Курс "методы решета". Лекция 1 (13 февраля 2020 г.)

Определение 1. Целое число $n \geq 2$ называется простым, если оно имеет ровно два делителя: 1 и n. В противном случае n называется составным числом. Единица не причисляется ни к простым, ни к составным числам.

Пример: числа $2, 3, 5, 7, 11, 13, 17$ — простые, числа $4 = 2^2$, $6 = 2 \cdot 3$, $8 = 2^3$, $9 = 3^2$, $10 = 2 \cdot 5$, $12 = 2^2 \cdot 3$ — составные.

Теорема 1 (основная теорема арифметики) Всякое целое число $n \geq 2$ разлагается в произведение простых чисел. Это разложение единственно с точностью до порядка следования сомножителей.

Замечание: Запись целого числа $n \geq 2$ в виде

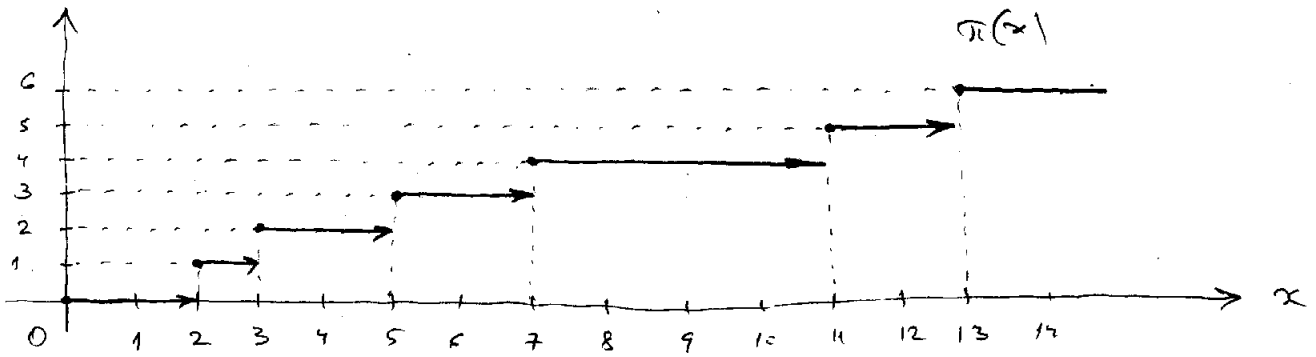
$$n = p_1^{\alpha_1} \dots p_s^{\alpha_s},$$

где $p_1, \dots, p_s$ — различные простые числа, $\alpha_1, \dots, \alpha_s \geq 1$, называется каноническим разложением n на простые сомножители.

Пример: $15 = 3 \cdot 5$, $16 = 2^4$, $18 = 2 \cdot 3^2$, $24 = 2^3 \cdot 3$, $30 = 2 \cdot 3 \cdot 5$, $55 = 5 \cdot 11$ и т. д.

Определение 2 Для вещественного $x \geq 0$ через $\pi(x)$ обозначается количество простых чисел, не превосходящих x.

Пример: $\pi(1) = 0$, $\pi(2{,}5) = 2$, $\pi(7) = 4$, $\pi(11) = 5$



Лемма 1 Наименьший отличный от единицы делитель целого числа $n \geq 2$ есть простое число.

Д-во. Очевидно.

Теорема 2 (Евклид). Простых чисел бесконечно много (или, что то же, $\pi(x) \to +\infty$ при $x \to +\infty$).

Д-во 1: Предположим противное: пусть $p_1, p_2, \dots, p_k$ – все простые числа. В силу леммы 1, наименьший простой делитель p числа $N = p_1 \dots p_k + 1$ есть простое число, но p отлично от $p_1, \dots, p_k$, т.к. N при делении на $p_1, \dots, p_k$ даёт в остатке 1. Противоречие.

Д-во 2: Предположим, как и выше, что $p_1, \dots, p_k$ – все простые числа. Зафиксируем произвольным целым $N > e^2$. Пусть $n \le N$. Тогда, в силу теоремы 1, n единственным образом представляется в виде $p_1^{\alpha_1} \dots p_k^{\alpha_k}$, где некоторые из чисел α_i могут быть равны нулю. Ввиду неравенств

$$2^{\alpha_i} \le p_i^{\alpha_i} \le n \le N$$

имеем: $0 \le \alpha_i \le \frac{\ln N}{\ln 2}$.

Следовательно, общее количество произведений вида $p_1^{\alpha_1} \dots p_k^{\alpha_k}$, не превосходящих N, не превосходит

$$\left(\left[\frac{\ln N}{\ln 2} \right] + 1 \right)^k \le \left(\frac{3}{2} \ln N + 1 \right)^k < (2 \ln N)^k.$$

С другой стороны, такие произведения дают все числа $n \le N$, т.е. $N < (2 \ln N)^k$. Беря N достаточно большим, приходим к противоречию.

Замечание. Первое доказательство теоремы 2 (принадлежащее Евклиду) позволяет получить неплохую оценку скорости роста $\pi(x)$ при возрастании x, хотя и достаточно грубую. Именно, нетрудно заключить, что

$$p_2 \le p_1 + 1 = 2 + 1 < 2^2,$$
$$p_3 \le p_1 p_2 + 1 < 2^{1+2} + 1 = 2^3 + 1 < 2^{2^2},$$
$$p_4 \le p_1 p_2 p_3 + 1 < 2^{1+2+2^2} + 1 < 2^{2^3}$$

и вообще,

$$p_{n+1} \le p_1 \dots p_n + 1 < 2^{1+2+2^2+\dots+2^{n-1}} + 1 = 2^{2^n - 1} + 1 < 2^{2^n}.$$

Пусть теперь $x > 16$. Определяя n из условий

$$2^{2^n} < x \le 2^{2^{n+1}},$$

будем иметь:

$\pi(x) \geq \pi(2^{2^k}) > \pi(p_{k+1}) = k+1$, ко

$2^{k+1} \geq \frac{\ln x}{\ln 2} > \ln x$, $k+1 > \frac{\ln\ln x}{\ln 2}$, так что окончательно имеем

$$\pi(x) > \frac{\ln\ln x}{\ln 2}.$$

Можно поставить следующую задачу: отыскать все простые числа, не превосходящие заданной величины N. Ее первое решение восходит к Эратосфену Киренскому ($\overline{\text{III}}$ – $\overline{\text{II}}$ в.в. до Р.Х.) и основано на следующем наблюдении.

Лемма 2 Всякое составное число n имеет простой делитель, не превосходящий $\sqrt{n}$.

Д-во: Если n – составное, то оно обладает по меньшей мере двумя простыми делителями: p_1 и p_2. Пусть, для определенности, p_1 – наименьший простой делитель n. Тогда $p_1^2 \leq p_1 p_2 \leq n$, откуда $p_1 \leq \sqrt{n}$.

Теорема 3 (решето Эратосфена). Пусть $N \geq 6$. Все простые числа, не превосходящие N, получим, вычеркнув из таблицы всех натуральных чисел кратные 2 (кроме самого числа 2), кратные 3 (кроме самого числа 3), ..., кратные p_k (кроме самого числа p_k), где p_k – наибольшее простое число, не превосходящее $\sqrt{N}$.

Д-во: следует из леммы 2 – всякое составное число $n \leq N$ имеет хотя бы один простой делитель, не превосходящий $\sqrt{N}$ и потому окажется вычеркнутым на одном из шагов

Пример (для $N = 64$).

Для "компьютерного" описания процедуры Теоремы 3 нам понадобится следующее

Определение 3 Функцией Мёбиуса μ называется арифметическая функция, определенная на множестве натуральных чисел равенствами:

$$\mu(n) = \begin{cases} 1, & \text{если } n = 1, \\ 0, & \text{если } n \text{ делится на квадрат простого числа,} \\ (-1)^k, & \text{если } n = p_1 \cdots p_k \text{ есть произведение } k \text{ различных простых сомножителей} \end{cases}$$

Например, $\mu(2) = \mu(3) = -1$, $\mu(4) = 0$, $\mu(5) = 0$, $\mu(6) = 1$, $\mu(7) = -1$, $\mu(8) = \mu(9) = 0$, $\mu(10) = 1$.

(Эта функция введена в 1831 г. немецким математиком Августом Фердинандом Мёбиусом, 1790–1868, в работе: Über eine besondere Art von Umkehrung der Reihen. Journal für die reine und angewandte Mathematik (Crelle's Journal), Vol. 9 (1832), s. 105–123)

<u>Лемма 4</u> Функция Мёбиуса мультипликативна, т.е. $\mu(mn) = \mu(m)\mu(n)$ для любых взаимно простых чисел m, n

<u>Д-во</u>: Непосредственно следует из определения.

<u>Теорема 4</u> (основное свойство функции Мёбиуса). При любом целом $n \geq 1$ справедливо равенство:

$$\sum_{d \mid n} \mu(d) = \begin{cases} 1, & \text{если } n = 1, \\ 0, & \text{в противном случае} \end{cases}$$

<u>Замечание</u>. Символ $\sum_{d \mid n}$ означает суммирование по всем делителям d числа n, включая единицу и само число n.

<u>Д-во</u>. Если $n = 1$, то равенство очевидно. Пусть $n > 1$ и $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ – каноническое разложение n. Тогда все делители n имеют вид $p_1^{\beta_1} \cdots p_k^{\beta_k}$, где $0 \leq \beta_i \leq \alpha_i$. Из них ненулевой вклад вносят лишь те, для которых все показатели β_i не превосходят единицы, т.е. делители вида $d = p_{i_1} \cdots p_{i_s}$, где $1 \leq i_1 < \ldots < i_s \leq k$. Для всякого такого делителя имеем: $\mu(d) = (-1)^s$. Далее, если s задано, $0 \leq s \leq k$, то количество таких

делителей есть, очевидно, C_k^s. Значит, сумма из условия леммы имеет вид

$$\sum_{s=0}^{k} (-1)^s C_k^s = C_k^0 - C_k^1 + C_k^2 - C_k^3 + \dots + (-1)^k C_k^k =$$

$$= (1-1)^k = 0, \text{ что и требовалось.}$$

<u>Следствие</u> Для любых целых чисел $n, n \geq 1$ справедливо равенство: $\sum_{d \mid (n,n)} \mu(d) = \begin{cases} 1, & \text{если } n, n \text{ взаимно просты,} \\ 0, & \text{в противном случае} \end{cases}$

<u>Теорема 5</u> ("явная формула" для $\pi(x)$). При любом $x > 2$ справедливо тождество

$$\pi(x) = \pi(\sqrt{x}) + \sum_{\substack{d \mid P \\ d \leq x}} \mu(d) \left[\frac{x}{d}\right],$$

где $P = \prod_{p \leq \sqrt{x}} p$

<u>Д-во</u> Действительно, пусть $\sqrt{x} < n \leq x$. Если n - составное, то $(n, P) > 1$ в силу леммы 2. Если n - простое, то $(n, P) = 1$. Поэтому, пользуясь следствием теоремы 4, находим:

$$\pi(x) - \pi(\sqrt{x}) = \sum_{\sqrt{x} < p \leq x} 1 = \sum_{\substack{\sqrt{x} < n \leq x \\ (n,P)=1}} 1 = \sum_{\substack{n \leq x \\ (n,P)=1}} 1 =$$

$$= \sum_{n \leq x} \sum_{d \mid (n,P)} \mu(d) = \sum_{\substack{d \mid P \\ d \leq x}} \mu(d) \sum_{\substack{n \leq x \\ n \equiv 0 \pmod d}} 1 =$$

$$= \sum_{\substack{d \mid P \\ d \leq x}} \mu(d) \left[\frac{x}{d}\right], \text{ что и требовалось.}$$

<u>Замечание</u> Теорема 5, по сути, дает выражение для количества чисел $n \leq x$, оставшихся невычеркнутыми после применения решета Эратосфена. Попытки преобразования суммы по $d \mid P$ наталкиваются на следующие трудности.

Замена $\left[\frac{x}{d}\right]$ разностью $\frac{x}{d} - \left\{\frac{x}{d}\right\}$ даёт:

$$\sum_{\substack{d|P \\ d\le x}} \mu(d)\left[\frac{x}{d}\right] = \sum_{d|P} \mu(d)\left[\frac{x}{d}\right] = \sum_{d|P} \mu(d)\left(\frac{x}{d} - \left\{\frac{x}{d}\right\}\right) =$$

$$= xW - S, \text{ где } W = \sum_{d|P} \frac{\mu(d)}{d}, \quad S = \sum_{d|P} \mu(d)\left\{\frac{x}{d}\right\}.$$

Очевидно, $W = \prod_{p|P}\left(1 - \frac{1}{p}\right) = \prod_{p\le\sqrt{x}}\left(1-\frac{1}{p}\right)$;

$$|S| \le \sum_{d|P} 1 = 2^{\pi(\sqrt{x})}.$$

Оценка суммы W не представляет затруднений; однако сумма S содержит слишком много слагаемых, и именно это не позволяет получить из теоремы 5 какие-либо содержательные утверждения о порядке роста $\pi(x)$.

Однако этого можно добиться некоторой модификацией рассуждений. Для этого нам потребуется следующее утверждение

<u>лемма 5</u>. При любом $x \ge 3$ справедливо неравенство:

$$\prod_{p\le x}\left(1-\frac{1}{p}\right) \le \frac{1}{\ln x}.$$

<u>Д-во</u>. Действительно, обозначая произведение через W, будем иметь:

$$W^{-1} = \prod_{p\le x}\left(1-\frac{1}{p}\right)^{-1} = \prod_{p\le x}\left(1+\frac{1}{p}+\frac{1}{p^2}+\cdots\right) = \sum_{n}{}' \frac{1}{n},$$

где штрих означает суммирование по всем n, в каноническое разложение которых участвуют лишь простые числа $p \le x$. В силу основной теоремы арифметики, в сумме по n встретится всякая дробь $\frac{1}{k}$, $1 \le k \le x$, и притом ровно один раз. Значит, $W^{-1} \ge \sum_{1\le k\le x} \frac{1}{k} \ge \int_1^{[x]+1} \frac{du}{u} = \ln([x]+1) > \ln x$,

что и требовалось.

Теорема 6. При $x \geq x_0$ справ. неравенство: $\pi(x) \leq \frac{3x}{\ln \ln x}$.

Следствие: $\pi(x) = \overline{o}(x)$.

Д-во. Зададимся произвольным числом u, $2 \leq u \leq \sqrt{x}$, и положим $P = \prod_{p \leq u} p$. Все простые числа n, удовлетворяющие $u < n \leq x$ находятся среди чисел, взаимно простых с P, так что

$$\pi(x) - \pi(u) \leq \sum_{\substack{u < n \leq x \\ (n,P)=1}} 1 = \sum_{\substack{n \leq x \\ (n,P)=1}} 1.$$

В силу основного свойства функции Мёбиуса,

$$\pi(x) \leq \pi(u) + \sum_{n \leq x} \sum_{d \mid (n,P)} \mu(d) = \pi(u) + \sum_{\substack{d \mid P \\ d \leq x}} \mu(d) \left[\frac{x}{d}\right]$$

$$= \pi(u) + \sum_{d \mid P} \mu(d) \left[\frac{x}{d}\right] = \pi(u) + \sum_{d \mid P} \mu(d) \left(\frac{x}{d} - \left\{\frac{x}{d}\right\}\right)$$

$$= \pi(u) + x \sum_{d \mid P} \frac{\mu(d)}{d} - \sum_{d \mid P} \mu(d) \left\{\frac{x}{d}\right\}.$$

Замечая, что $\pi(u) < u$, и что число слагаемых в последней сумме не превосходит числа делителей P, равного $2^{\pi(u)} < 2^u$, находим:

$$\pi(x) < u + 2^u + x \prod_{p \leq u} \left(1 - \frac{1}{p}\right) < \frac{x}{\ln u} + 2^u + u.$$

Возьмем $u = \frac{1}{2} \ln x$. Тогда $2^u + u = e^{\frac{\ln 2}{2} \cdot \ln x} + \frac{1}{2} \ln x < \sqrt{x}$, так что $\pi(x) < \frac{2x}{\ln x} + \sqrt{x} < \frac{3x}{\ln x}$, что и требовалось.