② Функция на Ойлер. Числови сравнения. Класовете остатъци по модул n (Z_n) и действията между тях.

Опр: (Функция на Ойлер)
Нека $n \in \mathbb{N}$.
$\varphi(n) = |\{ k \mid k \in \mathbb{N}, k < n, (k,n) = 1 \}|$

Свойство ①: $\varphi(p) = p - 1$, p - просто

Свойство ②: $\varphi(p^n) = p^n - p^{n-1}$, p - просто

Th: (Мултипликативност на функцията на Ойлер)
Ако $a, b \in \mathbb{N}$, $(a,b) = 1$, тогава $\varphi(ab) = \varphi(a) . \varphi(b)$

Доказателство:

1	2	...	a
$a+1$	$a+2$	...	$2a$
⋮	⋮	⋱	⋮
$(b-1)a+1$	$(b-1)a+2$	...	ba

Търсим числата, които са взаимнопрости, както с a, така и с b.

$$\begin{pmatrix} r \\ a+r \\ 2a+r \\ \vdots \\ (b-1)a+r \end{pmatrix}$$ - остатъкът е един и същ за целия стълб

Ако първото число на един стълб има общ делител с a, то всички числа надолу по стълба също ще имат общ делител. Аналогично, ако първото число е взаимно

просто на a, то и останалите от стълба са.

$$\begin{pmatrix} r = r_0 + q_0 \cdot b \\ a + r = r_1 + q_1 \cdot b \\ 2a + r = r_2 + q_2 \cdot b \\ \vdots \\ (b-1)a + r = r_{b-1} + q_{b-1} \cdot b \end{pmatrix}$$

$$0 \le r_i < b$$

Допускаме, че $\exists\, i \neq j : i, j \in \{0, \dots, b-1\}$, $r_i = r_j$.

Тогава $r_i + q_i b = ia + r$

$$\underline{r_j + q_j b = ja + r}$$

$$(q_i - q_j)b = (i-j)a \Rightarrow b \mid (i-j)a, \text{ но } (a,b) = 1$$

$\Rightarrow b \mid (i-j)$, но $0 < |i-j| < b \Rightarrow$ (↯) с $b \mid (i-j)$ и $|b| > |i-j|$

$\Rightarrow r_0, r_1, \dots, r_{b-1}$ са различни остатъци, т.е. цяла система от остатъци, т.е. това са числата от $0, 1, \dots, b-1$ в някакъв ред $\Rightarrow$ всеки възможен остатък от $0, 1, \dots, b-1$ се среща в един стълб $\Rightarrow$ във всеки един стълб има $\varphi(b)$ остатъка взаимно прости с b $\Rightarrow$ във всеки един от стълбовете $\varphi(b)$ от числата са взаимно прости с b.

Числата взаимно прости с a са всички числа от $\varphi(a)$ стълба. Във всеки един от тези стълбове има $\varphi(b)$ числа взаимно прости с b $\Rightarrow$ числата взаимно прости както с a, така и с b, т.е. взаимно прости с $a \cdot b$ са точно $\varphi(a) \cdot \varphi(b)$.

<u>Следствие:</u> Ако числото n е представено във вида $n = p_1^{k_1} p_2^{k_2} p_3^{k_3} \dots p_s^{k_s}$, където $p_1, \dots, p_s$ са различни прости числа, то $\varphi(n) = \varphi(p_1^{k_1}) \cdot \varphi(p_2^{k_2}) \cdot \varphi(p_3^{k_3}) \dots \varphi(p_s^{k_s}) = (p_1^{k_1} - p_1^{k_1-1}) \cdot (p_2^{k_2} - p_2^{k_2-1}) \cdot (p_3^{k_3} - p_3^{k_3-1}) \dots (p_s^{k_s} - p_s^{k_s-1}) = p_1^{k_1-1} \cdot p_2^{k_2-1} \cdot p_3^{k_3-1} \dots p_s^{k_s-1} \cdot (p_1-1)(p_2-1)(p_3-1)\dots(p_s-1) = \underbrace{p_1^{k_1} \cdot p_2^{k_2} \cdot p_3^{k_3} \dots p_s^{k_s}}_{n} \left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\left(1 - \frac{1}{p_3}\right)\dots\left(1 - \frac{1}{p_s}\right)$

Опр. Числото a е сравнимо с числото b, $a \equiv b \pmod n$, когато $n \mid (a,b)$, $n \neq 0 \Leftrightarrow a = b + kn \Leftrightarrow a, b$ имат еднакъв остатък при деление с n.

Свойства: (на сравненията)

1) $a \equiv a \pmod n$;
2) $a \equiv b \pmod n \Rightarrow b \equiv a \pmod n$;
3) $a \equiv b \pmod n,\ b \equiv c \pmod n \Rightarrow a \equiv c \pmod n$;

} $\Rightarrow$ сравнението при фиксирано $(\mathrm{mod}\ n)$ е релация на еквивалентност

4) $a + k \equiv b + k \pmod n$;
5) $a + a_1 \equiv b + b_1 \pmod n$;
6) $a \cdot c \equiv b \cdot c \pmod n$;
7) $a \cdot a_1 \equiv b \cdot b_1 \pmod n$;
8) $a^t \equiv b^t \pmod n,\ t \in \mathbb{N}$;
9) $f(a) \equiv f(b) \pmod n$, ако $f(x)$ е полином с цели коефициенти.

} при $a \equiv b \pmod n$, $a_1 \equiv b_1 \pmod n$.

(Тв.) Ако $k.a \equiv kb \pmod n \Rightarrow a \equiv b \left(\mathrm{mod}\ \frac{n}{(n,k)}\right)$

Доказателство:

Нека $(n,k) = d$ и $n = n_1 d$, $k = k_1 . d$, така че $(n_1, k_1) = 1$
Тъй като $n \mid (ka - kb)$, то $n_1 d \mid k_1 d (a-b) \Rightarrow n_1 \mid k_1 (a-b) \Rightarrow$
$\Rightarrow n_1 \mid (a-b) \Rightarrow a \equiv b \pmod{n_1} \Rightarrow a \equiv b \left(\mathrm{mod}\ \frac{n}{(n,k)}\right)$

Опр. Тъй като сравнението $(\equiv)$ е релация на еквивалентност, то тя разбива $\mathbb{Z}$ на непресичащи се класове на еквивалентност.

За $n \geq 2$, разглеждаме релацията $\equiv \pmod n$, т.е. $a \equiv b \pmod n \Leftrightarrow a, b$ дават еднакъв остатък $\Rightarrow \overline{r} = \{ r, r \pm n, r \pm 2n, \ldots \} = \{ r + sn \mid s \in \mathbb{Z} \}$, $\forall$ числа сравними по $(\mathrm{mod}\ n)$.

$\mathbb{Z} = \overline{0} \cup \overline{1} \cup \ldots \cup \overline{n-1}$ - класове остатъци по $(\mathrm{mod}\ n)$.

$\bar{a} + \bar{b} = \bar{r}_1$, където r_1 е остатъкът на $a+b$ разделено с n;
$\bar{a} . \bar{b} = \bar{r}_2$, където r_2 е остатъкът на $a.b$ разделено с n.

Опр.11 (Коректност на дефинициите)
Нека $\bar{a} = \bar{a}_1$ ($a \equiv a_1 \pmod n$), $\bar{b} = \bar{b}_1$ ($b \equiv b_1 \pmod n$)
$\Rightarrow a + b \equiv a_1 + b_1 \pmod n \Rightarrow$ остатъкът на $a+b$ и на a_1+b_1 по $\pmod n$ е един и същ;
$\Rightarrow a . b \equiv a_1 . b_1 \pmod n \Rightarrow$ остатъкът на $a.b$ и на $a_1.b_1$ по $\pmod n$ е един и същ.
Това е достатъчно да твърдим, че дефиницията е коректно зададена.

$\bar{a} + \bar{b} = \overline{a+b}$
$\bar{a} . \bar{b} = \overline{a.b}$