Лекция 13 22.12.21г.

Сравнения в мн. $\mathbb{Z}$

Нека a и b са две цели числа и n е фиксирано.

Деф. Казваме, че a и b са сравними по модул n и означаваме

$a \equiv b \pmod{n}$, ако

n дели $a-b$, т.е. $n \mid (a-b) \Leftrightarrow$

a и b дават един и същ остатък при деление на n, т.е. $a = nq_1 + r$, $b = nq_2 + r$, $0 \leq r < n$;

Свва: 1) $a \equiv a \pmod{n}$

2) $a \equiv b \pmod{n} \leftrightarrow b \equiv a \pmod{n}$

3) $a \equiv b \pmod{n}$ и $b \equiv c \pmod{n} \Rightarrow$
$a \equiv c \pmod{n}$

4) $a \equiv b \pmod{n}$ и $c \equiv d \pmod{n}$

а) $a+c \equiv b+d \pmod n$

б) $a-c \equiv b-d \pmod n$

в) $ac \equiv bd \pmod n$

г) $k \in \mathbb{N}$, $a^k \equiv b^k \pmod n$

5) Ако $k \in \mathbb{N}$ и $ka \equiv kb \pmod n$

$\Rightarrow a \equiv b \left(\mod \frac{n}{(n,k)}\right)$

В частност, ако $(n,k)=1 \Rightarrow a \equiv b \pmod n$

Релацията $\equiv$ по модул n е релация на еквивалентност ($1^{\text{ви}}$ з.) $\Rightarrow \mathbb{Z}$ се разбива на непресичащи се класове остатъци по модул n, т.е.

$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \dots, \overline{n-1}\}$

$\bar{a}$ – клас остатък по модул n

a – представител на този клас

$\mathbb{Z}_8 = \{\bar{0}, \bar{1}, \dots, \bar{7}\} = \{-\bar{3}, -\bar{2}, -\bar{1}, \bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

функция на Ойлер:

$n \in \mathbb{N}$, аритметична функция на Ойлер означаваме $\varphi(n) :=$ броя на всички естествени $\leq n$ и взаимно прости с n, като $\varphi(1) := 1$.

$\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$

$\varphi(5) = 4$, —, $\varphi(p) = p - 1$

p просто число, $k \in \mathbb{N}$

$$\varphi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$$

Т: функцията на Ойлер $\varphi(n)$ е мултипликативна функция, т.е. ако $(a, b) = 1 \Rightarrow \varphi(ab) = \varphi(a).\varphi(b)$.

$\forall\, n \in \mathbb{N}$, $n = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$, $k_i > 0$ как. разлагане на n

$$\varphi(n) = \varphi(p_1^{k_1} \cdots p_s^{k_s}) = \varphi(p_1^{k_1}) \cdots \varphi(p_s^{k_s}) =$$

$$= p_1^{k_1}\left(1 - \frac{1}{p_1}\right) p_2^{k_2}\left(1 - \frac{1}{p_2}\right) \cdots p_s^{k_s}\left(1 - \frac{1}{p_s}\right) \Rightarrow$$

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_s}\right)$$

Th (Ойлер-Ферма) Нека $a \in \mathbb{Z}$, $n \in \mathbb{N}$ и $(a,n)=1$, то $a^{\varphi(n)} \equiv 1 \pmod n$.

В частност, ако $n=p$ (просто число)

$$a^{p-1} \equiv 1 \pmod p \iff$$
$$a^p \equiv a \pmod p \quad (\text{Th Ферма})$$

Th (Уилсон): Ако p – просто число, то $(p-1)! \equiv -1 \pmod p$.

□

Полиноми на една променлива

Да напомним, че:

<u>Комутативен пръстен с 1</u> ($\mathbb{Z}$ пример)

A, $a+b$, ab, т.е. $\forall a,b \in A \Rightarrow \begin{array}{l} c=a+b\in A \\ d=ab\in A \end{array}$

като са изпълнени следните аксиоми:

1) $(A,+)$ е абелева група, т.е

а) асоц. з-н "+" $a+(b+c)=(a+b)+c$

б) $\exists\, 0\in A$: $a+0=0+a=a$, $\forall a\in A$
нула

в) $\forall a\in A, \exists\, (-a)\in A$: $a+(-a)=(-a)+a=0$
противоположен на a

г) комут. з-н "+" : $a+b=b+a$

2) $(A,\cdot)$ е полугрупа, т.е изпълнен е само асоциативен закон на "$\cdot$":
$\forall a,b,c\in A$: $(ab)c=a(bc)$

3) дистрибутивни закони в A:

$(a+b)c=ac+bc$, $\forall a,b,c\in A$

$a(b+c)=ab+ac$ (A-пръстен)

4) $\exists 1 \in A$: $a1 = 1a = a$ $\forall a \in A$
единица A – ир. с 1 $(1 \div 4)$

5) $\forall a,b \in A$: $ab = ba$, т.е. комут. закон на "." A – ком. ир. $(1 \div 3, 5)$

$1 \div 5 \Rightarrow$ <u>A е комут. ир. с 1.</u>

Пр: 1) $\mathbb{Z}$; 2) $\mathbb{Z}_n = \{\overline{0}, \overline{1}, \sim, \overline{n-1}\}$
$a+b$
ab
$\overline{a}+\overline{b} := \overline{a+b}$
$\overline{a}.\overline{b} := \overline{ab}$

комут. ир. с 1 е $\mathbb{Z}_n$

$\mathbb{Z}_8 = \{\overline{0}, \overline{1}, \sim, \overline{7}\}$ $\quad \overline{5}+\overline{6} = \overline{3}$
$\overline{5}.\overline{6} = \overline{6}$

<u>Деф.</u> Казваме, че $a,b \in A$ (ком. ир. с 1) са (нетривиални) делители на нулата, ако $a \neq 0$, $b \neq 0$, но $ab = 0$.

Деф Казваме че един комутативен пръстен с 1 A е област (на цялост), ако в A няма нетривиални делители на нулата.

Пример: 1) Целите числа $\mathbb{Z}$ – област

2) $\mathbb{Z}_p$, p просто число, $\mathbb{Z}_p$ – поле, и област

3) $\mathbb{Z}_n$, n-не е просто, в $\mathbb{Z}_n$ има нетривиални делители на нулата, т.е. $\mathbb{Z}_n$ не е област
n-съставно.

$\mathbb{Z}_8 = \{\bar{0}, \bar{1}, \sim, \bar{7}\}$ $\quad \bar{2} \neq \bar{0}, \bar{4} \neq \bar{0}$
$\bar{2}.\bar{4} = \bar{0}$

$\bar{2}, \bar{4}, \bar{6}$ – делители на нулата

Зад: $\mathbb{Z}_n$: $(n, a) = 1 \iff \bar{a}$ – обратим елемент

$(n, a) > 1 \iff \bar{a}$ – делител на нулата

Ако A е комут. пр. с 1 и е изпълнена аксиома

б) $\forall a \neq 0, a \in A$, $\exists a^{-1} \in A : aa^{-1} = a^{-1}a = 1$

обратен на a

, то тогава A е поле

$\mathbb{Z}$ - комут. пр. с 1; $\mathbb{Z}_p$ (p просто) поле

$\mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$, $\mathbb{Z}_p$ - полета.

Деф. Нека A - комут. пръст. с 1. I е непразно подмн. на A. Казваме I е идеал на A и означаваме $I \trianglelefteq A$, ако са изпълнени следните две условия:

1) $\forall a, b \in I \Rightarrow a - b \in I$
$a + (-b) \in I$ и $I \leq (A, +)$ подгрупа на адитивната гр. на A

2) $\forall a \in I, \forall r \in A \Rightarrow ar = ra \in I$
$\Rightarrow I \trianglelefteq A$.

Деф Главен идеал, породен от
елт $b \in A$ (к.ир. с 1) наричаме
$$\langle b \rangle = (b) = \{ br = rb \mid r \in A \} \trianglelefteq A$$

Тв. В комут. ир. с 1 ка целите числа
$\mathbb{Z}$ всеки идеал е главен, те
идеалите са: $\langle n \rangle$, n-фикс. ест число
$\langle n \rangle \trianglelefteq \mathbb{Z}$; $\langle 0 \rangle \trianglelefteq \mathbb{Z}$

Деф: $I, J \trianglelefteq A \Rightarrow$
$$I + J := \{ r = a + b \mid \begin{matrix} a \in I \\ b \in J \end{matrix} \} \trianglelefteq A$$
$$I \cap J := \{ x \in I, x \in J \} \trianglelefteq A$$
$$IJ := \{ x = a_1 b_1 + a_2 b_2 + \dots + a_k b_k \mid \begin{matrix} a_i \in I \\ b_i \in J \\ k \in \mathbb{N} \end{matrix} \}$$
$\trianglelefteq A$

Тв: $\mathbb{Z}$, $\langle n \rangle \trianglelefteq \mathbb{Z}$, $\langle m \rangle \trianglelefteq \mathbb{Z}$, $n, m \in \mathbb{N}$, фикс.
$$\langle n \rangle + \langle m \rangle = \langle (n, m) \rangle = ((n, m)) \trianglelefteq \mathbb{Z}$$
$$\langle n \rangle \cap \langle m \rangle = \langle [n, m] \rangle$$
$$\langle n \rangle \langle m \rangle = \langle nm \rangle$$

Нека F е поле и $1 \in F$, $0 \in F$, $0 \neq 1$

Деф а) Казваме, че F има характеристика 0, ако $1+1+\dots+1 \neq 0 \Leftrightarrow k1 \neq 0$ $\forall k \in \mathbb{N}$

и означаваме $\operatorname{char} F = 0$.

Полета $\mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C} \Rightarrow$ $\operatorname{char}\mathbb{Q} = 0$

$\operatorname{char}\mathbb{R} = 0$, $\operatorname{char}\mathbb{C} = 0$, $\operatorname{char}\mathbb{Q}(\sqrt{7}) = 0$

б) Казваме, че полето F има характеристика p, ако p е най-малкото естествено число, за което $\underbrace{1+1+\dots+1}_{p} = p1 = 0$ и означаваме $\operatorname{char} F = p$.

Доказва се, че p е винаги просто число.

и Полета $\mathbb{Z}_p = \{\bar{0}, \dots, \overline{p-1}\}$ са с характеристика p, т.е. $\operatorname{char}\mathbb{Z}_p = p$

Тв:

Пусть $a \in F$, $n \in \mathbb{N}$ и $an = 0$

$\Rightarrow$ а) $\mathrm{char} F = 0$ $\quad na = 0 \Rightarrow$ $a = 0 \in F$ (или $n = 0$)

$\Rightarrow$ б) $\mathrm{char} F = p$ $\quad na = 0 \Rightarrow$ $a = 0 \in F$ (или $p \mid n$) ↯

Полиноми над произвольна

Нека A - комут. ир с 1 (област) F поле

Да означим с

$B = \{ f = (a_0, a_1, \dots, a_n, 0, 0, \dots) \mid a_i \in A \}$

множеството на безкрайните редици с елементи от A, в които имат краен брой ненулеви елементи.

Нека $g = (b_0, b_1, \dots, b_m, 0, \dots, 0)$

и б.о.о. $m \leq n$

Дефинираме операциите "+" и "·" в B:

$$f + g := (a_0 + b_0, a_1 + b_1, \dots, a_m + b_m, a_{m+1}, \dots, a_n, 0, \dots) \in B$$

$fg := (c_0, c_1, \dots, c_k, 0, \dots) \in B$, където

$$c_s = \sum_{i+j=s} a_i b_j$$

$= (a_0 b_0, a_0 b_1 + a_1 b_0, a_0 b_2 + a_1 b_1 + a_2 b_0, \dots)$

$(B, f+g, fg)$ - комутативен ир с 1

A - област / F поле $\Rightarrow$ B - област

B – комутативна асоц. 1 / асоц. комут. област

$0 = (0, 0, \sim 0)$ нула в B

$1 = (1, 0, \sim 0)$ единица

$f = (a_0, a_1, \sim, a_n, 0, \sim)$

$(-f) = (-a_0, -a_1, \sim -a_n, 0, \sim)$

Еднакви f и g в B по дефиниция когато $a_n = b_n$ за $n = \overline{0, \infty}$

$f = g \Leftrightarrow a_0 = b_0, a_1 = b_1, \sim, a_n = b_n$ в A

Проверка на асоц. закон за умн.: $\forall f, g, h \in B$: $(fg)h = f(gh)$

Доказ:

$f = (a_0, a_1, \sim, a_n, 0, \sim)$ $\quad fg = (c_0, c_1, \sim, c_k, 0, \sim)$

$g = (b_0, b_1, \sim, b_m, 0, \sim)$ $\quad gh = (v_0, v_1, \sim, v_s, 0, \sim)$

$h = (d_0, d_1, \sim, d_e, 0, \sim)$

$c_k = \sum_{i+j=k} a_i b_j$

$(fg)h = (u_0, u_1, \sim, u_t, 0, \sim)$

$v_s = \sum_{j+t=s} b_j d_t$

$f(gh) = (y_0, y_1, \sim, y_z, 0, \sim)$

$$u_\tau = \sum_{k+b=\tau} c_k d_b = \sum_{k+b=\tau} \left(\sum_{i+j=k} a_i b_j \right) d_b = \overline{\overline{A}}$$

$$y_\tau = \sum_{i+s=\tau} a_i v_s = \sum_{i+s=\tau} a_i \left(\sum_{j+b=s} b_j d_b \right) = \overline{\overline{A}}$$

$$\Rightarrow$$

$$u_\tau = \sum_{i+j+b=\tau} a_i b_j d_b = y_\tau \Rightarrow f(gh) = (fg)h$$

$$\Rightarrow$$

$a = (a, 0, \dots, 0) \in B \Leftrightarrow a \in A \subseteq B$

a — комплексное число в пр. B

Да кажем $x := (0, 1, 0 \dots) \in B$

$$x^2 = (0, 1, 0, \dots)(0, 1, 0, \dots) = (0, 0, 1, 0, \dots)$$

$$x^3 = (0, 1, 0, \dots)(0, 0, 1, 0 \dots) = (0, 0, 0, 1, 0 \dots)$$

$$\overline{x^j} = (0, 0, \dots 0, \underbrace{1}_{j+1\text{-място}}, 0, \dots)$$

$$ax = (a, 0, \dots)(0, 1, 0 \dots) = (0, a, 0 \dots)$$

$$ax^j = (0, \dots 0, \underbrace{a}_{j+1 \text{ място}}, 0 \dots)$$

$$\Rightarrow$$

$f = (a_0, a_1, \dots, a_n, 0, \dots) = a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n$

$B = \{ f = a_0 + a_1 x + \dots + a_n x^n \mid a_i \in A, x - \text{променлива} \}$

и комут. пр. с 1 / област на цялостност на пространството от полиноми с коефициенти от A и означаваме (с условността)

$B = A[x] = \{ f = b_0 x^n + b_1 x^{n-1} + \dots + b_{n-1} x + b_n \mid b_j \in A \}$

полиномиален пръстен на полиномите на променливата x с коеф от A.

Нека $f = a_0 x^n + a_1 x^{n-1} + \dots + a_{n-1} x + a_n$ е произволен полином от $A[x]$.

a_0 - старши коефициент на f

a_i - коефициент на f; a_n - свободен коефициент

$\deg f := n$ - степен на полинома f

$\deg a := 0, a \in A, a \neq 0$; $\deg 0 := -\infty$

$f, g \in A[x]$, $\deg f = n$, $\deg g = m$

$\deg(f+g) \leq \max(\deg f, \deg g) = \max(n, m)$

$\deg(fg) = \deg f + \deg g = n+m$ е в сила само ако A – област.

$\forall$ полином $f \in A[x] \rightarrow$ функцията f

$$f: \begin{cases} A \to A \\ a \to f(a) = a_0 a^n + a_1 a^{n-1} + \dots + a_{n-1} a + a_n \end{cases}$$

полиноми

$f + g \Rightarrow (f+g)(a) = f(a) + g(a)$

$fg \Rightarrow (fg)(a) = f(a) \cdot g(a)$

$f = g$ (полиноми) $\Rightarrow f(a) = g(a)$ $\forall a \in A$ $\Rightarrow f = g$ като функции.

Обратното в общия случай не е вярно!

Пример: $\mathbb{Z}_p[x]$ $f = x^p$ и $g = x$

$f \neq g$ като полиноми

$x^p \equiv x \pmod p$ Пак. в $\mathbb{Z}_p[x]$ $x^p = x$ като функции в $\mathbb{Z}_p$

Пр. $\forall x \in \mathbb{Z}_p$ имаме ли $f(x) = x^p$?? $g(x) = x$

Нека F – поле и $F[x]$ – полиномиален пръстен над F (комутативен с 1, $\underbrace{\text{като област}}_{F[x]}$)

$f = a_0 x^n + a_1 x^{n-1} + \dots + a_n$, $a_0 \neq 0$.

$g = b_0 x^m + b_1 x^{m-1} + \dots + b_m$, $b_0 \neq 0$.

Деф: Казваме, че полином f е унитарен полином, ако старшият му коефициент е $a_0 = 1$.

Th (теорема за делене с частно и остатък в $F[x]$)

Нека $f, g \in F[x]$, $g \neq 0$. Тогава $\exists!$ полиноми $q(x)$ (наречен частно) и $r(x)$ (наречен остатък) такива че:

$$f(x) = g(x)q(x) + r(x)$$
$$\deg r < \deg g.$$

Док: $\exists!$ r сл $g = a \neq 0 \Rightarrow f = a_1 \underbrace{(a^{-1}f)}_{q} + \underbrace{0}_{r}$

$$\deg 0 = -\infty < \deg g = 0$$

$$\deg f < \deg g \Rightarrow f = g \cdot 0 + f$$
$$\deg r = \deg f < \deg g$$

Нека $f = a_0 x^n + a_1 x^{n-1} + \dots + a_n$, $a_0 \neq 0$

$0 \neq g = b_0 x^m + b_1 x^{m-1} + \dots + b_m$, $b_0 \neq 0$

$n \geq m > 0$. Индукция по $\deg f = n$

$f = a_0 x^n + \dots$ $\quad$ $g = b_0 x^m + \dots$

$-\, a_0 x^n + \dots$ $\quad$ $q_1 = b_0^{-1} a_0 x^{n-m}$

$f_1, \deg f_1 < n$ и ИП $\Rightarrow$

$f_1 = g q_1 + r_1, \quad \deg r_1 < \deg g$

$\|$

$f - g q_1 = f - g \cdot b_0^{-1} a_0 x^{n-m} \Rightarrow$

$f = g(a_0 b_0^{-1} x^{n-m} + q_1) + r_1$

$\deg r_1 < \deg g$

$q_1 = a_0 b_0^{-1} x^{n-m} + q_1, \quad r := r_1$

$\Rightarrow f = g q + r, \quad \deg r < \deg f$

!) $f = g q_1 + r_1 = g q_2 + r_2$ (док. провести)

$\deg r_1 < \deg g, \ \deg r_2 < \deg g$

$\Rightarrow g(q_1 - q_2) = r_2 - r_1$ в $F[x]$

$\deg g(q_1 - q_2) = \deg g + \deg(q_1 - q_2)$

$F[x]$ област

$\geq \deg g > \deg(r_1 - r_2)$

Противоречие !!!

тъй като $\deg r_1 < \deg g$

$\deg r_2 < \deg g$

$\exists!$ q - частно и r - остатък:

$f = gq + r$, $\deg r < \deg g$

Пример в сила, когато $F[x]$

ако A - област $\Rightarrow a \in A$, $a \neq 0$, то

a може да не е обратимо т.е. $\nexists a^{-1}$

Обяснение в $\mathbb{Z}_8[x]$, не е област

няма единственост на представянето

Пр. $f = \bar{4}x^3$, $g = \bar{4}x^2 + \bar{1}$ $\in \mathbb{Z}_8[x]$

$f = g(x + \bar{2}) + (x + \bar{2})$ $\mathbb{Z}_8 = \{\bar{0}, \bar{1}, \ldots, \bar{7}\}$

$f = g(x + \bar{4}) + (x + \bar{4})$

Пример: $\mathbb{Z}_5[x]$, $\mathbb{Z}_5 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$

$f = \bar{4}x^5 + x^3 + \bar{2}$ | $g = \bar{3}x^3 + \bar{2}x + \bar{4}$

$\underline{\bar{4}x^5 + x^3 + \bar{2}x^2}$ | $q = \bar{3}x^2$

$r = \bar{3}x^2 + \bar{2}$ $\quad \deg r < \deg g$