2. Ф-я на Ойлер. Числови сравнения. Класове остатъци по модул n ($\mathbb{Z}_n$) и действия между тях

Деф: Ф-я на Ойлер:

$n \in \mathbb{N}$ $\varphi(n)$ - ф-я на Ойлер

$$\varphi(n) = |\{k \mid k \in \mathbb{N},\ k < n,\ (k,n)=1\}|$$

броя на числата $< n$ са взаимно прости с n

$\varphi(2)=1$, $\varphi(3)=2$, $\varphi(7)=6$, $\varphi(31)=30 \Rightarrow$

об 1) $\Rightarrow \varphi(p) = p-1$, където p - просто

об 2) $\varphi(4)=2$, $\varphi(9)=6$, $\varphi(10)=8$

Ако p - просто $\varphi(p^n) = p^n - p^{n-1}$ $\quad \{1,2,\dots,p^n\} \setminus \{p^1, p^2 \dots p\cdot p^{n-1}\}$

$\Rightarrow \varphi(125) = 100$ (числа, които се делят на p)

Т-ма: Ако $a, b \in \mathbb{N}$, $(a,b)=1 \Rightarrow \varphi(ab) = \varphi(a)\cdot\varphi(b)$ — мултипликативност на ф-ята на Ойлер

1-во:)

1	2	...	3	a
$a+1$	$a+2$		$a+3$	$2a$
$(b-1)a+1$	$(b-1)a+2$		$(b-1)a+3$	ba

(горни числата взаимно прости колкото са и така и с b)

стълб на матр: $\begin{pmatrix} r \\ a+r \\ 2a+r \\ \vdots \\ (b-1)a+r \end{pmatrix}$ - остатъците при деление с a на числата от този стълб

Ако първото число на един стълб има общ делител с a, то всички числа нагоре по стълба също ще имат общ делител с a, а ако първото число е взаимно просто с a то и всички нагоре са взаимно прости с a.

Делим с остатък с b:

$$\begin{aligned} r &= r_0 + q_0 b \\ a+r &= r_1 + q_1 b \qquad 0 \le r_1 < b \\ 2a+r &= r_2 + q_2 b \\ &\vdots \\ (b-1)a+r &= r_{b-1} + q_{b-1} b \end{aligned}$$

Допускаме, че $\exists i \neq j$ $i, j \in \{0, \dots, b-1\}$: $r_i = r_j$ (има 2 равни ост)

$$\Rightarrow \quad r_i + q_i b = i \cdot a + r$$
$$- \quad r_j + q_j b = j a + r$$
$$(q_i - q_j) b = (i-j) a \quad \Rightarrow b \mid (i-j) a, \text{ но } (a, b) = 1 \Rightarrow$$

$\Rightarrow b \mid (i-j)$, но $0 < |i-j| < b$, което е (b | нещо < b)

$\Rightarrow$ $\underbrace{r_0, r_1 \dots r_{b-1}}_{b \text{ на бр.}}$ са различни т.е са пълна система от остатъци $\Rightarrow$ $\forall$ са $0, 1 \dots b-1$ в някакъв ред.

$\forall$ възможен остатък $(0, \dots, b-1)$ се среща веднъж на $\forall$ стълб.

Във $\forall$ стълб има $\varphi(b)$ остатъци взаимно прости с $b \Rightarrow$

във $\forall$ стълб $\varphi(b)$ ост. са взаимно прости с b

Числата взаимно прости с a, са същия брой от $\varphi(a)$-стълба.

Във $\forall$ други от тези стълбове има $\varphi(b)$ числа взаимно прости с b

$\Rightarrow$ числата взаимно прости с $a \cdot b$ са $\varphi(a) \cdot \varphi(b)$.

Следствие: $n = p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}$ ($p_1, \dots, p_s$ - различни прости числа

$$\varphi(n) = \varphi(p_1^{k_1}) \varphi(p_2^{k_2}) \dots \varphi(p_s^{k_s}) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \dots (p_s^{k_s} - p_s^{k_s-1}) =$$
$$= p_1^{k_1-1}(p_1 - 1) \dots p_s^{k_s-1}(p_s - 1) =$$
$$= \underbrace{p_1^{k_1} \dots p_s^{k_s}}_{n} \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_s}\right)$$

$\Rightarrow \varphi(3600) = 3600 \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)$

Деф: Сравнения при целите числа

Казваме, че $a \equiv b \pmod n$, когато $n \mid (a-b)$, $n \neq 0$

$a \equiv b (n) \Leftrightarrow a = b + kn \Rightarrow a, b$ имат еднакви остатъци при деление с n.

Св-ва: 1) $a \equiv a \pmod n$

2) ако $a \equiv b \pmod n \Rightarrow b \equiv a \pmod n$

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

т.е. сравнението при фиксиран mod n е релация на еквивалентност.

$\forall a \equiv b \pmod n$ $a_1 \equiv b_1 \pmod n$ $\forall$

4) $a \pm k \equiv b \pm k (n)$

5) $a \pm a_1 \equiv b + b_1 (n)$

6) $ac = bc (n)$

7) $a \cdot a_1 (n) = b b_1 (n)$

а) $a^t \equiv b^t \pmod n$ $t \in \mathbb{N}$

б) ако $f(x)$ е полином с цели коеф, $f(a) \equiv f(b) \pmod n$

1 - ва т.

~~Нека $ka \equiv kb \pmod n \Rightarrow a \equiv b \pmod{\frac{n}{(n,k)}}$~~

$a \cdot a_1 - b \cdot b_1 = aa_1 - ba_1 + ba_1 - bb_1 = \underbrace{(a-b)}_{n_1} a_1 + b\underbrace{(a_1 - b_1)}_{n} \Rightarrow$

$\Rightarrow n \mid (aa_1 - bb_1)$

(Тв.) Нека $ka \equiv kb \pmod n \Rightarrow a \equiv b \pmod{\frac{n}{(n,k)}}$

Д-во: $n \mid (ka - kb) \Rightarrow n \mid k(a-b) \Rightarrow \begin{matrix} n = n_1 d \\ k = k_1 d \end{matrix}$ и $(n_1, k_1) = 1$

$\Rightarrow n_1 d \mid k_1 d (a-b) \Rightarrow n_1 \mid k_1 (a-b) \Rightarrow n_1 \mid (a-b)$

$a \equiv b \pmod{n_1}$ $\quad a \equiv b \pmod{\frac{n}{(n,k)}}$

Пр. 2

Решаване $\equiv \pmod n$

$a \equiv b \pmod n \Leftrightarrow a, b$ дават еднакви остатъци.

Нека $\bar{r} = \{r, r \pm n, r \pm 2n, r \pm 3n, \dots\} = \{r + sn \mid s \in \mathbb{Z}\}$

клас на еквивалентност на числа сравними по $\pmod n$.

Пр:

ако $n = 10$

$\bar{3} = \{\dots, -17, -7, 3, 13, 23, \dots\}$ $\quad \mathbb{Z} = \bar{0} \cup \bar{1} \cup \bar{2} \cup \dots \cup \bar{9}$ $\quad (\mathbb{Z} \pmod{10}) \frac{n}{4}$

класовете еквивалентност или класове остатъци $\pmod{10}$

За $n \geq 2$

$\mathbb{Z} = \underbrace{\bar{0} \cup \bar{1} \cup \dots \cup \overline{n-1}}_{n}$

При $n = 2$ $\quad \bar{0}$ - четни $\quad \bar{1}$ нечетни

$\{\bar{0}, \bar{1}\}$ $\quad \bar{0} + \bar{0} = \bar{0}$, $\bar{0} \cdot \bar{1} = \bar{0}$

+	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

·	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$

$\{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$ $\quad \bar{a} = \{a + kn \mid k \in \mathbb{Z}\}$

Деф 1) $\bar{a} + \bar{b} = \bar{r}$, където r е ост. на $a+b$, разделено на n.

Деф 2) $\bar{a} \cdot \bar{b} = r_1$, където r_1 е ост. на ab разделено на n.

Коректност на дефиницията:

Нека $\bar{a} = \bar{a_1}$ $(a \equiv a_1 \pmod n)$

$\bar{b} = \bar{b_1}$ $(b \equiv b_1 \pmod n)$ — едни и същи.

$\Rightarrow a+b \equiv a_1 + b_1 \pmod n \Rightarrow$ ост. на $a+b$ и на a_1+b_1 при $\pmod n$ е

$a \cdot b \equiv a_1 \cdot b_1 \pmod n \Rightarrow ab$ и $a_1 b_1$ дават едни и същи остатък.

св: $\bar{a} + \bar{b} = \overline{a+b}$

св: $\bar{a} \cdot \bar{b} = \overline{ab}$

Разглеждаме $\mathbb{Z}_4$

+	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

·	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

— симетрична

---

3. Групи - определение примери и основни свойства. Подгрупи

Деф: Бинарна операция $\varphi: M \times M \to M$ е изображение, което на $\forall$ наредена двойка елементи от M съпоставя елемент от M.

$M \neq \emptyset$ $\varphi(a,b)$ $a \vee b$, $a \wedge b$, $a+b$, $a \cdot b$

Примери: (бинарни операции) - сума на 2 цели числа е цяло число

- сума на два вектора е вектор, - умножение на матрици,

- умножение на вектори - сума на матрици - сума на вектори...

(небинарни операции) - скаларно произведение на два вектора е число, - умножение на вектор с число

Деф за Група: Нека $G \neq \emptyset$ с бинарна операция „$*$", т.е за $(\forall a,b \in G \times G \to a*b = G$. G е група относно „$*$" ако са изпълнени свойствата:

1) асоциативност: $(a*b)*c = a*(b*c)$

2) $\exists e \in G: a*e = e*a = a, \forall a \in G$

3) $\forall a \in G, \exists b_{(a)} \in G: a*b = b*a = e$ Записване $(G,*)$

Пр: $\mathbb{Z}$ с операц „$+$", $(\mathbb{Z},+)$ е група

$\mathbb{Z}$ с „$\cdot$" не е група т.к не е изпълнено 3) св.

Други: $(\mathbb{Q},+)$ $(\mathbb{R},+)$ $(\mathbb{C},+)$