Напоминание

$\varphi(n)$ — ф-ия Эйлера
$n \in \mathbb{N}$

кол-во взаимно простых с n от 1 до n.

<u>Утв.</u> $\varphi(ab) = \varphi(a)\cdot\varphi(b)$, если $(a,b)=1$.

<u>Д-во</u>

Пример $a=4$
$b=5$

расставим в таблице числа x от 0 до $ab-1$

строка $= x \bmod a$
столбец $y \bmod b$

$\varphi(5)=4$

$x \bmod 4$ \ $x \bmod 5$	0	1	2	3	4
0	0	16	12	8	4
1	5	$\boxed{1}$	$\boxed{17}$	$\boxed{13}$	$\boxed{9}$
2	10	6	2	18	14
3	15	$\boxed{11}$	$\boxed{7}$	$\boxed{3}$	$\boxed{19}$

$\varphi(4)=2$

$2\times 4 = 8 = \varphi(20)$

Все числа в разных клетках, т.к. $\exists$ x и y в одной клетке в строке i и столбце j:

$$(1)\begin{cases} x \bmod a = i \\ x \bmod b = j \end{cases} \qquad \begin{cases} y \bmod a = i \\ y \bmod b = j \end{cases}$$

По Кит. Теор. об остатках $\exists!$ решение системы (1) по модулю $M = a\cdot b$. $\Rightarrow$ $x \underset{ab}{\equiv} y$

но у нас числа от 0 до $ab-1$, значит $x = y$.

Кроме того, все клетки заполнены (чисел $a\cdot b$, и клеток $a\cdot b$) (или по КТО есть решение в каждой клетке)

$0 \le x < a\cdot b$ $\quad (x, ab) = 1 \overset{?}{\Leftrightarrow}$ $\begin{matrix}(x \bmod a, a) = 1 \\ (x \bmod b, b) = 1\end{matrix}$

Проверим $\Leftrightarrow$, это будет значить, что в таблице взаимно простые с ab числа — это прямоугольник размера $\varphi(a) \times \varphi(b)$

$\boxed{\Rightarrow}$ От противного $\exists\ (x \bmod a, a) = d > 1$

т.е. $\exists\ \underbrace{x \bmod a}_{x - qa \text{ (деление с остатком)}} \vdots\, d,\ a \vdots d \Rightarrow$

$\Rightarrow x - qa \vdots d,\ a \vdots d \Rightarrow x \vdots d$

$x \vdots d \quad ab \vdots d \Rightarrow (x, ab) \geq d$ противореч.

$\boxed{\Leftarrow}$ $(x \bmod a, a) = 1$
$(x \bmod b, b) = 1$

От противного, $\exists\ (ab, x) = d \vdots p$ простое, $d > 1$

Тогда $ab \vdots p$ и $x \vdots p$

по $p \in P \Rightarrow a \vdots p$ или $b \vdots p$ (если $a \not\vdots\, p$ $\underset{\text{вз. просто ср}}{ab} \vdots p$)

если $a \vdots p$, то $x \vdots p$
$a \vdots p$

$x \bmod a = \underset{\vdots p}{x} - q\underset{\vdots p}{a} \vdots p \Rightarrow (\underbrace{x \bmod a}_{\vdots p}, \underset{\vdots p}{a}) \geq p > 1$ ∎

$\boxed{\text{Ф-ла вычисления } \varphi(n)}$

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_a^{k_a} \qquad (p_i^{k_i}, p_j^{k_j}) = 1$$

$$\varphi(n) = \varphi(p_1^{k_1}) \cdot \varphi(p_2^{k_2}) \cdot \ldots \cdot \varphi(p_a^{k_a}) =$$

$$= (p_1 - 1)\, p_1^{k_1 - 1} \cdot (p_2 - 1)\, p_2^{k_2 - 1} \cdot \ldots \cdot (p_a - 1)\, p_a^{k_a - 1}$$

$$= \boxed{n\, \frac{p_1 - 1}{p_1} \cdot \frac{p_2 - 1}{p_2} \cdot \ldots \cdot \frac{p_a - 1}{p_a}} = \boxed{n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \ldots \left(1 - \frac{1}{p_n}\right)}$$

Пример

$$\varphi(700) = \varphi(7 \cdot 2^2 \cdot 5^2) = 6 \cdot 1 \cdot 2^1 \cdot 4 \cdot 5^1 = 240.$$

У ф-ии Эйлера много свойств.

<u>Св-в.</u> Берем число n и все его делители.

$n = 12 \quad d_1 = 1 \quad d_2 = 2 \quad d_3 = 3 \quad d_4 = 4 \quad d_5 = 6 \quad d_7 = 12$

$$\sum_{n \vdots d} \varphi(d) = n$$

$\varphi(3)\varphi(4) = 2 \cdot 2$

$$\varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(6) + \varphi(12) = 12$$

$$1 + 1 + 2 + 2 + 2 + 4$$

<u>Д-во</u>

рассмотрим все дроби $\frac{1}{n} \quad \frac{2}{n} \quad \dots \quad \frac{n}{n}$ и

сократим их.

$\frac{1}{12} \quad \frac{2}{12} = \frac{1}{6} \quad \frac{3}{12} = \frac{1}{4} \quad \frac{4}{12} = \frac{1}{3} \quad \frac{5}{12} \quad \frac{6}{12} = \frac{1}{2}$

получим $\frac{1}{12} \quad \frac{5}{12} \quad \frac{7}{12} \quad \frac{11}{12}$ $\Big\}\ \varphi(12) = 4$

$\frac{2}{12} = \frac{1}{6} \quad \frac{5}{6} = \frac{10}{12}$ $\Big\}\ \varphi(6) = 2$

$\frac{3}{12} = \frac{1}{4} \quad \frac{3}{4} = \frac{9}{12}$ $\Big\}\ \varphi(4) = 2$

$\frac{4}{12} = \frac{1}{3} \quad \frac{2}{3} = \frac{8}{12}$ $\Big\}\ \varphi(3) = 2$

$\frac{1}{2} = \frac{6}{12}$ $\Big\}\ \varphi(2)$

$\frac{1}{1} = \frac{12}{12}$ $\Big\}\ \varphi(1)$

$\Sigma = 12$

Получим дроби вида $\frac{x}{d}$, где $n \vdots d$, $(x, d) = 1$

дробей со знаменателем d ровно $\varphi(d)$ штук.

А всего всех дробей n: $\frac{1}{n}, \dots, \frac{n}{n}$ ∎

Опр Полная система вычетов по модулю m — это множество из m целых чисел $\{a_1, a_2 \dots a_m\}$:

$a_i \not\equiv_m a_j$, если $i \neq j$.

Пример $\{0, 1, 2, 3\}$ — ПСВ mod 4

$\{0\ 3\ 6\ 9\}$ ——//——

Утв. мн-во $\{a_i \bmod m\}$ — это $\{0, 1, 2, \dots m-1\}$

— т.е. числа из ПСВ перебирают все остатки mod m.

$\{0\ 3\ 6\ 9\}$

$0 \bmod 4 = 0$
$3 \bmod 4 = 3$
$6 \bmod 4 = 2$
$9 \bmod 4 = 1$

Д-во. Остатков $a_i \bmod m$ будет m шт, т.к. чисел всего m, и они все разные. И остатков ровно m: $\{0, 1, 2, \dots m-1\}$. Значит, ровно они и получатся. ∎

Примеры mod 5: $\{0, 1, 2, 3, 4\}$
$\{0\ 2\ 4\ 6\ 8\}$
$\{-2\ -1\ 0\ 1\ 2\}$

Утв. Если $\{a_i\}$ — ПСВ mod m, то $\{a_i + x\}$ — тоже ПСВ mod m.

Пример mod 4: $\{0\,1\,2\,3\}$ — ПСВ $x = 10$
$\{10, 11, 12, 13\}$ — ПСВ

Д-во чисел останется m, $a_i + x \equiv_m a_j + x \iff$

$a_i \underset{m}{\equiv} a_j$. ∎

Утв. $\{a_i\}$ – ПСВ mod m, $x \in \mathbb{Z}$ $(x, m) = 1$

Тогда $\{a_i \cdot x\}$ – ПСВ mod m

Пример $\{0\ 1\ 2\ 3\}$ – ПСВ mod 4 $x = 11$ $(11, 4) = 1$

$\{0\ \ 11\ \ 22\ \ 33\}$ – ПСВ mod 4

mod 4: 0 3 2 1

Д-во Чисел $a_i \cdot x$ – m шт

$a_i x \underset{m}{\equiv} a_j x \iff a_i \underset{m}{\equiv} a_j$ потому что

сравнения можно сокращать на x, если $(x, m) = 1$ ∎

Опр Приведённая система вычетов mod m.

мн-во $\{a_i\}$: должно быть $\varphi(m)$ чисел, $a_i \underset{m}{\not\equiv} a_j$ $i \neq j$

и $(a_i, m) = 1$.

Пример. $\{1\ 2\ 3\ 4\}$ – ПрСВ mod 5. $\varphi(5) = 4$

$\{2\ \ 4\ \ 6\ \ 8\}$ – ПрСВ mod 5

$\{1, 3, 7, 9\}$ – ПрСВ mod 10 $\varphi(10) = 4$

$\{-3\ \ -1\ \ 1\ \ 3\}$ – ПрСВ mod 10

Утв. Если $\{a_i\}$ – ПрСВ.

$\{a_i \bmod m\}$ – это все числа от 1 до m, которые взаимно просты с m.

<u>Пример</u> $\{-3\ \ -1\ \ 1\ \ 3\}$ — ПрСВ mod 10

$-3 \bmod 10 = 7$ $\quad$ $1 \bmod 10 = 1$

$-1 \bmod 10 = 9$ $\quad$ $3 \bmod 10 = 3.$

$\{7, 9, 1, 3\}$ — все числа от 1 до 10, которые взаимно просты с 10

<u>Д-во</u>. $\{a_i \bmod m\}$ — $\varphi(m)$ шт.

$$0 \le a_i \bmod m < m$$

все $a_i \bmod m$ разные, т.к. $a_i \not\equiv_m a_j$

почему же $(a_i \bmod m, m) = 1$?

$$(\underbrace{a_i - q m}_{\vdots d}, \underset{\vdots d}{m}) = 1$$

$\overset{\vdots}{d} \Rightarrow a_i \vdots d \Rightarrow (a_i, m) \ge d$

Итого, у нас $\varphi(m)$ чисел от 0 до $m-1$ и все разные, и все взаимно просты с m. Кстати, по определению $\varphi(m)$ это как раз кол-во таких чисел. Значит, перечислены все взаимно простые остатки.

<u>Утв</u>. Если $\{a_i\}$ — ПрСВ mod m,

Если $(x, m) = 1$, то $\{a_i x\}$ — ПрСВ.

<u>Пример</u>. $\{-3, -1, 1, 3\}$ — Пр СВ mod 10

$x = 3$ $\quad$ $\{-9, -3, 3, 9\}$ — Пр СВ

$$\begin{array}{cccc} -9 & -3 & 3 & 9 \\ \downarrow {\scriptstyle \bmod 10} & \downarrow & \downarrow & \downarrow \\ 1 & 7 & 3 & 9 \end{array}$$

Д-во. $\{a_i x\}$ – $\varphi(m)$ чисел.

$$a_i x \underset{m}{\equiv} a_j x \iff a_i \equiv a_j$$

т.к. $(x,m)=1$

Проверим, что $(a_i x, m) = 1$

произведение взаимно простых – взаимно просто.

$a_i x \vdots d \vdots p \in \mathbb{P}$

$m \vdots d$

$a_i x \vdots p \Rightarrow a_i \vdots p$ или $x \vdots p$

$m \vdots p$

??

$(a_i, m) = 1$

??

$(x, m) = 1$

Th. Эйлера.

$a \in \mathbb{Z}$ $\quad m \in \mathbb{Z}$ $\quad (a,m)=1.$

Тогда $\boxed{a^{\varphi(m)} \underset{m}{\equiv} 1}$

Пример $\quad a = 3 \quad m = 10$

$3^{\varphi(10)} \underset{10}{\equiv} 1 \qquad 3^4 = 81 \underset{10}{\equiv} 1.$

Пример. $\quad a = 3 \quad m = 1001 \qquad \varphi(m) = \varphi(7 \cdot 11 \cdot 13) = \varphi(7)\varphi(11)\varphi(13) = 6 \cdot 10 \cdot 12 = 720$

$3^{720} \underset{1001}{\equiv} 1$ ← поверим.

Д-во Рассмотрим ПрСВ mod m.
(просто все числа от 1 до m, взаимно прост с m)

$\{a_i\}$ – ПрСВ т.к. $(a,m)=1$, $\{a \cdot a_i\}$ – ПрСВ

все вз.пр остатки mod m

все вз.пр.остатки mod m, в другом порядке

$$a_1 a_2 a_3 a_4 \dots a_{\varphi(m)} \underset{m}{\equiv} (a a_1)(a a_2) \dots (a a_{\varphi(m)})$$

Те же числа $(\bmod\ m)$ в другом порядке

$$\Rightarrow \boxed{a_1 a_2 \dots a_{\varphi(m)}} \underset{m}{\equiv} a^{\varphi(m)} \boxed{a_1 a_2 a_3 \dots a_{\varphi(m)}}$$

$(a_i, m) = 1$

$\Rightarrow$ произведение a_i тоже вз. просто с m.

$\Rightarrow$ можно сократить $\Rightarrow$ $1 \underset{m}{\equiv} a^{\varphi(m)}$. ∎