-I----------

ZAKRES MATERIAŁU

I. Kongruencje
II. Małe twierdzenie Fermata
III. Podzielność
IV. Operacje binarne
V. Reprezentacje liczb
VI. Największy wspólny dzielnik
VII. Faktoryzacja
VIII. Własności działań

[001] Czy dla $m,n \in Z_+$ i $a,b,c,d \in Z$ spełnione są poniższe warunki? Odpowiedź negatywną uzasadnij. (Z oznacza zbiór liczb całkowitych).

(a) $a \equiv b(\mathrm{mod}\, m) \Rightarrow b \equiv a(\mathrm{mod}\, m)$

(b) $(a \equiv b(\mathrm{mod}\, m) \wedge b \equiv c(\mathrm{mod}\, m)) \Rightarrow a \equiv c(\mathrm{mod}\, m)$

(c) $a \equiv b(\mathrm{mod}\, m) \Rightarrow -a \equiv -b(\mathrm{mod}\, m)$

(d) $a \equiv b(\mathrm{mod}\, m) \Rightarrow a^n \equiv b^n(\mathrm{mod}\, m)$

(e) $(a \equiv b(\mathrm{mod}\, m) \wedge c \equiv d(\mathrm{mod}\, m)) \Rightarrow a+c \equiv b+d(\mathrm{mod}\, m)$

(f) $(a \equiv b(\mathrm{mod}\, m) \wedge c \equiv d(\mathrm{mod}\, m)) \Rightarrow ac \equiv bd(\mathrm{mod}\, m)$

(g) $(a \equiv b(\mathrm{mod}\, m) \wedge c \equiv d(\mathrm{mod}\, m)) \Rightarrow a/c \equiv b/d(\mathrm{mod}\, m)$

---

[002] Czy dla $a,b,c,d \in Z$ spełnione są poniższe warunki? Odpowiedź negatywną uzasadnij. (Z oznacza zbiór liczb całkowitych).

(a) $(a \mid b \wedge b \mid c) \Rightarrow a \mid c$

(b) $a \mid b \Rightarrow b \mid a$

(c) $a \mid b \Rightarrow \forall c\ (ac \mid bc)$

(d) $(a \mid c \wedge b \mid c) \Rightarrow ab \mid c$

(e) $(c \mid a \wedge c \mid b) \Rightarrow \forall d,e\ (c \mid da+eb)$

(f) $(a \mid b \wedge b \neq 0) \Rightarrow |a| \leq |b|$

(g) $(a \mid b \wedge b \mid a) \Rightarrow |a| = |b|$

(h) $\forall a,b\ (b>0 \Rightarrow \exists q,r\ (a=qb+r \wedge 0 \leq r < b))$, q, r są jednoznacznie wyznaczone

---

[003] Wykonaj poniższe operacje w arytmetyce (mod m). Podaj najmniejsze rozwiązanie w zbiorze {0, 1, ..., m-1}.

(a) $x \equiv 36 * 82(\mathrm{mod}\, 35)$

(b) $x \equiv 16^2 * 12^3(\mathrm{mod}\, 41)$

(c) $x \equiv (6^5 + 8^3) \bmod 15$

(d) $x \equiv -38(\mathrm{mod}\, 34)$

---

[004] Znajdź najmniejsze rozwiązania poniższych kongruencji w zbiorze {0, 1, ..., m-1} dla modułu m.

(a) $3x \equiv 4(\mathrm{mod}\, 7)$

(b) $9x \equiv 12(\mathrm{mod}\, 21)$

(c) $27x \equiv 72(\mathrm{mod}\, 900)$

(d) $27x \equiv 25(\mathrm{mod}\, 256)$

---

[005] Zapisz liczbę c w systemie pozycyjnym o zadanej podstawie.

(a) $135 = (.....)_2$,

(b) $426 = (.....)_3$,

(c) $189 = (.....)_5$,

(d) $845 = (.....)_6$.

---

[006] Zapisz w systemie dziesiętnym liczbę c podaną w systemie pozycyjnym o podstawie p.

(a) $(1010111)_2$,

(b) $(120210)_3$,

(c) $(10431231)_5$,

(d) $(3502102)_6$.

---

[007] Rozłóż podaną liczbę na czynniki pierwsze

(a) 1591440

(b) 45864

(c) 4454100

(d) 323400

---

[008] Niech Z_m będzie zbiorem wszystkich nieujemnych reszt mod m oraz niech $\oplus$ i $\otimes$ będą odpowiednio operacjami dodawania i mnożenia w Z_m.

$$a \oplus b \overset{def}{=} \begin{cases} a+b & \text{gdy } a+b < m \\ a+b-m & \text{gdy } a+b-m \geq m \end{cases} \qquad a \otimes b \overset{def}{=} \text{reszta z dzielenia a*b przez m}$$

Z tak określonymi działaniami Z_m jest pierścieniem przemiennym z jedynką. Zaznacz, które własności spełniają operacje $\oplus$ i $\otimes$.

(a) Oba działania są łączne.

(b) Oba działania są przemienne.

(c) Oba działania mają elementy neutralne (0 dla dodawania i 1 dla mnożenia).

(d) Dla każdego $a \in Z_m$ istnieje do niego element przeciwny (względem dodawania), jest nim m-a.

(e) Dla każdego $a \in Z_m$ istnieje do niego element odwrotny (względem mnożenia), jest nim a^{-1}, taki że $a \otimes a^{-1} = a^{-1} \otimes a = 1$.

(f) Mnożenie jest rozdzielne względem dodawania.

---

[009] Zaznacz tylko niezbędne warunki. Zbiór R, w którym określone są dwa działania $\oplus$ i $\otimes$ jest pierścieniem przemiennym z jedynką wtw

(a) R jest grupą abelową względem działania $\oplus$,

(b) działanie $\otimes$ jest rozdzielne względem działania $\oplus$,

(c) działanie $\otimes$ jest łączne (wówczas czasami dodajemy, że pierścień jest łączny),

(d) działanie $\otimes$ jest przemienne,

(e) istnieje element neutralny działania $\otimes$,

(f) dla każdego $a \in R$ istnieje do niego element odwrotny (względem działania $\otimes$), jest nim a^{-1}, taki że $a \otimes a^{-1} = a^{-1} \otimes a = 1$.

---

[010] Zaznacz tylko niezbędne warunki. Zbiór R, w którym określone są dwa działania $\oplus$ i $\otimes$ jest pierścieniem przemiennym z jedynką wtw

(a) $\forall a,b,c\ (a \oplus b) \oplus c = a \oplus (b \oplus c)$
(b) $\exists e_0\ \forall a\ (e_0 \oplus a = a \oplus e_0 = a)$
(c) $\forall a\ \exists a'\ (a \oplus a' = a' \oplus a = e_0)$
(d) $\forall a,b\ (a \oplus b = b \oplus a)$
(e) $\exists e_1\ \forall a\ (e_1 \otimes a = a \otimes e_1 = a)$
(f) $\forall a\ \exists a''\ (a \otimes a'' = a'' \otimes a = e_1)$
(g) $\forall a,b\ (a \otimes b = b \otimes a)$
(h) $\forall a,b,c\ (a \otimes b) \otimes c = a \otimes (b \otimes c)$
(i) $\forall a,b,c\ (a \oplus b) \otimes c = (a \otimes b) \oplus (a \otimes c)$

---

[011] Wykonaj operację dodawania dwóch liczb binarnych a i b.
(a) a=101010101, b=11100101
(b) a=10110010, b=111111
(c) a=111111, b=111111

---

[012] Wykonaj operację mnożenia dwóch liczb binarnych a i b.
(a) a=111000, b=101010
(b) a=111100, b=10101
(c) a=111010, b=101000

---

[013] Oblicz ostatnią cyfrę liczby 2^{1000}.

---

[014] Oblicz resztę z dzielenia liczby 2^{100} przez 31.

---

[015] Oblicz ostatnie dwie cyfry liczby 2^{1000}.

---

[016] Znajdź najmniejszy dzielnik pierwszy liczby $n=2^{82}+1$.

---

[017] Oblicz dwie ostatnie cyfry liczby 9^{9^9}.

---

[018] Oblicz ostatnie dwie cyfry liczby $9^{9^{9^9}}$.

---

[019] Oblicz $2^{100000} \bmod 55$. Skorzystaj z poniższego twierdzenia.

[TW] Jeśli $NWD(a, m) = 1$ i $n \equiv r \pmod{\varphi(m)}$, to $a^n \equiv a^r \pmod m$.

---

[020] Zbadaj, czy liczba 10^8+1 jest pierwsza.

---

[021] Uzasadnij, że 10-tą potęgę dowolnej liczby całkowitej można zapisać jako 11k lub 11k+1 dla całkowitego k.

---

[022] Rozłóż na czynniki pierwsze liczbę a. Skorzystaj z poniższego twierdzenia.

[TW] Jeśli p jest dzielnikiem pierwszym liczby $b^n - 1$, to albo

(1) $p \mid b^d - 1$ dla pewnego właściwego dzielnika d liczby n, albo

(2) $p \equiv 1 \pmod n$

Jeśli p>2 i liczba n jest nieparzysta, to w przypadku (2) mamy $p \equiv 1 \pmod{2n}$.

(a) $a = 2^{11}-1=2047$
(b) $a = 3^{15}-1=14348906$

---

[023] Znajdź ostatnią cyfrę liczby a w systemie o podstawie p. Skorzystaj z poniższego twierdzenia.

[TW] Niech p będzie liczbą pierwszą. Jeśli $p \nmid a$ i $n \equiv m \pmod{p-1}$, to $a^n \equiv a^m \pmod p$

(a) $a=2^{1000}$, p=7
(b) $a=2^{10000}$, p=11
(c) $a=2^{1000}$, p=13

---

[024] Uzasadnij, że poniżej zdefiniowane w zbiorze Z_{13} działania $\oplus$, $\otimes$ spełniają warunki (a) – (i).

$(a \oplus b) \overset{df}{=} (a + b)_{13}$ $\qquad$ $(a \otimes b) \overset{df}{=} (a * b)_{13}$

(a) $\forall a,b,c\ (a \oplus b) \oplus c = a \oplus (b \oplus c)$ łączność działania $\oplus$
(b) $\forall a,b\ (a \oplus b = b \oplus a)$ przemienność działania $\oplus$
(c) $\exists e_0\ \forall a\ (e_0 \oplus a = a \oplus e_0 = a)$ istnienie elementu neutralnego (zerowego) działania $\oplus$
(d) $\forall a\ \exists a'\ (a \oplus a' = a' \oplus a = e_0)$ dla każdego elementu z Z_{13} istnieje do niego element przeciwny
(e) $\forall a,b,c\ (a \otimes b) \otimes c = a \otimes (b \otimes c)$ łączność działania $\otimes$
(f) $\forall a,b\ (a \otimes b = b \otimes a)$ przemienność działania $\otimes$
(g) $\exists e_1\ \forall a\ (e_1 \otimes a = a \otimes e_1 = a)$ istnienie elementu neutralnego (jedynkowego) działania $\otimes$
(h) $\forall a \neq e_0\ \exists a''\ (a \otimes a'' = a'' \otimes a = e_1)$ dla każdego elementu z Z_{13} (poza zerem) istnieje element odwrotny
(i) $\forall a,b,c\ (a \oplus b) \otimes c = (a \otimes b) \oplus (a \otimes c)$ rozdzielność $\otimes$ względem $\oplus$

---

[025] Niech p będzie ustaloną liczbą pierwszą. Uzasadnij, że zbiór Z_p z działaniami zdefiniowanymi poniżej jest **ciałem**. Definicję ciała znajdziesz na wykładzie (cez.wipb.pl).

$(a \oplus b) \overset{df}{=} (a + b)_p$ $\qquad$ $(a \otimes b) \overset{df}{=} (a * b)_p$

---

[026] Niech n będzie ustaloną liczbą naturalną większą lub równą 2. Uzasadnij, że zbiór Z_n z działaniami zdefiniowanymi poniżej jest **pierścieniem przemiennym z jedynką**. Definicję pierścienia znajdziesz na wykładzie (cez.wipb.pl).

$(a \oplus b) \overset{df}{=} (a + b)_n$ $\qquad$ $(a \otimes b) \overset{df}{=} (a * b)_n$

---

[027] Wyznacz NWD dla podanych niżej wartości.
(a) NWD(400,28),
(b) NWD(632,410),
(c) NWD(368,128),
(d) NWD(336,129),
(e) NWD(720, 2700, 2160, 120),
(f) NWD(27720, 1155, 6930).

-II----------

ZAKRES MATERIAŁU

I. Definicja systemu kryptograficznego
II. Szyfr z przesunięciem (szyfr Cezara)
III. Monoalfabetyczny szyfr podstawieniowy
IV. Szyfr Vigenere'a

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI
UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY
Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

V. Szyfr przestawieniowy (permutacyjny)
VI. Szyfry afiniczne
VII. Szyfr Hilla

[028] Podaj definicje poniższych pojęć
(a) kryptogram
(b) system kryptograficzny
(c) reguła szyfrowania
(d) szyfr monoalfabetyczny
(e) szyfr polialfabetyczny
---
[029] Zdefiniuj przestrzeń kluczy dla szyfru
(a) Cezara,
(b) monoalfabetycznego podstawieniowego,
(c) permutacyjnego,
(d) Vigenere'a.
(e) afinicznego
(f) Hilla
---
[030] Podaj regułę szyfrowania dla szyfru
(a) Cezara,
(b) monoalfabetycznego podstawieniowego,
(c) permutacyjnego,
(d) Vigenere'a.
(e) afinicznego
(f) Hilla
---
[031] Podaj regułę deszyfrowania dla szyfru
(a) Cezara,
(b) monoalfabetycznego podstawieniowego,
(c) permutacyjnego,
(d) Vigenere'a.
(e) afinicznego
(f) Hilla
---
[032] Podaj kryptogram dla tekstu jawnego "`abecadlo`" utajnionego przy pomocy szyfru Cezara. Dla sprawdzenia zapisz odszyfrowany kryptogram. Przyjmij następujące założenia.
- znaki alfabetu angielskiego utożsam z liczbami z zakresu [0,...,25],
- za klucz przyjmij wartość 11.

---
[033] Podaj kryptogram dla tekstu jawnego "`abecadlo`" utajnionego przy pomocy monoalfabetyczneo szyfru podstawieniowego. Dla sprawdzenia zapisz odszyfrowany kryptogram. Przyjmij następujące założenia.
- znaki alfabetu angielskiego utożsam z liczbami z zakresu [0,...,25],
- za klucz przyjmij następujący łańcuch znaków: "`ezoadnqpbhrtvmjfusiwxkcgyl`".

---
[034] Podaj permutacje odwrotne do następujących
(a) "`ezoadnqpbhrtvmjfusiwxkcgyl`",
(b) "`yahsbfnzgxktrwioqcudpljmev`",
(c) "`vbjeinszagcqmrtwokxdhufply`".
---
[035] Podaj kryptogram dla tekstu jawnego "`abecadlo`" utajnionego przy pomocy szyfru Vigenere'a. Dla sprawdzenia zapisz odszyfrowany kryptogram. Przyjmij następujące założenia.
- znaki alfabetu angielskiego utożsam z liczbami z zakresu [0,...,25],
- za klucz przyjmij następujący łańcuch znaków: "`liczba`".

---
[036] Podaj kryptogram dla tekstu otwartego "`abecadlo`" utajnionego przy pomocy szyfru permutacyjnego. Dla sprawdzenia zapisz odszyfrowany kryptogram. Przyjmij następujące założenia.
- znaki alfabetu angielskiego utożsam z liczbami z zakresu [0,...,25],
- za klucz przyjmij następujący łańcuch znaków: "`431265`".

---
[037] Podaj wszystkie możliwe klucze dla szyfru afinicznego, przy założeniu, że przestrzeń tekstów otwartych zawiera 32 znaki (utożsamiane z literami alfabetu polskiego).
---
[038] Wyznacz elementy odwrotne do podanych (o ile istnieją) w arytmetyce (mod m). Jeśli element odwrotny nie istnieje, uzasadnij dlaczego. Wskazówka: skorzystaj z klasy int26.
(a) m=26, a = 2, 4, 5, 7, 8, 11, 14, 16, 17, 19, 22, 24,
(b) m=32, a = 2, 4, 5, 7, 8, 11, 14, 16, 17, 19, 22, 24, 26, 28, 31,
(c) m=19, a = 2, 4, 5, 7, 8, 11, 14, 16, 17.

---
[039] Podaj kryptogram dla tekstu jawnego "`abecadlo`" utajnionego przy pomocy szyfru afinicznego. Dla sprawdzenia zapisz odszyfrowany kryptogram. Przyjmij następujące założenia.
- znaki alfabetu angielskiego utożsam z liczbami z zakresu [0,...,25],
- za klucz przyjmij dowolną (możliwą) parę liczb. Do odpowiedzi dołącz również wybrany klucz.

---
[040] Które z podanych niżej szyfrów są polialfabetyczne
(a) Cezara,
(b) monoalfabetyczny podstawieniowy,
(c) permutacyjny,
(d) Vigenere'a,
(e) afiniczny
(f) Hilla.
---
[041] Które z podanych niżej szyfrów są monoalfabetyczne
(a) Cezara,
(b) monoalfabetyczny podstawieniowy,
(c) permutacyjny,
(d) Vigenere'a,
(e) afiniczny
(f) Hilla.
---
[042] Wyjaśnij pojęcia
(a) macierz odwrotna,
(b) macierz odwracalna,
(c) dopełnienie algebraiczne,
(d) wyznacznik macierzy,
(e) minor elementu,
(f) macierz transponowana,
(g) macierz dołączona,

KAPITAŁ LUDZKI NARODOWA STRATEGIA SPÓJNOŚCI
UNIA EUROPEJSKA EUROPEJSKI FUNDUSZ SPOŁECZNY
Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

(h) macierz osobliwa.

---

[043] Wyznacz ręcznie macierze odwrotne do podanych (o ile istnieją). Skorzystaj z metody bazującej na macierzy dopełnień algebraicznych. W przypadku braku macierzy odwrotnej, uzasadnij dlaczego nie istnieje.

(a) $\begin{bmatrix} 1 & 2 & 1 \\ 3 & 0 & 1 \\ -1 & -1 & 4 \end{bmatrix}$ (b) $\begin{bmatrix} 1 & 4 & 4 \\ 3 & 3 & 1 \\ 8 & 1 & 4 \end{bmatrix}$ (c) $\begin{bmatrix} 1 & 4 & 4 \\ 3 & 2 & 3 \\ 1 & 6 & 4 \end{bmatrix}$

---

[044] Wyznacz ręcznie macierze dopełnień algebraicznych zadanych macierzy.

(a) $\begin{bmatrix} 1 & 2 & 1 \\ 3 & 0 & 1 \\ -1 & -1 & 4 \end{bmatrix}$ (b) $\begin{bmatrix} 1 & 4 & 4 \\ 3 & 3 & 1 \\ 8 & 1 & 4 \end{bmatrix}$ (c) $\begin{bmatrix} 1 & 4 & 4 \\ 3 & 2 & 3 \\ 1 & 6 & 4 \end{bmatrix}$

---

[045] Wyznacz macierze odwrotne do podanych w arytmetyce (mod m). W przypadku braku macierzy odwrotnej, uzasadnij dlaczego nie istnieje.

(a) m=26 $\begin{bmatrix} 1 & 3 & 2 & 3 \\ 2 & 6 & 3 & 11 \\ 3 & 4 & 8 & 20 \\ 1 & 21 & 12 & 8 \end{bmatrix}$ (b) m=32 $\begin{bmatrix} 4 & 3 & 2 & 3 \\ 2 & 6 & 5 & 10 \\ 3 & 4 & 8 & 20 \\ 3 & 23 & 12 & 8 \end{bmatrix}$ (c) m=41 $\begin{bmatrix} 1 & 3 & 2 & 3 \\ 2 & 6 & 5 & 1 \\ 3 & 1 & 8 & 20 \\ 3 & 23 & 12 & 8 \end{bmatrix}$

---

[046] Wyznacz macierze dopełnień algebraicznych zadanych macierzy w arytmetyce (mod m).

(a) m=26 $\begin{bmatrix} 1 & 3 & 2 & 3 \\ 2 & 6 & 3 & 11 \\ 3 & 4 & 8 & 20 \\ 1 & 21 & 12 & 8 \end{bmatrix}$ (b) m=32 $\begin{bmatrix} 4 & 3 & 2 & 3 \\ 2 & 6 & 5 & 10 \\ 3 & 4 & 8 & 20 \\ 3 & 23 & 12 & 8 \end{bmatrix}$ (c) m=41 $\begin{bmatrix} 1 & 3 & 2 & 3 \\ 2 & 6 & 5 & 1 \\ 3 & 1 & 8 & 20 \\ 3 & 23 & 12 & 8 \end{bmatrix}$

[047] Podaj kryptogram dla tekstu jawnego "`abecadlo`" utajnionego przy pomocy szyfru Hilla. Dla sprawdzenia zapisz odszyfrowany kryptogram. Przyjmij następujące założenia.

- znaki alfabetu angielskiego utożsam z liczbami z zakresu [0,...,25],
- za klucz przyjmij macierz

$$\begin{bmatrix} 1 & 3 & 2 & 3 \\ 2 & 6 & 3 & 11 \\ 3 & 4 & 8 & 20 \\ 1 & 21 & 12 & 8 \end{bmatrix}.$$

---

[048] Wyznacz ręcznie element odwrotny do $a \in Z_m$ (tj. element $a^{-1} \in Z_m$). Skorzystaj z rozszerzonego algorytmu Euklidesa.

(a) a=29, m=75
(b) a=11, m=101,
(c) a=5, m=13,
(d) a=13, m=17,
(e) a=19, m=23,

---

[049] Wyznacz ręcznie wyznaczniki poniższych macierzy. Skorzystaj z algorytmu z rozwinięciem Laplace'a.

(a) $\begin{bmatrix} 1 & 2 & 1 \\ 3 & 0 & 1 \\ -1 & -1 & 4 \end{bmatrix}$ (b) $\begin{bmatrix} 1 & 4 & 4 \\ 3 & 3 & 1 \\ 8 & 1 & 4 \end{bmatrix}$ (c) $\begin{bmatrix} 1 & 4 & 4 \\ 3 & 2 & 3 \\ 1 & 6 & 4 \end{bmatrix}$

---

[050] Wyznacz wyznaczniki zadanych macierzy w arytmetyce (mod m).

(a) m=26 $\begin{bmatrix} 1 & 3 & 2 & 3 \\ 2 & 6 & 3 & 11 \\ 3 & 4 & 8 & 20 \\ 1 & 21 & 12 & 8 \end{bmatrix}$ (b) m=32 $\begin{bmatrix} 4 & 3 & 2 & 3 \\ 2 & 6 & 5 & 10 \\ 3 & 4 & 8 & 20 \\ 3 & 23 & 12 & 8 \end{bmatrix}$ (c) m=41 $\begin{bmatrix} 1 & 3 & 2 & 3 \\ 2 & 6 & 5 & 1 \\ 3 & 1 & 8 & 20 \\ 3 & 23 & 12 & 8 \end{bmatrix}$

---

[051] Wypisz wszystkie możliwe klucze dla szyfru Cezara przy założeniu, że zbiór wszystkich możliwych komunikatów reprezentuje alfabet polski (32 litery).

---

[052] Określ zbiór możliwych kluczy i wyznacz jego liczność dla monoalfabetycznego szyfru podstawieniowego przy założeniu, że zbiór wszystkich możliwych komunikatów reprezentuje alfabet polski (32 litery).

---

[053] Określ zbiór możliwych 5-elementowych kluczy i wyznacz jego liczność dla szyfru Vigenere'a przy założeniu, że zbiór wszystkich możliwych komunikatów reprezentuje alfabet polski (32 litery).

---

[054] Określ zbiór możliwych 5-elementowych kluczy i wyznacz jego liczność dla szyfru permutacyjnego przy założeniu, że zbiór wszystkich możliwych komunikatów reprezentuje alfabet polski (32 litery).

---

[055] Zaimplementuj metodę znajdowania elementu odwrotnego do $a \in Z_m$. (rozszerzony algorytm Euklidesa)

---

[056] Zaimplementuj metodę wyznaczającą NWD(x, y) (algorytm Euklidesa).

---

[057]

(a) Zaimplementuj metodę wyznaczającą wyznacznik macierzy kwadratowej dowolnego rozmiaru.
(b) Zaimplementuj metodę wyznaczającą wyznacznik macierzy kwadratowej dowolnego rozmiaru w arytmetyce mod m.

---

[058]

(a) Zaimplementuj metodę wyznaczającą macierz dopełnień algebraicznych macierzy kwadratowej dowolnego rozmiaru.
(b) Zaimplementuj metodę wyznaczającą macierz dopełnień algebraicznych macierzy kwadratowej dowolnego rozmiaru w arytmetyce mod m.

---

[059]

(a) Zaimplementuj metodę wyznaczającą macierz odwrotną do odwracalnej macierzy kwadratowej dowolnego rozmiaru.
(b) Zaimplementuj metodę wyznaczającą macierz odwrotną do odwracalnej macierzy kwadratowej dowolnego rozmiaru w arytmetyce mod m.

-III----------

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI
UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY
Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

ZAKRES MATERIAŁU

Kryptoanaliza systemu Vigenere'a

I. Odgadywanie długości klucza
- **(A) Klasyczna metoda Kasiskiego**
- **(B) Statystyczna metoda Friedmana**

II. Ustalanie klucza przy znajomości jego długości

[060] Wyznacz tablicę częstości i tablicę prawdopodobieństw występowania poszczególnych liter alfabetu angielskiego w podanym niżej tekście. Spacje pomiń.

(a) "generally speaking the difference between bring and take is that we use "
(b) "bring when we carry something to somebody who is speaking and take w"
(c) "hen we carry something from somebody who is speaking for example you"
(d) " bring your book with you to the school whilst after the lesson you t"
(e) "ou take your book home with you"

---

[061] Wyznacz tablicę częstości i tablicę prawdopodobieństw występowania poszczególnych liter alfabetu polskiego w podanym niżej tekście. Spacje pomiń.

(a) "programowanie dynamiczne to technika projektowania algorytmów stoso"
(b) "wana często przy problemach optymalizacyjnych problem zostaje podzi"
(c) "elony na mniejsze problemy najpierw rozwiązywane są mniejsze podpro"
(d) "blemy a ich wyniki zostają przechowywane w celu ponownego wykorzyst"
(e) "ania do wyznaczenia podproblemów wyższego rzędu"

---

[062] Podaj kryptogram dla tekstu jawnego (podanego w zadaniu [061]) utajnionego przy pomocy monoalfabetycznego szyfru podstawieniowego. Dla sprawdzenia zapisz tekst otwarty po deszyfrowaniu. Skorzystaj z metod klasy podst_mono.

- za klucz przyjmij następujący łańcuch znaków "nądlfojśćżwhękzńperótuyźćmłasgbi".

---

[063] Poniższy kryptogram uzyskano przy wykorzystaniu szyfru Vigenere'a. Wyłapano w nim następujące powtarzające się ciągi znaków: kas, mvr, huo, tyx.

Pozycje znaku k podciągu "kas" w kryptogramie to 26, 602, 824, 1070, 1316, 1340,
Pozycje znaku m podciągu "mvr" w kryptogramie to 231, 519, 579, 1041,1185,
Pozycje znaku h podciągu "huo" w kryptogramie to 256, 1216, 1378,
Pozycje znaku t podciągu "tyx" w kryptogramie to 280, 625, 919, 932, 1261, 1297.
Na podstawie podanych informacji określ prawdopodobną długość klucza szyfru.

mrpihbqrrivlmaeusqofzgsqks**kas**pynmxffsoehtqktrbbgyajvfnwbcxrpydvmvndcrg
prnetbduorvwoansvghnmrflgnzusewpyrgkwiktvgsggoidqeipkhuekpyrifoskpczki
elhlvejhfsyrdlcsontkmcdiezrndajrazotibqnvaewofimdxhescreglwmvmfvmeevfl
ztzhbfyrreubbikaafesv**mvr**cadxyriffksamrpihvynrl**huo**yuhtbbdvvflztzhbbdhvk
bnwejycedhzlhlzefysamrpihvynrksfocixhxoyjaoeodbxmnxdgkwiktvdsldhvxbpby
gmwbxkvrqnxbvecbcecrfrvakxrgy**tyx**rrmrpihvynbxmvddfxgaytexqrcsrkwyinvxrg
ybvtbrhatmqbzyjrazotibqpbygmctbagamvcsllqrztzuzrdogeovxtvqhndtrvyfknue
waoaivflztrgoyiszlarknzgugrak**mvr**iaixvnmkruzrknuthgsmvlgvwpcxhbnethrrgi
kaqnbewnzcvaegwaqow**mvr**moubbtknuyiamtzhbfyf**kas**pbygmctbagawpzrfvsfc**tyx**gr
dhixogccrgprqrvthyirvwipodrlmzwekkwpmrpihbqrrivlesvlrvpfvksadeevflztzh
bxoyjyceontkmcdifgoandvvflztzhbvxtybgpksvtbrxdllseynrgsggoiddhllzvcezr
zoogohrlockiihtxoyjhbrpoixbpbygmwbxaewcaoffkrrmrpihvyn**kas**fokvrgnbectpr
veuhfxxongofkpluzvmaewocbimthruepbbgrijbbfdaevsgregkwiktvdslmaegcgleux
fvfeuyfbw**tyx**dhllzvyri**tyx**ofimdxhescreqeipkhuekpyrardhfwvncbvxbcbomxbgyb
vlspervtunsnjmqbwplmogsoetzyilzfwgodzgheedvkggrejxqhbikrwfkmr**mvr**wakbqn
vdvywastzhboksvwicyn**kas**nzpcbqndifgcscazwsamrpihvynvlgrxtztzyiajrazotib
qrxcirdgsoebgncgfhrncikloczlzxrhcekawfssuxtvxeuumgredxhuydzgkuscy**mvr**na
ktwfontkmcdeutbqpoipvndujx**huo**mflhpymdhbsyrdhtncydfsgbittzrxcirdgsoebgv
x**tyx**oczlzvogsoehtfonubbtwejlotosnaseo**tyx**grxdvksamouxgnxd**kas**eocvbjvxggt
fgidvvcqos**kas**zosjturlyllwaqaitbqymbxmtonvkogodsr**huo**pluzvmkvrcsdhvlsanei

---

[064] Wyznacz wskaźnik koincydencji dla tekstów pisanych w języku angielskim.

A	B	C	D	E	F	G	H	I	J	K	L	M
0,082	0,015	0,028	0,043	0,127	0,022	0,020	0,061	0,070	0,002	0,008	0,040	0,024
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0,067	0,075	0,019	0,001	0,060	0,063	0,091	0,028	0,010	0,023	0,001	0,020	0,001

Tab. Prawdopodobieństwa wystąpienia 26 liter alfabetu języka angielskiego

---

[065] Wyznacz wskaźnik koincydencji dla tekstów pisanych w języku polskim.

A	Ą	B	C	Ć	D	E	Ę	F	G	H	I	J
0,0861	0,0111	0,0149	0,0382	0,0056	0,0333	0,0878	0,0140	0,0036	0,0140	0,0093	0,0865	0,0281
K	L	Ł	M	N	Ń	O	Ó	P	R	S	Ś	T
0,0295	0,0219	0,0136	0,0335	0,0560	0,0012	0,0734	0,0079	0,0274	0,0372	0,0417	0,0084	0,0430
U	W	Y	Z	Ź	Ż							
0,0205	0,0425	0,0385	0,0567	0,0006	0,0124							

Tab. Prawdopodobieństwa wystąpienia 32 liter alfabetu języka polskiego

---

[066] Poniższy kryptogram uzyskano stosując szyfr Vigenere'a. Metodą Kasiskiego wyznaczono (prawdopodobną) długość klucza m=5. Podaj 5 podciągów poniższego ciągu znaków, dla których wskaźniki koincydencji (wyznaczane w metodzie Friedmana) będą (prawdopodobnie) najbardziej zbliżone do wartości 0,065. Zaszyfrowano tekst angielski.

"dfwkogusfuwvrwadzsqalfywckgeeivzxleckldtkiigicrfoenzrwhortslstewiyewhl"

---

[067] Wyznacz wskaźnik koincydencji dla poniższego kryptogramu. Zaszyfrowano tekst w języku angielskim.

"mrpihbqrrivlmaeusqofzgsqkskaspynmxffsoehtqktrbbgyajvfnwbcxrpydvmvndcrg"

---

[068] Wyznacz wzajemny indeks zgodności dla poniższych ciągów znaków

(a) s1="dfwkogusfuwvrwadzsqalfywck"
    s2="eeivzxleckldtkiigicrfoenzrwhortslst"
(b) s1="mrpihbqrrivlmaeusqof"
    s3="kskaspynmxffsoehtqktrbbgyajvf"

---

[069] Zdefiniuj pojęcia

(a) indeks zgodności (współczynnik koincydencji)
(b) wzajemny indeks zgodności

---

[070] Okazało się, że indeksy zgodności $I_c(T)$ i $I_c(X)$ (tekstu T i jego szyfrogramu X) są sobie równe. Na tej podstawie możemy stwierdzić, że do uzyskania szyfrogramu X najprawdopodobniej nie zastosowano szyfru

(a) Cezara
(b) monoalfabetycznego podstawieniowego
(c) permutacyjnego

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI
UNIA EUROPEJSKA EUROPEJSKI FUNDUSZ SPOŁECZNY
Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

(d) Vigenere'a
(e) afinicznego
(f) Hilla

-IV----------

ZAKRES MATERIAŁU

I. Entropia
II. Kodowania Huffmana

[071]
(a) Niech $P = \{a, b, c, d, e, f\}$ będzie zbiorem tekstów otwartych i niech prawdopodobieństwa a priori wystąpienia poszczególnych znaków tego zbioru będą równe odpowiednio p(a)=1/8, p(b)=1/4, p(c)=1/8, p(d)=3/16, p(e)=1/16, p(f)=1/4. Wyznacz entropię H(P) związaną z zapisaniem jednego znaku z podanego zbioru.
(b) Niech $P = \{a, b\}$ będzie przestrzenią tekstów jawnych oraz niech prawdopodobieństwa a priori wystąpienia poszczególnych znaków tego zbioru będą równe $p_P(a) = 1/4$ i $p_P(b) = 3/4$. Wyznacz entropię H(P).

---
[072] Eksperyment polega na n-krotnym rzucie symetryczną kostką sześcienną. Zbiór możliwych wyników jednego rzutu to X={I, II, III, IV, V, VI}. Które z poniższych kodowań jest wolne od przedrostków. Dla kodowań nie spełniających tej własności podaj odpowiedni kontrprzykład.
(a) f(I)=100, f(II)=101, f(III)=110, f(IV)=111, f(V)=00, f(VI)=01,
(b) g(I)=000, g(II)=001, g(III)=010, g(IV)=011, g(V)=100, g(VI)=101,
(c) h(I)=000, h(II)=001, h(III)=011, h(IV)=111, h(V)=101, h(VI)=010,
(d) p(I)=00, p(II)=01, p(III)=10, p(IV)=11, p(V)=001, p(VI)=010,

---
[073] Wyznacz średnią długość kodowania elementu z X w przypadku funkcji f, g, h, p z zadania [072].

---
[074] Wygeneruj drzewo kodów Huffmana do zakodowania poniżej podanego tekstu. Uwzględnij spacje.
(a) "ala ma kota a kot ma ale",
(b) "stol z powylamywanymi nogami",
(c) "chrzaszcz brzmi w trzcinie",
(d) "hipopotam".

---
[075] Przypisz kody znakom znajdującym się w liściach poszczególnych drzew Huffmana z zadania [074].

---
[076] Zakoduj tekst podany w poszczególnych podpunktach w zadaniu [074] przy pomocy wyznaczonych w zadaniu [075] kodów Huffmana.

---
[077] Na podstawie przypisanych znakom kodów Huffmana odczytaj zakodowany tekst. Odrzuć nadmiarowe zera z końcówki ciągu.
(a) `00110110111010000111001111000111100010101001011011001101010111`0
`o=111, d=000, i=1010, w=010, r=1011, a=0111, ń=0110, t=1101, p=001, b=1000, s=1100, e=1001 //18 znaków`
(b) `011011001111100000000`
`k=01, a=110, r=10, s=00, e=111 //5 znaków`
(c) `11110001101111001001100100000`
`k=111, a=10, r=00, u=011, t=010, y=110 //10 znaków`
(d) `11001011011000`
`k=11, a=10, r=00, s=01 //6 znaków`

---
[078] Wyznacz średnią długość kodowania znaku algorytmem Huffmana dla każdego z tekstów z zadania [074]. Kody znaków ustalono w zadaniu [075].

---
[079] Przypisz kody znakom znajdującym się w liściach drzewa Huffmana przeczytanego w porządku KLP (korzeń – lewy - prawy). Węzły wewnętrzne oznaczono znakiem '_'. "spc" oznacza spację.
(a) <KLP>: _, _, s, k, _, r, _, a, e,
(b) <KLP>: _, _, _, a, c, _, e, k, _, _, o, r, _, n, t,

---
[080] Zdefiniuj pojęcia
(a) entropia
(b) średnia długość kodowania

---
[081] Wyznacz
(a) entropię jednego rzutu monetą
(b) entropię n niezależnych rzutów monetą

---
[082] Niech X będzie zmienną losową przyjmującą trzy wartości a1, a2, a3 z prawdopodobieństwami p1=1/2, p2=1/4, p3=1/4. Wyznacz entropię losowo wybranej wartości ze zbioru X.

-V----------

ZAKRES MATERIAŁU

I. System kryptograficzny RSA
(A) Generowanie kluczy (publicznego i prywatnego)
(B) Szyfrowanie
(C) Deszyfrowanie
II. Sito Eratostenesa
III. Szybki algorytm potęgowania a^c (mod n)

[083] Określ przestrzeń kluczy w systemie RSA. Podaj regułę szyfrowania i deszyfrowania w tym systemie.

---
[084] Określ każdy ze składników klucza publicznego (n,b) i prywatnego (p,q,a) systemu RSA.

---
[085] Wygeneruj klucz publiczny i prywatny w systemie RSA dla poniższych danych. Jeśli wartości p i q nie spełniają narzucanych na nie warunków, uzasadnij dlaczego.
(a) p=11, q=107,
(b) p=17, q=23,
(c) p=8, q=13,
(d) p=19, q=29.

---
[086] System RSA jako szyfr blokowy. Dane są N-elementowy alfabet $\Sigma = \{0,1,...,N-1\}$ oraz wartości p, q. Ustal (dla szyfrowania) długość bloków tekstu jawnego. Jeśli dane nie spełniają narzucanych na nie warunków, uzasadnij dlaczego.
(a) p=13, q=11, $\Sigma = \{0,1,...,8\}$,
(b) p=19, q=13, $\Sigma = \{a, b, c, d, e, f, g, h, l, o\}$,
(c) p=13, q=17, $\Sigma = \{A, B, C, D, F, G, Ż\}$,
(d) p=4, q=13, $\Sigma = \{!, @, \#, \$, \%, \^{}\}$.

KAPITAŁ LUDZKI NARODOWA STRATEGIA SPÓJNOŚCI
UNIA EUROPEJSKA EUROPEJSKI FUNDUSZ SPOŁECZNY
Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

[087] System RSA w wersji blokowej. Podaj kryptogram zadanego tekstu jawnego i parametrów ustalonych w zadaniu [086].
(a) ”813432”,
(b) ”abecadlo”,
(c) ”BAGAŻ”,
(d) ”@%$!$#”.
---
[088] System RSA w wersji blokowej. Odszyfruj podany niżej kryptogram. Moduł RSA (n), wykładnik deszyfrowania (a) i alfabet (Σ) podano w nawiasie.
(a) aabalk (n=391, a=235, Σ =”abcdefghijklmnop”),
(b) alkbdl (n=391, a=235, Σ =”abcdefghijklmnop”),
(c) aggaem (n=299, a=53, Σ =”abcdefghijklmnop”),
(d) akxbcaazm (n=323, a=173, Σ =”abcdefklmnoprxyz”).
---
[089] Korzystając z szybkiego algorytmu potęgowania wykonaj poniższe operacje. Podaj rozwiązania w zbiorze {0, 1, ..., m-1} dla modułu m.
(a) $111^{341} \pmod{391}$,
(b) $131^{311} * 13^{41} \pmod{381}$,
(c) $8 * 31^{353} \pmod{83}$,
(d) $561^{(41+1)/2} \pmod{346}$.
---
[090] Wykonaj ręcznie następujące operacje. Skorzystaj z szybkiego algorytmu potęgowania (mod n).
(a) $111^{235} \pmod{391}$,
(b) $27^{235} \pmod{391}$,
(c) $78^{235} \pmod{391}$,
(d) $6^{3} \pmod{9}$,
(e) $5^{6} \pmod{11}$,
(f) $4^{8} \pmod{12}$,
(g) $13^{6} \pmod{13}$.
---
[091] Zaimplementuj metodę szybkiego potęgowania mod m.
---
[092] Wygeneruj klucze (prywatny i publiczny) i niezbędne parametry systemu RSA dla parametrów p = 11 i q = 23.
---
[093] Przeanalizuj (ręcznie) działanie szyfru RSA dla p=17, q=23, alfabetu Σ ={a,b,c,d,e,f,g,h,i,j,k,l,m,n,o,p} (16 znaków) i tekstu otwartego ”abecadlo”.
-VI----------

ZAKRES MATERIAŁU

I. Testy pierwszości liczb i faktoryzacja
(A) Sito Eratostenesa
(B) Algorytm Solovaya-Strassena - Probabilistyczny test na liczby pierwsze

[094] Ile iteracji wykona algorytm sita Eratostenesa w przypadku wyznaczania wszystkich liczb pierwszych mniejszych bądź równych od zadanej wartości. Zakładamy, że iteracje, w których nie następuje żadne wykreślenie również są wliczane.
(a) p=113,
(b) p=26,
(c) p=142,
(d) p=5231.
---
[095] Wyznacz, korzystając z algorytmu sita Eratostenesa wszystkie liczby pierwsze mniejsze bądź równe od podanej wartości.
(a) p=432,
(b) p=812,
(c) p=18,
(d) p=243.
---
[096] Podaj zbiór reszt kwadratowych dla modułu p.
(a) p=11,
(b) p=13,
(c) p=17,
(d) p=19,
---
[097] Wyznacz z definicji wartość symbolu Legendre’a.
(a) $\left(\frac{4}{11}\right)$ (b) $\left(\frac{8}{13}\right)$ (c) $\left(\frac{2}{17}\right)$ (d) $\left(\frac{5}{19}\right)$
---
[098] Wyznacz wartość symbolu Jacobiego. Zapisz z jakich własności korzystałeś w kolejnych krokach.
(a) $\left(\frac{431}{1111}\right)$ (b) $\left(\frac{832}{1331}\right)$ (c) $\left(\frac{213}{1527}\right)$ (d) $\left(\frac{1132}{1239}\right)$
---
[099] Algorytm Solovaya-Strassena sprawdzania pierwszości liczb. Dla zadanej liczby nieparzystej n i wylosowanej z zakresu [1,n-1] wartości a algorytm sprawdził, że spełniona jest własność $\left(\left(\frac{a}{n}\right) \equiv a^{(n-1)/2} \pmod{n}\right)$. Na tej podstawie możemy stwierdzić, że
(a) n jest liczbą pierwszą,
(b) n jest liczbą złożoną,
(c) n jest liczbą pseudopierwszą Eulera,
(d) n może być liczbą pierwszą albo liczbą pseudopierwszą Eulera.
---
[100] Zdefiniuj pojęcia
(a) liczby względnie pierwsze,
(b) pseudopierwsza liczba Eulera.
---
[101] Wypisz (po przecinku) liczby pierwsze znajdujące się w poniższym ciągu liczb naturalnych.
1,2,3,5,23,29,31,37,41,43,47,53,57,59,61,67,71,73,79,83,89,97,101,109,127,
131,133,137,139,151,153,157,163,167,173,177,179,181,183,191,193,197,199,811
---
[102] Zaimplementuj metodę sprawdzającą, czy zadana liczba jest pierwsza. Zastosuj sito Eratostenesa.
---
[103] Wybierz własności symbolu Jacobiego. Niech n będzie nieparzystą liczbą naturalną
(a) $\left(\frac{m}{n}\right) = 0$ wtw $NWD(m,n) \neq 1$

KAPITAŁ LUDZKI NARODOWA STRATEGIA SPÓJNOŚCI
UNIA EUROPEJSKA EUROPEJSKI FUNDUSZ SPOŁECZNY
Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

(b) $\left(\frac{1}{n}\right) = 1$

(c) jeśli m jest nieparzystą liczbą naturalną, to $\left(\frac{m}{n}\right) = \begin{cases} -\left(\frac{n}{m}\right) & \text{gdy } m \equiv n \equiv 3 (\mathrm{mod}\, 4) \\ \left(\frac{n}{m}\right) & \text{w przeciwnym przypadku} \end{cases}$

(d) jeśli $m_1 \equiv m_2 (\mathrm{mod}\, n)$, to $\left(\frac{m_1}{n}\right) = \left(\frac{m_2}{n}\right)$

(e) $\left(\frac{2}{n}\right) = \begin{cases} 1 & \text{gdy } n \equiv \pm 1 (\mathrm{mod}\, 8) \\ -1 & \text{gdy } n \equiv \pm 3 (\mathrm{mod}\, 8) \end{cases}$

(f) $\left(\frac{m_1 * m_2}{n}\right) = \left(\frac{m_1}{n}\right)\left(\frac{m_2}{n}\right)$

(g) $\left(\frac{a}{n}\right) = \prod_{i=1}^{k}\left(\frac{a}{p_i}\right)^{e_i}$, gdzie $p_1^{e_1} \ldots p_k^{e_k}$ - rozkład liczby n na czynniki pierwsze, $a \geq 0$ (a – liczba naturalna)

---

[104] Zaimplementuj metodę wyznaczającą wartość symbolu Jacobiego.

---

[105] Zdefiniuj pojęcia
(a) reszta kwadratowa
(b) niereszta kwadratowa

---

[106] Zdefiniuj pojęcia
(a) symbol Legendre'a
(b) symbol Jacobiego

---

[107] Jeśli NWD(a, r) = 1, to w zbiorze liczb A = {a*n+r: n∈N} istnieje
(a) co najwyżej $a^{\varphi(r)}$ liczb pierwszych,
(b) co najwyżej $\lfloor\sqrt{a}\rfloor$ liczb pierwszych,
(c) co najwyżej $\frac{\varphi(a)}{2}$ liczb pierwszych,
(d) nieskończenie wiele liczb pierwszych.

---

[108] Wybierz poprawne określenie dla pojęcia pseudopierwsza liczba Eulera.
(a) n∈N jest pseudopierwszą liczbą Eulera wtw ma dokładnie dwa różne dzielniki naturalne.
(b) n∈N jest pseudopierwszą liczbą Eulera przy podstawie a wtw $\left(\frac{a}{n}\right) \equiv a^{(n-1)/2} (\mathrm{mod}\, n)$.
(c) m∈N jest pseudopierwszą liczbą Eulera przy podstawie a wtw NWD(a, m) =1.
(d) n∈N jest pseudopierwszą liczbą Eulera przy podstawie a wtw n jest liczbą złożoną i $\left(\frac{a}{n}\right) \equiv a^{(n-1)/2} (\mathrm{mod}\, n)$

---

[109] Niech p będzie nieparzystą liczbą pierwszą. Liczba naturalna a (1<=a<p) jest resztą kwadratową modulo p, jeśli
(a) kongruencja $x^2 \equiv a \pmod p$ ma rozwiązanie
(b) $x^{(p-1)/2} \equiv 1 \pmod p$
(c) symbol Legendre'a (a/p) = 1
(d) symbol Legendre'a (a/p) = -1
(e) $a \equiv 0 \pmod p$

---

[110] Niech p będzie nieparzystą liczbą pierwszą. Liczba naturalna a (1<=a<p) jest niereszą kwadratową modulo p, jeśli
(a) kongruencja $x^2 \equiv a \pmod p$ ma rozwiązanie
(b) $x^{(p-1)/2} \equiv 1 \pmod p$
(c) symbol Jacobiego (a/p) = -1
(d) symbol Legendre'a (a/p) = -1
(e) $a \equiv 0 \pmod p$

---

[111] Niech n będzie nieparzystą liczbą naturalną, a≥0 i symbol Jacobiego (a/n)=m. Na tej podstawie możemy stwierdzić, że
(A) n jest liczbą pierwszą,
(B) n jest liczbą złożoną,
(C) n jest liczbą pseudopierwszą Eulera,
(D) n może być liczbą pierwszą albo liczbą pseudopierwszą Eulera
(E) podano za mało informacji, aby stwierdzić któryś z powyższych przypadków.
(a) m=1
(b) m=-1
(c) m=0

---

[112] Dla liczby N=51129 wyznacz największy czynnik mniejszy bądź równy $\sqrt{N}$. Skorzystaj z algorytmu sita kwadratowego i tablic odsiewania dla m_1=5, m_2=11 i m_3=17.

```
                0,1,2,3,4,5,6,7,8,9,10111213141516
m1=5,   S[1,x]  1,0,1,1,0
m2=11,  S[2,x]  0,1,1,0,1,0,0,1,00,1,1
m3=17,  S[3,x]  0,1,0,1,0,1,1,0,0,0,0,1,1,0,1,0,1
```

---

[113] Jaką odpowiedź da algorytm Solovay'a-Strassena dla danych a=10 i n=91. Czy odpowiedź jest poprawna?
(a) liczba pierwsza, odpowiedź poprawna
(b) liczba pierwsza, odpowiedź błędna
(c) liczba złożona, odpowiedź poprawna
(d) liczba złożona, odpowiedź błędna

-VII-

ZAKRES MATERIAŁU

I. Szyfr Rabina
II. Szyfr ElGamala

[114] Szyfr Rabina. Sprawdź, czy wartości p=11 i q=23 są prawidłowe i zaszyfruj tekst otwarty T=158. Dla sprawdzenia odszyfruj kryptogram.

KAPITAŁ LUDZKI NARODOWA STRATEGIA SPÓJNOŚCI
UNIA EUROPEJSKA EUROPEJSKI FUNDUSZ SPOŁECZNY
Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

[115] Szyfr ElGamala. Przeanalizuj algorytm szyfrowania i deszyfrowania dla tekstu otwartego T=7 i parametrów p=23, a=6, b=3, g=7. Sprawdź, czy zadane parametry są poprawne.

---

[116] Szyfr Rabina. Niech para (p, q) będzie ustalonym kluczem prywatnym. Określ klucz publiczny i kryptogram dla tekstu otwartego T.

(a) (11, 31), T=134
(b) (23, 31), T=234
(c) (11, 23), T=147

---

[117] Szyfr Rabina. Niech para (p, q) będzie ustalonym kluczem prywatnym. Określ klucz publiczny i wyznacz tekst jawny (cztery możliwości) dla kryptogramu X.

(a) (11, 31), X=224
(b) (23, 31), X=568

---

[118] Szyfr ElGamala. Niech p będzie ustaloną liczbą pierwszą, g - pierwiastkiem pierwotnym mod p oraz niech $a \in \{0,...,p-2\}$ i $b \in \{0,...,p-2\}$ reprezentują wykładniki wykorzystywane odpowiednio do generowania klucza publicznego i kryptogramu. Określ klucz publiczny, prywatny i kryptogram dla tekstu otwartego T.

(a) p=11, g=6, a=5, b=3, T=9
(b) p=47, g=13, a=26, b=3, T=31

---

[119] Szyfr ElGamala. Niech p będzie ustaloną liczbą pierwszą, g - pierwiastkiem pierwotnym mod p oraz niech $a \in \{0,...,p-2\}$ reprezentuje wykładnik wykorzystywany do generowania klucza publicznego. Określ klucz publiczny, prywatny i tekst otwarty dla kryptogramu (B, X).

(a) p=11, g=6, a=5, (B, X)=(7, 2)
(b) p=47, g=13, a=26, (B, X)=(35, 35)

-VIII-

ZAKRES MATERIAŁU

I. Grupy. Niezbędne fakty i definicje
II. Problem logarytmu dyskretnego
III. Algorytm Shanksa dla problemu logarytmu dyskretnego
IV. Protokół wymiany kluczy Diffiego-Hellmana
V. Schematy podpisów
VI. Schemat podpisu ElGamala

[120] Zaznacz tylko niezbędne warunki. Zbiór G, w którym określone jest działanie $\oplus$ jest grupą abelową wtw

(a) działanie $\oplus$ jest łączne.
(b) dla każdego elementu z G istnienie (dokładnie jeden) element odwrotny
(c) działanie $\oplus$ jest przemienne.
(d) istnieje element neutralny działania $\oplus$.

---

[121] Zaznacz tylko niezbędne warunki. Zbiór G, w którym określone jest działanie $\oplus$ jest grupą abelową wtw

(a) $\forall a,b,c\ (a \oplus b) \oplus c = a \oplus (b \oplus c)$
(b) $\exists e_0\ \forall a\ (e_0 \oplus a = a \oplus e_0 = a)$
(c) $\forall a\ \exists a'\ (a \oplus a' = a' \oplus a = e_0)$
(d) $\forall a,b\ (a \oplus b = b \oplus a)$

---

[122] Zaznacz poprawną definicję pojęcia grupy cyklicznej.

(a) G jest grupą cykliczną wtw $\exists g \in G\ \forall a \in G\ \exists n \in Z\ (g=a^n)$
(b) H jest grupą cykliczną wtw $[(a,b \in H) \Rightarrow (a \circ b \in H \wedge a^{-1} \in H)]$
(c) G jest grupą cykliczną wtw $\exists g \in G\ \forall a \in G\ NWD(a, g) = 1$.
(d) Grupą cykliczną nazywamy zbiór $G = \{\alpha^i : 0 \le i \le p-2\}$, gdzie p i α są dowolnymi, ustalonymi liczbami naturalnymi.

---

[123] Podaj wszystkie elementy zbioru Z_m^* (zbiór elementów odwracalnych w Z_m).

(a) m=14
(b) m=20
(c) m=21

---

[124] Jeśli p jest liczbą pierwszą, to

(a) $Z_p^* = Z_p \setminus \{0\}$,
(b) $\varphi(p^n) = p^n - p^{n-1}$ (φ - funkcja Eulera),
(c) $\varphi(p) = |Z_p| - 1$,
(d) jeśli p jest nieparzysta, to x jest resztą kwadratową modulo p wtw $x^{(p-1)/2} \equiv 1 (\mathrm{mod}\, p)$.

---

[125] Podaj wartość funkcji Eulera $\varphi(m)$ dla

(a) m=343
(b) m=60
(c) m=91

---

[126] Zaznacz własności związane z funkcją Eulera.

(a) $\varphi(m) = |Z_m^*| = |\{a \in Z: 1 \le a < m, NWD(a, m) = 1\}|$
(b) jeśli p jest liczbą pierwszą, to $\varphi(p^n) = p^n - p^{n-1}$
(c) dla n, m>1 jeśli NWD(n, m) = 1, to $\varphi(n*m) = \varphi(n)*\varphi(m)$
(d) jeśli p jest liczbą pierwszą, to $\varphi(p) = p-1$
(e) dla liczby naturalnej m>1 i $a \in Z_m$ jeśli NWD(a, m) = 1, to $a^{\varphi(m)} \equiv 1 \pmod m$
(f) dla różnych liczb pierwszych p, q $\varphi(p*q) = \varphi(p)*\varphi(q) = (p-1)(q-1)$

---

[127] Wybierz grupy cykliczne.

(a) Z_{23}^*
(b) (Z,+)
(c) $(Q\setminus\{0\},*)$
(d) Z_{16}^*
(e) (Q,+)
(f) (R,+)
(g) Z_{11}^*
(h) $(R\setminus\{0\},*)$

---

[128] Wypisz generatory grupy cyklicznej Z_p^* w kolejności od najmniejszego do największego.

(a) p=7

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI
UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY
Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

(b) p=11
(c) p=13
---

[129] Wypisz wszystkie podgrupy grupy Z_p^*.

(a) p=7
(b) p=11
(c) p=13
---

[130] Podaj rząd elementu a grupy Z_p^*.

(a) a=4, p=7
(b) a=3, p=11
(c) a=6, p=13
---

[131] Zaznacz własności grupy Z_p^* (przy dodatkowym założeniu, że p jest liczbą pierwszą).

(a) rząd grupy Z_p^* : $\varphi(p)=p-1$

(b) rząd każdego elementu grupy Z_p^* jest dzielnikiem liczby p-1

(c) Z_p^* jest grupą cykliczną

(d) wszystkie podgrupy grupy Z_p^* mają po p-1 elementów

(e) element $\alpha \in Z_p^*$ jest elementem pierwotnym mod p wtw $\{\alpha^i : 0 \le i \le p-2\} = Z_p^*$.
---

[132] Wyznacz wszystkie elementy pierwotne modulo p.
(a) p=7
(b) p=11
(c) p=13
---

[133] Dla parametrów p, α, β znajdź logarytm o podstawie α z wartości β w arytmetyce modulo p.
(a) p=7, α=3, β=5
(b) p=11, α=6, β=10
(c) p=13, α=11, β=8
---

[134] Podaj pary liczb (j,y) i (i,y), dla których w algorytmie Shanksa dla parametrów p, α, β wyznacza się logarytm dyskretny. Wynik zapisz (bez spacji) w następującym formacie (j,y),(i,y).
(a) p=7, α=3, β=5
(b) p=11, α=6, β=10
(c) p=13, α=11, β=8
---

[135] Podaj klucz ustalony w protokole wymiany klucza Diffiego-Hellmana dla następujących parametrów.
(a) p=17, α=5, aU=3, aV=4
(b) p=17, α=11, aU=5, aV=8
(c) p=17, α=12, aU=2, aV=5
---

[136] Do ochrony wiadomości zastosowano schemat podpisu ElGamala. B otrzymał wiadomość x opatrzoną podpisem sig(x)=(γ,δ). Zweryfikuj, czy wiadomość jest autentyczna. Wybierz odpowiedź i tajny parametr a.
(a) p=17, β=14, γ=22, δ=11, k=11, x='w' (22) // α=3,
(b) p=17, β=13, γ=5, δ=3, k=3, x='v' (21) // α=11,
---

[137] Do ochrony wiadomości zastosowano schemat podpisu ElGamala. Podaj wartości γ, δ podpisu sig(x) dla wiadomości x i następujących parametrów. Wynik przedstaw (bez spacji) w następującym formacie (γ,δ).
(a) p=17, α=3, β=14, k=11, x='w' (22) // a=9,
(b) p=17, α=11, β=13, k=3, x='v' (21) // a=12,

-IX-

ZAKRES MATERIAŁU

I. Algorytm Millera-Rabina
II. Sito kwadratowe
III. Algorytm p-1 Pollarda
IV. Algorytm Fermata
V. Wielomiany i krzywe eliptyczne

[138] Jaką odpowiedź zwróci dla N algorytm Millera-Rabina? Czy odpowiedź jest poprawna?
(a) N=165, a=3
(b) N=241, a=3
---

[139] Algorytm p-1 Pollarda. Rozłóż liczbę N na dwa czynniki. Za ograniczenie przyjmij wartość B, za parametr a przyjmij wartość 3.
(a) N=1516515, B=80, a=3
(b) N=37384039, B=10, a=3
---

[140] Algorytm Fermata. Rozłóż liczbę N na dwa czynniki.
(a) N=39767
(b) N=40755
---

[141] Zaimplementuj metodę realizującą rozkładanie liczby na dwa czynniki. Zastosuj algorytm Fermata.
---

[142] Wyznacz 0-1-kową tablicę odsiewania S dla zadanego m używaną w algorytmie faktoryzacji „sito kwadratowe" do znalezienia czynnika liczby N=51129.
(a) m_1=5
(b) m_2=11
(c) m_3=17
---

[143] Czy poniższe wielomiany są rozkładalne w pierścieniu $Z_2[x]$? Sprawdź, czy zostały dobrze rozłożone i wybierz poprawne odpowiedzi.
(a) $f(x)=(x^5+x^4+x^3+1)=(x^2+1)(x^3+x^2+1)$ rozkładalny z $Z_2[x]$
(b) $g(x)=(x^5+x^2+x+1)=(x^2+1)(x^3+x+1)$ rozkładalny z $Z_2[x]$
(c) $h(x)=(x^5+x^2+1)=(x^2+x+1)(x^3+x^2+1)$ rozkładalny z $Z_2[x]$
(d) $i(x)=(x^5+x^4+x^3+x)$ nierozkładalny z $Z_2[x]$
---

[144] Zaznacz każdy zbiór punktów, który stanowi podzbiór jakiejś krzywej eliptycznej E nad Z_5. Podaj parametry a i b.
(a) {(2,0),(3,2),(3,3),(4,1),(4,4)}

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI
UNIA EUROPEJSKA EUROPEJSKI FUNDUSZ SPOŁECZNY
Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego

(b) {(1,2),(1,3),(4,0)}
(c) {(0,2),(0,3),(0,4),(1,3),(2,2),(2,3)}
(d) {(0,1),(0,2)(0,3),(1,1),(1,2)}
---
[145] Dla jakich parametrów a, b$\in Z_5$ poniższe punkty są wybranymi elementami krzywej eliptycznej E nad Z_5.
{(1,2),(1,3),(2,1),(2,4),(3,0)}
---
[146] Wybierz podzbiór punktów krzywej eliptycznej E nad Z_7.
(a) E: $y^2=x^3+2x+1$
(b) E: $y^2=x^3+3x+1$
(A) {0,(0,1),(0,6),(1,2),(1,5)}
(B) {0,(0,1),(0,6),(2,1),(2,6),(3,3),(3,4),(4,0),(5,1),(5,6),(6,2),(6,5)}
(C) {0,(4,1),(4,6),(5,0),(6,1),(6,6)}
(D) {0,(4,1),(4,6),(5,0),(5,6),(6,1),(6,6)}
-X----------

ZAKRES MATERIAŁU

I. Algorytmy do zaimplementowania

[147] Zaimplementuj algorytmy szyfrowania i deszyfrowania
(a) dla szyfru Cezara
(b) dla monoalfabetycznego szyfru podstawieniowego
(c) dla szyfru Vigenere'a
(d) dla szyfru afinicznego
(e) dla szyfru Hilla
---
[148] Zaimplementuj algorytm ułatwiający kryptoanalizę monoalfabetycznego szyfru podstawieniowego dla tekstów polskich.
---
[149] Zaimplementuj metodę wyznaczającą NWD dla kilku liczb podanych w tablicy int[] x.
---
[150] Zaimplementuj algorytmy kompresji i dekompresji Huffmana.
---
[151] Zaimplementuj algorytmy szyfrowania i deszyfrowania RSA w wersji blokowej.
---
[152] Zaimplementuj algorytmy szyfrowania i deszyfrowania w systemie
(a) Rabina
(b) ElGamala.
---
[153] Zaimplementuj algorytm Solovaya-Strassena sprawdzania, czy zadana liczba nieparzysta jest pierwsza.
---
[154] Zaimplementuj algorytm Millera-Rabina sprawdzania, czy zadana liczba jest pierwsza.
---
[155] Zaimplementuj algorytm Shanksa dla problemu logarytmu dyskretnego.

KAPITAŁ LUDZKI
NARODOWA STRATEGIA SPÓJNOŚCI
UNIA EUROPEJSKA
EUROPEJSKI
FUNDUSZ SPOŁECZNY
Projekt współfinansowany ze środków Unii Europejskiej w ramach Europejskiego Funduszu Społecznego