Л№1 Простые и взаимно простые числа. Арифметические функции.

В.С.Панферов

Леопольду Кронекеру (7.12.1823 – 29.12.1891) принадлежит высказывание: Бог создал натуральные числа, всё остальное – дело рук человеческих.

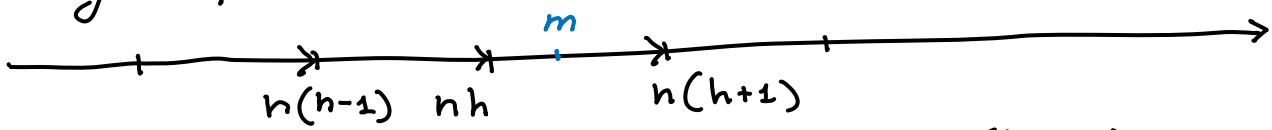
NB Пусть $\mathbb{N}$ – множество натуральных чисел, тогда любое $n \in \mathbb{N}$: $n = \underbrace{1+1+\ldots+1}_{n}$, т.е. 1 "порождает" всё множество $\mathbb{N}$.

Деление с остатком

I $\forall m \in \mathbb{Z}$ и $\forall n \in \mathbb{N}$ $\exists!\ h \in \mathbb{Z}$ и $r = 0, 1, \ldots, n-1$:

$$m = nh + r.$$

Д Разобьём числовую прямую на непересекающиеся полуинтервалы $[nh, n(h+1))$:



$$\mathbb{R} = \bigcup_{n=-\infty}^{+\infty} [nh, n(h+1)) = \bigcup_{n \in \mathbb{Z}} [nh, n(h+1)).$$

$\forall m \in \exists!\ h \in \mathbb{Z}$:

$$m \in [nh, n(h+1))$$

и однозначно определено число $r = m - nh = 0, 1, \ldots, n-1$.

Или единственность можно доказать так. Пусть $m = nh_1 + r_1 = nh_2 + r_2$ $(h_1, h_2 \in \mathbb{Z};\ r_1, r_2 = 0, 1, \ldots, n-1)$. Тогда $r_1 - r_2 = n(h_2 - h_1)$. Значит $r_1 = r_2 \Leftrightarrow h_1 = h_2$. Если же $r_1 \neq r_2 \Leftrightarrow h_1 \neq h_2$, то $|r_1 - r_2| < n$, а $|n(h_2 - h_1)| = n|h_2 - h_1| > n$.

NB

- Если $r = 0$, то m делится (нацело) на n или n делитель m $(n \mid m)$.
- Если $m = nh + r$, то пишем $m \equiv r \pmod n$.
- Если $a, b \in \mathbb{Z}$; $n \in \mathbb{N}$, то $a \equiv b \pmod n$ означает, что a и b имеют равные остатки при делении на n, или $a - b$ делится на n.

Простые числа

О Натуральное число p – простое, если его делители – это только 1 и p (тривиальные делители).
Натуральное число – составное, если оно имеет нетривиальные делители.

NB Ясно, что все числа (кроме 2) последовательности

$$2, 4, 6, 8, 10, \ldots, 2n, \ldots$$

являются составными. Значит, в частности, составных чисел бесконечно много.

Доказательство бесконечности числа простых содержится в в IX книге "Начал" Евклида (Евклид 325 до н.э – 265 до н.э.; Евклид: от "добрая слава", или "время рассвета")

Доказательство Евклида.

Пусть $p_1 = 2 < p_2 < \ldots < p_n$ – простые и других простых нет. Тогда число

$$N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1:$$

1) N – не простое, так как $N > p_n$;
2) N – не составное, так как $N \equiv 1 \pmod{p_k}$; $k = 1, 2, \ldots, n$, т.е. N не делится ни на одно простое.

Значит предположение о конечности множества простых неверно.

NB Пусть $N = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot \ldots \cdot p + 1$ (первое слагаемое – это произведение всех простых от 2 до p).
Число N – либо простое и $N > p$, либо любой простой делитель N (в частности, наименьший простой делитель N) больше, чем p.

Следствия из доказательства Евклида

I. Пусть: $p_1 = 2; p_2 = 3, \ldots, p_n, \ldots$ – нумерация простых по возрастанию. Тогда

I $\forall n \in \mathbb{N}$

$$p_{n+1} < 2^{2^n}.$$

NB При $n = 0$ $2 = p_1 = 2^{2^0}$.

Д По индукции.

1) $n=1: 3=p_2<2^{2^1}=4$; $n=2: 5=p_3<2^{2^2}=16$.

2) Пусть для всех $k=1,2,\dots,n-1$

$$p_{k+1}<2^{2^k}.$$

Так как p_{n+1} не больше, чем наименьший простой делитель числа $N=p_1p_2\dots p_n+1$, то

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

NB • Ясно, что для всех $n=1,2,\dots$ $p_n>n$.

• Полученная оценка "очень грубая".

• Более "тонкая" оценка:

$$p_n<e^{n+1}<3^n \quad (n=1,2,\dots).$$

• Пафнутий Львович Чебышов (Чебышев 4.5.1821–26.11.1894) доказал, что существуют такие константы α и β, $0<\alpha<\beta$, что для всех $n=2,3,\dots$

$$\alpha n\ln n<p_n<\beta n\ln n.$$

II Используя доказательство Евклида, докажем, что среди чисел: $n\equiv 2\pmod 3$, т.е. в арифметической прогрессии

$$2,5,8,11,14,17,20,23,\dots \qquad (2)$$

бесконечно много простых.

Д Рассмотрим ещё две последовательности:

$3,6,9,12,15,\dots$ – кратные 3 $(n\equiv 0\pmod 3)$; (0)

$1,4,7,10,13,\dots$ $(n\equiv 1\pmod 3)$. (1)

Заметим, что в последовательности (0) единственное простое – это 3, а произведение двух чисел из последовательности (1) принадлежит этой же последовательности (1):

$$(3x+1)(3y+1)=3(3xy+x+y)+1.$$

Значит среди простых делителей любого числа из (2) есть делитель из (2). Действительно. Ни один делитель числа из (2) не может лежать в (0), иначе число из (2) будет кратно (3). С другой стороны, если все простые делители числа из (2) лежат в (1), то их произведение, т.е. само число, тоже лежит в (1).

Заканчивая доказательство, рассмотрим число

$$M = 2\cdot 3\cdot 5\cdot 7\cdot 11\cdot \ldots \cdot p - 1,$$

первое слагаемое – это произведение всех простых от 2 до p.

Ясно, что $M \equiv 2 \pmod 3$, т.е. M из (2) и, конечно, M не делится ни на одно из простых от 2 до p.

Значит или M – простое и M из (2), $M > p$, или у M есть простой делитель $q > p$ и q лежит в (2).

Простые числа расположены "очень неравномерно".

1) $\underline{T}$ В $\mathbb{N}$ найдутся сколь угодно длинные отрезки: $M, M+1, M+2, \ldots, M+N$, состоящие из составных чисел.

$\underline{D}$
$$(N+1)! + 2 \quad - \text{ делится на } 2$$
$$(N+1)! + 3 \quad - \text{ делится на } 3$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$(N+1)! + (N+1) \quad - \text{ делится на } N+1$$

Все эти числа составные и их N штук.

2) $\underline{T}$ Не существует алгебраического многочлена

$$f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$$

с целыми коэффициентами $a_n, a_{n-1}, \ldots, a_1, a_0$; $n \geq 1$, $a_n \neq 0$ такого, что для любого $m = 1, 2, \ldots$ $f(m)$ – простое.

$\underline{D}$ Пусть $f(x)$ – многочлен, указанного вида. Тогда для достаточно большого $m_0 \in \mathbb{N}$ $|f(m_0)| > 1$.

Действительно:

$$|f(x)| = |a_n x^n - (-a_{n-1} x^{n-1} - \ldots - a_1 x - a_0)| \geq$$
$$\geq |a_n||x|^n - |a_{n-1} x^{n-1} + \ldots + a_1 x + a_0| \geq$$
$$\geq |a_n||x|^n - (|a_{n-1}||x|^{n-1} + \ldots + |a_1||x| + |a_0|) \geq \quad (\text{если } |x| \geq 1)$$
$$\geq |a_n||x|^n - |x|^{n-1}(|a_{n-1}| + \ldots + |a_1| + |a_0| + 1) = |x|^{n-1}(|a_n||x| - A),$$

где $A = |a_{n-1}| + \ldots + |a_0| + 1$.

Значит, если $|x| > A$, то $|f(x)| > 1$.

Пусть p – простой делитель $f(m_0)$, тогда

$$f(m_0 + kp) - f(m_0) = kp\, g(m_0, p, k), \quad \circledast$$

где $g(m_0, p, k)$ – целое.

Действительно

$$f(m_0+kp)-f(m_0)=\sum_{i=0}^{n} a_i\left((m_0+kp)^i-m_0^i\right)=$$
$$=\sum_{i=0}^{n} a_i\left(\sum_{l=1}^{i}(kp)^l m_0^{i-l} C_i^l\right).$$

Значит при любом $k=1,2,\ldots$ $f(m_0+kp)$ делится на p. Так как при больших k $|f(m_0+kp)|>p$, то теорема доказана.

Основная теорема арифметики

$\underline{T}$ $\forall n=2,3,\ldots$ $\exists!$ $2\le p_1<p_2<\ldots<p_m$ – простые и $a_1,a_2,\ldots,a_m$ – натуральные:

$$n=p_1^{a_1}\cdot p_2^{a_2}\cdot\ldots\cdot p_m^{a_m}. \quad \circledast$$

NB Представление натурального числа в виде $\circledast$ называют каноническим разложением числа на простые множители.

Обозначим через $[x]$ – целую часть числа x, т.е. $[x]$ – это наибольшее целое, не превосходящее x:

$$[x]\le x<[x]+1.$$

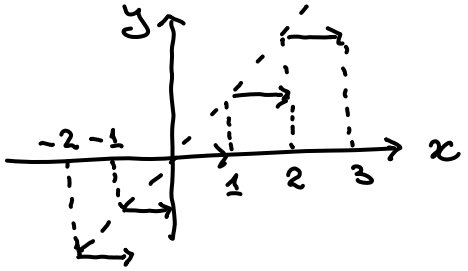
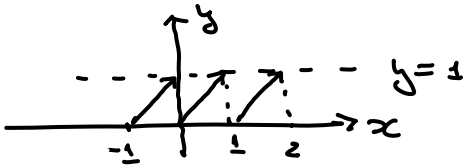


График функции $y=[x]$:

Функцию $y=x-[x]=\{x\}$ – называют дробной частью x. Эта функция переодическая с периодом равным 1



1. $\underline{T}$ Показатель $a_p=a_p(n)$, с которым простое число p входит в каноническое разложение числа $n!=1\cdot2\cdot3\cdot\ldots\cdot n$ на простые множители равен

$$a_p=\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\left[\frac{n}{p^3}\right]+\ldots$$

NB $\forall n\in\mathbb{N}$ и $\forall p$ – простого $\exists k\in\mathbb{N}: p^k>n$. Поэтому в этой сумме конечное число слагаемых, так как $\forall m=k,k+1,\ldots$ $\left[\frac{n}{p^m}\right]=0$.

$\underline{D}$ Среди чисел $1,2,\ldots,n$ имеется ровно $\left[\frac{n}{p}\right]$ делящихся на p, среди этих чисел $\left[\frac{n}{p^2}\right]$ делящихся на p^2, а среди этих чисел $\left[\frac{n}{p^3}\right]$ делящихся на p^3 и т.д.

Поэтому среди чисел $1, 2, \dots, n$ ровно $\left[\frac{n}{p^k}\right] - \left[\frac{n}{p^{k+1}}\right]$ чисел, которые делятся на p^k, но не делятся на p^{k+1}. Каждое такое число вносит в показатель a_p как слагаемое число k, а все эти числа вносят вклад равный $k\left(\left[\frac{n}{p^k}\right] - \left[\frac{n}{p^{k+1}}\right]\right)$. Значит если $p^{m_p} \le n < p^{m_p+1}$, то

$$a_p = \sum_{k=1}^{m_p} k\left(\left[\frac{n}{p^k}\right] - \left[\frac{n}{p^{k+1}}\right]\right) = \sum_{k=1}^{m_p} \left[\frac{n}{p^k}\right].$$

Число натуральных делителей

Пусть $n = p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_m^{a_m}$ – каноническое разложение натурального числа n.

Натуральное число d – делитель n тогда и только тогда, когда

$$d = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_m^{\alpha_m},$$

где $\alpha_k = 0, 1, \dots, a_k$ $(k = 1, 2, \dots, m)$.

Значит каждый делитель d числа n однозначно определяется набором

$$(\alpha_1, \alpha_2, \dots, \alpha_m);\ \alpha_k = 0, 1, 2, \dots, a_k;\ k = 1, 2, \dots, m.$$

Таких различных наборов

$$(\alpha_1 + 1)(\alpha_2 + 1) \cdot \dots \cdot (\alpha_m + 1) = d(n).$$

Наибольший общий делитель

О Пусть $n, m \in \mathbb{N}$. Число $\mathcal{D} \in \mathbb{N}$ называют наибольшим общим делителем чисел n и m ($\mathcal{D} = НОД(n, m)$ или $d = (n, m)$), если

i) $\mathcal{D}$ – общий делитель n и m, т.е. $\mathcal{D} \mid n$ и $\mathcal{D} \mid m$.

ii) Если $d \mid n$ и $d \mid m$, т.е. d – общий делитель n и m, то $d \mid \mathcal{D}$.

Нахождение наибольшего общего делителя

I Пусть заданы канонические разложения чисел n и m:

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdot \dots \cdot p_k^{a_k},\ k$$

$$m = q_1^{b_1} \cdot q_2^{b_2} \cdot \dots \cdot q_\ell^{b_\ell},$$

где наборы $p_1, p_2, \dots, p_k$ и $q_1, q_2, \dots, q_\ell$ состоят каждый

из различных простых; $a_1, \dots, a_k, b_1, \dots, b_e$ – натуральные.
Составим набор различных простых $r_1, \dots, r_s$:

$$\{p_1, p_2, \dots, p_k\} \cup \{q_1, q_2, \dots, q_e\} = \{r_1, \dots, r_s\}.$$

Запишем числа n и m в виде:

$n = r_1^{\alpha_1} \cdot r_2^{\alpha_2} \cdot \dots \cdot r_s^{\alpha_s}$; $m = r_1^{\beta_1} \cdot r_2^{\beta_2} \cdot \dots \cdot r_s^{\beta_s}$,

где $\alpha_i = a_j$, если $r_i = p_j$ и $\alpha_i = 0$, если r_i – не является делителем n. Аналогично, $\beta_i = b_j$, если $r_i = q_j$ и $\beta_i = 0$, если r_i не является делителем m.

Тогда $НОД(n,m) = r_1^{\min(\alpha_1, \beta_1)} \cdot r_2^{\min(\alpha_2, \beta_2)} \cdot \dots \cdot r_s^{\min(\alpha_s, \beta_s)}$.

NB 1) $\underline{O}$ Число k – наименьшее общее кратное чисел n и m ($k = НОК(n,m)$), если
   i) n/k и m/k, т.е. k – общее кратное n и m,
   ii) если n/K и m/K, то k/K, т.е. k делитель любого общего кратного n и m.

2) $НОК(n,m) = r_1^{\max(\alpha_1, \beta_1)} \cdot r_2^{\max(\alpha_2, \beta_2)} \cdot \dots \cdot r_s^{\max(\alpha_s, \beta_s)}$.

3) Для любых натуральных n и m:

$$НОД(n,m) \cdot НОК(n,m) = n \cdot m,$$

так как для любых α и β

$$\min(\alpha, \beta) + \max(\alpha, \beta) = \alpha + \beta.$$

II Эффективный метод нахождения наибольшего общего делителя даёт алгоритм Евклида. Пусть $a, b \in \mathbb{N}$ и $a \geq b$. Строим последовательность чисел: $a \geq b > r_1 > r_2 > \dots > r_n$

$$\text{(*)} \quad \begin{aligned} a &= b h_0 + r_1 && 0 < r_1 < b \\ b &= r_1 h_1 + r_2 && 0 < r_2 < r_1 \\ r_1 &= r_2 h_2 + r_3 && 0 < r_3 < r_2 \\ &\dots \\ r_{n-3} &= r_{n-2} \cdot h_{n-2} + r_{n-1} && 0 < r_{n-1} < r_{n-2} \\ r_{n-2} &= r_{n-1} h_{n-1} + r_n && 0 < r_n < r_{n-1} \\ r_{n-1} &= r_n h_n \end{aligned}$$

Докажем, что $НОД(a,b) = r_n$. Действительно:
1) двигаемся по таблице (*) "снизу – в верх" ↑

$r_n | r_{n-1}$; $r_n | r_{n-2}$; ...; $r_n | r_2$; $r_n | r_1$; $r_n | b$; $r_n | a$,
т.е. r_n – общий делитель a и b.

2) двигаемся по таблице (*) "сверху-вниз" ↓
если d – общий делитель a и b, то
$d | a$; $d | b$; $d | r_1$; $d | r_2$; ...; $d | r_{n-1}$; $d | r_n$.

Важнейшим инструментом использования наибольшего общего делителя является соотношение Безу (Этьен Безу 31.3.1730–27.9.1783).

Т Пусть $a, b \in \mathbb{Z}$ и одно из них не равно нулю
Тогда существуют такие $x, y \in \mathbb{Z}$, что

$$ax + by = НОД(a,b) (= (a,b)).$$

Или эквивалентное утверждение для натуральных
Пусть $a, b \in \mathbb{N}$. Тогда существуют такие целые p и q, что

$$ap + bq = (a,b)$$

NB $(2,3) = 3 \cdot 1 - 2 \cdot 1 = 2 \cdot 2 - 3 \cdot 1 = 1$.

Доказательство соотношения Безу.
Двигаясь по таблице (*) "снизу-вверх", получаем
($r_n = (a,b) = d$)

$$d = r_{n-2} \cdot 1 + r_{n-1} \cdot (-h_{n-1}).$$

Выражая r_{n-1} через r_{n-2} и r_{n-3} (из следующей строки), получаем

$$d = r_{n-2} \cdot 1 + (r_{n-3} + r_{n-2} \cdot (-h_{n-2}))(-h_{n-1}) =$$
$$= r_{n-3}(-h_{n-1}) + r_{n-2}(1 + h_{n-2} \cdot h_{n-1})$$

и т.д.
В итоге получим $d = ax + by$.

NB • Представление наибольшего общего делителя в таком виде неединственно. Действительно, если $x_0, y_0 \in \mathbb{Z}$ такие, что $d = ax_0 + by_0$, то для любого $k \in \mathbb{Z}$

$$a(x_0 + bk) + b(y_0 - ak) = ax_0 + by_0 = d.$$

• Важное дополнение к соотношению Безу.

$\forall a, b \in \mathbb{N} \quad \exists x, y \in \mathbb{Z}$:

$$ax + by = (a,b) = d$$

и $|x| < \frac{b}{d}$, $|y| < \frac{a}{d}$.

▷ Пусть $a = a_1 d$, $b = b_1 d$ $((a_1, b_1) = 1;\ a_1, b_1 \in \mathbb{N})$.

Тогда $a_1 x + b_1 y = 1$.

Если $x \in \mathbb{N}$, то $y < 0$ $(-y \in \mathbb{N})$ и $x \geq b_1$, тогда

$x = b_1 h + r$ $(0 < r < b_1)$ и

$1 = a_1(b_1 h + r) + b_1 y = a_1 r + b_1(a_1 h + y) \equiv a_1 r + b_1 c$,

где $c = a_1 h + y < 0$ и

$$a_1 r = 1 + b_1(-c).$$

Если $|c| = -c \geq a_1$, то

$$a_1 r = 1 + b_1(-c) \geq 1 + a_1 b_1,$$

но $a_1 r < a_1 b_1$. Значит $|x| < |b_1| = \left|\frac{b}{d}\right|$ и $|y| < |a_1| = \left|\frac{a}{d}\right|$.

Элегантное доказательство бесконечности множества простых получаем из следующего очевидного утверждения:

если последовательность натуральных чисел $\{m_n\}_{n=1}^{\infty}$ такова, что $\forall n_1, n_2 \in \mathbb{N}$ $(m_{n_1}, m_{n_2}) = 1$ (числа последовательности $\{m_n\}_{n=1}^{\infty}$ попарно взаимно простые), тогда простых бесконечно много.

Действительно, каждый простой делитель числа m_{n+1} отличен от любого простого делителя чисел $m_1, \dots, m_n$.

Важный пример такой последовательности дают числа Ферма (Пьер Ферма 1607–1665):

$$F_n = 2^{2^n} + 1;\ n = 0, 1, 2, \dots$$

Свойства чисел Ферма

1. Числа Ферма попарно взаимно простые.

Действительно, докажем, что для любого $n \geq 1$

$$F_0 \cdot F_1 \cdot \dots \cdot F_{n-1} = F_n - 2.$$

i) $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$

$n = 1$ $F_0 = F_1 - 2$; $n = 2$ $F_0 F_1 = F_2 - 2$

ii) Пусть $\prod_{k=0}^{n-1} F_k = F_n - 2$, тогда

$$\prod_{k=0}^{n} F_k = \left(\prod_{k=0}^{n-1} F_k\right) F_n = (F_n - 2) F_n = \left(2^{2^n} - 1\right)\left(2^{2^n} + 1\right) =$$

$$= 2^{2^{n+1}} - 1 = F_{n+1} - 2.$$

Если d – общий натуральный делитель F_k и F_n $(k < n)$, то d – делитель 2, т.е. $d = 1$ или $d = 2$.

Так как все числа Ферма нечётные, то $d \neq 2$.

Значит $d = 1$, т.е. $\forall k, n \in \mathbb{N}$ $(F_k, F_n) = 1$.

2. Последняя цифра в десятичной записи каждого F_n, при $n \geq 2$ равна 7.

▷ $F_2 = 17$. Если $n \geq 3$, то в числе $2^{2^n} = (2^4)^{2^{n-2}} = 16^{2^{n-2}}$ последняя десятичная цифра равна 6.

3. Среди чисел вида $2^n + 1$ только числа Ферма могут быть простыми.

▷ Если $n = (2k+1)m$ (т.е. n имеет нечётный делитель, отличный от 1), то

$$2^n + 1 = (2^m)^{2k+1} + 1^{2k+1} = (2^m + 1)(1 - 2^m + 2^{2m} - \ldots + 2^{2km}).$$

Значит $2^n + 1$ делится на $2^m + 1 \geq 3$.

Ферма высказал гипотезу: все числа Ферма – простые.

В 1732 Эйлер (Леонард Эйлер 15.4.1707 – 18.9.1783) показал, что

$$F_5 = 4294967297 = 641 \cdot 6700417$$

NB • В настоящее время известно, что все числа Ферма F_n, при $5 \leq n \leq 32$ являются составными.

• В августе 2017 г. было предъявлено наибольшее число – обобщённое число Ферма:

$$a^{2^n} + b^{2^n} \ (a, b \in \mathbb{N}),$$

$$919444^{1048576} + 1 \ (n = 20).$$

Проверка простоты этого числа с помощью специальной программы заняла 3 суток 23 час 53 мин. Число десятичных знаков этого числа равно 6 253 210.

Числа Мерсенна (Марен Мерсенн 1588-1648) – это числа вида $M_n = 2^n - 1$. Если $n = kl$ – составное, то M_n – составное:

$$M_n = 2^{kl} - 1 = (2^k)^l - 1^l =$$
$$= (2^k - 1)(2^{k(l-1)} + 2^{k(l-2)} + \dots + 1).$$

Значит M_n – простое если n – простое. Обратное утверждение неверно: $M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89$

12 октября 2024 г Люк Дюран предъявил самое большое простое число Мерсенна:

$$2^{136\,279\,841} - 1$$

Число десятичных знаков этого числа равно 41 024 320.