Matematyka dyskretna

Wykład 6: Ciała skończone i kongruencje

Gniewomir Sarbicki

15 maja 2023

Relacja przystawania

Definicja:

Mówimy, że liczby $a, b \in \mathbb{Z}$ przystają modulo m (co oznaczamy jako $a = b \pmod{m}$), jeżeli

$$m|(a-b)$$

Fakt:

Przystawanie zachowuje działania dodawania, odejmowania i mnożenia. Jeżeli $a = b \pmod{m}$ oraz $c = d \pmod{m}$, to

- $a + c = b + d \pmod{m}$
- $a - c = b - d \pmod{m}$
- $a \cdot c = b \cdot d \pmod{m}$

Zachowywanie działań

- dodawanie:

$$m|(a-b) \wedge m|(c-d) \implies a-b = k \cdot m \wedge c-d = l \cdot m$$
$$(a+c)-(b+d) = (k+l) \cdot m$$

- mnożenie:

$$m|(a-b) \wedge m|(c-d) \implies a-b = k \cdot m \wedge c-d = l \cdot m$$
$$ac - bd = ac - ad + ad - bd = a(c-d) + d(a-b)$$
$$= a \cdot l \cdot m + d \cdot k \cdot m = (a \cdot l + d \cdot k)m$$

- odejmowanie - ćwiczenie

Działania w zbiorze $\mathbb{Z}_m$

Wynik działania w zbiorze $\mathbb{Z}_m$ określamy jako klasę abstrakcji wyniku działania na reprezentantach argumentów działania.

Definiujemy działania na klasach abstrakcji $[a], [b] \in \mathbb{Z}_m$:

$$[a] +_m [b] = [a + b]$$
$$[a] -_m [b] = [a - b]$$
$$[a] \cdot_m [b] = [a \cdot b]$$

Działania w zbiorze $\mathbb{Z}_m$

Zbiór reszt jest zatem wyposażony w działania dodawania, odejmowania oraz mnożenia:

- dodawanie jest łączne i przemienne
- element $[0]$ jest elementem neutralnym dodawania oraz dla każdego elementu istnieje element przeciwny
- mnożenie jest łączne i przemienne
- $[1]$ jest elementem neutralnym mnożenia
- dodawanie jest rozdzielne względem mnożenia

Definicja:

Zbiór z tak określonymi działaniami jest **pierścieniem** (przemiennym z jedynką).

Tabelki działań w pierścieniach $\mathbb{Z}_4$ i $\mathbb{Z}_5$

$\mathbb{Z}_4$:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\times$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$\mathbb{Z}_5$:

$+$	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

$\times$	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

Dzielenie w $\mathbb{Z}_m$

Element $[a] \in \mathbb{Z}_m$ nazywamy odwracalnym, jeżeli istnieje element $[b] \in \mathbb{Z}_m$ do niego odwrotny, tj. taki, że $a \cdot b \pmod m = 1$.

Fakt: Element $[a]$ jest odwracalny $\iff$ $NWD(a, m) = 1$.

Dowód: Jeżeli $NWD(a, m) = 1$, to $xa + ym = 1$, zatem $xa - 1 = y \cdot m$
Z drugiej strony, jeżeli $[a] \cdot [b] = 1$, to $ab - 1 = k \cdot m \implies ab + (-k) \cdot m = 1$, zatem 1 jest wielokrotnością $NWD(a, m)$, więc $NWD(a, m) = 1$.

Wniosek: Elementu odwrotnego można szukać rozszerzonym algorytmem Euklidesa $xa + bm = 1 \implies [a]^{-1} = [x]$

Wniosek: W zbiorze $\mathbb{Z}_m$ określone jest dzielenie $\iff$ wszystkie jego niezerowe elementy są odwracalne $\iff$ m jest liczbą pierwszą.

Pierścień z dzieleniem nazywamy **ciałem**.

Ilość elementów odwracalnych

Fakt:

Funkcja Eulera $\phi(m)$ przypisuje liczbie m ilość elementów odwracalnych w $\mathbb{Z}_m$.

Przypomnienie:

- Jeżeli p jest liczbą pierwszą, to $\phi(p^\alpha) = p^{\alpha-1}(p-1)$. W szczególności $\phi(p) = p-1$ (wszystkie niezerowe elementy ciała $\mathbb{Z}_p$ są odwracalne).
- Jeżeli n, m są względnie pierwsze, to $\phi(n \cdot m) = \phi(n) \cdot \phi(m)$.

Ćwiczenie: Wyznaczyć ilość elementów odwracalnych w pierścieniach $\mathbb{Z}_4$, $\mathbb{Z}_{32}$, $\mathbb{Z}_{30}$, $\mathbb{Z}_{36}$

Małe twierdzenie Fermata

Twierdzenie Fermata:

Jeżeli p jest liczbą pierwszą, i $\sim p|a$, to:

$$a^{p-1} = 1 \ (\mathrm{mod}\ p)$$

Uogólnienie na liczby naturalne:

Twierdzenie Eulera

$$NWD(n,a) = 1 \implies a^{\phi(n)} = 1 \ (\mathrm{mod}\ n)$$

Dowód: Niech $\{r_1, \ldots, r_{\phi(n)}\}$ - liczby z przedziału $[1, n)$ względnie pierwsze z n. Liczby $a \cdot r_i (\mathrm{mod}\ n)$ są dalej względnie pierwsze z n, ponieważ są to liczby parami różne, są to te same liczby z dokładnością do permutacji:

$$a^{\phi(n)} r_1 \cdot \cdots \cdot r_{\phi(n)} = r_1 \cdot \cdots \cdot r_{\phi(n)} (\mathrm{mod}\ n)$$

$$a^{\phi(n)} = 1 (\mathrm{mod}\ n) \square$$

Pozwala to znajdować odwrotność dowolnego elementu odwracalnego $a \in \mathbb{Z}_n$:

$$a^{-1} = a^{\phi(n)-1} \ (\mathrm{mod}\ n)$$

Twierdzenie to będzie w dalszej części wykładu podstawą funkcji szyfrującej w szyfrowaniu RSA.

Pierścień wielomianów

Definicja:

Niech A będzie pewnym pierścieniem.

- **Wielomianem** nad A nazywamy wyrażenie formalne $f = \sum_{i=0}^{n} a_i x^i$, gdzie $a_i \in A, a_n \neq 0$. a_n nazywamy **najwyższym współczynnikiem**
- Liczbę n nazywamy **stopniem wielomianu** f i oznaczamy jako $\deg(f)$.
- Zbiór wielomianów nad A oznaczamy jako $A[X]$.

Fakt:

1. $A[X]$ ma dzielniki zera, wtw gdy A ma dzielniki zera.
2. $\deg(f+g) \leqslant \max(\deg f, \deg g)$,
3. $\deg(fg) \leqslant \deg f + \deg g$, równość wtw, gdy nie ma dzielników zera w A.

Rozkładalność wielomianów

Od tej chwili ograniczamy się do pierścieni wielomianów nad pewnym ciałem K.

Definicja:

- Mówimy, że wielomian g **dzieli** wielomian f, jeżeli $f = gh$ dla pewnego wielomianu h.
- Wielomian f jest **nierozkładalny**, jeżeli nie istnieje żaden rozkład $f = gh$, gdzie $\deg h > 0$ (element pierwszy pierścienia $K[X]$).
- Wielomiany f i g są **stowarzyszone**, jeżeli różnią się o skalar.
- Wielomian nazywamy **unormowanym**, jeżeli najwyższy współczynnik jest równy 1.

Rozkładalność wielomianów

Fakt:

1. Każdy wielomian można przedstawić jako iloczyn wielomianów nierozkładalnych. Rozkład jest jednoznaczny z dokładnością do kolejności czynników i stowarzyszenia.
2. Każdy wielomian unormowany można przedstawić jako iloczyn unormowanych wielomianów nierozkładalnych. Rozkład jest jednoznaczny z dokładnością do kolejności czynników.

Twierdzenie (Dzielenie wielomianów z resztą):

Niech $f, g \in K[X], g \neq 0$. Istnieją wówczas jednoznacznie wyznaczone wielomiany q, r takie że $f = qg + r$ i $\deg r < \deg g$. Wielomian r nazywamy *resztą z dzielenia f przez g* i oznaczamy jako $f \mod g$.

Największy wspólny dzielnik

Definicja:

Wielomian najwyższego stopnia spośród wielomianów unormowanych dzielących jednocześnie wielomiany f i g nazywamy ich **największym wspólnym dzielnikiem** i oznaczamy jako $NWD(f, g)$.

Definicja:

Wielomiany f, g nazywamy względnie pierwszymi, jeżeli $NWD(f, g) = 1$.

Największy wspólny dzielnik wielomianów f i g wyznaczamy za pomocą algorytmu Euklidesa.

Relacja przystawania

Definicja:

Mówimy, że dwa elementy $a, b \in K[X]$ przystają do siebie modulo f, jeżeli $f|(a-b)$.

Fakt:

Relacja przystawania jest relacją równoważności, zachowującą działania dodawania, mnożenia, odejmowania.

Dowód: Analogiczny jak dla relacji przystawania liczb modulo n.

Definicja:

Zbiór klas abstrakcji powyższej relacji oznaczamy jako $K[X]/f$ i nazywamy **pierścieniem reszt modulo** f.

Pierścienie reszt

Twierdzenie:

$K[X]/f \cong \{g \in K[X] : \ \deg g < \deg f\}$

Dowód: Ćwiczenie

O elementach pierścienia decyduje tylko stopień wielomianu f, natomiast jego postać decyduje o tabelce działań.

Twierdzenie:

Pierścień $K[X]/f$ jest ciałem wtw gdy f jest wielomianem nierozkładalnym w $K[X]$.

Dowód: Nierozkładalność zapewnia brak dzielników zera, a rozszerzony algorytm Euklidesa istnienie elementu odwrotnego.

Przykład: Pierścień $\mathbb{R}[X]/(X^2+1)$ jest ciałem.

Przykład pierścienia reszt

Wielomian $X^2 + 1 \in \mathbb{R}[X]$ jest nierozkładalny, zatem pierścień $\mathbb{R}[X]/(X^2 + 1)$ jest ciałem. Jego elementami są wielomiany stopnia $\leqslant 1$ nad R.

Pomnóżmy przez siebie dwa takie wielomiany $a_1x + b_1$ i $a_2x + b_2$. Otrzymamy wielomian:

$$\begin{aligned} & a_1a_2x^2 + (a_1b_2 + a_2b_1)x + b_1b_2 \\ = a_1a_2(x^2 + 1) & + (a_1b_2 + a_2b_1)x + (b_1b_2 - a_1a_2) \\ & \sim (a_1b_2 + a_2b_1)x + (b_1b_2 - a_1a_2) \end{aligned}$$

Co to za ciało?

Przyporządkowanie $ax + b = ai + b$ ustala *izomorfizm* między $\mathbb{R}[X]/(X^2 + 1)$ a $\mathbb{C}$ (taka sama definicja mnożenia).

Izomorfizm pierścieni

Definicja:

Izomorfizmem pierścieni A i B nazywamy bijekcję $\Phi : A \to B$ (odwzorowanie 1-1), która zachowuje strukturę pierścienia:

- $\Phi(a-b) = \Phi(a) - \Phi(b)$
  $(\implies \Phi(0_A) = 0_B, \quad \Phi(-A) = -\Phi(A))$
- $\Phi(a \cdot b^{-1}) = \Phi(a) \cdot \Phi(b)^{-1}$ $(\implies \Phi(1_A) = 1_B,$
  $\Phi(A^{-1}) = \Phi(A)^{-1}$ dla elementu odwracalnego)

Ćwiczenie: Pokazać, że $\Phi : \mathbb{R}[X]/(X^2+1) \to \mathbb{C}$ jest izomorfizmem pierścieni.

Definicja:

Niech 1 - element neutralny mnożenia w pierścieniu R.
Najmniejszą liczbę elementów sumy: $1 + \cdots + 1 = 0$ nazywamy **charakterystyką pierścienia** R i oznaczamy jako $\mathrm{char}(R)$.
Jeżeli nie istnieje tak suma, to przyjmujemy $\mathrm{char}(R) = 0$.

Przykłady:

- $\mathrm{char}(\mathbb{C}) = \mathrm{char}(\mathbb{R}) = \mathrm{char}(\mathbb{Q}) = \mathrm{char}(\mathbb{Z}) = 0$
- $\mathrm{char}(\mathbb{Z}_n) = n$
- $\mathrm{char}(R[X]) = \mathrm{char}(R)$

Twierdzenie:

- Jeżeli F jest ciałem skończonym to $\mathrm{char}(F) = p \in \mathcal{P}$ i $\#F = p^n$ dla pewnego $n \in \mathbb{N}$. Dla $n = 1$ $F = \mathbb{Z}_p$.
- Odwrotnie, $\forall p \in \mathcal{P}, n \in \mathbb{N}$ istnieje wielomian nierozkładalny stopnia n w $\mathbb{Z}_p \implies$ istnieje ciało o liczbie elementów p^n. Jest ono jedyne z dokładnością do izomorfizmu, oznaczamy je jako $\mathbb{F}_{p^n}$. W szczególności $\mathbb{F}_p = \mathbb{Z}_p$.

Przykład: Wszystkie wielomiany stopnia 2 nad $\mathbb{Z}_2$:
$x^2, x^2+1, x^2+x, x^2+x+1$. Tylko ostatni jest nierozkładalny.

Mnożenie dwóch wielomianów a_1x+b_1,a_2x+b_2 modulo x^2+x+1:

$$\begin{aligned} & a_1a_2x^2+(a_1b_2+a_2b_1)x+b_1b_2 \\ =\ & a_1a_2(x+1)+(a_1b_2+a_2b_1)x+b_1b_2 \\ =\ & (a_1b_2+a_2b_1+a_1a_2)x+(b_1b_2+a_1a_2) \end{aligned}$$

Tabelki działań w ciele $\mathbb{F}_4$:

$+$	00	01	10	11
00	00	01	10	11
01	01	00	11	10
10	10	11	00	01
11	11	10	01	00

$\times$	00	01	10	11
00	00	00	00	00
01	00	01	10	11
10	00	10	11	01
11	00	11	01	10

Kongruencje liniowe jednej zmiennej

Twierdzenie: Kongruencja liniowa $ax + b = 0 \pmod{n}$ ma rozwiązanie wtw, gdy $NWD(a, n)|b$.

Dowód: Szukamy rozwiązania w liczbach całkowitych równania:

$$-ax + ny = b$$

Wiemy, że równanie takie ma rozwiązanie wtw, gdy $NWD(a, n)|b$
□

Twierdzenie: Jeżeli $NWD(a, n)|b$ oraz $d = NWD(a, n) > 1$, to równania: $ax = b \pmod{n}$ oraz $\frac{a}{d}x = \frac{b}{d} \pmod{\frac{n}{d}}$ mają ten sam zbiór rozwiązań w $\mathbb{Z}$.

Twierdzenie: Jeżeli $NWD(a, n) = d$ i $d|b$ to równanie $ax = b \pmod{n}$ ma dokładnie d rozwiązań w $\mathbb{Z}_n$.

Chińskie twierdzenie o resztach

Twierdzenie:

Jeżeli liczby $n_1, \ldots, n_r$ są względnie pierwsze, to dla dowolnych liczb całkowitych $b_1, \ldots, b_r$ układ kongruencji liniowych:

$$x = b_i \ (\mathrm{mod}\ n_i), \quad i = 1, \ldots, r$$

posiada rozwiązanie. Jeżeli x_1 i x_2 są rozwiązaniami tego układu, to $x_1 = x_2 \ (\mathrm{mod}\ n_1 \cdot \cdots \cdot n_r)$.

Dowód: Indukcja względem r:
(P) Przypadek $r = 1$ jest oczywisty, zajmijmy się przypadkiem $r = 2$:

$$x = b_1 \ (\mathrm{mod}\ n_1) \qquad x = b_2 \ (\mathrm{mod}\ n_2)$$

Rozwiązaniem pierwszego równania jest $x = yn_1 + b_1, y \in \mathbb{Z}$.

Chińskie twierdzenie o resztach

Wstawiamy je do drugiego równania:

$$yn_1 + b_1 - b_2 = 0 \ (\mathrm{mod}\ n_2)$$

Kongruencja ta ma rozwiązania, ponieważ z założenia $NWD(n_1, n_2) = 1$. Jej rozwiązania wstawiamy do rozwiązania na x.

Dla dwóch rozwiązań układu mamy $n_1|x_1 - x_2$ oraz $n_2|x_1 - x_2$, zatem ponieważ $NWD(n_1, n_2) = 1$, to $n_1 n_2|x_1 - x_2$

(I) Załóżmy, że teza jest słuszna dla układu k kongruencji. Oznacza to, że układ ten można zapisać przy pomocy jednej kongruencji:

$$x = b \ (\mathrm{mod}\ n_1 \cdot \dots \cdot n_k)$$

Rozwiązujemy zatem układ dwóch kongruencji - powyższej i dla $k+1$. Układ ten posiada rozwiązania na mocy rozważań z punktu (P). Podobnie, dostaniemy że $x_1 = x_2 \ (\mathrm{mod}\ (n_1 \cdot \dots \cdot n_k) \cdot n_{k+1})$ $\square$

Chińskie twierdzenie o resztach

Przykład: Jaka jest reszta z dzielenia liczby $M = 1\ 997\ 199\ 919$ przez 15

Odpowiedź: $M = 4 \pmod 5$ oraz $M = 1 \pmod 3$, zatem $M = 4 \pmod{15}$.

Kongruencje wielomianowe jednej zmiennej

Definicja:

Element a nazywamy **pierwiastkiem wielomianu** f
$\iff (X-a)|f$

Twierdzenie: (Lagrange'a)

Jeżeli p jest liczbą pierwszą, to wielomian $a_n x^n + \cdots + a_0$ (gdzie $a_n \neq 0 \pmod p$) ma najwyżej n pierwiastków w $\mathbb{Z}_p$.
(jeżeli przynajmniej jeden ze współczynników wielomianu nie jest podzielny przez p)

Dowód: Wynika z braku dzielników zera w $\mathbb{Z}_p$.

Uwaga: Jeżeli wszystkie współczynniki wielomianu są podzielne przez p, to rozwiązaniem kongruencji jest dowolna liczba całkowita.
Dowód - proste ćwiczenie.

Kongruencje wielomianowe jednej zmiennej

Twierdzenie (o podnoszeniu):

Niech p jest liczbą pierwszą. Niech x_0 będzie rozwiązaniem kongruencji $F(x) = 0 \pmod{p^k}$. Definiujemy zbiór T:

$$T = \{t\},\ F'(x_0)t = -\frac{F(x_0)}{p^k} (\bmod p) \quad \text{gdy } p \nmid F'(x_0)$$
$$T = \emptyset \quad \text{gdy } p | F'(x_0) \ \wedge\ p^{k+1} \nmid F(x_0)$$
$$T = \{0, \ldots, p-1\} \quad \text{gdy } p | F'(x_0) \ \wedge\ p^{k+1} | F(x_0)$$

Rozwiązaniami kongruencji $F(x) = 0 (\bmod p^{k+1})$ redukującymi się do x_0 ($x = x_0 \pmod{p^k}$) są $x_0 + p^k t$, dla $t \in T$.

Wniosek: Jeżeli kongruencje $F(x) = 0 \pmod{p}$ oraz $F'(x) = 0 \pmod{p}$ nie mają wspólnych rozwiązań, to liczba rozwiązań kongruencji pierwszej z nich jest równa liczbie rozwiązań kongruencji $F(x) = 0 \pmod{p^k}$ dla dowolnego k.

Kongruencje wielomianowe jednej zmiennej

Wniosek: Jeżeli p jest liczbą pierwszą nie dzielącą an, to dla każdego naturalnego k kongruencje:

$$x^n = a \ (\mathrm{mod}\ p) \qquad \text{i} \qquad x^n = a \ (\mathrm{mod}\ p^k)$$

mają tyle samo rozwiązań.

Fakt: Jeżeli m ma rozkład $m = m_1^{\alpha_1} \cdot \dots \cdot m_r^{\alpha^n}$, to pierwiastki wielomianu F modulo m znajdujemy znajdując najpierw pierwiastki modulo potęgi czynników pierwszych, a następnie stosując chińskie twierdzenie o resztach.

Przykład: Rozwiążmy kongruencję $x^2 - 3x + 2 = 0 \ (\mathrm{mod}\ 6)$.

$$6|(x-1)(x-2) \quad \Longrightarrow \quad 2|(x-1)(x-2) \ \wedge \ 3|(x-1)(x-2)$$

Pierwsze równanie daje $x = 0 \ \vee \ x = 1 \ (\mathrm{mod}\ 2)$. Drugie daje $x = 1 \ \vee \ x = 2 \ (\mathrm{mod}\ 3)$. Rozwiązaniami w $\mathbb{Z}_6$ są: $1, 2, 4, 5$

Kongruencje wielomianowe jednej zmiennej

Ćwiczenie: Ile najwięcej rozwiązań może mieć wielomian $x^4 - 3x^3 + 4x^2 + 2x - 3 = 0$ w $\mathbb{Z}_{35}$?

Odpowiedź: W $\mathbb{Z}_5$ i w $\mathbb{Z}_7$ są maksymalnie 4 rozwiązania, zatem w $\mathbb{Z}_{35}$ będzie ich maksymalnie 16.

Ćwiczenie: Ile najwięcej rozwiązań może mieć wielomian $x^2 + 2x - 3$ w $\mathbb{Z}_{18}$?

Odpowiedź: W $\mathbb{Z}_3$ pierwiastkami wielomianu są $0, 1$, a pierwiastkiem pochodnej jest 2. Zatem w $\mathbb{Z}_9$ wielomian będzie miał również dwa rozwiązania. W $\mathbb{Z}_2$ wielomian może mieć najwyżej dwa rozwiązania, zatem w $\mathbb{Z}_{18}$ będzie ich najwyżej 4.

Literatura

- Władysław Narkiewicz *Teoria Liczb* PWN 2003
- Jerzy Rutkowski *Algebra abstrakcyjna w zadaniach* PWN 2006