Функция на Ойлер - $\varphi(x)$

Нека $n \in \mathbb{N}, n > 1$ ($\varphi(1) = 1$)

$\varphi(n)$ = броят на $\mathbb{N}$ x: $x < n$ и $(x, n) = 1$

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

$\varphi(2) = 1$ $\quad \varphi(7) = 6$

$\varphi(3) = 2$ $\quad \varphi(31) = 30$ $\Rightarrow \varphi(p) = p - 1$ → **Свойство 1**

p - просто

$\varphi(4) = 2$ $\quad \varphi(16) = 8$

$\varphi(9) = 6$ $\Rightarrow p$ - просто $\Rightarrow$

$\Rightarrow \varphi(p^n) = p^n - p^{n-1}$ → **Свойство 2**

Т Ако $a, b \in \mathbb{N}, (a, b) = 1 \Rightarrow \varphi(a.b) = \varphi(a)\varphi(b)$

↳ Мултипликативност на ф-ята на Ойлер

Доказателство:

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

→ 1 стълб!

$r \longrightarrow a$

$a+r$

⋮

$(b-1)a+r$

→ ако $(a, r) = 1$ или имат общ делител с a, то всички числа надолу по стълба са взаимно прости с a или този общ делител.

За b - делим стълба с частно и остатък.

$r = r_0 + q_0 b$

$a + r = r_1 + q_1 b$

$2a + r$ | $0 \le r_i < b$

⋮

$(b-1)a + r = r_{b-1} + q_{b-1} b$

Допускаме, че $\exists\ i \neq j, i, j \in [0, b) : r_i = r_j$

$\Rightarrow r_i + q_i b = ia + r$

$r_j + q_j b = ja + r$

$(q_i - q_j) b = (i - j) a \Rightarrow b \mid (i-j)a, (a, b) = 1 \Rightarrow b \mid (i-j) \Rightarrow 0 < |i-j| < b$ ↯

$\Rightarrow r_0 \dots r_{b-1}$ са различни числа $\Rightarrow$ всяко число от 0 до $b-1$ се среща по веднъж в някакъв ред. $\Rightarrow$ Всеки възможен остатък се среща по веднъж $\Rightarrow$ Във всеки стълб има $\varphi(b)$ остатъка, взаимно прости с b

$\Rightarrow$ Във всеки стълб има $\varphi(b)$ взаимно прости числа с b.

Числата, взаимно прости с a, са всички числа от $\varphi(a)$ стълба. Във всеки от тези стълбове има $\varphi(b)$ числа, взаимно прости с b $\Rightarrow$ Числата, взаимно прости и с a, и с b са $\varphi(a).\varphi(b)$ на брой.

Следствие: Ако $n = p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}$, $p_1 \dots p_s$ – едно от друго и прости

$\Rightarrow \varphi(n) = \varphi(p_1^{k_1}) \cdot \varphi(p_2^{k_2}) \dots \varphi(p_s^{k_s}) = (p_1^{k_1} - p_1^{k_1-1})(p_2^{k_2} - p_2^{k_2-1}) \dots (p_s^{k_s} - p_s^{k_s-1}) =$

$= p_1^{k_1-1} \dots p_s^{k_s-1} (p_1-1)(p_2-1) \dots (p_s-1) =$

$= \underbrace{p_1^{k_1} \dots p_s^{k_s}}_{n} (1 - 1/p_1) \dots (1 - 1/p_s)$

$\varphi(3600) = 3600(1-1/2)(1-1/3)(1-1/5)$

Сравнения при $\mathbb{Z}$ числа

a е сравнимо с b по модул n, когато $n \mid (a-b) \Leftrightarrow a \equiv b \pmod n \Leftrightarrow$

$\Leftrightarrow a \equiv b(n) \Leftrightarrow a = b + kn \Leftrightarrow a$ и b имат един и същи остатък при делене с n.

Свойства на сравненията:

1) $a \equiv a(n)$, $\forall n$
2) $a \equiv b(n) \Rightarrow b \equiv a(n)$
3) $a \equiv b(n)$ и $b \equiv c(n) \Rightarrow a \equiv c(n)$

} Сравнението при фиксирано n е релация на еквивалентност.

$a \equiv b(n)$; $a_1 \equiv b_1(n)$

4) $(a \pm k) \equiv (b \pm k)(n)$
5) $(a \pm a_1) \equiv (b \pm b_1)(n)$
6) $ac \equiv bc(n)$
7) $aa_1 \equiv bb_1(n)$
8) $a^t \equiv b^t(n)$, $t \in \mathbb{N}$
9) Ако $f(x)$ е полином с цели коефициенти, $f(a) \equiv f(b)(n)$.

Доказателства:

7) $aa_1 - bb_1 = aa_1 - ba_1 + ba_1 - bb_1 = (a-b)a_1 + b(a_1 - b_1) \Rightarrow n \mid (aa_1 - bb_1)$

Тв Нека $ka \equiv kb(n) \Rightarrow a \equiv b(n/(n,k))$

$n \mid (ka - kb) \Rightarrow n \mid k(a-b)$

$(n,k) = d \Rightarrow n = n_1 d$ и $k = k_1 d$, $(n_1, k_1) = 1$

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

$a \equiv b(n)$, $n_1 = n/(n,k)$

Нека $n \in \mathbb{N}$, $n \geq 2$. Разглеждаме релацията на еквивалентност $\equiv (n)$.

$a \equiv b(n) \Leftrightarrow a, b$ дават един и същи остатък при делене с n.

r-число $\Rightarrow \bar{r}$-класът на еквивалентност.

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

Пример: $n = 10 \rightarrow \bar{5} = \{5, 15, 25 \dots, -7, -17 \dots\} \Rightarrow \mathbb{Z} = \bar{0} \cup \bar{1} \dots \cup \bar{9}$

В ОБЩИЯ СЛУЧАЙ ЗА $n \geq 2$ ПОЛУЧАВАМЕ n НА БРОЙ КЛАСА В ЗАВИСИМОСТ ОТ ОСТАТЪЦИТЕ.

$n=2 \Rightarrow$ РАЗБИВАТ СЕ НА ЧЕТНИ И НЕЧЕТНИ

$\mathbb{Z}_2 = \{\bar{0}, \bar{1}\}$

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

*	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$

СЪЩОТО НЕЩО МОЖЕ ДА СЕ ДЕФИНИРА ЗА ВСЕКИ ОТ КЛАСОВЕТЕ ОСТАТЪЦИ ПРИ n - ПРОИЗВОЛНО.

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

$\bar{a} + \bar{b} = \bar{r}$, КЪДЕТО r Е ОСТАТЪКЪТ ОТ $(a+b) : n$

$\bar{a} . \bar{b} = \bar{r_1}$, КЪДЕТО r_1 Е ОСТАТЪКЪТ ОТ $(a.b) : n$

КОРЕКТНОСТ НА ДЕФИНИЦИИТЕ!

Т.К. ДЕФИНИЦИИТЕ ЗАВИСЯТ ОТ ЦЕЛИ МНОЖЕСТВА, ТРЯБВА ДА СЕ ПОДСИГУРИМ, ЧЕ СА ВЕРНИ ЗА КОЙ ДА СЕ Е ЕЛЕМЕНТ.

$a \equiv a_1 (n)$ $\quad a+b \equiv a_1 + b_1 (n) \Rightarrow$ ОСТАТЪКЪТ НА $a+b$ И a_1+b_1 ПО МОДУЛ n Е ЕДИН И СЪЩ.
$b \equiv b_1 (n)$

$ab \equiv a_1 b_1 (n) \Rightarrow ab$ И $a_1 b_1$ ДАВАТ ЕДИН И СЪЩИ ОСТАТЪК ПРИ ДЕЛЕНИЕ СЪС n.

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

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

$\Rightarrow$ В $\mathbb{Z}_n = \{\bar{0}, \bar{1}, \ldots \overline{n-1}\}$ МОЖЕМ ДА ДЕФИНИРАМЕ ОПЕРАЦИИТЕ + И . ТАКА

$\mathbb{Z}_4$

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

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

ГРУПИ

* ЛИНЕЙНО ПРОСТРАНСТВО - АБСТРАКТНО МНОЖЕСТВО, КОЕТО ИЗПЪЛНЯВА РАЗЛИЧНИ ОПЕРАЦИИ.

ГРУПА: МНОЖЕСТВО С ЕДНА БИНАРНА ОПЕРАЦИЯ.

↳ В ОБЩИЯ СЛУЧАЙ НЕ СЕ ИНТЕРЕСУВАМЕ ОТ ОБЕКТИТЕ. АКЦЕНТИРА СЕ ВЪРХУ СЪЩЕСТВУВАНЕТО НА БИНАРНА ОПЕРАЦИЯ.

$M \neq \emptyset \rightarrow$ БИНАРНА ОПЕРАЦИЯ: $\varphi : M \times M \rightarrow M$ - ИЗОБРАЖЕНИЕ НА ВСЯКА ДВОЙКА ЕЛЕМЕНТИ ОТ M СЪПОСТАВЯ ЕЛЕМЕНТ ОТ M.

! СКАЛАРНОТО ПРОИЗВЕДЕНИЕ НА ВЕКТОРИ ДАВА ЧИСЛО $\Rightarrow$ НЕ Е БИНАРНА ОПЕРАЦИЯ!