Dodawanie modulo n

Niech $n \in \mathbb{N}$. Na zbiorze liczb $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ wprowadzamy działanie $\oplus_n$.
Dla $a, b \in \mathbb{Z}_n$ $a \oplus_n b$ to reszta z dzielenia $a + b$ przez n.

Przykład
Dla $n = 4$ mamy tabliczkę dodawania:

$\oplus_4$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$0 \oplus_4 2 = 2$,
$3 \oplus_4 1 = 0$,
$2 \oplus_4 3 = 1$.

Własności
Dla każdego $n \in \mathbb{N}$ i dowolnych $a, b, c \in \mathbb{Z}_n$ zachodzi:

- Przemienność: $a \oplus_n b = b \oplus_n a$,
- Łączność: $(a \oplus_n b) \oplus_n c = a \oplus_n (b \oplus_n c)$,
- Neutralność zera: $a \oplus_n 0 = 0 \oplus_n a = a$,
- Istnieje element przeciwny do a (czyli odpowiednik $-a$) taki, że: $a \oplus_n (-a) = -a \oplus_n a = 0$, np. w $\mathbb{Z}_4$ mamy $-1 = 3$, bo $1 \oplus_4 (-1) = 1 \oplus_4 3 = 0$.

Mnożenie modulo n

Niech $n \in \mathbb{N}$. Na zbiorze liczb $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ wprowadzamy działanie $\odot_n$.
Dla $a, b \in \mathbb{Z}_n$ $a \odot_n b$ to reszta z dzielenia $a \cdot b$ przez n.

Przykłady
Dla $n = 4$ mamy tabliczkę mnożenia:

$\odot_4$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$1 \oplus_4 3 = 3$,
$2 \oplus_4 2 = 0$.

Dla $n = 5$ mamy tabliczkę mnożenia:

$\odot_5$	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

$1 \odot_5 2 = 2$,
$3 \odot_5 2 = 1$,
$4 \odot_5 3 = 2$.

Własności
Dla każdego $n \in \mathbb{N}$ i dowolnych $a, b, c \in \mathbb{Z}_n$ zachodzi:

- Przemienność: $a \odot_n b = b \odot_n a$,
- Łączność: $(a \odot_n b) \odot_n c = a \odot_n (b \odot_n c)$,
- Neutralność zera: $a \odot_n 1 = 1 \odot_n a = a$,
- Jeżeli n jest liczbą pierwszą i $a \neq 0$, to istnieje element odwrotny do a (czyli $1/a$ lub a^{-1}) taki, że: $a \odot_n a^{-1} = a^{-1} \odot_n a = 1$ np. w $\mathbb{Z}_5$ mamy $2^{-1} = 3$, bo $2 \odot_5 2^{-1} = 2 \odot_5 3 = 1$, podobnie $3^{-1} = 2$, ale w $\mathbb{Z}_4$ nie ma elementu odwrotnego do 2.

Zadanie
Napisz tabliczkę dodawania i mnożenia w $\mathbb{Z}_7$.

Kongruencje

Definicja
Niech $n \in \mathbb{N}$ oraz $a, b \in \mathbb{Z}$. Mówimy, że a przystaje do b modulo n, jeśli n dzieli $a - b$.

Zapis
$a \equiv b \mod n$, oraz rzadziej spotykany $a \equiv_n b$.

Dwie liczby przystają do siebie modulo n, gdy dają taką samą resztę z dzielenia przez n.

Przykłady

$$\begin{array}{rcllrcllrcl}
2 & \equiv & 9 & \mod 7, & \text{bo:} & 2 & = & 0 \cdot 7 + 2, & 9 & = & 1 \cdot 7 + 2 \\
14 & \equiv & 58 & \mod 11, & \text{bo:} & 14 & = & 1 \cdot 11 + 3, & 58 & = & 5 \cdot 11 + 3 \\
-2 & \equiv & 7 & \mod 3, & \text{bo:} & -2 & = & -1 \cdot 3 + 1, & 7 & = & 2 \cdot 3 + 1 \\
-26 & \equiv & 44 & \mod 10, & \text{bo:} & -26 & = & -3 \cdot 10 + 4, & 44 & = & 4 \cdot 10 + 4 \\
-1 & \equiv & 113 & \mod 6, & \text{bo:} & -1 & = & -1 \cdot 6 + 5, & 113 & = & 18 \cdot 6 + 5 \\
0 & \equiv & 35 & \mod 5, & \text{bo:} & 0 & = & 0 \cdot 5 + 0, & 35 & = & 7 \cdot 5 + 0
\end{array}$$

Własności
Dla dowolnych $a, b, c \in \mathbb{Z}$, $n \in \mathbb{N}$ zachodzi:

- $a \equiv a \mod n$,
- Jeśli $a \equiv b \mod n$, to $b \equiv a \mod n$,
- Jeśli $a \equiv b \mod n$ i $b \equiv c \mod n$, to $a \equiv c \mod n$.

Kongruencje można dodawać, odejmować i mnożyć stronami:
Jeśli $a \equiv b \mod n$ i $c \equiv d \mod n$, to:

- $a + c \equiv b + d \mod n$,
- $a - c \equiv b - d \mod n$,
- $a \cdot c \equiv b \cdot d \mod n$.

Nie wolno dzielić kongruencji stronami, np. $2 \equiv 14 \mod 12$, ale nieprawda, że $1 \equiv 7 \mod 12$.
Zamiast tego możemy mnożyć przez element odwrotny (jeśli istnieje).

Przykład
Rozwiąż kongruencję: $16x + 2 \equiv -x + 1 \mod 11$.

Przenosimy niewiadome na jedną stronę kongruencji:

$$17x \equiv -1 \mod 11$$

Ponieważ dla każdego x mamy $11x \equiv 0 \mod 11$, to możemy odjąć od lewej strony $11x$:

$$6x \equiv -1 \mod 11$$

Analogicznie do prawej strony możemy dodać 11:

$$6x \equiv 10 \mod 11$$

Teraz liczby w kongruencji są elementami zbioru $\mathbb{Z}_{11}$.

Chcielibyśmy "podzielić" kongruencję stronami przez 6. Tego nam nie wolno, ale możemy pomnożyć stronami przez element odwrotny do 6 w grupie $\mathbb{Z}_{11}$. Jest to 2, bo $2 \cdot 6 \equiv 12 \equiv 1 \mod 11$.

$$12x \equiv 20 \mod 11$$

Odejmujemy od lewej strony $11x$, od prawej 11:

$$x \equiv 9 \mod 11$$

Zatem rozwiązaniem są liczby całkowite dające resztę 9 przy dzieleniu przez 11.
Odp.: Kongruencję spełniają liczby postaci $11n + 9$ dla $n \in \mathbb{Z}$.

Kluczowym etapem rozwiązania było znalezienie $6^{-1} \mod 11$. Kiedy istnieje element odwrotny i jak go wyznaczyć?

Twierdzenie. Element odwrotny do a modulo b istnieje wtedy i tylko wtedy, gdy $\mathrm{NWD}(a, b) = 1$.

Wyznaczenie a^{-1} jest "efektem ubocznym" algorytmu Euklidesa do wyznaczania $\mathrm{NWD}(a, b)$. Analizując wstecz kroki tego algorytmu możemy przedstawić $\mathrm{NWD}(a, b)$ w postaci $ak + bl$ dla pewnych $k, l \in \mathbb{Z}$.

Przykład.
Wyznacz $12^{-1} \mod 41$.

$$\mathrm{NWD}(41, 12) = \mathrm{NWD}(12, 5) = \mathrm{NWD}(5, 2) = \mathrm{NWD}(2, 1) = 1$$

Zatem

$$1 = 5 - 2 \cdot 2 = 5 - 2 \cdot (12 - 2 \cdot 5) = 5 \cdot 5 - 2 \cdot 12 = 5 \cdot (41 - 3 \cdot 12) - 2 \cdot 12 = 5 \cdot 41 - 17 \cdot 12$$

Skoro $1 = 5 \cdot 41 - 17 \cdot 12$, to

$$1 \equiv 5 \cdot 41 - 17 \cdot 12 \equiv -17 \cdot 12 \mod 41$$

Czyli elementem odwrotnym do 12 jest

$$12^{-1} \equiv -17 \equiv -17 + 41 \equiv 24 \mod 41$$

Zadanie 1.
Korzystając z algorytmu Euklidesa wyznacz
a) $\mathrm{NWD}(43, 16)$ b) $\mathrm{NWD}(27, 20)$

Zadanie 2.
Przeanalizuj kroki z zadania 1, aby znaleźć rozwiązania kongruencji
a) $16x \equiv 1 \mod 43$ oraz $16x \equiv 5 \mod 43$
b) $20x \equiv 1 \mod 27$ oraz $20x \equiv 3 \mod 27$.

Zadanie 3:
Rozwiąż kongruencje:
a) $3x + 2 \equiv 1 \mod 5$
b) $22x + 1 \equiv 11 - 3x \mod 7$
c) $9x - 5 \equiv 2 \mod 13$
d) $32x + 5 \equiv 28 + 5x \mod 73$
e) $6x \equiv 2 \mod 4$
f) $3x \equiv 1 \mod 6$

Protokoły Diffiego-Hellmana oraz ElGamala

Jeden z pierwszych szyfrów - szyfr Cezara - polegał na zamianie każdej litery w tekście na literę o trzy pozycje późniejszą.

$$A \to D$$
$$B \to E$$
$$C \to F$$
$$\ldots$$
$$X \to A$$
$$Y \to B$$
$$Z \to C$$

np. tekst TEORIALICZB przechodzi na WHRULDOLFCE.
Jest to szyfrowanie symetryczne, tzn. szyfrowanie i odszyfrowywanie wymaga zastosowania tych samych operacji. Żeby odszyfrować tekst przesuwamy każdą literę o trzy pozycje w tył.

Można było skomplikować szyfr nakładając na tekst zmienny klucz. W szyfrze Cezara klucz był stały, równy 3 (lub C, jako litera). Jeśli kluczem będzie słowo KRYPTOGRAFIA, to przekaz TEORIALICZB zostanie zaszyfrowany jako EWNHCPSADFK (ostatnie A w kluczu jest niewykorzystane). Litera K jest 11 w alfabecie, T jest 20, więc ich suma to $31 \equiv 5 \mod 26$ (zakładamy, że poruszamy się w 26-literowym alfabecie łacińskim).

Zmienny klucz pozwala choć trochę zaburzyć gęstość występowania liter, co jest istotne w podejściu lingwistów do szyfrowania (dominującym aż do początku XX wieku - gdy lingwiści poddali się wobec Enigmy, a na scenę weszli matematycy).

Problemem jest przekazanie sobie klucza. Wspomniane Enigmy miały wielkie księgi kodów na dane dni - publikowane nawet na pół roku do przodu, żeby U-boot wypływający w rejs mógł się regularnie komunikować z bazą Kriegsmarine. W przypadku poddania lub uszkodzenia okrętu, księgi kodowe były niszczone jako pierwsze, żeby nie dostały się w ręce aliantów.

Protokół Diffiego-Hellmana pozwala na bezpieczne ustalenie klucza przez otwarte kanały komunikacji.

Alicja i Bartek chcą uzgodnić klucz do przesyłania komunikacji. Przyjmujemy, że tekst jest tu zamieniany na liczby. Ustalony klucz też będzie liczbą.

Protokół Diffiego-Hellmana
1. Alicja i Bartek uzgadniają dużą liczbę pierwszą p.
2. Wybierają pierwiastek pierwotny g modulo p.

Liczby p i g mogą być jawne.
3. Ala wybiera tajną liczbę $a < p$ i oblicza $A = g^a \mod p$. Przesyła Bartkowi A otwartym kanałem.
4. Bartek wybiera tajną liczbę $b < p$ i oblicza $B = g^b \mod p$. Przesyła Ali B otwartym kanałem.
5. Ala oblicza $B^a \mod p$, Bartek oblicza $A^b \mod p$.

Zauważmy, że

$$B^a \equiv (g^b)^a \equiv g^{ab} \equiv (g^a)^b \equiv A^b \mod p$$

g^{ab} jest wspólnym tajnym kluczem.
Jawne są g, p, g^a, g^b, ale a, b i w szczególności g^{ab} są tajne.
Złamanie szyfru sprowadza się do rozwiązania kongruencji

$$g^x \equiv A \mod p$$

czyli obliczenia tzw. **dyskretnego logarytmu** modulo p z liczby A, co jest trudne. Dla dużych liczb pierwszych p (poza szczególnymi przypadkami) nie ma istotnie lepszych algorytmów niż testowanie wartości g^x dla kolejnych x.

Dygresja
W protokole trzeba obliczać wysokie potęgi g. Ile operacji (mnożenia przez a lub podnoszenia do kwadratu) trzeba wykonać, żeby obliczyć a^{100}?

$$a \to a^2 \to a^3 \to a^6 \to a^{12} \to a^{24} \to a^{25} \to a^{50} \to a^{100}$$

Można pokazać, że jeśli wykładnik n ma w systemie dwójkowym k cyfr, to możemy obliczyć a^n wykonując co najwyżej $2k$ operacji.

Przykład
Ala i Bartek uzgodnili $p = 23$ oraz $g = 5$.
Ala ustala $a = 17$, oblicza $5^2 \equiv 2, 5^4 \equiv 4, 5^8 \equiv 16, 5^{16} \equiv 256 \equiv 3, 5^{17} \equiv 15$ i wysyła do Bartka $A = 15$.
Bartek ustala $b = 6$, oblicza $5^2 \equiv 2, 5^4 \equiv 4, 5^6 \equiv 8$ i wysyła do Ali $B = 8$.
Ala dostaje od Bartka $B = 8$ i oblicza $B^a \equiv 8^17 \equiv 13$.
Bartek dostaje od Ali $A = 15$ i oblicza $A^b \equiv 15^6 \equiv 13$.

Uzgodnionym kluczem jest 13. Osoby podsłuchujące znają $p = 23$, $g = 5$, $A = 15$, $B = 8$, ale chcąc wyznaczyć a lub b (potrzebne do uzyskania g^{ab}) musiałyby obliczać po kolei $5, 5^2, 5^3, \ldots$ aż uda im się "trafić" w jedną z przesyłanych liczb.

Zadanie
Ala i Bartek uzgodnili $p = 17$ i $g = 3$.
Ala wybiera $a = 7$, Bartek $b = 12$. Przeprowadź rachunki, jakie muszą wykonać Ala i Bartek i opisz, co może być przesyłane otwartym kanałem, a co jest tajne.

Protokół ElGamala
1. Generowanie klucza:
Ala generuje dużą liczbę pierwszą p i pierwiastek pierwotny g.
Wybiera liczbę $a < p$. Publikuje klucz jawny $A = g^a \mod p$ oraz liczby p, g.
2. Przesłanie wiadomości m:
Bartek wysyła liczbę b (klucz jednorazowy, efemeryczny), a następnie oblicza dwie liczby $c_1 = g^b \mod p$, $c_2 = mA^b \mod p$, czyli $c_2 = mg^{ab} \mod p$ i wysyła parę (c_1, c_2) do Ali.
3. Odczytywanie wiadomości:
Ala oblicza $c_1^a = g^{ab} \mod p$, a następnie $(c_1^a)^{-1} = (g^{ab})^{-1} \mod p$ oraz $m = c_2(c_1^a)^{-1} \mod p$.

Dlaczego to działa:

$$c_2(c_1^a)^{-1} \equiv mA^b((g^b)^a)^{-1} \equiv mg^{ab}(g^{ab})^{-1} \equiv m \mod p$$

Przykład
Niech $p = 47$, $g = 10$. Ala wybiera tajne $a = 7$ i oblicza $A = g^a = 10^7 \equiv 45 \mod 47$.
Bartek wysyła wiadomość $m = 35$. W tym celu wybiera jednorazowy klucz $b = 11$. Oblicza $c_1 = g^b = 10^{11} \equiv 22 \mod 47$, $c_2 = mA^b = 35 \cdot 45^{11} \equiv 42 \mod 47$.
Wysyła Ali parę $(22, 42)$.
Ala znając $a = 7$ oblicza $g^{ab} = c_1^a = 22^7 \equiv 20 \mod 47$,
$(c_1^a)^{-1} \equiv 20^{-1} \equiv 40 \mod 47$,
$m = c_2(c_1^a)^{-1} = 42 \cdot 40 \equiv 35 \mod 47$.

Publicznie przesyłane są p, g, klucz jawny Ali $A = g^a$, klucz jawny Bartka $c_1 = B = g^b$. Przy założeniu, że logarytm dyskretny jest trudny, wiadomość m nie zostanie przechwycona mimo znajomości c_2.

Zadanie

Ala wybiera liczbę pierwszą $p = 31$ oraz pierwiastek pierwotny $g = 3$.
Jako swój klucz prywatny Ala wybiera $a = 13$.
Bartek chcąc wysłać Ali wiadomość przesyła jej $c_1 = 19$, $c_2 = 8$. Znajdź klucz jawny Ali A, klucz jednorazowy Bartka b oraz wiadomość m.