Опр. С $\varphi(n)$ (ф-ция на Ойлер) означава-
ме броя на числата $< n$ ($\leq n$) и
взаимно прости с n

Забр.?

Пр. $\varphi(6)$ 1, 2, 3, 4, 5 1, 4, 3, 4, 5, 6

$\varphi(6) = 2$

ТС p - просто

1/ $\varphi(p) = p - 1$

2/ $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^{\alpha-1}(p-1) = p^\alpha\left(1 - \frac{1}{p}\right)$

за $\alpha \geq 2$ (б. и за $\alpha = 1$)

Д-во 2) $(a, p^\alpha) \neq 1 \Leftrightarrow (a, p) \neq 1 \Leftrightarrow (a, p) = p \Leftrightarrow p / a$

$(d = (a, p^\alpha)) \Rightarrow d = p^\beta,\ \beta \leq \alpha;\ \beta > 0 \Rightarrow p / p^\beta / a$

$a \in \{1, 2, \dots, p^\alpha\}$ и $(a, p^\alpha) \neq 1 \Leftrightarrow a = pk\quad k \in \{1, 2, \dots, p^{\alpha-1}\}$

Тези „a" са $p^{\alpha-1}$ на брой; $\forall$ са p^α

$\Rightarrow \varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$

Сл. $|\mathbb{Z}_n^*| = \varphi(n)$

Д-во $\mathbb{Z}_n^* = \{\bar{k} \mid 0 \leq k \leq n-1,\ (k, n) = 1\}$

Фокт: Ако G е група, $g \in G$ и $|G| = n$, то $g^n = e_G$

$\Rightarrow \forall \bar{a} \in \mathbb{Z}_n^*\quad \bar{a}^{\varphi(n)} = \bar{1}$

Теорема на Ойлер: $\forall a \in \mathbb{Z} : (a, n) = 1 \Rightarrow a^{\varphi(n)} \equiv 1 \pmod{n}$

Сл. (Теорема на Ферма) $\forall p$ - просто и $\forall a : p \nmid a \Rightarrow a^{p-1} \equiv 1 \pmod{p}$

Сл. (Ферма 2) $\forall p$ - просто и $\forall a$ $a^p \equiv a \pmod{p}$

Деф. $\mu : \mathbb{N} \to \mathbb{Z} \subseteq \mathbb{C}$; $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ (p_i - прости ; $\alpha_i \geq 1$)

$$\mu(n) = \begin{cases} 1, & n = 1 \quad (k = 0) \\ 0, & \exists \alpha_i \geq 2 \quad (p_i^2 \mid n) \\ (-1)^k, & \forall \alpha_i = 1 \quad (n \text{ е свободно от квадрати}) \end{cases}$$

Функция на Мебиус

Опр. $f: \mathbb{N} \to \mathbb{C}$ – мультипликативная, если

$\forall a, b \in \mathbb{N} : (a,b)=1 \Rightarrow f(ab) = f(a) \cdot f(b)$

Зам. $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ и f – мульт. $\Rightarrow$

$f(n) = f(p_1^{\alpha_1}) \cdot f(p_2^{\alpha_2}) \cdots f(p_k^{\alpha_k})$

Обозначения: $f: \mathbb{N} \to \mathbb{C}$; $F(n) := \sum_{d \mid n} f(d)$; $F: \mathbb{N} \to \mathbb{C}$

$\mu \to M$; $\varphi \to \phi$

Тв.2 $M(n) = \begin{cases} 1, & n=1 \\ 0, & n>0 \end{cases}$

Тс.1 μ – мультипликативна.

Тс. $\sum_{d/n} \varphi(d) = n$

Д-во Рассм. $A = \left\{ \frac{1}{n}, \frac{2}{n}, \dots, \frac{n}{n} \right\} =$

$\frac{k}{n} = \frac{\frac{k}{(k,n)}}{\frac{n}{(k,n)}}$ – несократимая дробь; $\frac{n}{(k,n)} \mid n$

$= \bigcup_{d/n} \left\{ \frac{k}{d} \;\middle|\; (k,d)=1,\ 1 \le k \le d \right\}$

A_d

Сами $\frac{k}{d} = \frac{k \cdot \frac{n}{d}}{n} \le n \in A \Rightarrow =$

$d_1 \mid n,\ d_2 \mid n,\ A_{d_1} = A_{d_2} \Rightarrow d_1 = d_2$

$\Rightarrow |A| = \sum_{d/n} |A_d|,\ |A_d| = \varphi(d)$

Зад. A_d са класове е РЕ (защо?!) в A:

$$\frac{a}{n} \sim \frac{b}{n} \overset{def}{\iff} (a,n) = (b,n)$$

$$\left[\frac{a}{n}\right] = \left[\frac{a/(a,n)}{n/(a,n)} \cdot \frac{(a,n)}{(a,n)}\right] = \left[\frac{(a,n)}{n}\right]$$

$$A = \bigcup_{\delta | n} \underbrace{\left[\frac{\delta}{n}\right]}_{A_{\frac{n}{\delta}}} \longrightarrow |A| = \sum_{\delta | n} \left|A_{\frac{n}{\delta}}\right| \overset{?}{=} \sum_{\delta | n} |A_\delta|$$

Зад. Получихме, че $\phi(n) = n$ и очевидно е мултипликативна функция ($\forall a,b$ $\phi(ab) = ab = \phi(a)\phi(b)$)

Тв. Ако f - мулт., то $F(n) = \sum_{\delta | n} f(\delta)$ също е мулт.

Lemma. $(a,b)=1$ $\quad \sum_{d \mid ab} a_d = \sum_{d_1 \mid a} \sum_{d_2 \mid b} a_{d_1 d_2}$

$\{ d \mid d \mid ab \} \overset{\text{bijection}}{\longleftrightarrow} \{ (d_1, d_2) \mid d_1 \mid a,\ d_2 \mid b \}$

$d \longmapsto \left((d, a),\ \frac{d}{(d,a)} \right)$ $\quad \frac{a}{(d,a)} \mid b$

$d_1 d_2 \longleftarrow\!\shortmid\ (d_1, d_2)$

D-Co $(a,b)=1$ $\quad$ | δ-argument. $(d_1, d_2)=1 \Leftarrow$ | $(a,b)=1$, $d_1 \mid a$, $d_2 \mid b$

$$F(ab) = \sum_{d \mid ab} f(d) = \sum_{d_1 \mid a} \sum_{d_2 \mid b} f(d_1 d_2) = \sum_{d_1 \mid a} \sum_{d_2 \mid b} f(d_1) f(d_2)$$

$$= \sum_{d_1 \mid a} f(d_1) \underbrace{\left[\sum_{d_2 \mid b} f(d_2) \right]}_{F(b)} = F(b) \cdot \underbrace{\sum_{d_1 \mid a} f(d_1)}_{F(a)} = F(b) \cdot F(a)$$

Сл. 1) M – мултип.

2) $\alpha \geq 1$, p – пр. $\Rightarrow M(p^\alpha) = \sum_{\delta \mid p^\alpha} \mu(\delta) \overset{\delta = p^\rho}{=} \sum_{\rho=0}^{\alpha} \mu(p^\rho) =$

$= \underbrace{\mu(1)}_{1} + \underbrace{\mu(p)}_{-1} + \underbrace{\mu(p^2) + \dots}_{=0} = 0$

3) $M(n) = \begin{cases} 1, & n = 1 \\ 0, & n = 0 \end{cases}$

Формули за обръщане на Мебиус

$f : \mathbb{N} \to \mathbb{C}$, $F(n) := \sum_{\delta \mid n} f(\delta)$. Тогава

$f(n) = \sum_{\delta \mid n} \mu\left(\frac{n}{\delta}\right) F(\delta) \overset{\text{ком.}}{=} \sum_{\delta \mid n} \mu(\delta) F\left(\frac{n}{\delta}\right) = \sum_{\delta_1 \delta_2 = n} \mu(\delta_1) F(\delta_2)$

Зад $\sum_{d_1 \mid n} \left(\sum_{d_2 \mid d_1} a(d_1, d_2) \right) = \sum_{d_2 \mid n} \left(\sum_{k \mid \frac{n}{d_2}} a(k d_2, d_2) \right)$

$\left(d_2 \mid d_1 \mid n \; ; \; \boxed{d_1 = k d_2} \; ; \; k d_2 \mid n \to k \mid \frac{n}{d_2} \right.$

$\left\{ (d_1, d_2) \mid d_1 \mid n, \; d_2 \mid d_1 \right\} = \left\{ (k d_2, d_2) \mid d_2 \mid n, k \mid \frac{n}{d_2} \right\}$

Д-Ф $\sum_{d \mid n} \mu\left(\frac{n}{d}\right) F(d) = \sum_{d \mid n} \mu\left(\frac{n}{d}\right) \left[\sum_{d_1 \mid d} f(d_1) \right] =$

$= \sum_{d \mid n} \sum_{d_1 \mid d} \mu\left(\frac{n}{d}\right) f(d_1) \overset{d = k d_1}{=} \sum_{d_1 \mid n} \sum_{k \mid \frac{n}{d_1}} \mu\left(\frac{n}{k d_1}\right) f(d_1) = \overset{\frac{n}{d_1} = 1}{\overset{\text{II}}{1}}$

$= \sum_{d_1 \mid n} f(d_1) \left[\sum_{k \mid \frac{n}{d_1}} \mu\left(\frac{\frac{n}{d_1}}{k}\right) \right] = \sum_{d_1 \mid n} f(d_1) \left[\sum_{k \mid \frac{n}{d_1}} \mu(k) \right] = \sum_{d_1 \mid n} f(d_1) M\left(\frac{n}{d_1}\right)$

$= f(n)$

Тв. $f: \mathbb{N} \to \mathbb{C}$; $F(n) := \sum_{d \mid n} f(d)$

F – мульт. $\Rightarrow$ f – мульт. $\left(\frac{a}{d_1}, \frac{b}{d_2}\right) = 1$; $(d_1, d_2) = 1$

Д-во $(a, b) = 1$

$$f(ab) = \sum_{d \mid ab} \mu\left(\frac{ab}{d}\right) F(d) = \sum_{d_1 \mid a} \sum_{d_2 \mid b} \mu\left(\frac{ab}{d_1 d_2}\right) F(d_1 d_2) =$$

мульт. $\underset{F, \mu}{=} \sum_{d_1 \mid a} \sum_{d_2 \mid b} \mu\left(\frac{a}{d_1}\right) \mu\left(\frac{b}{d_2}\right) F(d_1) F(d_2) =$

$$= \sum_{d_1 \mid a} \mu\left(\frac{a}{d_1}\right) F(d_1) \overbrace{\left[\sum_{d_2 \mid b} \mu\left(\frac{b}{d_2}\right) F(d_2)\right]}^{f(b)} =$$

$$= f(b) \cdot \left[\sum_{d_1 \mid a} \mu\left(\frac{a}{d_1}\right) F(d_1)\right] = f(b) f(a)$$

Сл. $f : \mathbb{N} \to \mathbb{C}$, $F(n) = \sum_{d \mid n} f(d)$. Тогда

f – мульт. $\Leftrightarrow$ F – мульт.

Сл. 1) φ – мульт. (ϕ – мульт.)

2) $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k} > 1 \Rightarrow$

$$\varphi(n) = \varphi(p_1^{\alpha_1}) \cdots \varphi(p_k^{\alpha_k}) = p_1^{\alpha_1 - 1} \cdots p_k^{\alpha_k - 1} (p_1 - 1) \cdots (p_k - 1) =$$

$$= n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_k}\right)$$

„Прост" док. на Теор. на Ойлер и Ферма

Опр. 1) $a_1, \dots, a_n$ — полная система вычетов, если

$\mathbb{Z}_n = \{\overline{a_1}, \overline{a_2}, \dots, \overline{a_n}\}$

2) $a_1, \dots, a_n$ — ПСО, если $\forall i \neq j \; a_i \not\equiv a_j \pmod n$

3) $a_1, \dots, a_{\varphi(n)}$ — приведенная система вычетов, если

$\mathbb{Z}_n^* = \{\overline{a_1}, \dots, \overline{a_{\varphi(n)}}\}$

4) $a_1, \dots, a_{\varphi(n)}$ — ПСО, если $\forall i \neq j \; a_i \not\equiv a_j \pmod n$ и $\forall i \; (a_i, n) = 1$

Зам. 1) $a_1, \dots, a_n$ — ПСО и $a \in \mathbb{Z} \Rightarrow \exists! i = \overline{1,n} : a \equiv a_i \pmod n$

2) $a_1, \dots, a_{\varphi(n)}$ — ПСО и $a \in \mathbb{Z}, (a, n) = 1 \Rightarrow \exists! i = \overline{1,n} : a \equiv a_i \pmod n$

Зад. φ ПСО $\rightarrow$ РСО

$\{1, \ldots, n\}$ $\quad$ $\{k \mid k \in \{1, \ldots, n\}, (k, n) = 1\}$

$\{0, \ldots, n-1\}$

Д-во на теор. на Дирих:

Нека $(a, n) = 1$ и $a_1, \ldots, a_{\varphi(n)} \in$ ПСО

Тогава за $b_i = aa_i$ за $i = 1, \ldots, \varphi(n)$

$b_1, \ldots, b_{\varphi(n)}$ също е РСО

- Ако $b_i \equiv b_j \pmod n \Rightarrow aa_i \equiv aa_j \pmod n \overset{(a,n)=1}{\Rightarrow} a_i \equiv a_j \Rightarrow i = j$
- $(a, n) = (a_i, n) = 1 \Rightarrow (aa_i, n) = 1$

$\Rightarrow \forall b_i \quad i=1 \to \varphi(n) \quad \exists! j_i : b_i \equiv a_{j_i} \pmod n$

$j_1 \to j_{\varphi(n)}$ — перестановка (возможно с)

Умножаем $\forall b_i$ на a_{j_i}

$b_1 b_2 \cdots b_{\varphi(n)} \equiv a_{j_1} a_{j_2} \cdots a_{j_{\varphi(n)}} = a_1 \cdots a_{\varphi(n)} \pmod n$

$a^{\varphi(n)}$ ||

$a \quad a_1 \cdots a_{\varphi(n)}$

$(a_1 a_2 \ldots a_{\varphi(n)}, n) = 1 \quad (\Leftarrow \forall (a_i, n) = 1)$

$\Rightarrow a^{\varphi(n)} \equiv 1 \pmod n$

Док. на Зерон

Т6. p - прост и $1 \le k \le p-1 \Rightarrow p \mid \binom{p}{k}$

Д-во $\binom{p}{k} = \frac{p}{k}\binom{p-1}{k-1}$; $k\binom{p}{k} = p\binom{p-1}{k-1}$

$\Rightarrow p \mid k\binom{p}{k} \xrightarrow{(k,p)=1} p \mid \binom{p}{k}$

Т6. p - пр. $\Rightarrow \underline{(a+b)^p} = a^p + \sum_{k=1}^{p-1} \underbrace{\binom{p}{k}}_{\text{е цяло число}} a^k b^{p-k} + b^p \equiv \underline{a^p + b^p} \pmod p$

Сл. (инд.) p - пр. $\Rightarrow (a_1 + a_2 + \dots + a_k)^p \equiv a_1^p + \dots a_k^p \pmod p$

Сл. инд. p - пр. $(a_1 + \dots + a_k)^{p^s} \equiv a_1^{p^s} + \dots + a_k^{p^s} \pmod p$

Сл. (Теор. Ферма) $\forall a \quad a^p \equiv a \pmod p$ за p-прост.

Д-во $k = p$; $a_1 = a_2 = \dots = a_k = 1$

$\Rightarrow (\underbrace{1 + \dots + 1}_{a})^p \equiv \underbrace{1^p + \dots + 1^p}_{a} = a \quad \Rightarrow a^p \equiv a$

Диофантови уравн.

$ax + by = c$; Дадени $a, b, c \in \mathbb{Z}$; Търсим $x, y \in \mathbb{Z}$

Линейно диофантово уравн. (на 2 неизв.)

Т6. $ax + by = c$ има реш. $\Leftrightarrow (a, b) \mid c$

($\Rightarrow$) Нека $x_0, y_0 \in \mathbb{Z}$ са реш. $\Rightarrow c = a \cdot x_0 + b \cdot y_0$

$\Rightarrow (a, b) \mid c$

($\Leftarrow$) Sean $(a,b) \mid c$

Bezout $\Rightarrow \exists u, v : ua + vb = (a,b)$. $\frac{c}{(a,b)}$

$a \frac{uc}{(a,b)} + b \frac{vc}{(a,b)} = c$

$\Rightarrow \left(\frac{uc}{(a,b)}, \frac{vc}{(a,b)} \right)$ es sol.

T6. Sean $(a,b) \mid c$ y (x_0, y_0) es sol. de $ax + by = c$. Todas las sol. son

$$\left\{ \left(x_0 + \frac{b}{(a,b)} t, \; y_0 - \frac{a}{(a,b)} t \right) \mid t \in \mathbb{Z} \right\}$$

D-Co Sean (x_1, y_1) es sol.

$\Rightarrow ax_1 + by_1 = ax_0 + by_0 = c$

$a(x_1 - x_0) = b(y_0 - y_1)$

$\Rightarrow b \mid a(x_1 - x_0) \Rightarrow \frac{b}{(a,b)} \mid x_1 - x_0$

$\Rightarrow \exists t: x_1 - x_0 = \frac{b}{(a,b)} t \Rightarrow x_1 = x_0 + \frac{b}{(a,b)} t$

$a \frac{b}{(a,b)} t = b(y_0 - y_1) \Rightarrow y_1 = y_0 - \frac{a}{(a,b)} t$

Далее, $\forall t \left(x_0 + \frac{b}{(a,b)} t, y_0 - \frac{a}{(a,b)} t\right)$ е
реш.