[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 2.

Treść: Skonstruować system podpisów cyfrowych ElGamala „dla małych liczb". Przyjąć odpowiedni klucz publiczny i prywatny. Podpisać dowolną wybraną wiadomość m i zweryfikować podpis.

Rozwiązanie :

1. Ustanawianie systemu. Wybieramy liczbę pierwszą np. $p = 13$. Jako generator grupy multiplikatywnej Z_{13}^* można wybrać $g = 2$, ponieważ $2^1 (mod 13) = 2$, $2^2 (mod 13) = 4$, $2^3 (mod 13) = 8$, $2^4 (mod 13) = 3$, $2^5 (mod 13) = 6$, $2^6 (mod 13) = 12$, $2^7 (mod 13) = 11$, $2^8 (mod 13) = 9$, $2^9 (mod 13) = 5$, $2^{10} (mod 13) = 10$, $2^{11} (mod 13) = 7$, $2^{12} (mod 13) = 1$ Jako klucz prywatny wybieramy losowo dowolną liczbę $x \in < 2, p-2 >$. Wybierzmy np. $x = 3$. Będzie to tajemnica strony podpisującej wiadomość. Ujawniamy klucz publiczny $y = g^x (mod p) = 2^3 (mod 13) = 8$.

2. Podpisywanie wiadomości (dokumentu) przez stronę dysponującą tajnym kluczem prywatnym x. Wybieramy jako wiadomość podpisywaną dowolna liczbę $m \in Z_{p-1}$ czyli w naszym przypadku $m \in Z_{12}$. Wiadomość jawna m jest więc jednym z elementów zbioru $0, 1, 2, \cdots, 11$. Wybierzmy jako wiadomość podpisywaną $m = 4$. Mając $m = 4$ i $x = 3$ tworzymy teraz podpis wiadomości $m = 4$ czyli odpowiednią parę uporządkowaną $(a, b) \in Z_p^* \times Z_{p-1}$. Losujemy $k \in Z_{p-1}$ takie, że $NWD(k, p-1) = 1$. Niech to będzie $k = 5$. Obliczamy k^{-1} w pierścieniu Z_{p-1} czyli w pierścieniu Z_{12}. Łatwo sprawdzić, że $k^{-1} = 5$. Obliczamy $a \in Z_p^*$ jako $g^k (mod p)$, mamy więc $2^5 (mod 13) = 6$. Obliczamy teraz $b \in Z_{p-1}$ jako $b = k^{-1} \otimes_{p-1} (m -_{12} x \otimes [a]_{p-1})$. Przy przyjętych i obliczonych wartościach mamy więc $b = 5 \otimes_{12} (4 -_{12} 3 \otimes_{12} 6) = 2$. Zatem podpis (a, b) wiadomości $m = 4$ ma postać pary uporządkowanej $(6, 2)$ a podpisywana wiadomość 4 z podpisem to para uporządkowana $(4, (6, 2))$.

3. Weryfikacja podpisu. Równanie weryfikacyjne dla podpisów ElGamala ma postać:

$$y^a \otimes_p a^b = g^m$$

gdzie podnoszenie do potęgi jest jak pierścieniu Z_p. Musimy sprawdzić dla $y = 8$, $a = 6$, $b = 2$, $m = 4$ i $g = 2$ czy równanie $(*)$ jest spełnione.

$$L = y^a \otimes_p a^b = 8^6 \cdot 2 (mod 13) = 3$$
$$P = g^m = 2^4 (mod 13) = 3$$

Mamy więc $L = P$ i równanie weryfikacyjne (*) jest spełnione, zatem przedstawiony do weryfikacji podpis akceptujemy.

1.3 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 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.

1.4 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 $3^{1105-1} - 1$.

1.5 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.

1.6 Zadanie 6.

Treść: Podać przykład szyfru Rabina „dla małych liczb". Podać przykład szyfrowania i deszyfracji.

Rozwiązanie: Generacja pary kluczy przebiega następująco:

- Wybieramy dwie liczby pierwsze p i q. Dla uproszczenia można wybrać liczby, które spełniają warunek $p \equiv q \equiv 3 \mod 4$.
- Obliczamy klucz publiczny $n = p \cdot q$.

Żeby zaszyfrować wiadomość potrzebny jest wyłącznie klucz publiczny n. Żeby odczytać wiadomość potrzebny jest również rozkład klucza na czynniki pierwsze p i q. Przykładowe wartości „dla małych liczb" - $p = 7$, $q = 11$, $n = 77$.
Szyfrowanie wiadomości $m \in P = \{0, \cdots, n-1\}$ polega na obliczeniu szyfrogramu $c = m^2 \mod n$. Przykładowo, chcąc zakodować wiadomość $m = 20$, obliczamy $c = 20^2 \mod 77 = 400 \mod 77 = 15$. Niestety, szyfrowanie nie jest jednoznaczne, ponieważ ten sam szyfrogram uzyskujemy dla czterech różnych wiadomości $m \in \{13, 20, 57, 64\}$.
Deszyfrowanie wiadomości wymaga obliczenia pierwiastków kwadratowych ze względu na obie części klucza prywatnego p i q.

$$\begin{array}{lcl} m_p & = & \sqrt{c} \mod p \\ m_q & = & \sqrt{c} \mod q \end{array}$$

Dla przykładowych małych liczb otrzymujemy $m_p = 1$ oraz $m_q = 9$. Następnie, używając rozszerzonego algorytmu Euklidesa, odnajdujemy y_p oraz y_q takie, że $y_p \cdot p + y_q \cdot q = 1$. Dla przykładowych danych $y_p = -3$ oraz $y_q = 2$. Teraz, korzystając z chińskiego twierdzenia o resztach, odnajdujemy cztery pierwiastki ($+r$, $-r$, $+s$ oraz $-s$) równania $c + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$:

$$\begin{array}{lcl} r & = & (y_p \cdot p \cdot m_q + y_q \cdot q \cdot m_p) \mod n \\ -r & = & n - r \\ s & = & (y_p \cdot p \cdot m_q - y_q \cdot q \cdot m_p) \mod n \\ -s & = & n - s \end{array}$$

Dla naszego przykładu pierwiastki tego równania przyjmują wartości $m \in \{64, 20, 13, 57\}$. Wśród nich jest zakodowana wiadomość $m = 20$.

1.7 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:

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

Dla ciała $GF(3)[x]$ mamy: $a, b, c, d \in \{0, 1, 2\}$. Aby otrzymać wielomian x^2+1, muszą być spełnione warunki: $ac \equiv 1 \mod 3$, $bd \equiv 1 \mod 3$. Zatem $a = b = c = d = 1$, co daje wielomian x^2+2x+1, a nie x^2+1.

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.

1.8 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 $a^{rzG} = 1$.

1.9 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:

$$
\begin{aligned}
\forall i \in M \quad a_i \pm b_i \mod m_i \\
\forall i \in M \quad a_i \cdot b_i \mod m_i
\end{aligned}
$$

Zatem:

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

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

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

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

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

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

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 RNS. Dodawanie:

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

Czyli uzyskaliśmy te same współczynniki. Teraz sprawdzamy poprawność mnożenia:

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

Czyli wykorzystane algorytmy dodawania i mnożenia dały poprawne rezultaty.

1.10 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.

2 Zadania przygotowujące do kolokwium #2 z PTKB

2.1 Zadanie 2.

Treść: Ile razy trzeba wykonać protokoł uwierzytelniania Fiata-Shamira by prawdopodobieństwo oszustwa było mniejsze od 10^{-100}.

Rozwiązanie: Patrz 1.1

2.2 Zadanie 3.

Treść: Pokazać jak musi spreparować protokół Fiata-Shamira Prover nie znający tajemnicy (a więc oszust lub zapominalski) by zawsze na wyzwanie $e = 1$ odpowiadać prawidłowo.

Rozwiązanie:

1. Porver nie znający tajemnicy s prawdziwego Provera (czyli nie znający klucza prywatnego) losuje liczbę $r \in Z_n, r \neq 0, 1$. Podnosi do kwadratu modulo n (przypominamy, że $n = pq$, gdzie p, q są różnymi liczbami pierwszymi) i przesyła w pierwszym kroku protokołu do Verifiera liczbę $x = (r^2(modn)(s^2(modn))^{-1})(modn)$, gdzie $s \in Z_n$ jest tajemnicą (kluczem prywatnym) prawdziwego Provera, $s^2(modn) \in Z$, kluczem publicznym a odwrotność jest n brana w pierścieniu Z_n.

2. Jeśli Verifier żąda w drugim kroku protokołu odpowiedzi na pytanie $e = 1$ to Prover wysyła do Verifiera liczbę $y = r$

3. Verifier sprawdza teraz równanie weryfikacyjne sprawdzając czy:

   $$y^2(modn) = (x * s^2)(modn)$$

   Równanie to jest dla $y = r$ i $x = (r^2(modn)(s^2(modn))^{-1})(modn)$ Proverowi udało się dobrze odpowiedzieć na pytanie $e = 1$ Verifiera.

2.3 Zadanie 9.

Treść: Niech G będzie skończoną grupą cykliczną rzędu n, a $g \in G$ generatorem tej grupy. Pokazać, że dla każdego $d \in \mathbb{N}$ g^d jest generatorem grupy G wtedy i tylko wtedy, gdy $NWD(d, n) = 1$.

Rozwiązanie: 1. Wynikanie w lewo. Niech $NWD(d, n) = 1$. Jeśli $(g^d)^{r_1} = (g^d)^{r_2}$ dla pewnych $r_1, r_2 \in \mathbb{N}$ to $g^{d(r_1 - r_2)} = 1$. Z uwagi na fakt, że g jest generatorem grupy G musimy mieć $d(r_1 - r_2) \equiv 0(\mathrm{mod}n)$ co oznacza, że $d(r_1 - r_2)$ jest wielokrotnością n. Wynika stąd, że jeśli $r_1, r_2 \in [1, n]$ to

$r_1 = r_2$. Kolejne potęgi $(g^d)^r$ dla $r = 1, 2, \cdots, n$ są więc parami różne, co dowodzi faktu, że g^d jest generatorem.
2. Wynikanie w prawo. Niech $\mathrm{NWD}(d, n) = r > 1$, wówczas istnieją takie $k_1, k_2 \in \mathbb{N}$, że $n = k_1 \cdot r$ oraz $d = k_2 \cdot r$. Oczywiście, ponieważ $r > 1$ musimy mieć $k_1 < n$. Zatem $(g^d)^{k_1} = (g^{k_2 \cdot r})^{k_1} = (g^{k_1 \cdot r})^{k_2} = (g^n)^{k_2} = 1$. Stąd wynika, że rząd elementu g^d jest co najwyżej równy k_1, a więc jest mniejszy od n, a więc g^d nie jest generatorem grupy G.

2.4 Zadanie 11.

Treść: Niech $GF(2^k)[x]$ będzie pierścieniem wielomianów o współczynnikach w ciele $GF(2^k)$. Wykazać, że dla każdego wielomianu x^n (gdzie $n \in \mathbb{N}$) z pierścienia $GF(2^k)[x]$ mamy:

$$x^n(\mathrm{mod}(x^4+1)) = x^{n(\mathrm{mod} 4)}$$

Rozwiązanie: 1. W ciele $Z_2 = \{0, 1\}$ dodawanie jest zwykłą sumą modulo 2 (oznaczaną symbolem $\oplus$). Również odejmowanie w Z_2 jest sumą modulo 2, bo mamy $1 \oplus 1 = 0$ i $0 \oplus 0 = 0$, więc $-a = a$ dla $a \in Z_2$ oraz $a -_2 b = a \oplus b$ dla $a, b \in Z_2$, gdzie $-_2$ jest odejmowaniem modulo 2 w Z_2.
2. W ciele $GF(2^k)$, którego elementami są słowa binarne o długości k, definiujemy działanie dodawania standardowo jako sumę wielomianów. W naszej sytuacji jest to jednocześnie suma modulo 2 po współrzędnych, tzn. jeśli $a = (a_1, a_2, \cdots, a_k) \in GF(2^k)$, gdzie $a_i \in \{0, 1\}$ oraz $b = (b_1, b_2, \cdots, b_k) \in GF(2^k)$, gdzie $b_i \in \{0, 1\}$ to:

$$a + b = (a_1 \oplus b_1, a_2 \oplus b_2, \cdots, a_k \oplus b_k)$$

oraz:

$$\begin{aligned} a -_2 b = (a_1 -_2 b_1, a_2 -_2 b_2, \cdots, a_k -_2 b_k) = \\ = (a_1 \oplus b_1, a_2 \oplus b_2, \cdots, a_k \oplus b_k) \end{aligned}$$

Dla $n < 4$ wzór jest zawsze prawdziwy (przypadek trywialny). Dla $n \geqslant 4$ istnieje takie $q \in \mathbb{N}$, że $n = q \cdot 4 + r$ i $0 \leqslant r < 4$, gdzie $r = n(\mathrm{mod} 4)$. Zauważmy jak przebiega dzielenie wielomianu x^n dla $n \geqslant 4$. Uwzględniając, że w ciele modulo 2 operacje dodawania i odejmowania są tożsame, mamy:

$$\begin{array}{lllllll}
x^{n-4} & + & x^{n-8} & + & \cdots & + & x^{n-q\cdot 4} \\ \hline
x^n & & & & & & \quad : \quad x^4+1 \\
x^n & + & x^{n-4} & & & & \\ \hline
 & & x^{n-4} & & & & \\
 & & x^{n-4} & + & x^{n-8} & & \\ \cline{3-7}
 & & & & \cdots & & \\ \cline{6-7}
 & & & & & & x^r
\end{array}$$

z czego wynika, że $x^n(\mathrm{mod}(x^4+1)) = x^{n(\mathrm{mod} 4)}$.

2.5 Zadanie 33.

Treść: Obliczyć wartość symbolu Legendre'a: a) $(\frac{35}{7})$ b) $(\frac{64}{5})$

Rozwiązanie:

1.
$$(\frac{35}{7}) = (\frac{5}{7})(\frac{7}{7}) = 0$$

2.
$$(\frac{64}{5}) = (\frac{4}{5}) = (\frac{2 \cdot 2}{5}) = 1$$

Symbol Legendre'a to funkcja $\left(\frac{a}{p}\right)$ (p musi być liczbą pierwszą większą od 2) zwracająca:
0, jeśli a jest wielokrotnością p
1, jeśli istnieje takie b, że $b^2 = a \mod p$
-1, jeśli nie istnieje żadne b, żeby $b^2 = a \mod p$

2.6 Zadanie 10.

Rozwiązanie: Patrz 1.10