[PTKB] Kolokwium 2 - opracowanie

1 Zadanie 1.

Treść: Ile razy trzeba wykonać protokół uwierzytelniania Fiata-Shamira by prawdopodobieństwo oszustwa było mniejsze od 10^{-1000}?

Rozwiązanie: Prawdopodobieństwo udanego oszustwa po wykonaniu n eksperymentów wynosi $(\frac{1}{2})^n$. Rozwiązujemy równanie $(\frac{1}{2})^x = 10^{-1000}$.

$$\begin{aligned}
(\tfrac{1}{2})^x &= 10^{-1000} \\
2^x &= 10^{1000} \\
x &= \log_2 10^{1000} \\
x &= 1000 \log_2 10 \\
x &\simeq 3321.928
\end{aligned} \tag{1}$$

Wybieramy $\lceil x \rceil = 3322$.

2 Zadanie 4.

Treść: Podać przykład liczby pseudopierwszej przy podstawie 2 i 3 jednocześnie. Czy takie liczby w ogóle istnieją?

Rozwiązanie: Liczba naturalna jest liczbą Carmichaela wtedy i tylko wtedy, gdy:

1. Jest liczbą złożoną.
2. Dla każdego $a \in \mathbb{N}$ z przedziału $1 < a < n$, względnie pierwszej z n, liczba $(a^{n-1} - 1)$ jest podzielna przez n.

Patrząc na najmniejsze liczby Carmichaela:

$$\begin{aligned}
561 &= 3 \cdot 11 \cdot 17 \\
1105 &= 5 \cdot 13 \cdot 17
\end{aligned} \tag{2}$$

widzimy, że liczba Carmichaela 1105 jest względnie pierwsza zarówno z 2, jak również 3, a więc pozwala ona stworzyć liczby pseudopierwsze $2^{1105-1} - 1$ oraz $3^{1105-1} - 1$.

3 Zadanie 7.

Treść: Wykazać, że wielomian x^2+1 jest nierozkładalny w pierścieniu wielomianów $GF(3)[x]$, a jest rozkładalny w pierścieniu wielomianów $GF(2)[x]$.

Rozwiązanie: Wielomian drugiego stopnia można rozłożyć za pomocą dwóch wielomianów pierwszego stopnia, więc:

$$\begin{aligned}
x^2 + 1 &= (ax + b) * (cx + d) \\
x^2 + 1 &= (ac)x^2 + (ad + bc)x + bd
\end{aligned} \tag{3}$$

Dla ciała $GF(3)[x]$, $b, d \in \{0, 1, 2\}$ oraz $a, c \in \{1, 2\}$ (bo wielomian musi być rozkładalny). Rozważmy wszystkie możliwe wartości $(ad+bc) \bmod 3$. Jeżeli $(ad+bc) \equiv 0 \mod 3 \Rightarrow a = 0 \wedge c = 0$, co jest sprzeczne z dziedziną, a więc wielomian nie może być rozkładalny.

Dla ciała $GF(2)[x]$, $b, d \in \{0, 1\}$ oraz $a, c \in \{1\}$. Jeżeli $(b + d) \equiv 0 \mod 2 \Rightarrow (b = 0 \wedge d = 0) \vee (b = 1 \wedge d = 1)$. Dla drugiego przypadku otrzymujemy w $GF(2)[x]$:

$$x^2 + 1 \equiv (x + 1) * (x + 1) \tag{4}$$

Zatem wielomian jest rozkładalny.