykładu

**Zadanie 1**

Trudność: łatwe Punktów: 2

Na wykładzie omówiliśmy algorytm przybliżania ułamków, który pozwala wysupłać z liczby $\frac{\gamma}{N} = \frac{\lfloor k\frac{N}{t} \rceil}{N}$ interesującą nas liczbę $\frac{k}{t}$. Niestety, jeśli $k$ i $t$ nie są względnie pierwsze, algorytm uprości ten ułamek i jego mianownikiem nie będzie $t$, tylko jakiś jego dzielnik. Pokaż, że z prawdopodobieństwem $\frac{1}{\text{poly}(n)}$ obwód wypluł taką liczbę $\gamma = \lfloor k\frac{N}{s} \rceil$, że $t$ i $s$ są względnie pierwsze.

**Zadanie 2 [Łamanie RSA]**

Trudność: łatwe Punktów: 2

W kryptosystemie RSA losuje się dwie duże liczby pierwsze $p$ i $q$. Obliczenia dokonują się w pierścieniu $\mathbb{Z}_N^*$, gdzie $N = p \cdot q$. Wybiera się $e$ (zazwyczaj równe 65537), które stanowi klucz publiczny, oraz $d$, takie że

$$e \cdot d \equiv 1 \mod (p-1)(q-1).$$

Wiadomość $m \in \mathbb{Z}_N$ szyfrujemy licząc $c = m^e \pmod N$. Deszyfrowanie polega na policzeniu $c^d \equiv m^{e \cdot d} \equiv m \pmod N$.

Znamy $N$ i szyfrogram $c$. Jak poznanie $\text{ord}(c)$ pomaga w odczytaniu wiadmości $m$?

# 2. Algorytm Shora

W kolejnych zadaniach mamy liczbę $N$ będącą iloczynem nieparzystych liczb pierwszych. Naszym celem jest poznanie tych liczb pierwszych.

**Zadanie 3**

Trudność: średnie Punktów: 3

Niech $p$ będzie nieparzystą liczbą pierwszą, zaś $x$ niech będzie losową (jednostajnie) resztą z dzielenia przez $p$. $k$ będzie *rzędem* $x$, czyli najmniejszą dodatnią potęgą, że $x^k \equiv 1 \pmod p$. Pokaż, że z prawdopodobieństwem przynajmniej $\frac{1}{2}$ (ze względu na wybór $x$) $k$ jest parzyste.

**Wskazówka:** Grupa multiplikatywna $\mathbb{Z}_p^*$ ma generatory.

**Zadanie 4**

Trudność: trudne Punktów: 4

Niech $N = p \cdot q$ będzie iloczynem dwóch różnych liczb pierwszych, zaś $x$ niech będzie losową resztą z dzielenia przez $N$. Udowodnij, że z prawdopodobieństwem przynajmniej $\frac{3}{8}$ rząd $k$ liczby $x$ jest parzysty i $x^{\frac{k}{2}} \not\equiv \pm 1 \pmod N$.

**Zadanie 5**

Trudność: łatwe Punktów: 1

Załóżmy, że $N$ jest potęgą nieparzystej liczby pierwszej $p$. Jak (klasycznie) znaleźć tę liczbę $p$?

**Zadanie 6**

Trudność: średnie Punktów: 2

Skonstruuj algorytm kwantowy do rozkładu liczby na czynniki pierwsze. Jaka jest złożoność tego algorytmu?

# 3. Hidden Subgroup Problem

W *Hidden Subgroup Problem* dostajemy funkcję $f : G \to \mathbb{N}$, o której wiemy, że istnieje jakaś podgrupa $H \leqslant G$, którą $f$ „ukrywa” — tj.

$$f(x) = f(y) \iff xH = yH.$$

**Zadanie 7 [Problem logarytmu dyskretnego]**

Trudność: trudne Punktów: 5

W problemie *logarytmu dyskretnego* dostajemy liczbę całkowitą $M$ i generator $g$ grupy multiplikatywnej $\mathbb{Z}_M^*$, to znaczy $\{g^0, g^1, \ldots, g^{N-1}\} = \mathbb{Z}_M^*$. Zakładamy, że $N$ jest nam znane. Dostajemy ponadto $a \in \mathbb{Z}_M^*$, a naszym zadaniem jest znaleźć najmniejsze $l$, że $g^l \equiv a \pmod M$.

Pokaż, że problem ten jest instancją HSP, z grupą $\mathbb{Z}_N \times \mathbb{Z}_N$.

**Zadanie 8**

Trudność: łatwe Punktów: 1

Okresem funkcji $f : \mathbb{Z}_N^k \to [M]$ jest taki wektor, $\mathsf{u} \in \mathbb{Z}_N^k$, że $\forall \mathsf{x} \in \mathbb{Z}_N^k,\ f(\mathsf{x}_1, \ldots, \mathsf{x}_k) = f(\mathsf{x}_1 + \mathsf{u}_1, \ldots, \mathsf{x}_k + \mathsf{u}_k)$ (wszystkie operacje dzieją się oczywiście w $\mathbb{Z}_N$). Pokaż, że problem jest instancją HSP.

**Zadanie 9 [Izomorfizm Grafów]**

Trudność: trudne Punktów: 5

Pokaż, że problem izomorfizmu grafów można sprowadzić do szczególnego przypadku HSP.