§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: $\boldsymbol{P_1}$ – первое по величине простое число (ясно, что $\boldsymbol{P_1 = 2}$),
- $\boldsymbol{P_2}$ – следующее простое число,
- $\boldsymbol{(P_2 = 3), (P_3 = 5), (P_4 = 7), (P_5 = 11), (P_6 = 13), (P_7 = 17), (P_8 = 19)}$ и т.д.
- Вообще $\boldsymbol{P_n}$ – n-ое простое число.
- К сожалению, не существует аналитической формулы $f(n)$, которая позволила бы вычислять любое простое число $\boldsymbol{P_n}$.

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

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

- 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*.

- **Теорема3. (основная теорема арифметики).** Для любого натурального числа $\boldsymbol{a \neq 1}$ имеет место равенство
- $\boldsymbol{a} = \quad P_1^{\alpha_1} \cdot P_2^{\alpha_2} \cdot \ldots \cdot P_k^{\alpha_k}$
- для некоторых неотрицательных целых
- $\boldsymbol{\alpha_1, \alpha_2, \ldots, \alpha_k}$ и натурального $\boldsymbol{k}$.
- Правая часть равенства называется разложением числа *a* в произведение простых чисел. Такое разложение при фиксированной нумерации множества простых чисел единственно.

Пример.

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

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

- **Определение 4.** Пусть $a,b \in N$. Число $\boldsymbol{c}$ называется общим делителем a и b , если оба они делятся на $\boldsymbol{c}$ 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

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

и

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

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

- **Следствие 6.**
- Пусть для натурального числа ***a*** имеет место равенство

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

- Тогда число делителей ***a*** вычисляется по формуле $\boldsymbol{(\alpha_1 + 1) \cdot (\alpha_2 + 1) \cdot \ldots \cdot (\alpha_n + 1)}$.

- **Теорема 7.** Пусть

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

и

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

- Тогда число

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

- является общим делителем чисел a и b в том и только в том случае, когда
- $\gamma_1 \le \min(\alpha_1, \beta_1), \gamma_2 \le \min(\alpha_2, \beta_2), \ldots, \gamma_n \le \min(\alpha_n, \beta_n)$.

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

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

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

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

- Тогда **НОД *(a,b)*=**

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

- где $\boldsymbol{\gamma_i = \min(\alpha_i, \beta_i)}$, $\boldsymbol{i = 1, 2, 3, \ldots, n}$.

- **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 N),*** если ***a*** делится на ***b*** или, что тоже самое, ***b*** есть делитель ***a***.
- Тот факт, что ***a*** делится на ***b***, будет обозначать как $b|a$.

- **Пример**. Пусть $b = 3$.
- Тогда кратным ему будут числа $3, 6, 9, 12, \ldots$. Их можно описать общей формулой

  $a = 3n \ (n \in N)$.
- 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*, …** .

- **Теорема 13.** Пусть,

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

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

- Тогда число

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

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

Доказательство.

Пусть ***a – общее кратное b и c***.

Так как ***a*** делится на ***b***, то

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

Так как ***a*** делится на ***c***, то

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

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 $i = 1, 2, 3, \ldots, n$,

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.**
- НОК $(3, 5) = 15$, НОК $(4, 6) = 12$,
- НОК $(36, 64) = 576$, НОК $(2, 8) = 8$,
- НОК $(a, a) = a$, НОК $(1, a) = a$.

- **Теорема 15**. Пусть

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

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

- Число

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

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

- **Следствие 16.**
- Любое общее кратное чисел b и c делится на НОК(b, c).

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

- **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

НОД *(b, c)* · НОК *(b, c)* = *b* · *c*.

- **Доказательство.** Пусть

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

и

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

- Тогда

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

- НОД(b,c)*НОК(b,c) =

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

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

$$= b \cdot c$$

- **Определение 19.** Числа a и b называются ***взаимно простыми***, если **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*** *φ (n)* называется **количество чисел меньших**, либо равных *n*, которые взаимно просты с *n*.
- **Примеры.**
- *1)* ***φ (12) = 4***.
- Перечислим все числа ≤ *12* и взаимно простые с *12: 1,5, 7, 11;*
- *2)* ***φ(36) = 12***.
- Перечислим все необходимые числа: *1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 31, 35;*
- *3)* ***φ(7) = 6***.

- **Теорема 21**.
- Пусть
- $n = P_{k_1}^{\alpha_1} \cdot P_{k_2}^{\alpha_2} \cdot \ldots \cdot P_{k_m}^{\alpha_m}$,
- причем $\alpha_i > 0$ и $k_i \neq k_j$ $(i \neq j)$,
- $i, j = 1, 2, \ldots, n$. Тогда

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

- **Примеры.**
- 1) $n=56=2^3 7^1$,

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

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

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

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