Конспект по дискретной математике.

Лектор - Посов И.А.

8.04.19

Утверждение: $a, b \in \mathbb{Z} \quad (a, b) = 1$
Тогда $\varphi(ab) = \varphi(a)\varphi(b)$

Доказательство:

$0\ 1\ 2\ \ \dots\ \ b-1 \longleftarrow$ ост. $mod\ b$

0
1
2
$\vdots$
$a-1$

$\uparrow$
ост. $mod\ a$

Итак, в таблице $a \times b$ клеток. Чисел $1 \dots ab$ - $a * b$ штук $\Rightarrow$ все клетки содержат ровно одно число

Числа от 1 до ab вставим в таблицу так:
x идет в строку $x\ mod\ a$
x идет в строку $x\ mod\ b$

Пример $a = 3$, $b = 4$

12	9	6	3
4	1	10	7
8	5	2	11

Докажем, что все числа попали в разные клетки

Пусть нет, тогда x, y в одной клетке

$x\ mod\ a = y\ mod\ a \Rightarrow x \equiv y \Rightarrow x - y \,\vdots\, a$

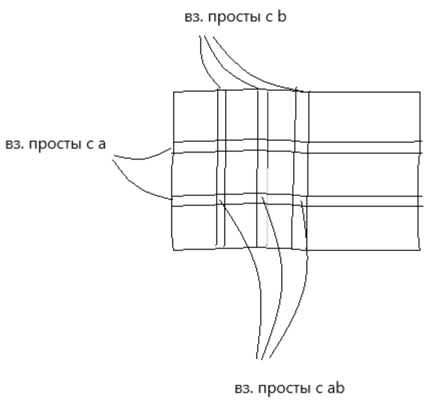
$x\ mod\ b = y\ mod\ b \Rightarrow x \equiv y \Rightarrow x - y \,\vdots\, b$

Так как $(a, b) = 1 \Rightarrow x - y \vdots ab$, но $1 \leqslant x, y \leqslant ab$
$\Rightarrow x = y$
$\square$

/*

Проверим, что $1 \leqslant x \leqslant ab$ взаимно прост с $ab \Leftrightarrow$ (xmoda,a) = 1, (xmodb,b) = 1
пусть доказали

*/



$\Rightarrow \varphi(ab) = \varphi(a)\varphi(b)$

Доказательство

1)

вне строк и столбцов - не взаимно просты

Пусть (x mod a,a) $= d > 1$

$\Rightarrow x\ mod\ a \vdots d \Rightarrow x - q\ a \vdots d \Rightarrow x \vdots d$

$a \vdots d \Rightarrow ab \vdots d$
$\Downarrow$
$(x, ab) \geqslant d > 1$

2)

Пусть (xmod a ,a) = 1
(xmod b ,b) = 1
но (от прот.)

Пусть $x \vdots d > 1$

$(x, ab) > 1 \;\; ab \vdots d > 1 \;\; x\ mod\ a = x - qa$

Пусть d - простое $a \vdots d$

$\Rightarrow a \vdots d$ или $b \vdots d \Rightarrow$ (x mod a ,a) $\geqslant d > 1$

Пусть $a \vdots d$ противоречие ??? $\square$

Теорема Эйлера

Если $(a, m) = 1$, где a, $m \in \mathbb{Z}$,
то $a^{\varphi(m)} \equiv 1$

Доказательство:

Возьмем приведенную систему вычетов(СВ) $mod\ m$
M - приведенная СВ $= \{a_1, a_2, \ldots, a_{\varphi(m)}\}$
$a * M$ - тоже приведенная СВ $= \{aa_1, aa_2, \ldots, aa_{\varphi(m)}\} = \{b_1, b_2, \ldots, b_{\varphi(m)}\} \forall$
$i\ a_i \equiv b_i$
$\prod_i a_i = a_1, a_2, \ldots, a_{\varphi(m)} = A$
$\prod_i b_i = b_1, b_2, \ldots, b_{\varphi(m)} = aa_1, aa_2, \ldots, aa_{\varphi(m)} = a^{\varphi(m)*A}$
$\Rightarrow A \equiv Aa^{\varphi(m)}$
$\Rightarrow 1 \equiv a^{\varphi(m)}$, если $(A, m) = 1$
но $A = a_1, \ldots, a_{\varphi(m)}$, где $(a_i, m) = 1$
$\Rightarrow (A, m) = 1$
$\square$

Следствие 1

Если $p \in \mathbb{P}$
тогда $a^{p-1} \equiv 1$
$\varphi(p) = p - 1$
$(a, p) = 1 \Leftrightarrow a$ не делится нацело на p
(Малая теорема Ферма)

Следствие 2

Если $p \in \mathbb{P}$
$a^p \equiv a$

Доказательство:

1) если a не делится нацело на p
$p^{p-1} \equiv 1 * a$

2) $a \vdots p \Rightarrow a^p \equiv a \equiv 0$

Тесты на простоту

Полная проверка на простоту - вычислительно, но трудно

Вероятностные тесты дают ответ неточно

Ошибаются только, отвечая, что простое. (если тест сказал "составное"$\Rightarrow$ прав)

1. тест Ферма

Дано p. Выбрать случайное a от 1 до p и проверить $a^p \equiv ?1$

Если $\neq 1 \Rightarrow$ точно составное, иначе проверить несколько раз.

Числа Кармайкла - составные, но на них всегда ошибается тест (561 и ∞)