

§5. Некоторые теоретико-числовые приложения комбинаторики

- **Определение 1.**
- **Натуральное число называется простым,** если оно имеет ровно два разных делителя: 1 и само себя.
- **Натуральное число называется составным,** если оно имеет более двух различных делителей.

- **Примеры.** Числа $2, 3, 5, 7, 11$ простые, числа $4, 6, 18, 100$ составные. Отметим, что число 1 не является ни простым, ни составным.
- Существует стандартная система обозначений простых чисел: P_1 – первое по величине простое число (ясно, что $P_1 = 2$),
- P_2 – следующее простое число,
- $(P_2 = 3), (P_3 = 5), (P_4 = 7), (P_5 = 11), (P_6 = 13), (P_7 = 17), (P_8 = 19)$ и т.д.
- Вообще P_n – n -ое простое число.
- К сожалению, не существует аналитической формулы $f(n)$, которая позволила бы вычислять любое простое число P_n .

- **Теорема 2.** Простых чисел существует бесконечно много.
- **Доказательство.** Допустим, существует лишь конечное число простых чисел. Перечислим их:
- P_1, P_2, \dots, P_N .
- Значит, любое другое натуральное число содержит в качестве делителя по крайней мере одно из
- P_i ($i = 1, 2, \dots, N$).
- Рассмотрим число
- $P = P_1 P_2 \dots P_N + 1$.
- Очевидно, что это число не делится ни на одно из чисел

$$P = P_1 \cdot P_2 \cdot \dots \cdot P_N$$

- так как при делении на любое из этих чисел P дает в остатке 1 .
- Значит, допущение о конечности множества простых чисел неверно. Простых чисел существует бесконечно много.
- **Замечание.** По дошедшим до нас историческим источникам это доказательство принадлежит Евклиду и является первым примером в математике доказательства «методом от противного».
- Простые числа являются «кирпичиками» из которых строятся все остальные натуральные и целые числа, отличные от 0 , -1 , 1 .

- **Теорема 3. (основная теорема арифметики).**
Для любого натурального числа $a \neq 1$ имеет место равенство
- $a = P_1^{\alpha_1} \cdot P_2^{\alpha_2} \cdot \dots \cdot P_k^{\alpha_k}$
- для некоторых неотрицательных целых
- $\alpha_1, \alpha_2, \dots, \alpha_k$ и натурального k .
- Правая часть равенства называется разложением числа a в произведение простых чисел. Такое разложение при фиксированной нумерации множества простых чисел единственно.

Пример.

$$10 = 2 \cdot 5 = 2^1 \cdot 3^0 \cdot 5^1, \quad 81 = 3^4 = 2^0 \cdot 3^4,$$

$$200 = 2 \cdot 100 = 8 \cdot 25 = 2^3 \cdot 5^2 = 2^3 \cdot 3^0 \cdot 5^2.$$

- **Определение 4.** Пусть $a, b \in \mathbb{N}$. Число c называется общим делителем a и b , если оба они делятся на c без остатка.
- **Примеры.** Пусть $a = 24$, $b = 36$.
- Тогда общими делителями a и b будут числа $1, 2, 3, 4, 6$ и 12 .
- Число 8 не будет общим делителем чисел 24 и 36 .
- Пусть $a = 10$, $b = 30$.
- Общие делители – $1, 2, 5$.
- Пусть $a = 16$, $b = 35$.
- Общий делитель, равный 1 , единственный.

Теорема 5. Пусть

$$a = P_1^{\alpha_1} \cdot P_2^{\alpha_2} \cdot \dots \cdot P_n^{\alpha_n}$$

и

$$b = P_1^{\beta_1} \cdot P_2^{\beta_2} \cdot \dots \cdot P_n^{\beta_n}$$

- Число ***b*** является делителем ***a*** в том и только в том случае, когда $\beta_i \leq \alpha_i$ для любого $i = 1, \dots, n$.

- **Следствие 6.**

- Пусть для натурального числа a имеет место равенство

$$a = P_1^{\alpha_1} \cdot P_2^{\alpha_2} \cdot \dots \cdot P_n^{\alpha_n}$$

- Тогда число делителей a вычисляется по формуле $(\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdot \dots \cdot (\alpha_n + 1)$.

- Теорема 7. Пусть

$$a = P_1^{\alpha_1} \cdot P_2^{\alpha_2} \cdot \dots \cdot P_n^{\alpha_n}$$

и

$$b = P_1^{\beta_1} \cdot P_2^{\beta_2} \cdot \dots \cdot P_n^{\beta_n}$$

- Тогда число

$$c = P_1^{\gamma_1} \cdot P_2^{\gamma_2} \cdot \dots \cdot P_n^{\gamma_n}$$

- является общим делителем чисел a и b в том и только в том случае, когда

$$\gamma_1 \leq \min(\alpha_1, \beta_1), \gamma_2 \leq \min(\alpha_2, \beta_2), \dots, \gamma_n \leq \min(\alpha_n, \beta_n).$$

- **Определение 8.**
- Число c называется **наибольшим общим делителем** чисел a и b
- (обозначение: $c = \text{НОД}(a, b)$),
- если c является самым большим из всех общих делителей чисел a и b .
- **Примеры.** Пусть $a = 24$, $b = 30$.
- Тогда $\text{НОД}(24, 30) = 6$.
- Если $a = 10$, $b = 33$, то $\text{НОД}(10, 33) = 1$;
- $\text{НОД}(a, a) = a$.
- Пусть $a = 12$, $b = 48$.
- Тогда $\text{НОД}(12, 48) = 12$.

- **Теорема 9.** Пусть a и b натуральные числа,

$$a = P_1^{\alpha_1} \cdot P_2^{\alpha_2} \cdot \dots \cdot P_n^{\alpha_n}$$

$$b = P_1^{\beta_1} \cdot P_2^{\beta_2} \cdot \dots \cdot P_n^{\beta_n}$$

- Тогда **НОД** $(a,b)=$

$$P_1^{\gamma_1} \cdot P_2^{\gamma_2} \cdot \dots \cdot P_n^{\gamma_n}$$

- где $\gamma_i = \min(\alpha_i, \beta_i)$, $i = 1, 2, 3, \dots, n$.

- **Следствие 10.**
- Любой общий делитель чисел a и b является также делителем НОД (a, b) .
- **Определение 11.**
- Число a называется кратным числу b ($a, b \in \mathbb{N}$), если a делится на b или, что тоже самое, b есть делитель a .
- Тот факт, что a делится на b , будет обозначать как $b \mid a$.

- **Пример.** Пусть $b = 3$.
- Тогда кратным ему будут числа $3, 6, 9, 12, \dots$.
Их можно описать общей формулой
$$a = 3n \quad (n \in \mathbb{N}).$$
- Этот пример показывает, что в отличие от делителей, количество кратных любому натуральному числу b бесконечно.

- **Определение 12.**

- Если число a делится на число b и c , то a называется общим кратным чисел b и c .

- **Примеры.**

- Если $b = 6$, $c = 8$, то общее кратное этих чисел равно 24 .

- Также общими кратными являются числа $48, 72, \dots$.

- **Теорема 13.** Пусть,

$$c = P_1^{\gamma_1} \cdot P_2^{\gamma_2} \cdot \dots \cdot P_n^{\gamma_n}$$

$$b = P_1^{\beta_1} \cdot P_2^{\beta_2} \cdot \dots \cdot P_n^{\beta_n}$$

- Тогда число

$$a = P_1^{\alpha_1} \cdot P_2^{\alpha_2} \cdot \dots \cdot P_n^{\alpha_n}$$

- является общим кратным чисел b и c тогда и только тогда, когда
- $\alpha_1 \geq \max(\beta_1, \gamma_1)$, $\alpha_2 \geq \max(\beta_2, \gamma_2)$, ..., $\alpha_n \geq \max(\beta_n, \gamma_n)$.

Доказательство.

Пусть a – общее кратное b и c .

Так как a делится на b , то

$$\alpha_i \geq \beta_i, \quad i = 1, 2, 3, \dots, n.$$

Так как a делится на c , то

$$\alpha_i \geq \gamma_i, \quad i = 1, 2, 3, \dots, n.$$

Так как $\alpha_i \geq \beta_i$ и $\alpha_i \geq \gamma_i$, то $\alpha_i \geq \max(\beta_i, \gamma_i)$.

Докажем

в другую сторону.

Так как $\alpha_i \geq \max(\beta_i, \gamma_i)$, то $\alpha_i \geq \beta_i$

для каждого $i = 1, 2, 3, \dots, n$,

значит a делится на b .

Аналогично, a делится на c , то есть

a – общее кратное b и c .

- **Определение 14.**
- **Самое маленькое** из всех общих кратных натуральных чисел b и c называется **наименьшим общим кратным** b и c и обозначается **НОК** (b, c) .
- **Примеры.**
- $\text{НОК}(3, 5) = 15,$ $\text{НОК}(4, 6) = 12,$
- $\text{НОК}(36, 64) = 576,$ $\text{НОК}(2, 8) = 8,$
- $\text{НОК}(a, a) = a,$ $\text{НОК}(1, a) = a.$

- Теорема 15. Пусть

$$b = P_1^{\beta_1} \cdot P_2^{\beta_2} \cdot \dots \cdot P_n^{\beta_n}$$

$$c = P_1^{\gamma_1} \cdot P_2^{\gamma_2} \cdot \dots \cdot P_n^{\gamma_n}$$

- Число

$$a = P_1^{\alpha_1} \cdot P_2^{\alpha_2} \cdot \dots \cdot P_n^{\alpha_n}$$

- является НОК (b, c) в том и только в том случае, когда
- $\alpha_i = \max(\beta_i, \gamma_i), i = 1, 2, 3, \dots, n$

- **Следствие 16.**
- Любое общее кратное чисел b и c делится на $\text{НОК}(b, c)$.

- **Лемма 17.** Для любых чисел x, y
- $\max(x, y) + \min(x, y) = x + y$.

- **Доказательство.** Рассмотрим три случая:
- 1) $x = y$, тогда
- $\max(x, y) = x$, $\min(x, y) = x$, ПОЭТОМУ
 $\max(x, y) + \min(x, y) = 2x$ и $x + y = 2x$;
- 2) $x > y$, тогда
- $\max(x, y) = x$, $\min(x, y) = y$,
- следовательно
 $\max(x, y) + \min(x, y) = x + y$;
- 3) $x < y$, тогда
- $\max(x, y) = y$, $\min(x, y) = x$,
- ПОЭТОМУ $\max(x, y) + \min(x, y) = y + x = x + y$.

- **Теорема 18.**

- Для любых натуральных чисел b и c

$$\text{НОД}(b, c) \cdot \text{НОК}(b, c) = b \cdot c.$$

- **Доказательство.** Пусть

$$b = P_1^{\beta_1} \cdot P_2^{\beta_2} \cdot \dots \cdot P_n^{\beta_n}$$

и

$$c = P_1^{\gamma_1} \cdot P_2^{\gamma_2} \cdot \dots \cdot P_n^{\gamma_n}$$

- Тогда

$$b \cdot c = P_1^{\beta_1 + \gamma_1} \cdot P_2^{\beta_2 + \gamma_2} \cdot \dots \cdot P_n^{\beta_n + \gamma_n}$$

- $\text{НОД}(b, c) \cdot \text{НОК}(b, c) =$

$$= P_1^{\min(\beta_1, \gamma_1) + \max(\beta_1, \gamma_1)} \cdot \dots \cdot P_n^{\min(\beta_n, \gamma_n) + \max(\beta_n, \gamma_n)}$$

$$= P_1^{\beta_1 + \gamma_1} \cdot \dots \cdot P_n^{\beta_n + \gamma_n} =$$

$$= b \cdot c$$

- **Определение 19.** Числа a и b называются *взаимно простыми*, если $\text{НОД}(a, b) = 1$. Другими словами, если a и b не имеют общих делителей, отличных от 1 .
- **Примеры.**
 - $3, 8$ – взаимно просты,
 - $1, 5$ взаимно просты,
 - $4, 6$ – не взаимно просты.

- **Определение 20.**
- **Функцией Эйлера $\varphi(n)$** называется количество чисел меньших, либо равных n , которые взаимно просты с n .
- **Примеры.**
- **1) $\varphi(12) = 4$.**
- Перечислим все числа ≤ 12 и взаимно простые с 12: 1, 5, 7, 11;
- **2) $\varphi(36) = 12$.**
- Перечислим все необходимые числа: 1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35;
- **3) $\varphi(7) = 6$.**

- Теорема 21.

- Пусть

- $n = P_{k_1}^{\alpha_1} \cdot P_{k_2}^{\alpha_2} \cdot \dots \cdot P_{k_m}^{\alpha_m}$,

- причем $\alpha_i > 0$ и $k_i \neq k_j$ ($i \neq j$),

- $i, j = 1, 2, \dots, m$. Тогда

$$\varphi(n) = n \cdot \left(1 - \frac{1}{P_1}\right) \cdot \left(1 - \frac{1}{P_2}\right) \cdot \dots \cdot \left(1 - \frac{1}{P_m}\right)$$

- **Примеры.**

- 1) $n=56=2^3 7^1,$

$$\varphi(56) = 56\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{7}\right) = 4 \cdot 1 \cdot 6 = 24;$$

- 2) $n=16=2^4,$

$$\varphi(16) = 16\left(1 - \frac{1}{2}\right) = 8;$$

- 3) $\varphi(11) = 11\left(1 - \frac{1}{11}\right) = 10.$