KOLOKWIUM I

1. Rozwiąż kongruencje a) $52x + 65 = 39 \pmod{91}$, b) $63x = 25 \pmod{35}$. (po 1.5 pkt)

2. Podaj rozwiązanie układu kongruencji (3 pkt.)

$$\begin{cases} 2x = 5 \pmod 7 \\ 3x = 5 \pmod 8 \\ 5x = 2 \pmod 9) \end{cases}$$

3. Wyznacz wartość funkcji Eulera dla liczby $n = 63$. Na tej podstawie określ podzbiór wartości $k \in \{1, 2, \ldots, \phi(n)\}$, dla których zachodzi $10^k = 1 \pmod{63}$. W szczególności jaka jest najmniejsza taka liczba k. Postaraj się przeprowadzić swoje obliczenia optymalnie, to jest tak, by wykonać jak najmniej mnożeń. (3 pkt.)

4. Wyznacz wszystkie rozwiązania $x^{13} + 4x^6 + 1 = 0 \pmod{21}$ korzystając z Chińskiego tw. o resztach. (3 pkt.)

5. Jakie są 2 ostatnie cyfry liczby 18^{241} ? (3 pkt.)

KOLOKWIUM II

1. Wyznacz NWP wielomianów $u(x) = x^5 + x^3 + x + 1$ i $w(x) = x^6 + 1$ w arytmetyce $\mathbb{Z}_2$. (3 pkt.)

2. Znajdź iloraz i resztę z dzielenia wielomianu $w(x) = 2x^7 + x^5 + 2x^4 + x^3 + 2x + 1$ przez $u(x) = 2x^3 + x + 2$ w arytmetyce $\mathbb{Z}_3$. (3 pkt.)

3. Wyprowadź wzór na mnożnenie elementów $ax+b$ i $cx+d$ w pierścieniu ilorazowym $\mathbb{Z}_3[x]/(x^2+x+1)$. (3 pkt.) Czy ten pierścień jest ciałem? (1 pkt.)

4. Które z wielomianów $u(x) = x^2 + 3x + 1$, $v(x) = x^2 + 4x + 1$, $w(x) = x^3 + x + 2$ są rozkładalne, a które nierozkładalne w pierścieniu $\mathbb{Z}_5[x]$? (3 pkt.)

5. Jak długie muszą być binarne słowa kodowe, by można było przesyłać przy ich pomocy 40-bitowe porcje danych z automatyczną korektą a) jednego lub b) dwóch bitów? (3 pkt.)

Wielomiany nierozkładalne nad $\mathbb{Z}_2$

st. 1: X, $X + 1$

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

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

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

Wielomiany nierozkładalne nad $\mathbb{Z}_3$

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

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

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

ROZWIĄZANIA — KOL. I

I.1. a) $52x = 39 - 65 = -26 = 65 \pmod{91}$. Ponieważ $\mathrm{NWP}(91, 52) = 13$ oraz prawa strona 65 także dzieli się przez 13, równanie przekształcamy do równoważnej postaci $4x = 5 \pmod 7$. Rozwiązanie ma postać $x = 3 \pmod 7$, a więc podstawowe rozwiązania wyjściowej kongruencji $52x = 65 \pmod{91}$ to

$$x \;=\; 3 + 7k \qquad \text{dla} \;\; k = 0, 1, 2, \ldots 12\,,$$

czyli $x = 3,\ 10,\ 17,\ 24,\ \ldots\ ,\ 87$.

b) Ponieważ $\mathrm{NWP}(63, 35) = 7$ oraz prawa strona kongruencji 25 jest niepodzielna przez 7, nie istnieją rozwiązania.

I.2. Rozwiązujemy poszczególne równania układu otrzymując rónoważną postać

$$\begin{cases} x = 6 \pmod 7 \\ x = 7 \pmod 8 \\ x = 4 \pmod 9\,. \end{cases}$$

Obliczamy $M = 7 \cdot 8 \cdot 9 = 504$ i kolejno

$$\begin{array}{rclcrclcrcl} M_1 & = & 72 & & M_2 & = & 63 & & M_3 & = & 56 \\ M_1^{-1} & = & 4 \pmod 7 & & M_2^{-1} & = & 7 \pmod 8 & & M_3^{-1} & = & 5 \pmod 9 \end{array}$$

Stąd $x \;=\; 6 \cdot 72 \cdot 4 \;+\; 7 \cdot 63 \cdot 7 \;+\; 4 \cdot 56 \cdot 5 \;=\; 5935 \;=\; 391 \pmod{504}$.
Sprawdzamy poprawność wyniku: $391 \bmod 7 = 6$, $391 \bmod 8 = 7$, $391 \bmod 9 = 4$.

I.3. Obliczamy $\phi(63) = \phi(7 \cdot 9) = 6 \cdot 2 \cdot 3 = 36$. Ponieważ $\mathrm{NWP}(63, 10) = 1$, z twierdzenia Eulera wynika, że $10^{36} = 1 \pmod{63}$. Najmniejsze $1 \le k \le \phi(n)$, dla którego $10^k = 1 \pmod{63}$, czyli *rząd* liczby 10 mod 63, musi być dzielnikiem 36. Wystarczy więc poszukać odpowiedzi wśród liczb 2, 3, 4, 6, 9, 12, 18, zaczynając od najmniejszych. Kolejno

$$10^2 = 37 \pmod{63}, \quad 10^3 = 55 \pmod{63}, \quad 10^4 = 46 \pmod{63}, \quad 10^6 = 1 \pmod{63}\,.$$

Stąd $10^k = 1 \pmod{63}$ zachodzi dla $k = 6, 12, 18, 24, 30$ i 36.

I.4. Zauważmy najpierw, że $x = 0$ nie jest rozwiązaniem podanego równania. Rozkładając $21 = 3 \cdot 7$, zapisujemy równoważny układ 2 równań odpowiednio mod 3 i mod 7 i upraszczamy go:

$$\begin{array}{rcl} x^{13} + 4x^6 + 1 & = & 0 \pmod 3 \\ x^{13} + 4x^6 + 1 & = & 0 \pmod 7 \end{array} \qquad \rightarrow \qquad \begin{array}{rcl} x & = & 1 \pmod 3 \\ x & = & 2 \pmod 7\,. \end{array}$$

Pierwsze z tych równań otrzymamy korzystając z faktu, że $\phi(3) = 2$, a więc $x^2 = 1 \pmod 3$ dla $x \neq 0$ oraz z uproszczeń modulo 3. Drugie równanie wynika podobnie z faktu, że $\phi(7) = 6$, a więc $x^6 = 1 \pmod 7$ dla $x \neq 0$ i uproszczeń mod 7.

Stosując teraz Chińskie tw. o resztach mamy $M_1 = 7$, $M_1^{-1} = 1 \pmod 3$, $M_2 = 3$, $M_2^{-1} = 5 \pmod 7$. Stąd

$$x \;=\; 1 \cdot 7 \cdot 1 \;+\; 2 \cdot 3 \cdot 5 \;=\; 37 \;=\; 16 \pmod{21}\,.$$

Jest to zatem jedynie rozwiązanie $x^{13} + 4x^6 + 1 = 0 \pmod{21}$.

I.5. Ponieważ $\mathrm{NWP}(100, 18) = 2 \neq 1$, rozkładamy $100 = 2^2 \cdot 5^2$ i tożsamość $x = 18^{241} \pmod{100}$ zamieniamy w podwójny układ, od razu go upraszczając mod 4 i mod 25:

$$\begin{array}{rcl} x & = & 18^{241} \pmod 4 \\ x & = & 18^{241} \pmod{25} \end{array} \qquad \rightarrow \qquad \begin{array}{rcl} x & = & 0 \pmod 4 \\ x & = & 18 \pmod{25}\,. \end{array}$$

Pierwsze równanie wynika z tego że $x = 18^{241} = 2^{241} \cdot 9^{241}$ dzieli się przez 4, a drugie z zastosowania tw. Eulera: skoro $\mathrm{NWP}(25, 18) = 1$ oraz $\phi(25) = 5 \cdot 4 = 20$, mamy $18^{241} = (18^{20})^{12} \cdot 18^1 = 18 \pmod{25}$. Rozwiązując układ obliczamy $M^1 = 25$, $M_1^{-1} = 1 \pmod 4$ oraz $M_2 = 4$, $M_2^{-1} = 19 \pmod{25}$. Stąd

$$x \;=\; 0 \cdot 25 \cdot 1 \;+\; 18 \cdot 4 \cdot 19 \;=\; 1368 \;=\; 68 \pmod{100}\,.$$

ROZWIĄZANIA — KOL. II

II.1. Ponieważ $x^5+x^3+x+1=(x+1)(x^4+x^3+1)$ oraz $x^6+1=(x+1)^2(x^2+x+1)^2$ w $\mathbb{Z}_2$, ich NWP to wielomian $x+1$.

II.2. $w(x)=2x^7+x^5+2x^4+x^3+2x+1 \;=\; (2x^3+x+2)\cdot(x^4+2) \;+\; 0$ w $\mathbb{Z}_3$.

II.3. $(ax+b)(cx+d) \;=\; (ad+bc+2ac)x \;+\; (bd+2ac) \pmod{x^2+x+1}$ w arytmetyce $\mathbb{Z}_3$. Ten pierścień ilorazowy nie jest ciałem, ponieważ wielomian generujacy $x^2+x+1=(x+2)^2$ jest rozkładalny w $\mathbb{Z}_3[x]$. Dla przykładu: $(2x+1)(x+2) \;=\; (4+1+4)x \;+\; (2+4) \;=\; 0x+0$ w arytmetyce $\mathbb{Z}_3$.

II.4. Wielomian stopnia 2 może się rozkładać tylko na czynniki liniowe $x-a$, wystarczy więc sprawdzić czy którekolwiek $a\in\mathbb{Z}_5$ jest jego pierwiastkiem. Ponieważ dla $u(x)=x^2+3x+1$ mamy $u(1)=0$, $u(x)$ dzieli się przez $(x-1)=(x+4) \pmod 5$. Podobnie dla $v(x)=x^2+4x+1$ sprawdzamy: $v(0)=1,\ v(1)=1,\ v(2)=3,\ v(3)=2,\ v(4)=3$, a więc ten wielomian jest nierozkładalny.

Jeśli $w(x)=x^3+x+2$ jest rozkładalny, jego czynniki mogą mieć tylko stopnie 1 i 2. A więc znowu wystarczy zbadać czy $w(x)$ posiada choć jeden pierwiastek w $\mathbb{Z}_5$. Ponieważ $w(4)=0$, dzieli się on przez $x-4=x+1 \pmod 5$. Rzeczywiście $w(x)=(x^2+4x+2)(x+1) \pmod 5$, a x^2+4x+2 jest już nierozkładalny

II.5. Zgodnie z opisem zadania mamy $n=40+p$, gdzie p jest liczbą bitów pomocniczych. Musimy dobrać p tak, by spełniona była odpowiednia nierówność:

a) $2^{n-40}=2^p \;\geq\; 1+n=41+p\,,$ b) $2^{n-40}=2^p \;\geq\; 1+n+\dfrac{n(n-1)}{2} \;=\; 41+p+\dfrac{(40+p)(39+p)}{2}\,.$

Najmniejsze p spełniające nierówność a) to $p=6$, natomiast b) spełniona jest dla $p\geq 11$. Zatem zabezpieczenie 40 bitów na poziome zdolności korekcyjnej 1 bitu wymaga dodania 6 bitów pomocniczych, natomiast możliwość korekty 2 bitów wymaga dodania 11 bitów kontrolnych.