Matematyka Dyskretna
Wykład 3.
Arytmetyka modularna.

Czesław Bagiński
c.baginski@pb.edu.pl

Wydział Informatyki
Politechnika Białostocka

Plan wykładu

1. Relacja przystawania modulo i jej własności
2. Działania na klasach kongruencji
3. Pierścień $\mathbb{Z}_m$
4. Funkcja Eulera
5. Twierdzenie Eulera i Małe Twierdzenie Fermata
6. Chińskie Twierdzenie o Resztach
7. System kryptograficzny RSA

Definicja

Niech $m > 1$ będzie ustaloną liczbą naturalną. Jeżeli a i b są liczbami całkowitymi, to mówimy, że a *przystaje do* b *modulo* m *(*lub *według modułu* m*)*, jeśli $m|(a-b)$. Symbolicznie ten fakt zapisujemy następująco:

$$a \equiv b \pmod{m}.$$

Stwierdzenie

Dla ustalonej liczby naturalnej m relacja przystawania modulo m ma następujące własności:

(i) *Dla dowolnego* $a \in \mathbb{Z}$,
$a \equiv a \pmod{m}$, *(relacja jest zwrotna);*

(ii) *Dla dowolnych* $a, b \in \mathbb{Z}$,
jeśli $a \equiv b \pmod{m}$, *to* $b \equiv a \pmod{m}$,
(relacja jest symetryczna);

(iii) *Dla dowolnych* $a, b, c \in \mathbb{Z}$,
jeśli $a \equiv b \pmod{m}$ *i* $b \equiv c \pmod{m}$,
to $a \equiv c \pmod{m}$ *(relacja jest przechodnia).*

(iv) *Dla dowolnych* $a, b, c, d \in \mathbb{Z}$,
jeśli $a \equiv c \pmod{m}$ *i* $b \equiv d \pmod{m}$,
to $a + b \equiv c + d \pmod{n}$ *oraz* $ab \equiv cd \pmod{m}$
(zgodność relacji z działaniami dodawania i mnożenia).

Klasy kongruencji

Dzięki trzem pierwszym własnościom zbiór wszystkich liczb całkowitych można podzielić na rozłączne zbiory składające się z liczb, których ta relacja nie rozróżnia lub inaczej – zbiorów wszystkich liczb całkowitych, które podzielone przez m dają taką samą resztę. Zbiory te nazywamy *klasami kongruencji* lub *klasami reszt modulo m*. Są to:

$$\begin{aligned} m\mathbb{Z} &= \{mk : \ k \in \mathbb{Z}\}, \\ 1 + m\mathbb{Z} &= \{1 + mk : \ k \in \mathbb{Z}\}, \\ 2 + m\mathbb{Z} &= \{2 + km : \ k \in \mathbb{Z}\}, \\ &\dots \\ (m-1) + m\mathbb{Z} &= \{m - 1 + km : \ k \in \mathbb{Z}\}. \end{aligned}$$

Definicja

Niech $\mathbb{Z}_m$ będzie zbiorem wszystkich reszt z dzielenia przez m, tzn.

$$\mathbb{Z}_m = \{0, 1, 2, \ldots, m-1\}.$$

Definiujemy w nim działania dodawania i mnożenia modulo m.

$$\begin{aligned} a \oplus_m b &\stackrel{\text{def.}}{=} \text{reszta z dzielenia liczby } a+b \text{ przez } m, \\ a \odot_m b &\stackrel{\text{def.}}{=} \text{reszta z dzielenia liczby } a \cdot b \text{ przez } m, \end{aligned} \tag{1}$$

Własności działań

1. Dodawanie jest łączne: dla dowolnych $a, b, c \in \mathbb{Z}_m$, $(a \oplus b) \oplus c = a \oplus (b \oplus c)$.
2. Dodawanie jest przemienne: dla dowolnych $a, b \in \mathbb{Z}_m$, $a \oplus b = b \oplus a$.
3. Dodawanie ma element neutralny, jest nim 0: dla dowolnego $a \in \mathbb{Z}_m$ $a \oplus 0 = a = 0 \oplus a$.
4. Dla każdego elementu a istnieje do niego przeciwny: jeśli $a \in \mathbb{Z}_m$, to $m - a \in \mathbb{Z}_m$ oraz $a \oplus (m - a) = 0$.
5. Mnożenie jest łączne: dla dowolnych $a, b, c \in \mathbb{Z}_m$, $(a \odot b) \odot c = a \odot (b \odot c)$.
6. Mnożenie jest przemienne: dla dowolnych $a, b \in \mathbb{Z}_m$, $a \odot b = b \odot a$.
7. Mnożenie ma element neutralny, jest nim 1: dla dowolnego $a \in \mathbb{Z}_m$ $a \odot 1 = a = 1 \odot a$.
8. Mnożenie jest rozdzielne względem dodawania: dla dowolnych $a, b, c \in \mathbb{Z}_m$, $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$.

Definicja

Zbiór, wraz z dwoma działaniami o powyższych własnościach nazywamy *pierścieniem*. Jeżeli dodatkowo spełniony jest warunek

9. każdy element różny od 0, ma odwrotność:
   dla każdego a istnieje b takie, że

   $$a \odot b = 1.$$

to mówimy zbiór z takimi działaniami jest *ciałem*. Pierwowzorem pierścienia jest zbiór liczb całkowitych z naturalnymi operacjami dodawania i mnożenia liczb, natomiast pierwowzorem ciała – zbiór liczb wymiernych z tymi działaniami.

Definicja

W zbiorze liczb całkowitych tylko 1 i -1 mają odwrotności będące liczbami całkowitymi. Pozostałe liczby nie mają odwrotności w tym zbiorze. Natomiast w $\mathbb{Z}_m$ może istnieć więcej elementów a, dla których istnieje x, taki że $a \odot_m x = 1$. Taki element a nazwiemy *odwracalnym*. Niech

$$\mathbb{Z}_m^* \stackrel{\text{def.}}{=} \{a \in \mathbb{Z}_m : \ NWD(a, b) = 1\} \tag{2}$$

Twierdzenie

Niech $m > 1$ będzie ustaloną liczbą naturalną. Wówczas $\mathbb{Z}_m^*$ jest zbiorem wszystkich elementów odwracalnych z $\mathbb{Z}_m$.

Twierdzenie

Pierścień $\mathbb{Z}_m$ jest ciałem wtedy i tylko wtedy, gdy m jest liczbą pierwszą.

Definicja

Niech $\varphi(n)$ będzie liczbą wszystkich elementów odwracalnych z $\mathbb{Z}_n$, tzn.:

$$\varphi(n) \stackrel{\text{def}}{=} |\mathbb{Z}_n^*|.$$

Funkcję $\varphi(n)$ nazywamy *funkcją Eulera*.

Przykład

Wartości funkcji Eulera dla małych argumentów można wyliczyć bezpośrednio z definicji:

n	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\varphi(n)$	1	2	2	4	2	6	4	6	4	10	4	12	6	8	8

.

n	17	18	19	20	21	22	23	24	25	26	27	28
$\varphi(n)$	16	6	18	8	12	10	22	12	20	12	18	12

.

Stwierdzenie

Funkcja φ spełnia następujące warunki:

(i) *Jeśli p jest liczbą pierwszą, to dla dowolnej liczby naturalnej n*

$$\varphi(p^n) = p^{n-1}(p-1)$$

(ii) *Jeśli m i n są liczbami względnie pierwszymi, to*

Stwierdzenie

Funkcja φ spełnia następujące warunki:

(i) *Jeśli p jest liczbą pierwszą, to dla dowolnej liczby naturalnej n*

$$\varphi(p^n) = p^{n-1}(p-1)$$

(ii) *Jeśli m i n są liczbami względnie pierwszymi, to*

$$\varphi(m \cdot n) = \varphi(m) \cdot \varphi(n).$$

(iii) *Jeśli $n = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$, to*

$$n = p_1^{n_1-1}(p_1-1)p_2^{n_2-1}(p_2-1)\cdots p_k^{n_k-1}(p_k-1) =$$
$$= n(1-\tfrac{1}{p_1})(1-\tfrac{1}{p_2})\cdots(1-\tfrac{1}{p_k})$$

Wniosek

Jeżeli p i q są różnymi liczbami pierwszymi, to

$$\varphi(p \cdot q) = \varphi(p) \cdot \varphi(q) = (p-1) \cdot (q-1).$$

5. Twierdzenie Eulera i Małe Twierdzenie i Fermata

Twierdzenie Eulera

Niech $m > 1$ będzie ustaloną liczbą naturalną. Jeżeli a jest dowolną liczbą całkowitą, która jest względnie pierwsza z m), to

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Twierdzenie Eulera – druga wersja

Niech $m > 1$ będzie ustaloną liczbą naturalną. Jeżeli $a \in \mathbb{Z}_m$, to

$$\underbrace{a \odot_m a \odot_m \cdots \odot_m a}_{\varphi(m)} = 1.$$

Małe Twierdzenie Fermata

Niech p będzie ustaloną liczbą pierwszą. Jeżeli a jest dowolną liczbą całkowitą niepodzielną przez p, to

$$a^{p-1} \equiv 1 \pmod{p}.$$

Chińskie Twierdzenie o Resztach

Niech $m_1,\ m_2,\ \ldots,\ m_k$ będą ustalonymi liczbami naturalnymi większymi od 1, takimi że $NWD(m_i, m_j) = 1$ dla $i \neq j$. Niech ponadto $N = m_1 m_2 \cdots m_k$. Wówczas dla dla dowolnych liczb całkowitych $a_1,\ a_2,\ \ldots,\ a_k$ istnieje dokładnie jedna liczba całkowita x taka, że $0 \leqslant x < N$ i

$$\begin{aligned} x &\equiv a_1 \pmod{m_1}, \\ x &\equiv a_2 \pmod{m_2}, \\ &\ldots \\ x &\equiv a_k \pmod{m_k}. \end{aligned} \tag{3}$$

Ponadto, jeśli x_1, x_2 są dowolnymi liczbami spełniającymi ten układ kongruencji, to

$$x_1 \equiv x_2 \pmod{N}.$$

RSA

Podstawa systemu: para liczb naturalnych N i a.

$$N = p \cdot q$$

gdzie p, q są pierwsze.
a, jest dobrana tak, aby
$NWD(a, \varphi(N)) = NWD(a, (p-1)(q-1)) = 1$.
Kluczem publiczny: (N, a).
Tajnymi pozostają liczby pierwsze p i q, jak również wartość $\varphi(N) = (p-1)(q-1)$.
Klucz rozszyfrowujący b wyznaczamy korzystając z rozszerzonego algorytmu Euklidesa na podstawie liczb a i $\varphi(N)$, korzystając z tego, że

$$ab \equiv 1 \pmod{\varphi(N)}.$$

RSA – c.d.

Jeśli m jest jednostką informacji zamienioną na liczbę, to szyfrowanie polega na podniesieniu tej liczby do potęgi a.

$$c = m^a \pmod{N}.$$

Dysponując liczbą b, której wyznaczenie może być obliczeniowo trudne, praktycznie niewykonalne, jeśli nie jest znane $\varphi(N)$, ale przy znajomości $\varphi(N)$ – bardzo łatwe (patrz rozszerzony algorytm Euklidesa), otrzymany szyfrogram c nietrudno zamieniamy na wiadomość m:

$$c^b \equiv (m^a)^b \equiv m^{ab} \equiv m^{1+k\varphi(N)} \equiv m \cdot (m^{\varphi(N)})^k \equiv m \pmod{N}$$

Korzystaliśmy tu z faktu, iż $m^{\varphi(N)} \equiv 1 \pmod{N}$.

RSA

Liczby a i b mogą być bardzo duże, wiec zarówno szyfrowanie, jak i deszyfrowanie mogą zająć wiele czasu. By ten czas możliwie radykalnie skrócić korzystamy z algorytmu szybkiego potęgowania modularnego.
Niech $a = (a_{n-1}\, a_{n-2}\, \ldots\, a_1\, a_0)_2$ będzie zapisem klucza szyfrującego w postaci binarnej. Jeśli teraz chcemy obliczyć $m^a \pmod N$ wyliczamy najpierw ciąg

$$m_0 = m \equiv m^{2^0} \pmod N,\ m_1 \equiv m_1^2 \equiv m^2 \pmod N,\ \ldots,\ m_{n-1} \equiv m_{n-}^2$$

a następnie wymnażamy liczby m_i dla, których $a_i \neq 0$. Mamy bowiem

$$m^a = m^{a_0 + a_1 \cdot 2 + a_2 \cdot 2^2 + \cdots + a_{n-1} \cdot 2^{n-1}} = m^{a_0} m_1^{a_1} m_2^{a_2} \cdots m_{n-1}^{a_{n-1}} \pmod N.$$

Autorzy systemu

Ronald Rivest, Adi Shamir, Leonard Adlemann

Definicja

Jednostka tekstu jawnego (blok tekstu podlegający) szyfrowaniu: ciąg bitów ustalonej długości m traktowany jako liczba $< 2^m$
Jednostka szyfrogramu: ciąg bitów ustalonej długości $k > m$ traktowany jako liczba $< 2^k$
Parametry systemu:
Tajne: różne liczby pierwsze p i q, takie, że $2^m < N = p \cdot q < 2^k$ liczba naturalna d taka, że $NWD(d, \varphi(N)) = 1$
Jawne: para (N, e), gdzie $e \cdot d = 1 \pmod{\varphi(N)}$
Szyfrowanie: $x \to x^e \pmod{N} = y$
Deszyfrowanie:pause
$y \to y^d \pmod{N} = (x^e)^d = x^{ed} = x^{1+u\varphi N} = x \cdot \left(x^{\varphi(N)}\right)^u = x$

Bolek buduje system

(1) Bolek generuje dwie liczby pierwsze

(2) Bolek oblicza $N = p \cdot q$ i $\varphi(N) = (p-1)(q-1)$

(3) Bolek wybiera losowo liczbę e $(1 < e < \varphi(n))$, taki że $NWD(e, \varphi(N)) = 1$.

(4) Za pomocą rozszerzonego algorytmu Euklidesa Bolek oblicza $d = e^{-1} \pmod{\varphi(N)}$

(5) Bolek publikuje w informatorze swój klucz publiczny (N, e)

Algorytm szybkiego potęgowania

Niech $e = (e_{n-1}\, e_{n-2}\, \ldots\, e_1\, e_0)_2$ $e_{n-1} = 1 < \varphi(N)$. Liczbę x podnosimy do potęgi e modulo N

(1) $y \leftarrow x^{e_{n-1}}$, $i \leftarrow n-2$;

(2) $y \leftarrow y^2 \pmod N$;

(3) Jeżeli $e_i = 1$, podstaw $y \leftarrow y \cdot x$;

(4) $i \leftarrow i-1$, jeżeli $i \geqslant 0$ idź do (2);

(5) Zwróć p.

Gardner

W 1977 roku Martin Gardner opublikował w Scientific American artykuł zatytułowany *'Nowy rodzaj szyfru'*, którego złamanie trwałoby miliony lat. W artykule zamieścił zaszyfrowany tekst z użyciem RSA. Podał klucz jawny $N = pq$, gdzie

$p =$ 32 769 132 993 266 709 549 961 988 190 834 461
413 177 642 967 992 942 539 798 288 533

$q =$ 3 490 529 510 847 650 949 147 849 619 903 898
133 417 764 638 493 387 843 990 820 577

Rozkład liczby N na czynniki p i q został odkryty po 17 latach od daty opublikowania.

$N =$
114 381 625 757 888 867 669 235 779 976 146 612 010 218 296 721 242
362 562 561 842 935 706 935 245 733 897 830 597 123 563 958 705 058
989 075 147 599 290 026 879 543 541