**KOLOKWUM II (zestaw A)**

**1.** Znajdź iloraz i resztę z dzielenia wielomianu $w(X) = X^8 + X^5 + X^4 + X + 1$ przez $u(X) = X^3 + X^2 + 1$ w arytmetyce $\mathbb{Z}_2$. (3 punkty)

**2.** Rozłóż podane wielomiany na czynniki nierozkładalne we wskazanym pierścieniu: (po 1 punkcie)

a) $w(X) = X^6 + X^5 + X^2 + 1$ w $\mathbb{Z}_2[X]$
b) $w(X) = X^5 + X^3 + X$ w $\mathbb{Z}_2[X]$
c) $w(X) = X^4 + 2X^3 + 2X + 2$ w $\mathbb{Z}_3[X]$

Wskazówka: $w(a) = 0$ wtedy i tylko wtedy gdy $w(X)$ dzieli się przez $(X - a)$.

**3.** Zbuduj tabelkę mnożenia dla pierścienia ilorazowego $\mathbb{Z}_2[X]/(X^2 + X + 1)$. (3 punkty)
Czy pierścień ten jest ciałem? (1 punkt)
Czy pierścien ten zawiera pierwiastki wielomianu generującego? Jeśli tak, wskaż je. (2 punkty)

**4.** Zamierzamy przesyłać 48 bitowe bloki przez łącze o poziomie szumu 0.2 %. Wówczas prawdopodobieństwo jednoczesnego przekłamania co najmniej 3 bitów w bloku jest mniejsze niż 0.013 %, a więc by zabezpieczyć transmisję na tym poziomie, należy umożliwić korektę 2 przekłamanych bitów. Ile spośród 48 bitów bloku należy przeznaczyć w tej sytuacji na bity kontrolne? (3 punkty)

**5.** Bloki długości 63 bitów zawierają po 11 bitów kontrolnych, zabezpieczających przed przekłamaniami podczas transmisji. Ile przekłamanych bitów da się automatycznie korygować przy takim zabezpieczeniu, a ile jednoczesnych przekłamań będzie wykrywalnych? (3 punkty)

**Wielomiany nierozkładalne nad $\mathbb{Z}_2$**

st. 1: $X, \quad X + 1$

st. 2: $X^2 + X + 1$

st. 3: $X^3 + X + 1, \quad X^3 + X^2 + 1$

st. 4: $X^4 + X + 1, \quad X^4 + X^3 + 1, \quad X^4 + X^3 + X^2 + X + 1$

**Wielomiany nierozkładalne nad $\mathbb{Z}_3$**

st. 1: $X, \quad X + 1, \quad X + 2$

st. 2: $X^2 + 1, \quad X^2 + X + 2, \quad X^2 + 2X + 2$

st. 3: $X^3 + 2X + 1, \quad X^3 + 2X + 2, \quad X^3 + X^2 + 2, \quad X^3 + X^2 + X + 2, \quad X^3 + X^2 + 2X + 1, \quad X^3 + 2X^2 + 1,$
$X^3 + 2X^2 + X + 1, \quad X^3 + 2X^2 + 2X + 2$

**KOLOKWUM II (zestaw B)**

**1.** Znajdź iloraz i resztę z dzielenia wielomianu $w(X) = X^8 + X^7 + X^3 + X^2 + 1$ przez $u(X) = X^3 + X + 1$ w arytmetyce $\mathbb{Z}_2$. (3 punkty)

**2.** Rozłóż podane wielomiany na czynniki nierozkładalne we wskazanym pierścieniu: (po 1 punkcie)

a) $w(X) = X^6 + X^4 + X^3 + X^2 + X + 1$ w $\mathbb{Z}_2[X]$
b) $w(X) = X^7 + X^6 + X^5 + X^3 + 1$ w $\mathbb{Z}_2[X]$
c) $w(X) = X^4 + 2$ w $\mathbb{Z}_3[X]$

Wskazówka: $w(a) = 0$ wtedy i tylko wtedy gdy $w(X)$ dzieli się przez $(X - a)$.

**3.** Zbuduj tabelkę mnożenia dla pierścienia ilorazowego $\mathbb{Z}_2[X]/(X^2 + 1)$. (3 punkty)
Czy pierścień ten jest ciałem? (1 punkt)
Czy pierścien ten zawiera pierwiastki wielomianu generującego? Jeśli tak, wskaż je. (2 punkty)

**4.** Zamierzamy przesyłać 32 bitowe bloki przez łącze o poziomie szumu 0.25 %. Wówczas prawdopodobieństwo jednoczesnego przekłamania co najmniej 3 bitów w bloku jest mniejsze niż 0.008 %, a więc by zabezpieczyć transmisję na tym poziomie, należy umożliwić korektę 2 przekłamanych bitów. Ile spośród 32 bitów bloku należy przeznaczyć w tej sytuacji na bity kontrolne? (3 punkty)

**5.** Zamierzamy przesyłać 24-bitowe paczki informacji użytkowej. Ilu dodatkowych bitów kontrolnych potrzeba by zabezpieczyć transmisję możliwością korekty 1 przekłamanego bitu? Ile jednoczesnych przekłamań będzie można wówczas wykryć? (3 punkty)

**Wielomiany nierozkładalne nad $\mathbb{Z}_2$**

st. 1: $X, \quad X + 1$

st. 2: $X^2 + X + 1$

st. 3: $X^3 + X + 1, \quad X^3 + X^2 + 1$

st. 4: $X^4 + X + 1, \quad X^4 + X^3 + 1, \quad X^4 + X^3 + X^2 + X + 1$

**Wielomiany nierozkładalne nad $\mathbb{Z}_3$**

st. 1: $X, \quad X + 1, \quad X + 2$

st. 2: $X^2 + 1, \quad X^2 + X + 2, \quad X^2 + 2X + 2$

st. 3: $X^3 + 2X + 1, \quad X^3 + 2X + 2, \quad X^3 + X^2 + 2, \quad X^3 + X^2 + X + 2, \quad X^3 + X^2 + 2X + 1, \quad X^3 + 2X^2 + 1,$
$X^3 + 2X^2 + X + 1, \quad X^3 + 2X^2 + 2X + 2$

**ROZWIĄZANIA**

**1.** Zestaw A: $w(X) = X^8 + X^5 + X^4 + X + 1 \;=\; (X^3 + X^2 + 1)(X^5 + X^4 + X^3 + X^2 + X) \;+\; X^2 + 1$
Zestaw B: $w(X) = X^8 + X^7 + X^3 + X^2 + 1 \;=\; (X^3 + X + 1)(X^5 + X^4 + X^3) \;+\; X^2 + 1$

**2.** Zestaw A: a) $w(X) \;=\; (X+1)(X^2+X+1)(X^3+X^2+1)$
b) $w(X) \;=\; X(X^2+X+1)^2$
c) $w(X) \;=\; (X^2+1)(X^2+2X+2)$

Zestaw B: a) $w(X) \;=\; (X+1)^2(X^4+X+1)$
b) $w(X) \;=\; (X^2+X+1)^2(X^3+X^2+1)$
c) $w(X) = (X+1)(X+2)(X^2+1)$.

**3.** Notacja: para $ab$ oznacza wielomian $aX + b$.

Zestaw A

| | 01 | 10 | 11 |
|---|---|---|---|
| 01 | 01 | 10 | 11 |
| 10 | 10 | 11 | 01 |
| 11 | 11 | 01 | 10 |

Jest ciałem.
Pierwiastkami $X^2 + X + 1$ są $X = 10$ i $X = 11$.

Zestaw B

| | 01 | 10 | 11 |
|---|---|---|---|
| 01 | 01 | 10 | 11 |
| 10 | 10 | 01 | 11 |
| 11 | 11 | 11 | 00 |

Nie jest ciałem.
Pierwiastkami $X^2 + 1$ są $X = 01$ i $X = 10$.

**4.** Zestaw A: $n = 48$ oraz $t = 2$, szukamy więc największego $k$ dla którego spełniona jest nierówność

$$2^{48-k} \;\geq\; 1 + 48 + \frac{48 \cdot 47}{2} \;=\; 1177\,.$$

Ponieważ $2^{11} = 2048 > 1177 > 1024 = 2^{10}$, mamy $48 - k = 11$. Zatem liczba bitów użytkowych wynosi $k = 37$, a bitów kontrolnych jest 11.

Zestaw B: Obliczamy podobnie

$$2^{32-k} \;\geq\; 1 + 32 + \frac{32 \cdot 31}{2} \;=\; 529\,.$$

Stąd $32 - k = \lceil \log_2 529 \rceil = 10$. Potrzeba więc 10 bitów kontrolnych, a pozostałe 22 bity to bity użytkowe.

**5.** Zestaw A: $n = 63$, $k = n - 11 = 52$. Szukamy największego $t$, dla którego

$$2^{11} \;=\; 2048 \;\geq\; \binom{63}{0} + \binom{63}{1} + \cdots + \binom{63}{t}\,.$$

Widać, że największe $t$ to 2, $2048 > 1 + 63 + 63 \cdot 62/2 = 2017$. Taki kod potrafi więc korygować przekłamania na $t = 2$ bitach, a zatem jego odległość detekcyjna wynosi co najmniej $2t = 4$ bity

Zestaw B: Niech $p$ oznacza liczbę dodatkowych bitów kontrolnych, zatem $n = 24+p$. Szukamy więc najmniejszego $p$, dla którego zachodzi nierówność

$$2^p \;\geq\; \binom{n}{0} + \binom{n}{1} \;=\; 1 + n \;=\; 1 + 24 + p\,.$$

Jest to liczba $p = 5$. Kod korygujący 1 bit potrafi wykrywać (bez możliwości korekty) jednoczesne przekłamania 2 lub 3 bitów.