ZAKRES MATERIAŁU

[Zadanie 01] Wykonaj poniższe operacje w arytmetyce mod m. Podaj najmniejsze rozwiązanie w zbiorze {0, 1, ..., m-1}.

(a) $x \equiv 36*82 \pmod{35}$

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

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

(d) $x \equiv -38 \pmod{34}$

(e) $x \equiv 141^{314} * 15^{41} \pmod{281}$

(f) $x \equiv (16^4 - 32^3) \bmod 41$

Rozwiązanie
Wskazówka: Skorzystaj z metod klasy int26.

(a) $36 \pmod{35} = 1$, $82 \pmod{35} = 12$, $1*12 \pmod{35} = 12$, x=12

(b) $16^2 \pmod{41} = 10$, $12^3 \pmod{41} = 6$, $10*6 \pmod{41} = 19$, x=19

(c) $6^5 \pmod{15} = 6$, $8^3 \pmod{15} = 2$, $(6+2) \bmod 15 = 8$, x=8

(d) $-38 \pmod{34} = 30$, x=30

(e) $141^{314} \pmod{281}$=279, $15^{41} \pmod{281}$=42, 279*42 (mod 281)=197, x=197

(f) $16^4 \pmod{41}$=18, $32^3 \pmod{41}$=9, (18-9)mod 41=9, x=9

[Zadanie 02] Znajdź najmniejsze rozwiązania poniższych kongruencji w zbiorze {0, 1, ..., m-1} dla modułu m. Skorzystaj z następującego twierdzenia.

[TW01] Weźmy kongruencję liniową $ax \equiv b \pmod m$. Załóżmy (bez straty ogólności), że $0 \le a, b<m$.

- jeśli $NWD(a,m) = 1$, to jej rozwiązanie x_0 łatwo znaleźć. Wszystkie inne rozwiązania mają postać $x = x_0 + mn$ dla $n \in Z$.
- jeśli $NWD(a,m) = d$, to jej rozwiązanie istnieje wtw d|b.
  W tym przypadku jest ona równoważna (ma takie same rozwiązania) jak kongruencja $a'x \equiv b' \pmod{m'}$, gdzie $a' = a/d$, $b' = b/d$, $m' = m/d$.

(a) $3x \equiv 4 \pmod 7$

(b) $9x \equiv 12 \pmod{21}$

(c) $27x \equiv 72 \pmod{900}$

(d) $27x \equiv 25 \pmod{256}$

(e) $3x \equiv 4 \pmod{12}$

Rozwiązanie

(a) $NWD(3,7) = 1$, $3x = 7*2+4$ dla x=6,

(b) $NWD(9,21) = 3$ i 3|12, więc szukamy rozwiązań kongruencji $3x \equiv 4 \pmod 7$; rozwiązaniem jest x=6,

(c) $NWD(27,900) = 9$ i 9|72, więc szukamy rozwiązań kongruencji $3x \equiv 8 \pmod{100}$; $NWD(3,100) = 1$, $3x = 100*1+8$ dla x=36,

(d) $NWD(27,256) = 1$, $27x = 256*23+25$ dla x=219.

(e) $NWD(3,12)=3$ i $3 \nmid 4$, więc na mocy tw01 kongruencja nie ma rozwiązań.

[Zadanie 03] Znajdź ostatnią cyfrę liczby a w systemie o podstawie p. Skorzystaj z poniższego twierdzenia.

[TW02] 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

Rozwiązanie

(a) $7 \nmid 2$ i $1000 \equiv 4 \pmod 6$, więc $2^{1000} \equiv 2^4 = 16 \equiv 2 \pmod 7$. Ostatnią cyfrą jest 2.

(b) $11 \nmid 2$ i $10000 \equiv 0 \pmod{10}$, więc $2^{10000} \equiv 2^0 = 1 \equiv 1 \pmod{11}$. Ostatnią cyfrą jest 1.

(c) $13 \nmid 2$ i $1000 \equiv 4 \pmod{12}$, więc $2^{1000} \equiv 2^4 = 16 \equiv 3 \pmod{13}$. Ostatnią cyfrą jest 3.

[Zadanie 04] Oblicz resztę z dzielenia liczby 2^{100} przez 31.

Rozwiązanie

$2^5 \equiv 1 \pmod{31}$, więc $2^{100} \equiv 1 \pmod{31}$. Stąd reszta z dzielenia liczby 2^{100} przez 31 wynosi 1.

[Zadanie 05] Oblicz 2^{100000} mod 55. Skorzystaj z poniższego twierdzenia.

[TW03] Jeśli $NWD(a, m) = 1$ i $n \equiv r \pmod{\varphi(m)}$, to $a^n \equiv a^r \pmod m$.

Rozwiązanie

$\varphi(55) = \varphi(5)*\varphi(11) = 4*10 = 40$

Ponieważ $NWD(2, 55) = 1$ i $100000 \equiv 0 \pmod{40}$, więc $2^{100000} \equiv 2^0 = 1 \equiv 1 \pmod{55}$

[Zadanie 06] Oblicz ostatnią cyfrę liczby 2^{1000}.

Rozwiązanie

(*) $\forall k \in N\ 6^k \equiv 6 \pmod{10}$ (dowód indukcja ze względu na k)

(1) $6^1 \equiv 6 \pmod{10}$

(2) zał. ind. Niech $6^k \equiv 6 \pmod{10}$

Należy pokazać, że wówczas również $6^{k+1} \equiv 6 \pmod{10}$.

$6^{k+1} = 6^k * 6 \equiv 6*6 \equiv 6 \pmod{10}$, co należało pokazać. Stąd na mocy zasady indukcji matematycznej zachodzi (*).

(**) $2^4 \equiv 6 \pmod{10}$, więc $2^{1000} = 2^{4*250} \equiv 6^{250} \pmod{10}$

z (**) i (*) $2^{1000} \equiv 6^{250} \equiv 6 \pmod{10}$. Stąd ostatnią cyfrą liczby 2^{1000} jest 6.

[Zadanie 07] Oblicz ostatnie dwie cyfry liczby 2^{1000}.
Rozwiązanie

(*) $\forall k \in N\ 76^k \equiv 76 (\mathrm{mod}\, 100)$ (dowód indukcja ze względu na k)

(1) $76^1 \equiv 76 (\mathrm{mod}\, 100)$

(2) zał. ind. Niech $76^k \equiv 76 (\mathrm{mod}\, 100)$

Należy pokazać, że wówczas również $76^{k+1} \equiv 76 (\mathrm{mod}\, 100)$.

$76^{k+1} = 76^k * 76 \equiv 76 * 76 = 5776 \equiv 76 (\mathrm{mod}\, 100)$, co należało pokazać.

Stąd na mocy zasady indukcji matematycznej zachodzi (*).

(**) $2^{10} \equiv 24 (\mathrm{mod}\, 100)$, więc $2^{20} \equiv 24^2 = 576 \equiv 76 (\mathrm{mod}\, 100)$

z (**) i (*) $2^{1000} = 2^{20*50} \equiv 76^{50} \equiv 76 (\mathrm{mod}\, 100)$ .Ostatnie dwie cyfry to 7 i 6.

[TW04] (Małe twierdzenie Fermata)
Niech p będzie liczbą pierwszą. Wówczas

- każda liczba a spełnia kongruencję $a^p \equiv a (\mathrm{mod}\, p)$
- każda liczba a niepodzielna przez p spełnia kongruencję $a^{p-1} \equiv 1 (\mathrm{mod}\, p)$.

[Zadanie 08] Uzasadnij, że 10-tą potęgę dowolnej liczby całkowitej można zapisać jako 11k lub 11k+1, gdzie $k \in Z$
Rozwiązanie
Niech a będzie ustaloną liczbą całkowitą.

Jeśli $11 \mid a$, to $a = 11k_1$, więc $a^{10} = 11(11^9 k_1^{10}) = 11k$.

Jeśli $11 \nmid a$, to z MtF $a^{11-1} \equiv 1 (\mathrm{mod}\, 11)$, czyli $a^{10} = 11k + 1$.

[Zadanie 09] Rozłóż na czynniki pierwsze liczbę a. Skorzystaj z poniższego twierdzenia.
[TW05] 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) $p \equiv 1 (\mathrm{mod}\, n)$

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

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

(a) Niech $p \mid 2^{11} - 1$. Wówczas (z tw05) $p \equiv 1 (\mathrm{mod}\, 22)$ (ponieważ p>2 i 11 jest liczbą nieparzystą)

Sprawdzamy ręcznie liczby pierwsze p postaci $22*k+1 \le \lfloor \sqrt{2047} \rfloor = \lfloor 45.2437841 \rfloor = 45$, tzn. tu tylko p=23.

Widać, że 2047=23*89

(b) Korzystając z tw05 szukamy czynników pierwszych liczb postaci $b^d - 1$ dla d=1, 3, 5.

Dzielnikiem pierwszym liczby $3^1 - 1 = 2$ jest 2.

Dzielnikami pierwszymi liczby $3^3 - 1 = 26$ są liczby 2, 13.

Dzielnikami pierwszymi liczby $3^5 - 1 = 242$ są liczby 2, 11.

$14348906 = 2*11^2*13*4561$.

p=4561 jest liczbą pierwszą. Jest to liczba spełniająca warunek $4561 \equiv 1 (\mathrm{mod}\, 2*15)$ ($p \equiv 1 (\mathrm{mod}\, 2n)$).

[Zadanie 10] 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)
Rozwiązanie
(a) NWD(400,28)=4
(b) NWD(632,410)=2
(c) NWD(368,128)=16
(d) NWD(336,129)=3
(e) NWD(720,2700,2160,120)=60
(f) NWD(27720,1155,6930)=1155

[Zadanie 11] Wykonaj operację dodawania dwóch liczb binarnych a i b.
(a) a=101010101, b=11100101
(b) a=10110010, b=111111
(c) a=111111, b=111111
Rozwiązanie
(a) a+b = 1000111010
(b) a+b = 11110001
(c) a+b = 1111110

[Zadanie 12] Wykonaj operację mnożenia dwóch liczb binarnych a i b.
(a) a=111000, b=101010
(b) a=111100, b=10101
(c) a=111010, b=101000
Rozwiązanie
(a) a*b = 100100110000
(b) a*b = 10011101100
(c) a*b = 100100010000

[Zadanie 13] Zapisz liczbę c w systemie pozycyjnym o zadanej podstawie.
(a) $135=(.....)_2$,
(b) $426=(.....)_3$,
(c) $189=(.....)_5$,
(d) $845=(.....)_6$.
Rozwiązanie
(a) $135=(10000111)_2$,
(b) $426=(120210)_3$,
(c) $189=(1224)_5$,
(d) $845=(3525)_6$.

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

[Zadanie 14] Zapisz w systemie dziesiętnym liczbę c podaną w systemie pozycyjnym o podstawie p.
(a) $(1010111)_2$,
(b) $(120210)_3$,
(c) $(10431231)_5$,
(d) $(3502102)_6$.
Rozwiązanie
(a) $(1010111)_2=87$,
(b) $(120210)_3=426$,
(c) $(10431231)_5=92691$,
(d) $(3502102)_6=179318$.

[Umowa] $(a)_p$ ozn. resztę z dzielenia liczby całkowitej a przez p
---
[Zadanie 15] 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 $\oplus$
Rozwiązanie
Działania $\oplus$, $\otimes$ są dobrze określone w zbiorze $Z_{13}=\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$, ponieważ reszta z dzielenia (a+b) i (a*b) przez 13 należy do zbioru Z_{13}.
(a) $\forall a,b,c \in Z_{13}\ (a \oplus b) \oplus c = a \oplus (b \oplus c)$?
Niech a, b, $c \in Z_{13}$.
(*) $(a+b+c)_{13} = ((a+b)_{13}+c)_{13} = ((a \oplus b)+c)_{13} = (a \oplus b) \oplus c$
(**) $(a+b+c)_{13} = (a+(b+c)_{13})_{13} = (a+(b \oplus c))_{13} = a \oplus (b \oplus c)$
Z (*) i (**) mamy (a).
(b) $\forall a,b \in Z_{13}\ (a \oplus b = b \oplus a)$?
Niech a, $b \in Z_{13}$.
$a \oplus b = (a+b)_{13} = (b+a)_{13} = b \oplus a$
(c) $\exists e_0 \in Z_{13}\ \forall a \in Z_{13}\ (e_0 \oplus a = a \oplus e_0 = a)$?
$e_0 = 0$ – element neutralny dodawania
(d) $\forall a \in Z_{13}\ \exists a' \in Z_{13}\ (a \oplus a' = a' \oplus a = e_0)$?
Elementem przeciwny do 0 jest 0, ponieważ $0 \oplus 0 = 0$
Elementem przeciwnym do $a \neq 0$ jest $(13\text{-}a)_{13}$, ponieważ $(a \oplus (13\text{-}a)_{13}) = (a+(13\text{-}a)_{13})_{13} = 0$
(e) $\forall a,b,c \in Z_{13}\ (a \otimes b) \otimes c = a \otimes (b \otimes c)$? (analogicznie jak (a))
(f) $\forall a,b \in Z_{13}\ (a \otimes b = b \otimes a)$? (analogicznie jak (b))
(g) $\exists e_1 \in Z_{13}\ \forall a \in Z_{13}\ (e_1 \otimes a = a \otimes e_1 = a)$?
$e_1=1$ – element neutralny mnożenia
(h) $\forall a \in Z_{13} (a \neq e_0)\ \exists a'' \in Z_{13}\ (a \otimes a'' = a'' \otimes a = e_1)$?
[Lem] Jeśli NWD(m, n) = 1, to istnieją liczby całkowite c, d, dla których cm+dn = 1.
Ponieważ 13 jest liczbą pierwszą i $0<a<13$, więc NWD(a, 13) = 1.
Więc istnieją liczby całkowite c, d, dla których ac+13d = 1.
Biorąc resztę z dzielenia przez 13, otrzymujemy $a(c)_{13} = 1$
Zatem elementem odwrotnym do a jest $(c)_{13}$.
(i) $\forall a,b,c \in Z_{13}\ (a \oplus b) \otimes c = (a \otimes b) \oplus (a \otimes c)$?
(*) $\forall a,b \in Z\ ((a)_{13}*(b)_{13})_{13} = (a*b)_{13}$, więc
(**) $(a \oplus b) \otimes c = ((a+b)_{13}*c)_{13} = ((a+b)*c)_{13}$
(***) $(a \otimes b) \oplus (a \otimes c) = ((a*b)_{13}+(a*c)_{13})_{13} = ((a*b)+(a*c))_{13}$
Z (**) i (***) mamy (i).

[Zadanie 16] 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).

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

[Zadanie 17] 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).

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

[Zadanie 18] Uzupełnij ciało każdej z metod klasy int26 tak, aby realizowała operacje dowolnego pierścienia przemiennego z jedynką.

```
//klasa operacji na liczbach zbioru Z_{m}
class int26{
private int x, m;
public int26(int m){…}
public int26(int x, int m){…}
//dodaje liczbę
public int26 plus(int26 b){…}
//odejmuje liczbę
public int26 minus(int26 b){…}
//mnoży przez liczbę
public int26 mnoz(int26 b){…}
//kopiuje obiekt
public int26 copy(){…}
//zwraca odwrotność mod m (rozszerzony algorytm Euklidesa)
public int26 odwr(){…}
//szybkie potęgowanie mod m
public int26 pow26(int e){…}
//zwraca moduł
public int get_m(){…}
public int get_x(){…}
public void set_x(int k){…}
public String toString(){…}
}
```

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