Лекция №
Простые числа

Лектор: Н.Ю. Золотых Записал: М. Гусева

18 октября 2008

Содержание

1. О распределении простых чисел

Обозначим $\pi(x)$ количество простых чисел, не превосходящих x.

Теорема 1 (Чебышев, 1850 г.)**.** *Существуют такие положительные константы* $_1$, $_2$, *что для любого* $n > 1$

$$\frac{c_1 x}{\ln x} < \pi(x) < \frac{c_2 x}{\ln x}$$

Следствие 1. *Пусть* p_n *— n-е простое число, тогда существуют такие положительные* c_3, c_4, *что для всех достаточно больших* n

$$c_3 n \ln n < p_n < c_4 n \ln n. \tag{1}$$

Доказательство. Используя теорему 1, можем записать неравенство

$$\frac{c_1 x}{\ln x} < \pi(x) < \frac{c_2 x}{\ln x}.$$

Подставим $x = p_n$:

$$\frac{c_1 p_n}{\ln p_n} < \pi(p_n) < \frac{c_2 p_n}{\ln p_n},$$

где

$$\pi(p_n) = n.$$

Таким образом,

$$\frac{c_1 p_n}{\ln p_n} < n < \frac{c_2 p_n}{\ln p_n}. \tag{2}$$

Докажем правую часть неравенства (1). Из (2) получаем

$$n < \frac{c_2 p_n}{\ln p_n},$$

откуда

$$p_n > \frac{n \ln n}{c_2} = c_4 n \ln n.$$

Докажем левую часть неравенства (1). Логарифмируя левое из неравенств (2), получаем Рассмотрим

$$\ln n > \ln \frac{c_1 p_n}{\ln p_n} = \ln c_1 + \ln \frac{p_n}{\ln p_n} = \ln c_1 + \ln p_n - \ln \ln p_n.$$

Однако $\ln c_1 + \ln p_n - \ln(\ln p_n) > c_3 \ln p_n$ для некоторого c_3, поскольку

$$\lim_{n->\infty} \frac{\ln c_1 + \ln p_n - \ln(\ln p_n)}{c_3 \ln p_n} = 1.$$

□

Следствие 2. *Существуют такие положительные константы c_6 и c_7, что*

$$c_6 \ln n < p_{n+1} - p_n < c_7 \ln n.$$

Доказательство. По следствию 1 имеем $c_3 n \ln n < p_n < c_4 n \ln n$. Для p_{n+1} имеем

$$c_3(n+1)\ln(n+1) < p_{n+1} < c_4(n+1)\ln(n+1) \qquad (*)$$

Далее,

$$-c_4 n \ln n < -p_n < -c_3 n \ln n \qquad (**)$$

Сложим $(*)$ и $(**)$:

$$c_3(n+1)\ln(n+1) - c_4 n \ln n < p_{n+1} - p_n < c_4(n+1)\ln(n+1) - c_3 n \ln n.$$

Так как $\ln(n+1) > \ln(n)$, то

$$(c_4 - c_3)\ln(n) + c_3 \ln n < p_{n+1} - p_n < (c_4 - c_3) n \ln(n) + c_4 \ln n.$$

Так как $c_4 < c_3$, то $c_4 - c_3 < 0$, то получаем

$$c_3 \ln n < p_{n+1} - p_n < c_4 n \ln n.$$

□

Теорема 2 (Адамар, Валле-Пуссен, 1896; элементарное доказательство — Серберг, 1949)**.**

$$\pi(x) \sim \frac{x}{\ln x} \qquad x \to \infty.$$

2. Проверка простоты числа

2.1. Решето Эратосфена

Это алгоритм нахождения простого числа при помощи перебора всех простых чисел до заданного n. Сложность $O(\sqrt{n}\log^2 n)$.

2.2. Критерий Вильсона

Теорема 3 (Э. Варинг, 1770)**.** *Пусть n — целое число, $n \geq 2$. Для того, чтобы n было простым необходимо и достаточно, чтобы* $(n-1)! \equiv -1 \pmod{n}$.

2.3. Малая теорема Ферма и числа Кармайкла

Теорема 4. *Пусть p — простое и* НОД$(a, p) = 1$*, тогда*

$$a^{p-1} \equiv 1 \pmod{p}. \qquad (3)$$

Доказательство. Доказательство следует из свойств группы Z_p^*, состоящей из чисел $1, 2, \ldots, p-1$ с операцией умножения по модулю p. Действительно, порядок любого элемента a должен делить порядок группы, поэтому $a^{p-1} \equiv 1 \pmod{p}$. □

Проверка (3) для заданного числа p не требует больших вычислений, но, к сожалению, утверждение, обратное малой теореме Ферма, неверно. Более того, имеются составные числа p, обладающие свойством (3) для любого целого a, взаимно простым с p. Эти числа называются числами Кармайкла.

Определение 1. Целое n ($n \geq 2$) называется *псевдопростым по основанию* a ($1 < a < n$), если НОД$(a, n) = 1$ и $a^{n-1} \equiv 1 \pmod{n}$.

Пример 1.

$$a = 2,\ n = 341 = 11 \cdot 31,$$
$$a = 3,\ n = 91 = 7 \cdot 13,$$
$$a = 5,\ n = 217 = 7 \cdot 31,$$
$$a = 7,\ n = 25 = 5 \cdot 5.$$

Определение 2. Составное n называется *числом Кармайкла*, если оно псевдопростое по любому основанию a ($1 < a < n$).

Пример 2.

$$561 = 3 \cdot 11 \cdot 17$$

Теорема 5 (Кармайкл, 1912)**.**

1. *Число Кармайкла свободно от квадратов.*
2. *Если $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$, где $p_1, p_2, \ldots, p_k$ — попарно различные простые числа, то для того, чтобы n было числом Кармайкла необходимо и достаточно, чтобы $(n-1) \vdots (p_i - 1)$ $(i = 1, \ldots, k)$.*
3. *Если $n = p_1 \cdot p_2 \cdot \ldots \cdot p_k$ — число Кармайкла, где $p_1, p_2, \ldots, p_k$ — попарно различные простые числа, то $k \geq 3$.*

Доказательство. Рассмотрим сначала несколько вспомогательных утверждений.

Утверждение 1 (Теорема о разложении мультипликативной группы кольца Z_m.)**.** *Если $m = m_1, m_2, \ldots, m_s$, где m_i попарно взаимно просты, то $Z_m^* \cong Z_{m_1}^* \times \ldots \times Z_{m_s}^*$.*

Утверждение 2. *Группа Z_n^* циклическая для всех $n \geq 1$.*

Перейдем к доказательству теоремы.

1.

2. Пусть $n = p^{e_1} \ldots p^{e_r}$ разложение n на простые числа. По утверждению 1 имеем изоморфизм групп $Z_n^* \to Z_{p_1^{e_1}}^* \times \ldots \times Z_{p_r^{e_r}}^*$ Поэтому, если для любого $a \in Z_n^*$ выполняется $a^{n-1} = 1$, то и для любого $a_i \in Z_{p_i^{e_i}}^*$ выполняется $a_i^{n-1} = 1$. По утверждению 2 группа $Z_{p_i^{e_i}}^*$ циклическая, т.е. в ней имеется элемент a_i порядка $|Z_{p_i^{e_i}}^*| = \Phi(p_i^{e_i}) = p_i^{e_i - 1}(p_i - 1)$. Поэтому $n-1$ делится на этот порядок, а значит $e_i = 1$ и $n-1$ делятся на $p_i - 1$. Наоборот, если $e_i = 1$ и $n-1$ делится на $p_i - 1$ при всех i, то для любого $a_i \in Z_p^*$ выполняется $a_i^{n-1} = 1$. Значит, для любого $a \in Z_n^*$ выполняется $a^{n-1} = 1$.

3. Предположим, что n — число Кармайкла и $n = pq$, где p, q различные простые числа. Тогда $n-1$ делится на $p-1$ и $q-1$. Имеем $n - 1 = (p-1)q + (q-1)$. Тогда $p-1$ делится на $q-1$. Аналогично $q-1$ делится на $p-1$, откуда $p = q$. Противоречие. □