Algorytmy Kwantowe

Lista 7

1. Period Finding

Zadanie 1

Trudność: średnie Punktów: 3

Dokończyć algorytm: jak z losowych wielokrotności $\frac{N}{s}$ wyłuskać s? Bardziej precyzyjnie, algorytm z wykładu wypluje z jednakowym prawdopodobieństwem jedną z liczb $0 \cdot \frac{N}{s}, 1 \cdot \frac{N}{s}, 2 \cdot \frac{N}{s}, \ldots, (s-1) \cdot \frac{N}{s}$.

Wskazówka:

$$\sum_{p \text{ pierwsze}} \frac{1}{p^2} \leq \sum_{n \in \mathbb{N}} \frac{1}{n^2}.$$

1.1 Algorytm dla $s \nmid N$

W następnych zadaniach będziemy chcieli znaleźć okres s funkcji $f : \mathbb{Z} \to [M]$ — tym razem bez założenia, że s coś dzieli. Ustalmy $N \gg M$ (na przykład $N = 2^{(\lceil \lg(M) \rceil^{10})}$). Obwód będzie wyglądał tak jak poprzednio, tylko analiza będzie trochę trudniejsza.

Zadanie 2

Trudność: łatwe Punktów: 1

Niech $\frac{D}{N}$ będzie prawdopodobieństwem zmierzenia koloru r (po zastosowaniu wyroczni dla funkcji f). Ile może wynosić D?

Zadanie 3

Trudność: łatwe Punktów: 1

Jaki stan ma obwód po zmierzeniu koloru r i zastosowaniu Kwantowej Transformaty Fouriera na pozostałych bitach?

Zadanie 4

Trudność: średnie Punktów: 3

Interesują nas takie stany $|\gamma\rangle$, że $(\gamma \cdot s \mod N) \in [-\frac{s}{2}; \frac{s}{2})$. Niech α_γ będzie amplitudą takiego stanu wyliczoną w poprzednim zadaniu. Pokaż, że $|\alpha_\gamma| > \frac{0{,}35}{\sqrt{s}}$.

Wskazówka: Jaki będzie maksymalny kąt między liczbami zespolonymi w sumie opisującej tę amplitudę?

Widzimy zatem, że każda z liczb $\lfloor k\frac{N}{s} \rceil$[1] dla $0 \leqslant k < s$ zostanie wypluta przez obwód z prawdopodobieństwem większym niż $\frac{0{,}12}{s}$. Teraz musimy jakoś wykorzystać te zaokrąglenia do wyliczenia s.

Zadanie 5

Trudność: łatwe Punktów: 2

Najlepszą *aproksymacją diofantyczną* liczby rzeczywistej x nazywamy taką liczbę wymierną $\frac{p}{q}$, że

$$\left| x - \frac{p}{q} \right| \leqslant \left| x - \frac{p'}{q'} \right|$$

dla każdej liczby $\frac{p'}{q'}$, że $q' \leqslant q$. Jak uzyskać taką aproksymację dla określonego q?

Uwaga: W tym zadaniu nie trzeba prezentować dowodu. Wystarczy nam algorytm.

Zadanie 6

Trudność: średnie Punktów: 4

Algorytm z poprzedniego zadania pozwala nam wysupłać z liczby $\frac{\gamma}{N} = \frac{\lfloor k\frac{N}{s} \rceil}{N}$ interesującą nas liczbę $\frac{k}{s}$. Niestety, jeśli k i s nie są względnie pierwsze, algorytm uprości ten ułamek i jego mianownikiem nie będzie s, 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 k i s są względnie pierwsze.

Wskazówka: Ile jest liczb pierwszych mniejszych niż s?

1.2 Algorytm Shora

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

Zadanie 7 [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 65535), 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. Skonstruuj algorytm kwantowy, który pozwoli odszyfrować m. Jaka jest złożoność tego algorytmu?

Zadanie 8

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.

[1] $\lfloor x \rceil$ to zaokrąglenie x do najbliższej liczby całkowitej.

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

Zadanie 9

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 10

Trudność: łatwe Punktów: 1

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

Zadanie 11

Trudność: średnie Punktów: 2

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