1. Podzielność

Oznaczmy przez Z zbiór liczb całkowitych. Niech $a, b \in Z$. Liczba b dzieli a, co zapisujemy $b \mid a$, jeśli istnieje liczba całkowita k, dla której $a = k \cdot b$.

Przykłady:

$5 \mid 10$, ponieważ istnieje liczba $k = 2$, dla której $10 = 2 \cdot 5$

$-7 \mid 21$, ponieważ istnieje liczba $k = -3$, dla której $21 = -3 \cdot (-7)$

$10 \mid -250$, ponieważ istnieje liczba $k = -25$, dla której $-250 = -25 \cdot 10$

Zadania:

Sprawdź, które z poniższych podzielności są prawdziwe, a które nie:

a) $7 \mid 0$ (odp.: tak)

b) $9 \mid 162$ (odp.: tak)

c) $13 \mid 1333$ (odp.: nie)

d) $3 \mid 123432$ (odp.: tak)

e) $5 \mid 12345$ (odp.: tak)

f) $2 \mid 12121$ (odp.: nie)

2. Kongruencje

Oznaczmy przez N zbiór liczb naturalnych. Niech $a, b \in Z$, zaś $n \in N$. Liczba a przystaje (jest kongruentna) do b modulo n, co zapisujemy $a \equiv b \bmod n$, jeśli $n \mid (a - b)$. Liczbę n nazywamy modułem kongruencji.

Przykłady:

$17 \equiv 2 \bmod 5$, ponieważ $5 \mid (17 - 2)$, tzn. $(17 - 2) = 3 \cdot 5$

$23 \equiv -5 \bmod 7$, ponieważ $7 \mid (23 - (-5))$, tzn. $(23 - (-5)) = 4 \cdot 7$

$-5 \equiv 4 \bmod 3$, ponieważ $3 \mid (-5 - 4)$, tzn. $(-5 - 4) = -3 \cdot 3$

Zadania:

Sprawdź, które z poniższych kongruencji są prawdziwe, a które nie:

a) $10 \equiv 2 \bmod 3$ (odp.: nie)

b) $3 \equiv 5 \bmod 2$ (odp.: tak)

c) $7 \equiv 10 \bmod 6$ (odp.: nie)

d) $-9 \equiv 11 \bmod 10$ (odp.: tak)

e) $-13 \equiv -27 \bmod 5$ (odp.: nie)

f) $-11 \equiv 14 \bmod 5$ (odp.: tak)

g) $-43 \equiv -11 \bmod 12$ (odp.: nie)

h) $32 \equiv -17 \bmod 7$ (odp.: tak)

3. Redukcja modularna

Jeżeli a i $b \in Z$ podzielimy przez $n \in N$ to odpowiednio otrzymamy $a = k_1 \cdot n + r_1$, $b = k_2 \cdot n + r_2$ (k_1, k_2, r_1, $r_2 \in Z$), gdzie reszty z dzielenia r_1 i r_2 nazywane resztami modulo n spełniają warunek: $0 \leq r_1, r_2 \leq n - 1$. Nietrudno zauważyć, że $a \equiv b \bmod n$ wtedy i tylko wtedy, gdy $r_1 = r_2$. Do oznaczenia reszty r_1 będziemy używać zapisu $a \bmod n$, natomiast dla reszty r_2 odpowiednio $b \bmod n$. Mamy wówczas, że $a \bmod n = b \bmod n$ wtedy i tylko wtedy, gdy $a \equiv b \bmod n$. Zastępując a przez $a \bmod n$ mówimy, że liczba całkowita a została zredukowana modulo n. Zbiór liczb całkowitych od 0 do $n - 1$ tworzy zupełny zbiór reszt modulo n. Oznacza to, że dla każdej liczby całkowitej a jej reszta modulo n jest jedną z liczb od 0 do $n - 1$. Oznaczmy przez $\lfloor x \rfloor$ największą liczbę całkowitą nie większą niż x, wtedy $a \bmod n = a - n \cdot \lfloor a / n \rfloor$. Jeżeli $a \geq 0$, to $a \bmod n$ można traktować jako resztę z dzielenia a przez n.

Przykłady:

$7 \bmod 3 = 1$, co implikuje $7 \equiv 1 \bmod 3$ ale nie odwrotnie, bo $7 \equiv 4 \bmod 3$, a $7 \bmod 3 \neq 4$

$10 \bmod 4 = 2$

$16 \bmod 8 = 0$

$-13 \bmod 6 = 5$

$-5 \bmod 9 = 4$

Zadania:

Przeprowadź redukcję modularną:

a) $10 \bmod 3$ (odp.: 1)

b) $-12 \bmod 5$ (odp.: 3)

c) $8 \bmod 1$ (odp.: 0)

d) $0 \bmod 21$ (odp.: 0)

e) $-7 \bmod 13$ (odp.: 6)

f) $-5 \bmod 5$ (odp.: 0)

g) $123 \bmod 256$ (odp.: 123)

h) $358 \bmod 128$ (odp.: 102)

4. Arytmetyka modularna

Arytmetyka modularna ma właściwości charakterystyczne dla zwykłej arytmetyki: są spełnione prawa przemienności, łączności i rozdzielności. Także redukowanie wyników pośrednich modulo n daje taki sam wynik jak wykonanie wszystkich obliczeń, a następnie zredukowanie wyniku modulo n.

$(a + b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n$

$(a - b) \bmod n = ((a \bmod n) - (b \bmod n)) \bmod n$

$(a \cdot b) \bmod n = ((a \bmod n) \cdot (b \bmod n)) \bmod n$

$(a \cdot (b + c)) \bmod n = (((a \cdot b) \bmod n) + ((a \cdot c) \bmod n)) \bmod n$

Przykłady:

$(135273 + 261909 + 522044) \bmod 9 = (135273 \bmod 9 + 261909 \bmod 9 + 522044 \bmod 9) \bmod 9 = (3 + 0 + 8) \bmod 9 = 11 \bmod 9 = 2$

$(324547 - 345 - 34234) \bmod 5 = (324547 \bmod 5 - 345 \bmod 5 - 34234 \bmod 5) \bmod 5 = (2 - 0 - 4) \bmod 5 = -2 \bmod 5 = 3$

$(12543 \cdot 4321) \bmod 2 = (12543 \bmod 2 \cdot 4321 \bmod 2) \bmod 2 = (1 \cdot 1) \bmod 2 = 1$

Zasada arytmetyki modularnej ma zastosowanie również do potęgowania w postaci a^t, tzn. obliczenie a^t w arytmetyce mod n jest równoważne obliczeniu a^t w klasyczny sposób i zredukowaniu wyniku mod n. Słuszność tej zasady wynika z równoważności potęgowania i wielokrotnego mnożenia.

Przykłady:

$5^8 \bmod 9 = ((5^2)^2)^2 \bmod 9 = ((25 \bmod 9)^2 \bmod 9)^2 \bmod 9 = (7^2 \bmod 9)^2 \bmod 9 = (49 \bmod 9)^2 \bmod 9 = 4^2 \bmod 9 = 16 \bmod 9 = 7$

$3^5 \bmod 7 = (3 \cdot 3^4) \bmod 7 = ((3^2)^2 \cdot 3) \bmod 7 = (((9 \bmod 7)^2 \bmod 7) \cdot 3) \bmod 7 = ((2^2 \bmod 7) \cdot 3) \bmod 7 = (4 \cdot 3) \bmod 7 = 12 \bmod 7 = 5$

$4^{25} \bmod 6 = (4 \cdot 4^{24}) \bmod 6 = (4 \cdot 4^8 \cdot 4^{16}) \bmod 6 = (4 \cdot ((4^2)^2)^2 \cdot (((4^2)^2)^2)^2) \bmod 6 = ((((4^2 \cdot 4)^2)^2)^2 \cdot 4) \bmod 6 = (((((((16 \bmod 6) \cdot 4) \bmod 6)^2 \bmod 6)^2 \bmod 6)^2 \bmod 6) \cdot 4) \bmod 6 = ((((((4 \cdot 4) \bmod 6)^2 \bmod 6)^2 \bmod 6)^2 \bmod 6) \cdot 4) \bmod 6 = (((((16 \bmod 6)^2 \bmod 6)^2 \bmod 6)^2 \bmod 6) \cdot 4) \bmod 6 = ((((4^2 \bmod 6)^2 \bmod 6)^2 \bmod 6) \cdot 4) \bmod 6 = (((4^2 \bmod 6)^2 \bmod 6) \cdot 4) \bmod 6 = ((4^2 \bmod 6) \cdot 4) \bmod 6 = (4 \cdot 4) \bmod 6 = 4$

Jeśli wykładnik $t \geq n$, to zredukowanie $t \bmod n$ może zniekształcić wynik, $(a^{t \bmod n}) \bmod n$ może być różne od $a^t \bmod n$. Zatem w ogólnym przypadku $(a^{t \bmod n}) \bmod n \neq a^t \bmod n$.

Przykłady:

$(2^{5 \bmod 3}) \bmod 3 = 1$, ale $2^5 \bmod 3 = 2$

$(4^{7 \bmod 5}) \bmod 5 = 1$, ale $4^7 \bmod 5 = 4$

Obliczenia w arytmetyce modularnej dają wymierną korzyść w postaci ograniczenia wielkości wyników pośrednich. Oznacza to, że na przykład możemy dokonywać potęgowania na dużych liczbach unikając wielkich wyników pośrednich.

Zadania:

Wykonaj obliczenia metodą redukcji wyników pośrednich:

a) $(1234 + 1004) \bmod 3$ (odp.: 0)

b) $(529 - 121) \bmod 5$ (odp.: 3)

c) $(329 \cdot 998) \bmod 9$ (odp.: 4)

d) $(13 \cdot (18 + 23)) \bmod 7$ (odp.: 1)

e) $(13 \cdot 14 + 15 \cdot 20 - 7 \cdot 13 - 21) \bmod 7$ (odp.: 6)

f) $((9 \cdot 13 + 14 \cdot 4) \bmod 4 - (15 \cdot 18 - 31 \cdot 17) \bmod 5) \bmod 6$ (odp.: 4)

g) $((13 + 9) \bmod 4 + ((14 + 12) \bmod 5 \cdot (3 - 7) \bmod 3) \bmod 7) \bmod 5$ (odp.: 4)

h) $((15 \cdot 20 + 35 \cdot 17) \bmod 8 \cdot (8 \cdot 8 - 7 \cdot 15) \bmod 7) \bmod 10$ (odp.: 7)

i) $8^8 \bmod 10$ (odp.: 6)

j) $2^{10} \bmod 9$ (odp.: 7)

k) $3^{25} \bmod 5$ (odp.: 3)

l) $4^{17} \bmod 6$ (odp.: 4)

m) $7^7 \bmod 3$ (odp.: 1)

n) $10^{10} \bmod 7$ (odp.: 4)

o) $12^5 \bmod 8$ (odp.: 0)

p) $13^{13} \bmod 2$ (odp.: 1)

5. Pierścień Z_n

Oznaczmy przez Z_n zbiór liczb całkowitych $\{0, 1, 2, ..., n - 1\}$ z określonymi działaniami dodawania + i mnożenia · w ten sposób, że wyniki rzeczywistych działań są redukowane modulo n. Powyższe działania w Z_n mają podstawowe własności działań arytmetycznych:

1. Dodawanie jest zamknięte: $a, b \in Z_n, a + b \in Z_n$

2. Dodawanie jest przemienne: $a, b \in Z_n, a + b = b + a$

3. Dodawanie jest łączne: $a, b, c \in Z_n, (a + b) + c = a + (b + c)$

4. Zero jest elementem neutralnym względem dodawania:

$$a \in Z_n,\ a + 0 = 0 + a = a$$

5. Elementem przeciwnym do $a \in Z_n$ jest $n - a$:

$$a + (n - a) = (n - a) + a = 0$$

6. Mnożenie jest zamknięte: $a, b \in Z_n,\ a \cdot b \in Z_n$

7. Mnożenie jest przemienne: $a, b \in Z_n,\ a \cdot b = b \cdot a$

8. Mnożenie jest łączne: $a, b, c \in Z_n,\ (a \cdot b) \cdot c = a \cdot (b \cdot c)$

9. Jedynka jest elementem neutralnym względem mnożenia:

$$a \in Z_n,\ a \cdot 1 = 1 \cdot a = a$$

10. Dodawanie i mnożenie są działaniami rozdzielnymi:

$$a, b, c \in Z_n,\ (a + b) \cdot c = a \cdot c + b \cdot c,\ a \cdot (b + c) = a \cdot b + a \cdot c$$

Zbiór Z_n z dodawaniem tworzy strukturę algebraiczną zwaną grupą przemienną (abelową), natomiast Z_n z działaniami dodawania i mnożenia jest pierścieniem przemiennym. Jeżeli dodatkowo dla każdego $a \in Z_n - \{0\}$ istnieje element odwrotny a^{-1} (tzn. $a \cdot a^{-1} = 1 = a^{-1} \cdot a$), to pierścień przemienny Z_n nazywamy ciałem. Przykładowo ciałem jest system algebraiczny R, natomiast system algebraiczny Z nie jest ciałem, gdyż liczby całkowite różne od ± 1 nie mają elementów odwrotnych w Z. W ogólnym przypadku Z_n jest ciałem wtedy i tylko wtedy, gdy $n = p$ jest liczbą pierwszą (liczba naturalna $p > 1$ jest liczbą pierwszą wtedy i tylko wtedy, gdy nie istnieje liczba $t \in N$ ($t \neq 1$ i $t \neq p$) taka, że $t \mid p$).

Przykłady:

Jeśli $n = 2$, mamy do czynienia z pierścieniem dwuelementowym $Z_2 = \{0, 1\}$. Działania modulo 2 zdefiniowane są następująco:

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

Łatwo zauważyć, że w Z_2 elementem przeciwnym do 1 jest 1, gdyż $1 + 1 = 0$ w Z_2. Pierścień Z_2 jest ciałem, ponieważ jedyny element niezerowy 1 jest też swoją odwrotnością, tzn. $1 \cdot 1 = 1$ w Z_2.

Prześledźmy konstrukcję działań dla bardziej rozbudowanego pierścienia Z_5. Działania modulo 5 zdefiniowane są następująco:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

·	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Pierścień Z_5 jest ciałem, ponieważ każdy niezerowy element jest odwracalny, np. odwrotnością 2 jest 3, gdyż $2 \cdot 3 = 1$ w Z_5. Elementem przeciwnym np. do 4 jest 1, ponieważ $4 + 1 = 0$ w Z_5. Równanie $3 \cdot x = 2$ ma w Z_5 jedyne rozwiązanie $x = 4$.

Dla pierścienia Z_6 działania modulo 6 zdefiniowane są następująco:

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

·	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Dla przykładu elementem przeciwnym do 2 jest 4, gdyż $2 + 4 = 0$ Z_6. Pierścień Z_6 nie jest ciałem, ponieważ nie wszystkie niezerowe elementy są odwracalne, np. 2, 3 i 4 nie mają swoich odwrotności w Z_6. Równanie $3 \cdot x = 0$ ma trzy rozwiązania w Z_6 ($x_1 = 0$, $x_2 = 2$, $x_3 = 4$), natomiast równanie $4 \cdot x = 3$ nie ma rozwiązania w Z_6.

Zadania:

1. Wyznacz tabelki działań (+, ·) dla pierścieni:

a) Z_3

b) Z_7

c) Z_8

d) Z_{11}

e) Z_{12}

f) Z_{15}

g) Z_{26}

2. Które z powyższych pierścieni są ciałami?

3. Znajdź (jeśli istnieją) elementy przeciwne i odwrotne do:

a) 1, 2 w Z_3

b) 0, 2, 5 w Z_7

c) 1, 3, 4 w Z_8

d) 5, 8, 10 w Z_{11}

e) 2, 3, 7, 8, 10 w Z_{12}

f) 4, 5, 9, 12 w Z_{15}

4. Ile rozwiązań i jakie ma równanie?

a) $2 \cdot x = 1$ w Z_3

b) $3 \cdot x = 5$ w Z_7

c) $7 \cdot x = 4$ w Z_8

d) $8 \cdot x = 10$ w Z_{11}

e) $4 \cdot x = 9$ w Z_{12}

f) $6 \cdot x = 13$ w Z_{15}

6. Kodowanie alfabetu

Za zwyczaj zależy nam na utajnieniu jakiejś wiadomości zapisanej przy pomocy liter danego alfabetu. Przekształcenia kryptograficzne są natomiast przekształceniami matematycznymi zwykle operującymi na liczbach. Zatem ciąg znaków musi zostać w jakiś sposób przekształcony na liczby. Służą do tego kody. Przykładowo aby zakodować 26 liter alfabetu łacińskiego numerujemy je kolejno od 0 do 25 jak zostało to przedstawione w poniższej tabeli. Zatem każdy tekst zapisany przy użyciu tego alfabetu może być przedstawiony jako ciąg elementów pierścienia Z_{26}.

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12

N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Przykłady:

Tekst KRYPTOGRAFIA będzie odpowiadał ciągowi liczb 10, 17, 24, 15, 19, 14, 6, 17, 0, 5, 8, 0.

Ciąg liczb 22, 0, 17, 18, 25, 0, 22, 0 będzie odpowiadał tekstowi WARSZAWA.

Zadania:

1. Zakoduj wyrazy:

a) MATEMATYKA (odp.: 12, 0, 19, 4, 12, 0, 19, 24, 10, 0)

b) KONGRUENCJA (odp.: 10, 14, 13, 6, 17, 20, 4, 13, 2, 9, 0)

c) PODZIELNOSC (odp.: 15, 14, 3, 25, 8, 4, 11, 13, 14, 18, 2)

d) PIERSCIEN (odp.: 15, 8, 4, 17, 18, 2, 8, 4, 13)

2. Odkoduj ciągi:

a) 10, 14, 13, 8, 4, 2, 11, 4, 10, 2, 9, 8 (odp.: koniec lekcji)

b) 2, 25, 4, 17, 22, 14, 13, 24, 10, 0, 15, 19, 20, 17, 4, 10 (odp.: czerwony kapturek)

c) 10, 14, 15, 2, 8, 20, 18, 25, 4, 10 (odp.: kopciuszek)

d) 15, 17, 25, 4, 17, 22, 0, 13, 0, 15, 0, 15, 8, 4, 17, 14, 18, 0 (odp.: przerwa na papierosa)

Innym przykładem kodu jest powszechnie używany w komputerach kod ASCII, w którym znaki alfanumeryczne są zwykle kodowane przy pomocy 8-bitowych wartości.

7. Szyfr przesuwający

Wprowadźmy oznaczenia: P – skończony zbiór możliwych jednostek tekstu jawnego (tekstu odkrytego), C – skończony zbiór możliwych jednostek tekstu zaszyfrowanego (szyfrogramu), K – skończony zbiór możliwych kluczy, e_k – przekształcenie szyfrujące, d_k – przekształcenie deszyfrujące. Dla szyfru przesuwającego przyjmujemy, że $P = C = K = Z_{26}$, $x \in P$, $y \in C$, $k \in K$.

Szyfrowanie: $y = e_k(x) = x + k \bmod 26$

Deszyfrowanie: $x = d_k(y) = y - k \bmod 26 = y + (-k) \bmod 26$

Łatwo zauważyć, że szyfrowanie polega na zastąpieniu danej litery przez literę leżącą k pozycji dalej w alfabecie traktowanym jako cykl zamknięty. Deszyfrowanie natomiast jest procesem odwrotnym. Zauważmy, że dla $k = 13$ funkcja szyfrująca jest równa funkcji deszyfrującej, tzn. $e_k = d_k$., czyli $x = e_k(e_k(x))$. Fakt ten wynika z tego, że liczba 13 jest swoją przeciwnością (odwrotnością addytywną) w Z_{26}, tzn. $13 + 13 \bmod 26 = 0$. Ciekawostką jest, że dla $k = 3$ szyfr ten był używany przez Juliusza Cezara (żył w latach 100–40 p.n.e.).

W podawanych przykładach tekst jawny będziemy zapisywali przy pomocy liter małych, a szyfrogram przy pomocy liter dużych, pomijamy spacje i dzielimy ewentualnie oba teksty na grupy pięcioliterowe.

Przykłady:

1. Weźmy szyfr przesuwający z $k = 11$ i tekst jawny: spotk aniej utror ano.

tekst jawny	s	p	o	t	k	a	n	i	e	j	u	t	r	o	r	a	n	o
x	18	15	14	19	10	0	13	8	4	9	20	19	17	14	17	0	13	14
y	3	0	25	4	21	11	24	19	15	20	5	4	2	25	2	11	24	25
szyfrogram	D	A	Z	E	V	L	Y	T	P	U	F	E	C	Z	C	L	Y	Z

Tekst zaszyfrowany brzmi: DAZEV LYTPU FECZC LYZ

Opisany powyżej kryptosystem nie jest bezpieczny. Do jego złamania możemy kolejno sprawdzać wartości klucza $k = 1, 2, ..., 25$ aż otrzymamy sensowny tekst jawny. Średnio należy wykonać $26 / 2 = 13$ prób. Opisana metoda kryptoanalizy nazywa się przeszukiwaniem przestrzeni klucza (atak brutalny). Zatem warunkiem koniecznym (ale nie dostatecznym) bezpieczeństwa kryptosystemu jest to, aby przestrzeń klucza była możliwie duża, co uniemożliwi przeszukanie jej w realnym czasie.

Zadania:

1. Zaszyfruj przy użyciu szyfru przesuwnego poniższy tekst:

a) szyfr przes uwny, $k = 7$ (odp.: ZGFMY WYGLZ BDUF)

b) klucz prywa tny, $k = 21$ (odp.: FGPXU KMTRV OIT)

c) nazwa miejscowości, w której mieszkasz (zapisana przy pomocy alfabetu angielskiego), używając klucza k = (rok_urodzenia · dzień_urodzenia – miesiąc_urodzenia) mod 26

d) swoje imię i nazwisko (zapisane przy pomocy alfabetu angielskiego), używając klucza k = dzień_urodzenia mod 26

2. Odszyfruj przy użyciu szyfru przesuwnego poniższy tekst:

a) KVEBI PGKFJ PJKVD EZVAV JKSVQ GZVTQ EP, $k = 17$ (odp.: ten kryptosystem nie jest bezpieczny)

b) CJIPB CIWOD BIMJX I, $k = 10$ (odp.: szyfr symetryczny)

c) RTMNZ VAMXE LCGBY BTVV, $k = 13$ (odp.: egzamin z kryptologii)

d) AIUWL ZIJQI UXZIK MLWUW EM, $k = 8$ (odp.: sam odrabiam prace domowe)

8. Największy wspólny dzielnik

Niech $a, b \in Z$ i nie są równe jednocześnie zeru. Największy wspólny dzielnik (ang. *greatest common divisor*) liczb a i b, oznaczany $\gcd(a, b)$ (lub czasami prościej (a, b)), jest to największa liczba całkowita dzieląca zarówno a, jak i b. Jeśli a i b są jednocześnie równe zeru, to ponieważ każda liczba całkowita dzieli zero, nie można tu zastosować powyższej definicji. Wygodnie jest przyjąć, że $\gcd(0, 0) = 0$. Z podanej definicji w oczywisty sposób wynika, że

$$\gcd(a, b) = \gcd(b, a),$$
$$\gcd(a, b) = \gcd(-a, b),$$
$$\gcd(a, b) = \gcd(|a|, |b|),$$
$$\gcd(a, a) = |a|,$$
$$\gcd(a, 0) = |a|.$$

Przykłady:

a) $\gcd(9, 15) = 3$

b) $\gcd(21, 49) = 7$

c) $\gcd(7, 13) = 1$

Jeżeli $\gcd(a, b) = 1$, to a i b nazywamy liczbami względnie pierwszymi.

9. Algorytm Euklidesa

Łatwym i efektywnym sposobem poszukiwania największego wspólnego dzielnika dwóch liczb jest algorytm Euklidesa. Euklides opisał algorytm w swojej książce *Elementy* napisanej około 300 r. p.n.e., ale nie był on prawdopodobnie jego pomysłem. Historycy są przekonani, że algorytm może być 200 lat starszy.

Idea algorytmu Euklidesa jest następująca. Aby znaleźć $\gcd(a, b)$ dla dwóch dodatnich liczb całkowitych a i b, gdzie $a > b$, najpierw dzielimy a przez b i zapisujemy iloraz q_1 i resztę r_1: $a = q_1 \cdot b + r_1$. Następnie wykonujemy drugie dzielenie, w którym b gra rolę a i r_1 gra rolę b: $b = q_2 \cdot r_1 + r_2$. Następnie dzielimy r_1 przez r_2: $r_1 = q_3 \cdot r_2 + r_3$. Kontynuujemy to postępowanie, za każdym razem dzieląc przedostatnią resztę przez ostatnią, otrzymując nowy iloraz i nową resztę. Gdy wreszcie otrzymamy resztę, która dzieli poprzednią, kończymy dzielenie. Ostatnia niezerowa reszta jest największym wspólnym dzielnikiem liczb a i b.

Przykład:

Znajdź gcd(1547, 560).

$1547 = 2 \cdot 560 + 427$

$560 = 1 \cdot 427 + 133$

$427 = 3 \cdot 133 + 28$

$133 = 4 \cdot 28 + 21$

$28 = 1 \cdot 21 + 7$

$21 = 3 \cdot 7$

a	b	q	r
1547	560	2	427
560	427	1	133
427	133	3	28
133	28	4	21
28	21	1	7
21	7	3	0

Ponieważ $7 \mid 21$, więc otrzymaliśmy wynik $\gcd(1547, 560) = 7$.

Łatwo zauważyć, że wyliczanie q nie jest potrzebne do policzenia $\gcd(a, b)$, natomiast reszta r jest de facto resztą $a \bmod b$. Zatem do wyliczenia $\gcd(a, b)$ można użyć poniżej zapisanego algorytmu.

Algorytm:

1. Jeśli $b = 0$, to algorytm zatrzymuje się z odpowiedzią a.
2. Przyjmij: $r \leftarrow a \bmod b$, $a \leftarrow b$, $b \leftarrow r$ i wróć do kroku 1.

Przykład:

Znajdź gcd(1547, 560).

a	b	r
1547	560	427
560	427	133
427	133	28
133	28	21
28	21	7
21	7	0
7	0	–

$\gcd(1547, 560) = 7$

Zadania:

Znajdź największy wspólny dzielnik:

a) gcd(128, 98) (odp.: 2)

b) gcd(888, 654) (odp.: 6)

c) gcd(1079, 689) (odp.: 13)

d) gcd(1450, 841) (odp.: 29)

10. Odwrotność multiplikatywna modulo *n*

Niech $n \in N$, $a \in Z_n$. Mówimy, że a posiada odwrotność multiplikatywną modulo n, wtedy i tylko wtedy, gdy istnieje $a^{-1} \in Z_n$ takie, że $a \cdot a^{-1} \bmod n = 1$.

Przykłady:

a) 3 i 5 są odwrotnościami mod 7, bo $3 \cdot 5 \bmod 7 = 15 \bmod 7 = 1$

b) 3 i 7 są odwrotnościami mod 10, bo $3 \cdot 7 \bmod 10 = 21 \bmod 10 = 1$

c) 7 i 15 są odwrotnościami mod 26, bo $7 \cdot 15 \bmod 26 = 105 \bmod 26 = 1$

Zadania:

Sprawdź, które z poniżej podanych par liczb są swoimi odwrotnościami multiplikatywnymi modulo n, a które nie są.

a) $a = 5, b = 8, n = 13$ (odp.: tak)

b) $a = 3, b = 13, n = 19$ (odp.: tak)

c) $a = 19, b = 20, n = 24$ (odp.: nie)

d) $a = 17, b = 23, n = 26$ (odp.: tak)

e) $a = 5, b = 11, n = 21$ (odp.: nie)

f) $a = 7, b = 13, n = 30$ (odp.: tak)

Nurtujące może być pytanie dla jakich a istnieje odwrotność multiplikatywna modulo n. Otóż okazuje się, że liczba a posiada odwrotność multiplikatywną modulo n, wtedy i tylko wtedy, gdy a i n są liczbami względnie pierwszymi, tj. $\gcd(n, a) = 1$.

Przykłady:

a) dla $a = 5$ istnieje odwrotność multiplikatywna mod 9, ponieważ $\gcd(9, 5) = 1$

b) dla $a = 12$ istnieje odwrotność multiplikatywna mod 25, ponieważ $\gcd(25, 12) = 1$

c) dla $a = 10$ nie istnieje odwrotność multiplikatywna mod 45, ponieważ gcd(45, 10) = 5

Zadania:

Sprawdź, dla których z poniżej podanych liczb istnieją odwrotności multiplikatywne modulo n, a dla których nie istnieją.

a) $a = 10, n = 19$ (odp.: tak)
b) $a = 14, n = 77$ (odp.: nie)
c) $a = 23, n = 58$ (odp.: tak)
d) $a = 79, n = 113$ (odp.: tak)
e) $a = 123, n = 861$ (odp.: nie)
f) $a = 131, n = 913$ (odp.: tak)

11. Rozszerzony algorytm Euklidesa

Algorytm Euklidesa można rozszerzyć w ten sposób, że wraz z obliczaniem gcd(n, a) można obliczać jednocześnie liczby całkowite u i v takie, że $u \cdot n + v \cdot a = \gcd(n, a)$.

Algorytm:

1. Przyjmij: $i \leftarrow 0$, $(u_0, v_0) \leftarrow (0, 1)$, $(u_0', v_0') \leftarrow (1, 0)$, $n_0 \leftarrow n$, $a_0 \leftarrow a$.
2. Wyznacz: $q_i \leftarrow \lfloor n_i / a_i \rfloor$, $r_i \leftarrow n_i \bmod a_i$.
3. Jeśli $r_i = 0$ to algorytm się zatrzymuje.
4. Przyjmij: $i \leftarrow i + 1$, $n_i \leftarrow a_{i-1}$, $a_i \leftarrow r_{i-1}$,
   $u_i' \leftarrow u_{i-1}$, $u_i \leftarrow u_{i-1}' - q_{i-1} \cdot u_{i-1}$,
   $v_i' \leftarrow v_{i-1}$, $v_i \leftarrow v_{i-1}' - q_{i-1} \cdot v_{i-1}$ i wróć do kroku 2.

Po zatrzymaniu algorytmu wartość $a_i = \gcd(n, a)$. Dodatkowo w każdym kroku algorytmu (dla każdego i) spełnione są równości: $u_i \cdot n + v_i \cdot a = a_i$, $u_i' \cdot n + v_i' \cdot a = n_i$.

Przykład:

Wyznacz gcd(1769, 551) przy użyciu rozszerzonego algorytmu Euklidesa.

i	u_i	u_i'	v_i	v_i'	n_i	a_i	q_i	r_i
0	0	1	1	0	1769	551	3	116
1	1	0	–3	1	551	116	4	87
2	–4	1	13	–3	116	87	1	29
3	5	–4	–16	13	87	29	3	0

Zatem $u = u_3 = 5$, $v = v_3 = -16$. Wobec tego $\gcd(1769, 551) = a_3 = u_3 \cdot n + v_3 \cdot a = 5 \cdot 1769 - 16 \cdot 551 = 8845 - 8816 = 29$

Zadania:

Znajdź przy użyciu rozszerzonego algorytmu Euklidesa wartości u, v oraz $\gcd(n, a)$

a) gcd(567, 224) (odp.: 7) b) gcd(1280, 312) (odp.: 8)

c) gcd(1222, 702) (odp.: 26) d) gcd(1551, 1188) (odp.: 33)

12. Obliczanie odwrotności multiplikatywnej modulo *n*

Wiadomo, że a ma odwrotność multiplikatywną modulo n, gdy $\gcd(n, a) = 1$. Zatem załóżmy, że a i n są względnie pierwsze. W takim wypadku korzystając z rozszerzonego algorytmu Euklidesa otrzymamy $u \cdot n + v \cdot a = 1$. Przenosząc 1 na lewą stronę, a $u \cdot n$ na prawą dostajemy $v \cdot a - 1 = -u \cdot n$, stąd mamy, że $v \cdot a \equiv 1 \bmod n$. Zatem $a^{-1} = v \bmod n$ jest odwrotnością $a \bmod n$. Ponieważ v przyjmuje wartości z zakresu $-n < v < n$, dlatego aby otrzymać wynik z zakresu $0 < v < n$ konieczna jest redukcja $v \bmod n$.

Jak widać rozszerzony algorytm Euklidesa może posłużyć do obliczania odwrotności multiplikatywnej modulo n.

Przykłady:

Oblicz odwrotność multiplikatywną mod n do liczby a gdzie:

a) $a = 25$, $n = 31$

i	u_i	u_i'	v_i	v_i'	n_i	a_i	q_i	r_i
0	0	1	1	0	31	25	1	6
1	1	0	–1	1	25	6	4	1
2	–4	1	5	–1	6	1	6	0

Odwrotnością multiplikatywną mod n do liczby a jest $a^{-1} = v_2 \bmod n = 5 \bmod 31 = 5$.

b) $a = 31$, $n = 71$

i	u_i	u_i'	v_i	v_i'	n_i	a_i	q_i	r_i
0	0	1	1	0	71	31	2	9
1	1	0	–2	1	31	9	3	4
2	–3	1	7	–2	9	4	2	1
3	7	–3	–16	7	4	1	4	0

Odwrotnością multiplikatywną mod n do liczby a jest $a^{-1} = v_3 \bmod n = -16 \bmod 71 = 55$.

Zadania:

Oblicz odwrotność multiplikatywną mod n do liczby a gdzie:

a) $a = 7, n = 23$ (odp.: 10) b) $a = 13, n = 45$ (odp.: 7)

c) $a = 36, n = 67$ (odp.: 54) d) $a = 43, n = 80$ (odp.: 67)

e) $a = 27, n = 131$ (odp.: 34) f) $a = 97, n = 184$ (odp.: 129)

g) $a = 849, n = 1234$ (odp.: 125) h) $a = 997, n = 1539$ (odp.: 1309)

i) $a = 1250, n = 1869$ (odp.: 779) j) $a = 534, n = 1369$ (odp.: 1228)

13. Szyfr afiniczny

Dla szyfru afinicznego przyjmujemy, że $P = C = Z_{26}$, $x \in P$, $y \in C$, $k \in K$. Funkcja szyfrująca ma postać:

$$y = e_k(x) = (a \cdot x + b) \bmod 26.$$

Jest więc to uogólnienie szyfru przesuwającego (dla $a = 1$ otrzymujemy szyfr przesuwający z kluczem b). O ile liczba $b \in Z_{26}$ może być w szyfrze afinicznym dowolna, to $a \neq 0$ musi spełniać pewien warunek w celu otrzymania jednoznacznej funkcji deszyfrującej. Otóż dla równania $y = (a \cdot x + b) \bmod 26$ musi istnieć jedyne rozwiązanie ze względu na zmienną x. Czyli dla a musi istnieć odwrotność multiplikatywna $a^{-1} \in Z_{26}$. Wiadomo, że odwrotność taka istnieje dla a, które są względnie pierwsze z 26, tzn. $\gcd(26, a) = 1$. Wprowadźmy oznaczenie $Z_n^* = \{a: a \in Z_n, \gcd(n, a) = 1\}$. Zatem Z_{26}^* jest zbiorem wartości odwracalnych w Z_{26}. Stąd przestrzenią klucza jest zbiór $K = \{(a, b): a \in Z_{26}^*, b \in Z_{26}\}$.

Przekształcenie deszyfrujące będzie miało postać:

$$x = d_{k'}(y) = (a^{-1} \cdot y + (-a^{-1} \cdot b)) \bmod 26$$

gdzie $a^{-1} \in Z_{26}^*$ jest odwrotnością multiplikatywną liczby a w Z_{26}. Klucz deszyfrujący $k' = (a^{-1}, -a^{-1} \cdot b)$ jest jednoznacznie wyznaczony przez k i może być łatwo obliczony stosując rozszerzony algorytm Euklidesa do obliczania a^{-1}. Pomimo istnienia dwóch kluczy (jednego do szyfrowania, a drugiego do deszyfrowania) jest to kryptosystem symetryczny, ponieważ znajomość klucza szyfrującego równoważna jest znajomości klucza deszyfrującego.

Łatwo jest wyznaczyć $Z_{26}^* = \{1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25\}$. Niech $\#X$ oznacza ilość elementów zbioru X. Ponieważ $\#Z_{26}^* = 12$, zatem szyfr afiniczny ma $12 \cdot 26 = 312$ możliwych kluczy. Jest to liczba zbyt mała, aby zapewnić bezpieczeństwo kryptosystemu.

Dla $n \in N$ oznaczamy przez $\varphi(n) = \#Z_n^*$. Innymi słowy $\varphi(n)$ jest funkcją określającą ilość liczb w Z_n względnie pierwszych z n, jest to tzw. funkcja Eulera. Jeśli $n = p$ jest liczbą pierwszą, wtedy $\varphi(p) = p - 1$, natomiast dla liczby złożonej n po uwzględnieniu jej rozkładu na czynniki pierwsze

$$n = \prod_{i=1}^{k} p_i^{e_i}$$

gdzie p_i są różnymi liczbami pierwszymi, a wykładniki e_i określają liczbę powtórzeń p_i w rozkładzie, funkcja Eulera wyraża się wzorem

$$\varphi(n) = \prod_{i=1}^{k} p_i^{e_i - 1} \cdot (p_i - 1)$$

Przykładowo dla:

$n = 24 = 2^3 \cdot 3^1$, $\varphi(24) = 2^2 \cdot (2 - 1) \cdot 3^0 \cdot (3 - 1) = 8$,

$n = 26 = 2^1 \cdot 13^1$, $\varphi(26) = 2^0 \cdot (2 - 1) \cdot 13^0 \cdot (13 - 1) = 12$.

Twierdzenie Fermata

Jeżeli p jest liczbą pierwszą, to dla każdej liczby $a \in Z$ takiej, że $\gcd(a, p) = 1$ zachodzi

$$a^{p-1} \bmod p = 1$$

Uogólnienie Eulera

Dla każdego $a \in Z$ i $n \in N$ takich, że $\gcd(a, n) = 1$ zachodzi

$$a^{\varphi(n)} \bmod n = 1$$

Podane przez Eulera uogólnienie twierdzenia Fermata dostarcza algorytmu wyznaczania odwrotności multiplikatywnej modulo n. Jeżeli pomnożymy obie strony równania z twierdzenia Eulera przez a^{-1}, to dostaniemy $a^{-1} \cdot a^{\varphi(n)} \bmod n = a^{-1}$, a stąd mamy, że $a^{-1} = a^{\varphi(n)-1} \bmod n$. Jeżeli n jest liczbą pierwszą, to rozwiązanie upraszcza się do postaci $a^{-1} = a^{n-2} \bmod n$. Jeżeli nie jest znane $\varphi(n)$, to a^{-1} można policzyć korzystając z rozszerzonego algorytmu Euklidesa.

Przykład:

Rozważmy szyfr afiniczny z kluczem $k = (7, 3)$. Mamy $\gcd(7, 26) = 1$ więc znajdujemy $7^{-1} \bmod 26 = 7^{12-1} \bmod 26 = 15$. Stąd $a^{-1} \cdot b = 15 \cdot 3 \bmod 26 = 19$, czyli $-a^{-1} \cdot b = 26 - 19 = 7$.

Funkcja szyfrująca zatem ma postać:

$$y = e_k(x) = (7 \cdot x + 3) \bmod 26,$$

natomiast funkcja deszyfrująca:

$$x = d_k(y) = (15 \cdot y - 19) \bmod 26 = (15 \cdot y + 7) \bmod 26.$$

Korzystając z powyższych wzorów zaszyfrujemy tekst jawny: krypt ograf ia.

tekst jawny	k	r	y	p	t	o	g	r	a	f	i	a
x	10	17	24	15	19	14	6	17	0	5	8	0
y	21	18	15	4	6	23	19	18	3	12	7	3
szyfrogram	V	S	P	E	G	X	T	S	D	M	H	D

Po wykonaniu koniecznych obliczeń otrzymujemy szyfrogram: VSPEG XTSDM HD.

Zadania:

1. Zaszyfruj:

a) ochro nadan ych, $k = (15, 13)$ (odp.: PROIP ANGNA JRO)

b) szyfr afini czny, $k = (21, 9)$ (odp.: XOTKC JKVWV ZOWT)

c) nazwa miejscowości, w której mieszkasz, $k = (17,$ miesiąc_urodzenia mod 26)

d) swoje imię i nazwisko, $k = (23,$ (rok_urodzenia · dzień_urodzenia – miesiąc_urodzenia) mod 26)

2. Odszyfruj:

a) HLMGI HMVOY ZI, $k = (17, 8)$ (odp.: droga do nieba)

b) JGWKO OQMMK VORKM GI, $k = (19, 10)$ (odp.: picasso w warszawie)

c) AJCTR RGBKN KURXR GH, $k = (23, 7)$ (odp.: litwo ojczyzno moja)

d) SVIIN BVTQN HMVIJ PNOFP D, $k = (5, 21)$ (odp.: pan nowak zostanie ojcem)

3. Wylicz $\varphi(n)$ dla:

a) $n = 60$ (odp.: 16)

b) $n = 216$ (odp.: 72)

c) $n = 1764$ (odp.: 504)

d) $n = 1800$ (odp.: 480)

14. Szyfr Vigenère'a

Zarówno w szyfrze przesuwającym, jak i w szyfrze afinicznym każdy ze znaków tekstu jawnego zamieniany jest na odpowiadający mu pewien znak szyfrogramu. Kryptosystemy o tej własności nazywane są monoalfabetycznymi. Istnieją jednak kryptosystemy (tzw. polialfabetyczne), w których poszczególne znaki tekstu jawnego mogą być przekształcane na różne znaki szyfrogramu. Przykładem kryptosystemu polialfabetycznego jest szyfr Vigenère'a.

Niech $m \in N$ oraz $P = C = K = (Z_{26})^m$. Dla klucza $k = (k_1, k_2, \ldots, k_m)$ definiujemy przekształcenie szyfrujące

$$y = e_k(x_1, x_2, \ldots, x_m) = ((x_1 + k_1) \bmod 26, (x_2 + k_2) \bmod 26, \ldots, (x_m + k_m) \bmod 26)$$

i deszyfrujące

$$x = d_k(y_1, y_2, \ldots, y_m) = ((y_1 - k_1) \bmod 26, (y_2 - k_2) \bmod 26, \ldots, (y_m - k_m) \bmod 26)$$

gdzie $x = (x_1, x_2, \ldots, x_m) \in P$, $y = (y_1, y_2, \ldots, y_m) \in C$.

Widać, że przy pomocy m-znakowego klucza, za jednym razem szyfrowany jest ciąg m liter tekstu jawnego. Liczba kluczy w szyfrze Vigenère'a jest równa 26^m (np. dla $m = 5$ przestrzeń klucza jest większa niż $1{,}1 \cdot 10^7$), istnieją jednak metody kryptoanalizy, które umożliwiają złamanie szyfru Vigenère'a w czasie krótszym niż pełne przeszukiwanie przestrzeni klucza.

Jeżeli w szyfrze Vigenère'a długość użytego klucza jest równa długości tekstu jawnego, to nazywamy go szyfrem z kluczem bieżącym. Jeżeli dodatkowo klucz ten jest losowym ciągiem znaków i użyty jest tylko jeden raz, to jest to szyfr z kluczem jednokrotnym (ang. *one time pad*).

Przykład:

Niech $m = 5$, k = „szyfr" = (18, 25, 24, 5, 17). Tekst jawny: tenkr yptos ystem nieje stbez piecz ny.

tekst jawny	t	e	n	k	r	y	p	t	o	s	y	s	t	e	m
x	19	4	13	10	17	24	15	19	14	18	24	18	19	4	12
k	18	25	24	5	17	18	25	24	5	17	18	25	24	5	17
y	11	3	11	15	8	16	14	17	19	9	16	17	17	9	3
szyfrogram	L	D	L	P	I	Q	O	R	T	J	Q	R	R	J	D

tekst jawny	n	i	e	j	e	s	t	b	e	z	p	i	e	c	z	n	y
x	13	8	4	9	4	18	19	1	4	25	15	8	4	2	25	13	24
k	18	25	24	5	17	18	25	24	5	17	18	25	24	5	17	18	25
y	5	7	2	14	21	10	18	25	9	16	7	7	2	7	16	5	23
szyfrogram	F	H	C	O	V	K	S	Z	J	Q	H	H	C	H	Q	F	X

Po wyliczeniach dostajemy tekst zaszyfrowany: LDLPI QORTJ QRRJD FHCOV KSZJQ HHCHQ FX.

Zadania:

1. Zaszyfruj:

a) odwro tnosc multi plika tywna, k = „cialo" (odp.: QLWCC VVODQ OCLEW RTIVO VGWYO)

b) szyfr polia lfabe tyczn y, k = „alfabet" (odp.: SKDFS THLTF LGEUE EDCAR R)

c) nazwa miejscowości, w której mieszkasz, używając za klucz nazwę swojego miesiąca urodzenia

d) swoje imię i nazwisko, używając za klucz nazwę miejscowości, w której mieszkasz

2. Odszyfruj:

a) QRVOR WEDAG ALJGD, k = „wakacje" (odp.: urlop na hawajach)

b) RYGOU FMAEA TBEWH IPY, k = „auto" (odp.: renault megane coupe)

c) EGUKS EGDLP MZVMO LBB, k = „system" (odp.: microsoft windows xp)

d) IQWAW IETIM JEQJP CWTIQ AICZ, k = „inwokacja" (odp.: adam mickiewicz pan tadeusz)

Szyfr Hilla

W kryptosystemach opisywanych powyżej, każda z liter tekstu jawnego była przekształcana niezależnie od pozostałych liter tekstu jawnego w literę szyfrogramu. W szyfrze Hilla szyfrowane są jednocześnie m-literowe bloki, a każda litera szyfrogramu z bloku m-literowego zależy w pewien sposób od wszystkich z tego bloku liter tekstu jawnego.

Niech $m \in N$, $P = C = (Z_{26})^m$. Kluczem w szyfrze Hilla jest odwracalna modulo 26 macierz K o wymiarach $m \times m$. Warunkiem istnienia macierzy K^{-1} odwrotnej modulo 26 do K jest to, aby gcd(det K, 26) = 1. Jeśli $x = (x_1, x_2, ..., x_m) \in P$ i $y = (y_1, y_2, ..., y_m) \in C$ są odpowiednio jednostkami tekstu jawnego i szyfrogramu, to przekształcenia szyfrujące i deszyfrujące mają postać

$$y = e_K(x) = (x \cdot K) \bmod 26$$

$$x = d_{K^{-1}}(y) = (y \cdot K^{-1}) \bmod 26$$

a dokładniej dla przekształcenia szyfrującego

$$(y_1, y_2, ..., y_m) = e_K(x_1, x_2, ..., x_m) = (x_1, x_2, ..., x_m) \cdot \begin{pmatrix} k_{11} & k_{12} & \dots & k_{1m} \\ k_{21} & k_{22} & \dots & k_{2m} \\ \vdots & \vdots & & \vdots \\ k_{m1} & k_{m2} & \dots & k_{mm} \end{pmatrix} \bmod 26$$

i dla przekształcenia deszyfrującego

$$(x_1, x_2, ..., x_m) = d_{K^{-1}}(y_1, y_2, ..., y_m) = (y_1, y_2, ..., y_m) \cdot \begin{pmatrix} k_{11}^{-1} & k_{12}^{-1} & \dots & k_{1m}^{-1} \\ k_{21}^{-1} & k_{22}^{-1} & \dots & k_{2m}^{-1} \\ \vdots & \vdots & & \vdots \\ k_{m1}^{-1} & k_{m2}^{-1} & \dots & k_{mm}^{-1} \end{pmatrix} \bmod 26$$

Przykład:

Niech $m = 2$, $K = \begin{pmatrix} 11 & 8 \\ 3 & 7 \end{pmatrix}$, $x = (x_1, x_2) \in P$, $y = (y_1, y_2) \in C$. Ponieważ $y = x \cdot K \bmod 26$ więc $y_1 = (11 \cdot x_1 + 3 \cdot x_2) \bmod 26$, $y_2 = (8 \cdot x_1 + 7 \cdot x_2) \bmod 26$. Niech dany będzie tekst jawny: komputer. Digramom: ko, mp,

ut, er odpowiadają pary liczb (10, 14), (12, 15), (20, 19), (4, 17). Po obliczeniach znajdujemy odpowiadające elementy szyfrogramu: (22, 22), (21, 19), (17, 7), (17, 21), tzn. digramy: WW VT RH RV.

Macierz deszyfrująca jest macierzą odwrotną do macierzy K modulo 26, czyli $K^{-1} = \begin{pmatrix} 7 & 18 \\ 23 & 11 \end{pmatrix}$. Ponieważ $x = y \cdot K^{-1}$ więc deszyfrowanie będzie przebiegać według wzorów: $x_1 = (7 \cdot y_1 + 23 \cdot y_2) \bmod 26$, $x_2 = (18 \cdot y_1 + 11 \cdot y_2) \bmod 26$.

Zadania:

1. Zaszyfruj:

a) kl aw ia tu ra, $m = 2$, $K = \begin{pmatrix} 5 & 6 \\ 17 & 19 \end{pmatrix}$ (odp.: DJ KC OW TA HY, $K^{-1} = \begin{pmatrix} 1 & 12 \\ 21 & 3 \end{pmatrix}$)

b) tel ewi zor, $m = 3$, $K = \begin{pmatrix} 9 & 3 & 4 \\ 7 & 2 & 1 \\ 6 & 5 & 8 \end{pmatrix}$ (odp.: FQM ESY JGQ, $K^{-1} = \begin{pmatrix} 25 & 24 & 17 \\ 14 & 24 & 3 \\ 5 & 19 & 5 \end{pmatrix}$)

2. Odszyfruj:

a) YD DD ZI WB, $m = 2$, $K = \begin{pmatrix} 3 & 15 \\ 6 & 1 \end{pmatrix}$ (odp.: internet, $K^{-1} = \begin{pmatrix} 23 & 19 \\ 18 & 17 \end{pmatrix}$)

b) DRG KZB RHU DKA UKF, $m = 3$, $K = \begin{pmatrix} 17 & 9 & 10 \\ 5 & 12 & 8 \\ 7 & 3 & 1 \end{pmatrix}$ (odp.: linux plus, $K^{-1} = \begin{pmatrix} 2 & 3 & 8 \\ 11 & 11 & 10 \\ 5 & 24 & 19 \end{pmatrix}$)