Элементы теории чисел

Лектор: Королев Максим Александрович

7 октября 2024 г.

Конспект: Кирилл Яковлев, 108 группа tg: @fourkenz

Содержание

Введение. Следующие понятия считаются интуитивно ясными:

1. Понятие натурального ряда $\mathbb{N} = \{1, 2, 3, 4, 5, \dots\}$.
2. У каждого натурального числа n существует единственное натуральное число $m = n + 1$ следующее за ним.
3. Понятие отрицательных чисел и нуля.
4. Понятие суммы, разности и произведения двух целых чисел.

Аксиома. Если $M \subset \mathbb{N}$ обладает следующими свойствами: $(1 \in M)$ и $(\forall n \in M$ выполнено $n + 1 \in M)$, то $M = \mathbb{N}$.

Следствие 1. Всякое непустое подмножество натурального ряда содержит минимальный элемент.

Следствие 2. Всякое непустое конечное подмножество натурального ряда содержит максимальный элемент.

Следствие 3. (Принцип математической индукции)
Если известно, что некоторое утверждение о натуральных числах выполнено для натурального числа a, а также из предположения о том, что утверждение верно при некотором n следует справедливость этого утверждения и для числа $n+1$, то это утверждение верно для всех натуральных чисел, больше или равных a.

1 Делимость целых чисел

Определение 1.1. Пусть $a, b \in \mathbb{N}, b \neq 0$. Говорят что a делится на b, если существует $c \in \mathbb{Z}$, такое, что $a = bc$.

Замечание. a называется делимым, а b называется делителем числа a. Запись $b \mid a$ означает, что b делит a. Если b не делит a, то пишут $b \nmid a$.

Лемма 1.1. Пусть $a, b, c \in \mathbb{Z}$, тогда:

1. $1 \mid a$.
2. $a \neq 0 \Rightarrow a \mid a$.
3. $a \mid b \Rightarrow a \mid bc$.
4. $a \mid b$ и $b \mid c \Rightarrow a \mid c$.

5. $a \mid b$ и $a \mid c \Rightarrow a \mid (b + c)$.

6. $a \mid b$ и $b \neq 0 \Rightarrow |a| \leq |b|$.

Теорема 1.1. Если $a \in \mathbb{Z}, b \in \mathbb{N}$, то существует единственная пара целых чисел q и r, такие, что $a = bq + r$, где $0 \leq r \leq b - 1$.

Доказательство. Докажем существование: Если a делится на b, то $a = bc$. В таком случае возьмем $q = c, r = 0$. Теперь пусть a не делится на b. Рассмотрим непустое множество M натуральных чисел, представимых в виде $a - kb, k \in \mathbb{Z}$, возьмем $k = -(|a| + 1)$, тогда $a - kb = b(|a| + 1) + a \geq b(|a| + 1) - |a| \geq 1 \cdot (|a| + 1) - |a| = 1 \Rightarrow a - kb$ - натуральное. Значит, у M есть минимальный элемент $a - kb$. Возьмем $q = k, r = a - kb = a - bq > 1$. Осталось показать, что $0 \leq r \leq b - 1$. Предположим, что $r \geq b$. Если $r = b$, то $a = bq + b = b(q + 1)$ получаем противоречие, так как a не делится на b. Значит, $r = b + m, m \geq 1$. Получаем $1 \leq m = r - b < r$, при этом $a = bq + r = bq + b + m = b(q + 1) + m \Rightarrow m = a - b(q + 1) \Rightarrow m \in M$ и $m < r$, получаем противоречие, так как a не делится на b. Доказано, что $r < b \Rightarrow$ представление $a = bq + r$ - искомое. Докажем единственность: предположим, что для некоторого a и b имеются пары чисел с указанным свойством: q, r и q_1, r_1, причем $0 \leq r \leq r_1 \leq b - 1$. Тогда $a = bq + r = bq_1 + r_1 \Rightarrow 0 \leq b(q - q_1) = r_1 - r$. Значит, b делит разность $r_1 - r$. Допустим, что $q \neq q_1$, тогда по пункту 6 леммы 1.1 получаем $b \leq r_1 - r$ и в то же время $r_1 - r \leq b - 1 < b$. Получаем противоречие, поэтому $q = q_1$, следовательно, и $r = r_1$. □

2 Наименьшее общее кратное и наибольший общий делитель (НОК и НОД)

Определение 2.0. $n \geq 2, a_1, \ldots, a_n \in \mathbb{N}$ пусть натуральное число k делится на каждое из этих чисел. Тогда k - общее кратное чисел $a_1, \ldots, a_n$.
Пусть $a_1, \ldots, a_n$ - целые числа не все равные нулю. Натуральное число d называется общим делителем $a_1, \ldots, a_n$, если d делит каждое из этих чисел.

Замечание. Множество таких k непусто, в нем лежит, например, произведение всех этих чисел.
Множество таких d конечно: если $a_i \neq 0$, то d находится среди делителей числа a_i, (по пункту 6 леммы 1.1) $d \leq |a_i|$, значит числа d образуют конечное множество, оно непусто, так как содержит единицу.

Определение 2.1. Наименьшее натуральное число, делящееся на каждое из чисел $a_1, \ldots, a_n$, называют их наименьшим общим кратным, его обозначают $[a_1, \ldots, a_n]$.

Теорема 2.1. Каждое общее кратное натуральных чисел $a_1, \ldots, a_n$ делится на их НОК.

Доказательство. Пусть M - общее кратное $a_1, \ldots, a_n$, $K = [a_1, \ldots, a_n]$. Поделим M на K с остатком: $M = kq + r, 0 \leq r \leq k - 1 \leq k$. Допустим, что $K \neq 0$. По определению, всякое число a_i делит оба числа M и $K \Rightarrow a_i$ делит разность $k = M - qK$, значит k является общим кратным для $a_1, \ldots, a_n$, но $k < K$, получаем противоречие, так как какое-то кратное оказалось меньше минимального. Значит, $k = 0$ и $M = qK$. □

Определение 2.2. Наибольшее из натуральных чисел d, делящих каждое из чисел $a_1, \ldots, a_n$, называют наибольшим общим делителем $a_1, \ldots, a_n$, его обозначают $(a_1, \ldots, a_n)$.

Определение 2.3. Числа a и b называется взаимно простыми, если $(a, b) = 1$. Числа $a_1, \ldots, a_n$ называются взаимно простыми в совокупности, если $(a_1, \ldots, a_n) = 1$. Числа $a_1, \ldots, a_n$ попарно взаимно просты, если $(a_i, a_j) = 1$ $\forall i, j : 1 \leq i < j \leq n$.

Теорема 2.2. $[a, b] \cdot (a, b) = ab, \forall a, b \in \mathbb{N}$.

Доказательство. ab - общее кратное a и b. По теореме 2.1 ab делится на $[a, b]$, то есть $ab = c[a, b]$, где $c \geq 1$ - натуральное число. Покажем, что a и b делятся на c. Действительно, $a = \frac{ab}{[a,b]} \cdot \frac{[a,b]}{b} = c \cdot \frac{[a,b]}{b}$, $b = \frac{ab}{[a,b]} \cdot \frac{[a,b]}{a} = c \cdot \frac{[a,b]}{a}$, но оба числа $\frac{[a,b]}{a}$ и $\frac{[a,b]}{b}$ - натуральные, значит c - общий делитель a и b. Пусть теперь d - произвольный общий делитель a и b, тогда $\frac{ab}{d} = a \cdot \frac{b}{d}$, то есть число $\frac{ab}{d}$ делится нацело на каждое из чисел a и b. По теореме 2.1, оно делится на $[a, b]$, то есть $\frac{ab}{d} = [a, b]m$, где $m \geq 1$ - натуральное число, но тогда $\frac{ab}{[a,b]} = c = dm$, то есть d делит c. В силу пункта 6 леммы 1.1 $d \leq c$, значит $c = (a, b)$. □

Теорема 2.3. Пусть $a, b, c \in \mathbb{N}$, причем $a \mid bc$ и $(a, b) = 1$, тогда $a \mid c$.

Доказательство. $(a, b) = 1 \Rightarrow$ (по теореме 2.2) bc делится нацело на $[a, b] = ab$, то есть $bc = abm$, где $m \geq 1$ - натуральное число. Сократим обе части на b, получим $c = am$. □

Теорема 2.4. Пусть $\Delta = (a, b) \geq 1 \Rightarrow (\frac{a}{\Delta}, \frac{b}{\Delta}) = 1$.

Доказательство. Пусть $m \in \mathbb{N}$ и $m \mid \frac{a}{\Delta}, m \mid \frac{b}{\Delta}$ предположим, что $m > 1 \Rightarrow cm = \frac{a}{\Delta}, dm = \frac{b}{\Delta} \Rightarrow \Delta cm = a, \Delta dm = b \Rightarrow \Delta m \mid a$ и $\Delta m \mid b \Rightarrow \Delta m$ - общий делитель a и b. Но т.к. $m > 1$, то $\Delta m > \Delta \Rightarrow \Delta = (a, b) \leq \Delta m$ - противоречие, поскольку Δ - НОД $\Rightarrow m = 1 \Rightarrow (\frac{a}{\Delta}, \frac{b}{\Delta}) = 1$. □

3 Алгоритм Евклида

Лемма 3.1. Пусть $a \in \mathbb{Z}, b \in \mathbb{N}$ и $b \mid a$. Тогда $(a, b) = b$.

Доказательство. Пусть $(a, b) = c \Rightarrow c \mid b \Rightarrow$ (по лемме 1.1) $c \leq b$, но $b \mid a$, $b \mid b \Rightarrow b$ - общий делитель a и $b \Rightarrow b \leq c \Rightarrow b = c = (a, b)$. □

Лемма 3.2. Пусть $a \in \mathbb{Z}, b \in \mathbb{N}, a = bq + r : r, q \in \mathbb{Z}, r \geq 0$. Тогда $(a, b) = (b, r)$.

Доказательство. Пусть $\Delta = (a, b), \delta = (b, r)$. Имеем $\delta \mid b \Rightarrow \delta \mid bq, \delta \mid r \Rightarrow$ (лемма 1.1) $\delta \mid bq + r = a \Rightarrow \delta \mid a, \delta \mid b \Rightarrow \delta$ - общий делитель a и $b \Rightarrow \delta \leq \Delta$. $\Delta \mid b, \Delta \mid bq, \Delta \mid a \Rightarrow$ (лемма 1.1) $\Delta \mid a - bq = r \Rightarrow \Delta$ - общий делитель b и $r \Rightarrow \Delta \leq \delta \Rightarrow \Delta = \delta$. □

Алгоритм. Получаем, что при поиске НОД a и b, (a, b) можно заменять любой парой $(b, r) = (b, a - bq), q \in \mathbb{Z}$. Положим $r_0 = a, r_1 = b$.
Выполняем деление с остатком:

$$r_0 = r_1 q_1 + r_2, 0 < r_2 < r_1 \Rightarrow (r_0, r_1) = (r_1, r_2)$$
$$r_1 = r_2 q_2 + r_3, 0 < r_3 < r_2 \Rightarrow (r_1, r_2) = (r_2, r_3)$$
$$r_2 = r_3 q_3 + r_4, 0 < r_4 < r_3 \Rightarrow (r_2, r_3) = (r_3, r_4)$$
$$\vdots$$
$$r_{n-2} = r_{n-1} q_{n-1} + r_n, 0 < r_n < r_{n-1} \Rightarrow (r_{n-2}, r_{n-1}) = (r_{n-1}, r_n)$$
$$r_{n-1} = r_n q_n$$
$$\Rightarrow \text{(лемма 3.1)}(r_{n-1}, r_n) = r_n \Rightarrow (a, b) = r_n$$

4 Решение в целых числах линейного уравнения с двумя неизвестными

Рассмотрим уравнение $(*)$ $ax + by = c$, такое, что $a, b, c \in \mathbb{Z}, a$ и b не равняются нулю одновременно. $x, y \in \mathbb{Z}$ - неизвестные.

Теорема 4.1. (1) Уравнение $(*)$ разрешимо $\Leftrightarrow \Delta = (a,b) \mid c$.
(2) В случае разрешимости, множество решений этого уравнения бесконечно, все решения имеют вид $x = x_0 + \frac{b}{\Delta}t, y = y_0 - \frac{a}{\Delta}t$, где x_0, y_0 - произвольное решение, а $t \in \mathbb{Z}$.

Доказательство. Докажем первый пункт:

($\Rightarrow$) Если x, y - решение, то $\Delta \mid ax, \Delta \mid by \Rightarrow$ (лемма 1.1) $\Delta \mid ax + by \Rightarrow \Delta \mid c$.

($\Leftarrow$) Не теряя общности, можем считать, что $a \geq b \geq 0$. Доказываем индукцией по сумме $a + b$.
База: $a + b = 1 \Rightarrow b = 0$ и $a = 1 \Rightarrow$ уравнение имеет вид $ax = c \Rightarrow x = c$. Можем предъявить решение $x = c, y = 0$. В этом случае $\Delta = (1,0) \mid 1$.
Шаг: $n \geq 1$, считаем, что утверждение доказано для всех уравнений с условием $a \geq b \geq 0$, $1 \leq a + b \leq n$. Пусть $ax + by = c$, где $a \geq b \geq 0$, $a + b = n + 1$ и $\Delta = (a,b) \mid c \Rightarrow$ докажем, что есть хотя бы одно решение. Пусть $b = 0, ax = c, \Delta = (a,0) = a, a \mid c \Rightarrow c = am \Rightarrow x = m, y = 0$ - решение. Пусть $b \geq 1$. Рассмотрим уравнение $(a-b)X + bY = c$, $a-b \geq 0, b \geq 1 > 0$. $(a-b)+b = (a+b)-b = n+1-b \leq n$. $(a-b,b) = (a,b) \mid c$ $\Rightarrow$ по предположению индукции есть целочисленное решение X_0, X_0. $(a-b)X_0 + bY_0 = c \Rightarrow aX_0 - b(Y_0 - X_0) = c \Rightarrow x = X_0, y = Y_0 - X_0$ - решение.
Докажем второй пункт (проверим, что x_0, y_0 - решение): $a(x_0 + \frac{b}{\Delta}t) + b(y_0 - \frac{a}{\Delta}t) = ax_0 + \frac{ab}{\Delta}t + ay_0 - \frac{ab}{\Delta}t = ax_0 + by_0$. Обратно: пусть x_0, y_0 и x, y - различные решения. $ax_0 + by_0 = c, ax + by = c$
$\Rightarrow a(x - x_0) + b(y - y_0) = 0 \Rightarrow a(x - x_0) = b(y_0 - y)$. $\Delta = (a,b)$
$\Rightarrow a = \alpha\Delta, b = \beta\Delta \Rightarrow$ (теорема 2.4) $(\alpha, \beta) = 1$
$\Rightarrow \alpha\Delta(x - x_0) = \beta\Delta(y_0 - y) \Rightarrow \alpha(x - x_0) = \beta(y_0 - y)$
$\Rightarrow \alpha \mid \beta(y_0 - y) \Rightarrow \alpha \mid (y_0 - y) \Rightarrow y_0 - y = \alpha t \Rightarrow \alpha(x - x_0) = \beta\alpha t$
$\Rightarrow x - x_0 = \beta t$.

□

5 Простые числа

Определение 5.1. Натуральное число $n > 1$ называется простым, если оно имеет ровно два делителя: 1 и n. В противном случае это число называется составным.

Замечание. Единица не причисляется ни к простым, ни к составным.

Лемма 5.1. Наименьший делитель натурального числа $n > 1$, отличный от единицы - простое число.

Доказательство. Пусть $d \mid n, 1 < d \leq n$, и d - наименьший с этими свойствами. Пусть d - составное. Тогда $\exists k : k \mid d$ и $1 < k < d$. По лемме 1.1 $k \mid n$, но $1 < k < d$ - противоречие с тем, что d - минимальный. □

Теорема 5.1. Множество простых чисел бесконечно.

Доказательство. Пусть множество простых конечно: $p_1 < p_2 < \cdots < p_n$ - все простые числа. Рассмотрим число $N = p_1 p_2 \dots p_n + 1$. По лемме 5.1 наименьший делитель $p > 1$ числа N - простое число. Но p отлично от $p_1 \dots p_k, p$ делит N нацело, а N при делении на каждое из $p_1 \dots p_n$ дает остаток 1 - противоречие. □

Пусть $x > 0$, через $\pi(x)$ обозначим количество простых чисел на отрезке $[0, x]$ ($\pi(x)$ - количество простых чисел не превосходящих x).

$$\pi(x) = \sum_{p \leq x} 1$$

(Теорема 5.1) $\Leftrightarrow \pi(x)$ - не ограничена сверху $\Leftrightarrow \pi(x) \to +\infty$ при $x \to +\infty$.
Гипотеза Лежандра: $\pi(x) = \frac{x}{\ln x - C}$, где $C = 1,08366$. Позднее Гаусс выдвинет более сложное и более точное предположение. Из доказательства теоремы Чебышева: $\forall \varepsilon > 0 \exists x_0 = x_0(\varepsilon)$, т.ч. $\forall x \geq x_0$ выполнено неравенство:

$$(A - \varepsilon)\frac{x}{\ln x} < \pi(x) < (B + \varepsilon)\frac{x}{\ln x}$$

$$A = \ln\left(\frac{2^{\frac{1}{2}}\ 3^{\frac{1}{3}}\ 5^{\frac{1}{5}}}{30^{\frac{1}{30}}}\right), B = \frac{6}{5}A$$

Асимптотический закон распределения простых чисел:

$$\lim_{x \to +\infty}\left(\frac{\pi(x)}{\frac{x}{\ln x}}\right) = 1 \Leftrightarrow A = B = 1 \Leftrightarrow \pi(x) = (1 + \bar{\bar{o}}(1))\frac{x}{\ln x}$$

Лемма 5.2. Пусть N - составное число, p - наименьший простой делитель. Тогда $p \leq \sqrt{N}$.

Доказательство. N - составное $\Rightarrow \exists a, b : 1 < a < N, 1 < b < N$ и $ab = N$. Значит $a \mid N, b \mid N, p$ - наименьший $\Rightarrow p \leq a, p \leq b \Rightarrow p^2 \leq ab = N$
$\Rightarrow p \leq \sqrt{N}$. □

Решето Эратосфена. Выписываем все числа от 2 до N, первое число в таблице - простое, это 2. Вычеркиваем все числа кратные 2, кроме нее самой. Первое невычеркнутое число после 2 - это 3 - значит оно простое. Вычеркиваем все числа, кратные 3, кроме самой 3. Первое невычеркнутое число после 3 - простое и т.д. После того как найдено наибольшее простое p не превосходящее $\sqrt{N}$ и вычеркнуты все числа кратные p, в таблице останутся лишь простые числа, не превосходящие N и только они.

Теорема 5.2. (Основная теорема арифметики)
Каждое целое число, большее 1, раскладывается в произведение простых чисел, притом единственным способом (с точностью до порядка сомножителей).

Доказательство. Существование:
Индукция по $n > 1$. Числа $n = 2, n = 3$ - простые, для них это утверждение справедливо. Пусть $n > 3$, и допустим, что справедливость утверждения проверена для всех $m < n$. Если n - простое, то утверждение очевидно. Пусть n - составное. По лемме 5.1 его наименьший делитель - простое число $\Rightarrow n = p_1 k$, но $k = \frac{n}{p_1} \leq \frac{n}{2} < n$. По предположению индукции $k = p_2 \dots p_r$, где $p_2, \dots, p_r$ - простые. $\Rightarrow n = p_1 k = p_1 p_2 \dots p_r$ - искомое разложение.
Единственность:
Пусть $n = p_1 \dots p_r = q_1 \dots q_s$, где p_i, q_i - простые числа и $r \leq s$. Тогда
$p_1 \dots p_r = q_1 a_1$, где $a_1 = q_2 \dots q_s \Rightarrow p_1 \mid q_1 a_1$. Возможно два случая:
1) $(p, q) > 1 \Rightarrow p_1 = q_1$.
2) $(p, q) = 1 \Rightarrow$ (теорема 2.3) $p_1 \mid a_1 = q_2 \dots q_s, a_1 = q_2 a_2, a_2 = q_3 \dots q_s$,
$p_1 \mid q_2 a_2 \Rightarrow$ либо $p_1 = q_2$, либо $p_1 \mid a_2$ и т.д. Но $a_1 > a_2 > \dots \geq 1 \Rightarrow$ на одном из шагов обязательно будет иметь место равенство $p_1 = q_k, k \leq s$ (иначе оказалось бы, что $p_1 \mid 1$, а это невозможно). Итак, p_1 совпадает с одним из чисел $q_1, \dots, q_s$. Будем считать, что $p_1 = q_1 \Rightarrow p_2 \dots p_r = q_2 \dots q_s$ продолжаем рассуждение и получаем, что p_2 совпадает с одним из $q_2, \dots q_s$, пусть $p_2 = q_2$ и т.д. Если $r < s$ после r шагов получили бы противоречивое равенство: $1 = q_{r+1} \dots q_s$
$\Rightarrow r = s$ и множества $\{p_1, \dots, p_r\}$ и $\{q_1, \dots, q_s\}$ совпадают. □

Замечание. $n > 1, n = q_1 \dots q_s \Rightarrow n$ можно записать в виде $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}$, $p_1 < p_2 < \dots < p_k$ - каноническое разложение n на простые сомножители.

Определение 5.2. Пусть $n = p_1^{\alpha_1} \dots p_k^{\alpha_k}, p$ - простое. Тогда

$$\nu_p(n) = \begin{cases} 0, \text{ если } p \nmid n, \\ \alpha, \text{ если} p = p_i. \end{cases}$$

Лемма 5.3. (Свойства $\nu_p(n)$)

1. Для любых целых чисел $a, b > 1$ и любого простого p справедливо равенство: $\nu_p(ab) = \nu_p(a) + \nu_p(b)$.
2. Пусть $m, n > 1$ - целые числа, тогда $m \mid n \Leftrightarrow \nu_p(m) \leq \nu_p(n)$ для любого простого p.

Доказательство.

1. При перемножении степеней с одинаковыми основаниями, их показатели складываются.
2. ($\Rightarrow$) Пусть $n = km \Rightarrow \nu_p(n) = \nu_p(k) + \nu_p(m) \geq \nu_p(m)$.

   ($\Leftarrow$) Все разности $\nu_p(n) - \nu_p(m)$ - целые неотрицательные. Рассмотрим число:

   $$k = \prod_p p^{\nu_p(n) - \nu_p(m)}$$

   Если $k = 1$, то $\nu_p(n) = \nu_p(m)$ для всех p и $m = n$. В силу основной теоремы арифметики, в этом случае $m \mid n$. Пусть $k > 1$, тогда в силу пункта 1:

   $$km = \prod_p p^{\nu_p(n) - \nu_p(m)} \cdot \prod_p p^{\nu_p(m)} = \prod_p p^{\nu_p(n)} = n$$

   то есть $m \mid n$.

□

Лемма 5.4. Для любых $a, b \in \mathbb{N}$ справедливы равенства:

$$[a, b] = \prod_p p^{\max(\nu_p(a), \nu_p(b))}$$

$$(a, b) = \prod_p p^{\min(\nu_p(a), \nu_p(b))}$$

Доказательство. Обозначим $K = [a, b]$, $N = \prod_p p^{\max(\nu_p(a), \nu_p(b))}$ поскольку $\nu_p(a) \leq \nu_p(N)$, $\nu_p(b) \leq \nu_p(N)$, то a и b делят N в силу леммы 5.3. Значит N - общее кратное чисел a и b. С другой стороны, поскольку a и b делят K, то по лемме 5.3 имеем $\nu_p(a) \leq \nu_p(K), \nu_p(b) \leq \nu_p(K)$, так что $\nu_p(K) \geq \max(\nu_p(a), \nu_p(b)) = \nu_p(N)$ для любого простого p. Значит, $N \mid K$, но $N \leq K \Rightarrow N = K$. Вторая часть утверждения следует из первой, если воспользоваться равенством

$$(a, b) = \frac{ab}{[a, b]}$$

и тем, что $x + y = \max(x, y) + \min(x, y)$ $\forall x, y \in \mathbb{R}$. □

6 Мультипликативные функции

Обозначения и пояснения:

1. Обозначение $\sum\limits_{d|n} f(d)$ - сумма значений функции f по всем делиителям d числа n.

2. Двойная сумма вычисляется следующим образом:

$$\sum_{m=1}^{M}\sum_{n=1}^{N} g(mn) = \sum_{n=1}^{N} g(1,n) + \sum_{n=1}^{N} g(2,n) + \cdots + \sum_{n=1}^{N} g(M,n)$$

Определение 6.1. Функция f, определенная на множестве $\mathbb{N}$ называется мультипликативной, если для любых взаимно простых $a, b \in \mathbb{N}$ выполнено равенство:

$$f(ab) = f(a)f(b)$$

Теорема 6.1. (Простейшие свойтсва мультипликативных функций)
Пусть f, g - мультипликативные функции. Тогда:

1. Если $f \not\equiv 0$, то $f(1) = 1$.

2. Если $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ - каноническое разложение n, то $f(n) = f(p_1^{\alpha_1}) \dots f(p_r^{\alpha_r})$.

3. Функция h, определенная для любого $n \in \mathbb{N}$ равенством $h(n) = f(n)g(n)$ - мультипликативна.

Доказательство. Так как $f \not\equiv 0$, то $\exists a \in \mathbb{N} : f(a) \neq 0$. Тогда $f(a) = f(a \cdot 1) = f(a)f(1) \Rightarrow f(1) = 1$. □

Для исседование дальнейших свойств мультипликативных функций потребуется несколько вспомогательных лемм

Лемма 6.1. Пусть $r \geq 2$ и пусть целые числа $a_1, \dots, a_r$ попарно взаимно просты. Тогда найдется номер $1 \leq s \leq r$ такой, что $p \mid a_s$.

Доказательство. Индукция по r. Если $r = 2$, то это есть очевидно следствие теоремы 2.3. Пусть $m \geq 3$ и утверждение доказано для всех $r \leq m-1$. Пусть $a_1, \dots a_m$ попарно взаимно просты и $p \mid a_1 \cdot \dots \cdot a_m$. Полагая $a = a_1 \cdot \dots \cdot a_{m-1}$ будем иметь: $p \mid aa_m$. Если $(p, a) = 1$, то $p \mid a_m$ по теореме 2.3. Пусть $(p, a) > 1$. Так как p - простое, то $(p, a) = p$ и p делит некоторый сомножитель a_s : $1 \geq s \geq m-1$. □

Лемма 6.2. Пусть $b \mid a$, $c \mid a$, причем $(b, c) = 1$. Тогда $bc \mid a$.

Доказательство. Из условия следует, что a - общее кратное b и c. По теореме 2.1 a делится на $[b, c]$, по теореме 2.2 $[b, c] = bc$. □

Следствие. Пусть $r \geq 2$, и пусть целые числа $b_1 \dots b_r$ попарно взаимно просты, причем $b_1 \mid a, \dots, b_r \mid a$. Тогда $b_1 \dots b_r \mid a$.

Доказательство. Индукция по r. Если $r = 2$, получаем утверждение леммы. Пусть $m \geq 3$ и утверждение доказано для всех $r \leq m - 1$. Пусть $b_1, \dots b_m$ попарно взаимно просты и каждое из них делит a. В силу предложения индукции, a делится на произведение $b_1 \dots b_{m-1}$. Заметим, что $(b, b_m) = 1$. Действительно, в противном случае найдется простое число p, делящееся как на b_m так и на b. По лемме 6.1 p будет делить и некоторые $b_\xi : 1 \geq \xi \geq m - 1$. Следовательно $(b_m, b_\xi) \geq p > 1$, что противоречит условию. Так как a делится на b и b_m, и $(b, b_m) = 1$, то в силу леммы 6.2 a делится на $bb_m = b_1 \dots b_m$. □

Лемма 6.3. Пусть числа a и b взаимно просты, и пусть d_1 и d_2 пробегают соответственно множества всех делителей a и b. Тогда величина $d = d_1 d_2$ пробегает без повторений всё множество делителей числа ab.

Доказательство.

1. Если $d_1 \mid a$, $d_2 \mid b$, то $a = kd_1$, $b = md_2$ при некоторых $k, m \in \mathbb{Z}$, так что $ab = kmd_1 d_2$, то есть $d_1 d_2$ - делитель ab.

2. Допустим, что $d_1 d_2 = \delta_1 \delta_2$ для некоторых чисел d_1, δ_1 делящих a и некоторых чисел d_2, δ_2, делящих b. Очевидно, что $(d_1, \delta_2) = 1$, так как в противном случае нашлось бы простое p, делящееся одновременно и a и b, что невозможно. Но $d_1 \mid \delta_1 \delta_2$ по теореме 2.3 $d_1 \mid \delta_1$ и, следовательно $d_1 \leq \delta_1$. Аналогично доказывается, что $\delta_1 \mid d_1$ и $\delta_1 \leq d_1$. Значит $d_1 = \delta_1, d_2 = \delta_2$, то есть все произведения d_1 и d_2 различны.

3. Докажем, наконец, что всякий делитель d числа ab встретится среди произведений $d_1 d_2$. Если $d = 1$, то это очевидно. Пусть $d \geq 2$ и $p_1^{\alpha_1} \dots p_r^{\alpha_r}$ - каноническое разложение d. Число $q_1 = p_1^{\alpha_1} \mid ab$. Из теоремы 2.3 следует, что q_1 делит либо a, либо b (но не оба сразу). То же верно и для чисел $q_\xi = p_\xi^{\alpha_\xi}, \xi = 2, 3, \dots, r$. Пусть, для определенности, $q_1, \dots, q_t$ - все сомножители, делящие a, и $q_{t+1}, \dots, q_r$ - все сомножители, делящие b. По следствию леммы 6.2 произведение $d_1 = q_1 \dots q_t$ делит a, произведение $d_2 = q_{t+1}, \dots, q_r$ делит b, но $d_1 d_2 = d$.

□

Теорема 6.2. Пусть функция f мультипликативна. Тогда функция F, определенная при любом $n \in \mathbb{N}$ равенством:

$$F(n) = \sum_{d|n} f(d)$$

мультипликативна.

Доказательство. Пусть $(a, b) = 1$. По лемме 6.3, все делители ab получим без повторений, рассмотрев все произведения $d = d_1 d_2$, где $d_1 \mid a$, $d_2 \mid b$. Значит

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

$$= (\sum_{d_1|a} f(d_1))(\sum_{d_2|b} f(d_2)) = F(a)F(b).$$

Взаимная простота d_1 и d_2 очевидна. □

Следствие. Если $p_1^{\alpha_1} \dots p_r^{\alpha_r}$ - каноническое разложение n, а F - функция из условия теоремы, то

$$F(n) = \prod_{i=1}^{r} (1 + f(p_i) + f(p_i^2) + \dots + f(p_i^{\alpha_i}))$$

(при условии что $f \not\equiv 0$).

Определение 6.2. Функция Мебиуса $\mu(n)$ определяется равенствами:

$$\mu(n) = \begin{cases} 1, \text{ если } 1, \\ 0, \text{ если } n \text{ делится на квадрат простого числа}, \\ (-1)^k, \text{ если } n = p_1 \dots p_k - \text{различные простые числа}. \end{cases}$$

Примеры: $\mu(2) = (-1)^1 = -1, \mu(3) = -1, \mu(4) = 0, \mu(5) = -1, \mu(6) = (-1)^2 = 1, \mu(7) = -1, \mu(8) = \mu(9) = 0, \mu(10) = (-1)^2 = 1$ $n = p_1 \dots p_k$, $m = q_1 \dots q_r$, $(m, n) = 1 \Rightarrow mn = p_1 \dots p_k q_1 \dots q_r \Rightarrow \mu(mn) = (-1)^{k+r} = (-1)^k (-1)^r = \mu(m)\mu(n)$. p - простое $\Rightarrow \mu(p) = -1, \mu(p^2) = 0, \mu(p^3) = 0, \dots$

Теорема 6.3. (Основное свойство функции Мебиуса)

$$\sum_{d|n} \mu(d) = \begin{cases} 1, \text{ если } n = 1, \\ 0, \text{ если во всех остальных случаях.} \end{cases}$$

Доказательство. Пусть $F(n) = \sum\limits_{d|n} \mu(d) \Rightarrow$ (По теореме 6.2) F - мультипликативна. Пусть p - простое, $n = p^\alpha, \alpha \geq 1 \Rightarrow F(p^\alpha) = \sum\limits_{d|p^\alpha} \mu(d) = \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^\alpha) = 1 - 1 = 0.$ □

Определение 6.3. Функция Эйлера $\varphi(n)$ определяется для натурального n как количество чисел m с условиями $1 \leq m \leq n$, таких, что $(m, n) = 1$

Примеры. $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 1 + 1 + 0 = 2$, $\varphi(4) = 1 + 0 + 1 + 0 = 2$, $\varphi(5) = 1 + 1 + 1 + 1 + 0 = 4$, $\varphi(6) = 1 + 0 + 0 + 0 + 1 + 0 = 2$

Теорема 6.4. Функция Эйлера φ мультипликативна. Кроме того, если $p_1, \ldots, p_k$ - все различные делители n, тогда:

$$\varphi(n) = n \prod_{p|n} (1 - \frac{1}{p}) = n(1 - \frac{1}{p_1}) \ldots (1 - \frac{1}{p_k})$$

Доказательство. Надо подсчитать число тех m, для которых $(m, n) = 1$. По теореме 6.3

$$\sum_{d|(m,n)} \mu(d) = \begin{cases} 1, & \text{если } (m, n) = 1, \\ 0, & \text{иначе.} \end{cases}$$

$$\Rightarrow \varphi(n) = \sum_{1 \leq m \leq n} \sum_{d|(m,n)} \mu(d) = \sum_{d|n} \mu(d) \sum_{d \leq m \leq n, d|m} 1$$

$$1 \leq m = kd \leq n \Rightarrow 1 \leq k \leq \frac{n}{d}$$

$$\Rightarrow \sum_{d|n} \mu(d) \sum_{d \leq m \leq n, d|m} 1 = \sum_{d|n} \mu(d) \frac{n}{d} = n \sum_{d|n} \frac{\mu(d)}{d}$$

Функции $\mu(d)$ и $\frac{1}{d}$ - мультипликативные $\Rightarrow \frac{\mu(d)}{d}$ - мультипликативна $\Rightarrow$ по теореме 6.2 $\Rightarrow \sum\limits_{d|n} \frac{\mu(d)}{d}$ - мультипликативна $\Rightarrow \varphi(n)$ - мультипликативна.

$n = p^\alpha$, p - простое, $\alpha \geq 1$

$$\Rightarrow \varphi(p^\alpha) = p^\alpha \sum_{d|p^\alpha} \frac{\mu(d)}{d} = p^\alpha (\frac{\mu(1)}{1} + \frac{\mu(p)}{p} + \frac{\mu(p^2)}{p^2} + \cdots + \frac{\mu(p^\alpha)}{p^\alpha}) =$$

$$= p^\alpha (1 + \frac{\mu(p)}{p}) = p^\alpha (1 + \frac{1}{p})$$

.

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

$$= p_1^{\alpha_1} \ldots p_k^{\alpha_k} (1 - \frac{1}{p_1}) \ldots (1 - \frac{1}{p_k}) = n \prod_{p|n} (1 - \frac{1}{p}).$$

□

Теорема 6.5. (Формула обращения Мебиуса) Пусть $\forall n \geq 1$ функции f и g связаны соотношением

$$f(n) = \sum_{d|n} g(d) \tag{1}$$

Тогда $\forall n \geq 1$ выполнено равенство

$$g(n) = \sum_{d|n} \mu(d) f(\frac{n}{d}) \tag{2}$$

Обратно, если $\forall n \geq 1$ f и g связаны соотношением (2), то $\forall n \geq 1$ верно (1).

Доказательство. ($\Rightarrow$) Пусть выполнено (1), преобразуем величину

$$\sum_{d|n} \mu(d) f(\frac{n}{d}) = \sum_{d|n} \mu(d) \sum_{\delta|\frac{n}{d}} g(\delta) = \sum_{d\delta|n} \mu(d) g(\delta) = \sum_{\delta|n} g(\delta) \sum_{d|\frac{n}{\delta}} \mu(d) =$$

$$= (\text{по теореме 6.3})\ g(n).$$

Пояснение:

$$\sum_{d|\frac{n}{\delta}} \mu(d) = \begin{cases} 1, & \text{если } \frac{n}{\delta} = 1, \\ 0, & \text{если } \frac{n}{\delta} > 1. \end{cases} \quad \Leftrightarrow \quad \begin{cases} 1, & \text{если } n = \delta, \\ 0, & \text{если } n > \delta. \end{cases}$$

($\Leftarrow$) Пусть есть (2), преобразуем

$$\sum_{d|n} \mu(d) f(\frac{n}{d}) = \sum_{d|n} \sum_{\delta|d} \mu(\delta) f(\frac{d}{\delta}) =$$

$$(\delta \mid d \Rightarrow d = \Delta\delta \Rightarrow \frac{d}{\delta} = \Delta)$$

$$= \sum_{\Delta\delta|d} \mu(\delta) f(\Delta) = \sum_{\Delta|n} f(\Delta) \sum_{\delta|\frac{n}{\Delta}} \mu(\delta) = (\text{по теореме 6.3})\ f(n)$$

□

Следствие.

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

Доказательство. Выше доказали, что

$$\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d}$$

это равенство (2), где $g(n) = \varphi(n), f(k) = k$. По формуле обращения Мебиуса, для этих функций выполнено (1): $f(n) = n = \sum_{d|n} g(n) = \sum_{d|n} \varphi(n)$ □

Определение 6.4. Функция делителей $\tau(n)$ определяется, как число делителей натурального $n \geq 1$.

$$\tau(n) = \sum_{d|n} 1.$$

Замечание. $f(1) \equiv 1$ - мультипликативна $\Rightarrow$ (по теореме 6.2) $\tau(n)$ - мультипликативна.

Утверждение 6.1. $n = p^\alpha$, p - простое.

$$\tau(p^\alpha) = \sum_{d|p^\alpha} 1 = \alpha + 1$$

$n = p_1^{\alpha_1} \dots p_k^{\alpha_k} \Rightarrow \tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_k + 1)$.