[PTKB] Kolokwium 2 - opracowanie

1 Kolokwium 2 z PTKB (11.01.2012)

1.1 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 $(\frac{1}{2})^x = 10^{-1000}$.

$$\begin{array}{lcl} (\frac{1}{2})^x & = & 10^{-1000} \\ 2^x & = & 10^{1000} \\ x & = & \log_2 10^{1000} \\ x & = & 1000 \log_2 10 \\ x & \simeq & 3321.928 \end{array}$$

Wybieramy $\lceil x \rceil = 3322$.

1.2 Zadanie 3.

Treść: Wykazać, że charakterystyka ciała skończonego (czyli najmniejsza taka liczba n, że spełniona jest równość $\underbrace{1+1+1+\cdots+1}_{\text{n}} = 0$) jest zawsze liczbą pierwszą.

Rozwiązanie: Załóżmy, że $\mathrm{char} K = n$ i liczba $n = m_1 m_2$, gdzie $m_1, m_2 \in \mathbb{N}$, a więc $n \cdot 1 = (m_1 m_2) \cdot 1 = 0$. Z łączności dodawania i rozdzielności mnożenia względem dodawania w ciele K mamy $(m_1 m_2) \cdot 1 = (m_1 \cdot 1)(m_2 \cdot 1)$, zatem:

$$(m_1 \cdot 1)(m_2 \cdot 1) = 0$$

Jeśli $m_1 < n$ to z definicji charakterystyki dostajemy, że $m_1 \cdot 1 \neq 0$, zatem istnieje element odwrotny $(m_1 \cdot 1)^{-1}$ do $m_1 \cdot 1$. Mnożąc lewostronnie równość $(m_1 \cdot 1)(m_2 \cdot 1) = 0$ przez $(m_1 \cdot 1)^{-1}$ dostajemy $m_2 \cdot 1 = 0$, ponieważ jednak $1 \leqslant m_2 \leqslant n$ to biorąc pod uwagę definicję charakterystyki ciała musimy mieć $m_2 = n$. Wynika stąd, że liczba n nie jest podzielna przez żadną liczbę różną od n i 1, a zatem jest liczbą pierwszą.

Można też rozumować nieco inaczej. Załóżmy, że $\mathrm{char} K = n$ i liczba n daje się przedstawić w postaci $n = m_1 m_2$, gdzie $m_1, m_2 \in \mathbb{N}$ i $m_1, m_2 \geqslant 2$, czyli n nie jest liczbą pierwszą. Wówczas $n \cdot 1 = (m_1 m_2) \cdot 1 = (m_1 \cdot 1)(m_2 \cdot 1) = 0$. Ponieważ $m_1 \cdot 1 \neq 0$ i $m_2 \cdot 1 \neq 0$ oraz $(m_1 \cdot 1)(m_2 \cdot 1) = 0$ co nie jest możliwe, bo ciało nie ma niezerowych dzielników zera. Zatem założenie, że n nie jest liczbą pierwszą prowadzi do sprzeczności.

1.3 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:

$$\begin{array}{lcl} 561 & = & 3 \cdot 11 \cdot 17 \\ 1105 & = & 5 \cdot 13 \cdot 17 \end{array}$$

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 $3^{1105-1} - 1$.

1.4 Zadanie 5.

Treść: Podać przykład ciała $GF(3^2)$, czyli ciała o 9 elementach.

Rozwiązanie: Ciało $GF(p^n)$, gdzie p jest liczbą pierwszą oraz $n \in \mathbb{N}$, można wygenerować:

- Znajdując wielomian $f(x)$ stopnia n nierozkładalny w pierścieniu $GF(p)[x]$.
- Znajdując wszystkie możliwe reszty z dzielenia wielomianu $f(x)$ w pierścieniu $GF(p)[x]$.
- Wykorzystując działania dodawania i mnożenia wielomianów modulo $f(x)$.

Wielomianem drugiego stopnia nierozkładalnym w ciele $G(3)[x]$ jest $x^2 + 1$ (patrz: *Zadanie 7.*). Wszystkie możliwe reszty z dzielenia tego wielomianu w pierścieniu $G(3)[x]$ to: $2x+2$, $2x+1$, $2x$, $x+2$, $x+1$, x, 2, 1.

1.5 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:

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

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 $(ad+bc)$ mod 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 $GF(2)[x]$:

$$x^2+1 \equiv (x+1)*(x+1)$$

Zatem wielomian jest rozkładalny.

1.6 Zadanie 8.

Treść: Wykazać, że w grupie skończonej dla każdego $a \in G$ mamy: $a^{rzG}=1$, gdzie rzG oznacza rząd grupy G. Wykazać, wykorzystując ten fakt, twierdzenie Eulera. (Wskazówka: wykorzystać twierdzenie Lagrange'a: dla grup skończonych rząd podgrupy jest dzielnikiem rzędu grupy).

Rozwiązanie: W ciągu $a^1, a^2, \cdots, a^{rzG}, a^{rzG+1}$ muszą być dwa elementy równe, tzn. dla pewnych $k', k'' \in [1, rzG+1], k' < k''$ musimy mieć $a^{k'} = a^{k''}$. Zatem $a^{k''-k'}=1$. Istnieje więc takie $k \in [1, rzG](k=k''-k')$, że $a^k=1$. Niech r będzie najmniejszym takim k, że $a^k=1$, wówczas zbiór $H=\left\{a^1, a^2, \cdots, a^r\right\}$ stanowi podgrupę cykliczną rzędu r grupy G. Ponieważ, z twierdzenia Lagrange'a, r jest dzielnikiem rzędu grupy G, więc również $a^{rzG}=1$.

Twierdzenie Eulera: jeśli $n \in \mathbb{N}$, $n \geqslant 2$ i $a \in \mathbb{N}$ oraz $NWD(a,n)=1$ to $a^{\phi(n)} \equiv 1 \mod n$, gdzie ϕ jest funkcją Eulera. Rozważmy grupę multiplikatywną Z_n^*. Grupa Z_n^* ma rząd równy $\phi(n)$. Zatem korzystając z $a^{rzG}=1$ dostajemy, że dla każdego $a \in Z_n^*$ mamy $a^{\phi(n)} \equiv 1 \mod n$. Warunek $a \in Z_n^*$ jest równoznaczny warunkowi $NWD(a,n)=1$. Zatem twierdzenie Eulera jest prostym wnioskiem z ogólnego twierdzenia teoriogrupowego $a^{rzG}=1$.

1.7 Zadanie 9.

Treść: Mamy zapis RNS z modułami $m_1=5$, $m_2=7$, $m_3=11$, $m_4=13$, za pomocą którego zapisujemy liczby całkowite ze zbioru $[0, m_1 \cdot m_2 \cdot m_3 \cdot m_4 - 1]$. Dodać i pomnożyć dwie liczby $a=(3,5,9,11)$ oraz $b=(1,3,7,9)$ stosując typowy dla RNS algorytm. Czy uzyskane wyniki są poprawne?

Rozwiązanie: W RNS można wykonywać operację mnożenia i dodawania według poniższego algorytmu, dla każdego elementu z bazy:

$$\begin{array}{ll} \forall i \in M & a_i \pm b_i \mod m_i \\ \forall i \in M & a_i \cdot b_i \mod m_i \end{array}$$

Zatem:

$$\begin{array}{c} (a+b) = (3+1 \bmod 5, 5+3 \bmod 7, \\ 9+7 \bmod 11, 11+9 \bmod 13) = \\ = (4,1,5,7) \end{array}$$

$$\begin{array}{c} (a \cdot b) = (3 \cdot 1 \bmod 5, 5 \cdot 3 \bmod 7, \\ 9 \cdot 7 \bmod 11, 11 \cdot 9 \bmod 13) = \\ = (3,1,8,8) \end{array}$$

Aby sprawdzić poprawność tego rozwiązania, musimy wyznaczyć liczby a oraz b. Zapis RNS przedstawia liczby w postaci układu kongruencji w modulo bazy, a więc:

$$\begin{array}{rcl} a & \equiv & 3 \mod 5 \\ a & \equiv & 5 \mod 7 \\ a & \equiv & 9 \mod 11 \\ a & \equiv & 11 \mod 13 \end{array}$$

Układ ten można sprowadzić do $a \equiv -2 \mod 5005$. Analogicznie dla b:

$$\begin{array}{rcl} b & \equiv & 1 \mod 5 \\ b & \equiv & 3 \mod 7 \\ b & \equiv & 7 \mod 11 \\ b & \equiv & 9 \mod 13 \end{array}$$

Układ ten można sprowadzić do $b \equiv -4 \mod 5005$. Wyznaczmy sumę $a+b$.

$$a+b \equiv -6 \mod 5005$$

Wyznaczmy iloczyn $a \cdot b$.

$$a*b \equiv 8 \mod 5005$$

Teraz sprawdźmy poprawność wyników uzyskanych przez algorytmy dodawania i mnożenia w RMS. Dodawanie:

$$\begin{array}{rcl} -6 & \equiv & 4 \mod 5 \\ -6 & \equiv & 1 \mod 7 \\ -6 & \equiv & 5 \mod 11 \\ -6 & \equiv & 7 \mod 13 \end{array}$$

Czyli uzyskaliśmy te same współczynniki. Teraz sprawdzamy poprawność mnożenia:

$$\begin{array}{rcll} 8 & \equiv & 3 & \mod 5 \\ 8 & \equiv & 1 & \mod 7 \\ 8 & \equiv & 8 & \mod 11 \\ 8 & \equiv & 8 & \mod 13 \end{array}$$

Czyli wykorzystane algorytmy dodawania i mnożenia dały poprawne rezultaty.

1.8 Zadanie 10.

Treść: Załóżmy, że mamy dwie niezależne zmienne losowe X_1 oraz X_2 o wartościach w zbiorze $Z_2 = \{0,1\}$. Wykazać, że jeśli X_1 ma rozkład równomierny, to również $X_1 \oplus X_2$ ma rozkład równomierny. Ten fakt jest podstawą protokołu o nazwie „rzut monetą przez telefon".

Rozwiązanie: Najpierw wykażemy, że odwzorowanie $Y = X_1 \otimes X_2$ jest zmienną losową. Ogólnie rzecz biorąc, jeśli $(\Omega, \mathfrak{M})$ jest przestrzenią mierzalną, $(E_t, \mathfrak{F}_t)_{t\in T}$ jest dowolną rodziną przestrzeni mierzalnych, a odwzorowania $f_t : \Omega \to E_t$ są $(\mathfrak{M}, \mathfrak{F}_t)$ mierzalne dla każdego $t \in T$ to odwzorowanie $\underset{t\in T}{P} f_t : \Omega \to \underset{t\in T}{P} E_t$ jest $(\mathfrak{M}, \underset{t\in T}{P} \mathfrak{F}_t)$ mierzalne. Stosując ten ogólny fakt do naszej sytuacji stwierdzamy, że odwzorowanie (X_1, X_2) jest $(\mathfrak{M}, 2^{\{0,1\}} \otimes 2^{\{0,1\}})$ mierzalne. Odwzorowanie $S : \{0,1\} \times \{0,1\} \ni (x_1, x_2) \to x_1 \oplus x_2 \in \{0,1\}$ jest oczywiście $(2^{\{0,1\}} \otimes 2^{\{0,1\}}, 2^{\{0,1\}})$ mierzalne, zatem $Y = X_1 \oplus X_2$ jako superpozycja odwzorowań mierzalnych (X_1, X_2) i S jest $(\mathfrak{M}, 2^{\{0,1\}})$ mierzalne, jest więc zmienną losową.

Udowodnimy teraz równomierność rozkładu zmiennej losowej $Y = X_1 \oplus X_2$. Oznaczmy:

$$\begin{array}{rcl} A_0 & = & \{\omega \in \Omega; X_1(\omega) = 0, X_2(\omega) = 0\}, \\ A_1 & = & \{\omega \in \Omega; X_1(\omega) = 1, X_2(\omega) = 0\}, \\ B_0 & = & \{\omega \in \Omega; X_1(\omega) = 1, X_2(\omega) = 1\}, \\ B_1 & = & \{\omega \in \Omega; X_1(\omega) = 0, X_2(\omega) = 1\}. \end{array}$$

Wówczas zdarzenia A_0, A_1, B_0, B_1 są parami rozłączne. Stąd i z niezależności zmiennych losowych X_1 i X_2 oznaczając $P(X_1 = 0) = p_0$, $P(X_1 = 1) = p_1$ dostajemy:

$$\begin{gathered} P(Y=1) = P(A_1 \cup B_1) = P(A_1) + P(B_1) = \\ = P(X_1 = 1) \cdot P(X_2 = 0) + \\ + P(X_1 = 0) \cdot P(X_2 = 1) = \\ = p_1 \cdot \tfrac{1}{2} + p_2 \cdot \tfrac{1}{2} = \tfrac{1}{2} \end{gathered}$$

ponieważ $p_0 + p_1 = 1$. Podobnie:

$$\begin{gathered} P(Y=0) = P(A_0 \cup B_0) = P(A_0) + P(B_0) = \\ = P(X_1 = 0) \cdot P(X_2 = 0) + \\ + P(X_1 = 1) \cdot P(X_2 = 1) = \\ = p_1 \cdot \tfrac{1}{2} + p_2 \cdot \tfrac{1}{2} = \tfrac{1}{2} \end{gathered}$$

a więc istotnie zmienna losowa $Y = X_1 \oplus X_2$ ma rozkład równomierny.