Sławomir Górawski

Lista 7, zadanie 1. (Założenie DL) Niech $p = 2q+1$ (p, q–pierwsze) i g rzędu q w $\mathbb{Z}_p^*$. Załóżmy, że istnieje wielomianowy algorytm probabilistyczny obliczający dla losowych g, g^x liczbę x z prawdopodobieństwem co najmniej $1/w(l)$ gdzie w jest wielomianem a l długością p. Skonstruuj wielomianowy algorytm probabilistyczny obliczający x dla zadanych g, g^x z prawdopodobieństwem 0.9999.

Rozwiązanie. Niech A będzie istniejącym algorytmem z zadania. Konstruujemy nowy algorytm B z parametrem m:

```
dla i od 1 do m
    uruchom A
    jeśli otrzymano wynik, zwróć go
```

Musimy dobrać m tak żeby prawdopodobieństwo otrzymania wyniku przez B było większe lub równe 0.9999. Patrząc na zdarzenia przeciwne, B nie zwróci wyniku jeśli A nie zwróci wyniku w żadnej z m prób. Prawdopodobieństwo tego to $(1 - \frac{1}{w(l)})^m$ i chcemy, żeby było mniejsze lub równe 0.00001. Możemy z tego wyliczyć m:

$$\begin{aligned}
\left(1 - \frac{1}{w(l)}\right)^m &\leqslant 10^{-5} \\
\ln\left(\left(1 - \frac{1}{w(l)}\right)^m\right) &\leqslant \ln(10^{-5}) \\
m \ln\left(1 - \frac{1}{w(l)}\right) &\leqslant -5\ln 10
\end{aligned}$$

Korzystamy teraz z nierówności $1 - \frac{1}{x} \leqslant \ln x$ dla $x > 0$:

$$\begin{aligned}
m\left(1 - \frac{1}{1 - \frac{1}{w(l)}}\right) &\leqslant -5\ln 10 \\
m\left(\frac{-1}{w(l) - 1}\right) &\leqslant -5\ln 10 \\
-m &\leqslant -5\ln(10)(w(l) - 1) \\
m &\geqslant 5\ln(10)(w(l) - 1)
\end{aligned}$$

Widzimy że $5\ln 10$ jest stałą, więc $m \geqslant O(w(l))$. Algorytm B uruchamia m razy wielomianowy algorytm A. Jego złożoność to iloczyn wielomianów, więc sam też jest wielomianowy.