

Обоснование теста Миллера–Рабина для проверки простоты чисел

Записал Дм. Потапов

1. Свидетели простоты

Пусть $n \in N$, где n — нечётно, тогда n можно представить в виде:

$$n - 1 = 2^s t \quad (1)$$

где t — также нечётно.

Определение 1. Число $1 < b < n$ назовём *свидетелем простоты* числа n , если n — сильно псевдопростое по основанию b , т. е. $\text{НОД}(b, n) = 1$ и выполняется

$$b^t \equiv 1 \pmod{n} \quad (2)$$

или

$$\exists k \in \{1, \dots, s-1\} : b^{2^k t} \equiv -1 \pmod{n} \quad (3)$$

Множество всех свидетелей простоты числа n обозначим B . Здесь и далее будем предполагать что n нечётно и не кратно трём.

2. Лжесвидетели

Определение 2. Число $a \in Z_n^*$ назовём *лжесвидетелем* числа n если выполняется одно из следующих условий:

- 1) $a^{n-1} \not\equiv 1 \pmod{n}$
- 2) $a^k \not\equiv -1 \pmod{n}, \forall k \in N$ и для некоторого простого числа p , такого что n делится на него без остатка, порядок a по модулю p равен $p-1$ (т. е. $\forall k \in \{1, \dots, p-2\} : a^k \not\equiv 1 \pmod{n}, a^{p-1} \equiv 1 \pmod{n}$)

Множество всех лжесвидетелей числа n обозначим A .

3. Теорема Рабина

Лемма 1. Произведение лжесвидетеля и свидетеля простоты не является свидетелем простоты, т. е.

$$a \in A, b \in B \Rightarrow ab \pmod{n} \notin B \Rightarrow B \cap aB = \emptyset \quad (4)$$

Доказательство. Рассмотрим два случая:

1) Пусть $a^{n-1} \not\equiv 1 \pmod{n}$, тогда: $(ab)^{n-1} \not\equiv b^{n-1} \pmod{n}$, но по определению свидетеля $b^{n-1} \equiv 1 \pmod{n}$, т. е. $(ab)^{n-1} \not\equiv 1 \pmod{n}$, следовательно $ab \pmod{n} \notin B$

2) Пусть теперь $a^{n-1} \equiv 1 \pmod{n}$ и $\exists p$ — простой делитель n и порядок a по модулю p равен $p-1$ и $a^k \not\equiv -1 \pmod{n}, \forall k \in N$

Воспользуемся формулой (1). Рассмотрим минимальное $k \in \{1, \dots, s-1\} : a^{2^k t} \equiv 1 \pmod{n}$, так как p — делитель n , то $a^{2^k t} \equiv 1 \pmod{p}$, а так как a имеет порядок $p-1$ по модулю p , то $2^k t$ должно делиться на $p-1$ без остатка.

так как t — нечётно, а $p-1$ — чётно, то $2^k t \neq t \Rightarrow k \geq 1 \Rightarrow a^t \not\equiv 1 \pmod{p} \Rightarrow a^t \not\equiv 1 \pmod{n}$

Воспользуемся исходными данными: $\text{НОД}(b, n) = 1$, и n делится на $p \Rightarrow \text{НОД}(b, p) = 1$. Для всех $j : k \leq j \leq s$, $2^j t$ делится на $p - 1$, по малой теореме Ферма будем иметь:

$$b^{2^j t} \equiv 1 \pmod{p} \Rightarrow b^{2^j t} \not\equiv -1 \pmod{n} \quad (5)$$

$$b \in B \Rightarrow b^{2^j t} \equiv 1 \pmod{n}, \forall j : k \leq j \leq s \text{ и } b^{2^{k-1} t} \equiv \pm 1 \pmod{n} \quad (6)$$

Отсюда имеем:

$$(ab)^{2^j t} \equiv b^{2^j t} \equiv 1 \pmod{n}, \forall j : k \leq j \leq s \quad (7)$$

и

$$(ab)^{2^{k-1} t} \equiv \pm a^{2^{k-1} t} \not\equiv \pm 1 \pmod{n} \quad (8)$$

$$(\text{Так как } a^{2^{k-1} t} \not\equiv 1 \pmod{n} \text{ и } a^k \not\equiv -1 \pmod{n}, \forall k \in N) \quad (9)$$

Следовательно ab не является свидетелем простоты числа n . $\square$

Лемма 2. Пусть n — нечётное число, число n — простое и n делится на p^2 без остатка, тогда множество

$$\{1 + kn/p, k = 0, \dots, p-1\} \quad (10)$$

образует подгруппу в Z_n^* порядка n и все элементы за исключением единицы имеют порядок n .

Доказательство. Возьмем любые два элемента из данной подгруппы и перемножим их:

$$(1 + kn/p)(1 + k'n/p) = 1 + (k + k')n/p + kk'n^2/p^2 \equiv 1 + (k + k')n/p \pmod{n} \quad (11)$$

т. е.

$$(1 + kn/p)(1 + k'n/p) \equiv 1 + (k + k')n/p \pmod{n} \quad (12)$$

Из этого равенства видно что данная подгруппа изоморфна циклической группе порядка n . $\square$

Лемма 3. Пусть $a, b \in Z_n^*$, $a \neq b$, тогда $Ba \cap Bb = \emptyset \iff B \cap Bab^{-1} = \emptyset$

Доказательство. Очевидно. Отображение $x \mapsto xa$ задаёт взаимно однозначное соответствие между B и Ba . множества B и Ba равномоцны и целиком содержатся в Z_n^* ($a \in Z_n^*$). $\square$

Лемма 4. Пусть n делится на p^2 (p — простое), тогда мощность множества B не превосходит $\frac{\phi(n)}{p}$.

Доказательство. Рассмотрим группу $G = \{1 + kn/p, k = 0, \dots, p-1\}$ из Леммы 2, так как n делится на p , следовательно $n - 1$ на p не делится, следовательно $\forall a \in G (a \neq 1) : a^{n-1} \not\equiv 1 \pmod{n}$, что означает что a — лжесвидетель. По Лемме 1, $B \cap Ba = \emptyset$, воспользуемся Леммой 3:

$$\forall g_1, g_2 \in G, g_1 \neq g_2 : B \cap Bg_2g_1^{-1} = \emptyset \text{ (} a \text{ обозначили как } g_2g_1^{-1} \text{)} \Rightarrow Bg_1 \cap Bg_2 = \emptyset \quad (13)$$

Все Bg содержатся в Z_n^* , а значит и их объединение тоже, следовательно:

$$\left| \bigcup_{g \in G} Bg \right| \leq |Z_n^*| = \phi(n) \quad (14)$$

Но все Bg попарно не пересекаются и равномоцны, а значит:

$$\left| \bigcup_{g \in G} Bg \right| = p|B| \leq \phi(n) \Rightarrow |B| \leq \frac{\phi(n)}{p} \quad (15)$$

$\square$

Лемма 5 (Теорема Рабина). Пусть n свободно от квадратов, тогда мощность множества B не превосходит $\frac{\phi(n)}{4}$.

Доказательство. Пусть $p_1, p_2, \dots, p_k$ — все простые делители n , ($3 < p_k < \dots < p_2 < p_1$, $k \geq 2$). Пользуясь китайской теоремой об остатках и теоремой о существовании первообразного элемента выберем a_1 и a_2 ($a_1 \neq a_2$) такие что

$$\begin{aligned} a_1 &\equiv 1 \pmod{p_2}, a_1 \equiv 1 \pmod{p_3}, \dots, a_1 \equiv 1 \pmod{p_k}, \text{ord}_{p_1} a_1 = p_1 - 1, \\ a_2 &\equiv 1 \pmod{p_1}, a_2 \equiv 1 \pmod{p_3}, \dots, a_2 \equiv 1 \pmod{p_k}, \text{ord}_{p_2} a_2 = p_2 - 1. \end{aligned}$$

Заметим что:

$$a_i \equiv 1 \pmod{\frac{n}{p_i}} \Rightarrow \forall j \in N : a_i^j \equiv 1 \pmod{\frac{n}{p_i}} \Rightarrow \forall j \in N : a_i^j \not\equiv -1 \pmod{n} \quad (16)$$

Значит a_1, a_2 — лжесвидетели. Рассмотрим два случая:

$k = 2$: если для некоторого $j : (a_1 a_2)^j \equiv 1 \pmod{n} \Rightarrow (a_1 a_2)^j \equiv 1 \pmod{p_1} \Rightarrow a_1^j \equiv 1 \pmod{p_1} \Rightarrow j$ делится на $p_1 - 1$. $n - 1$ не делится на $p_1 - 1$ (так как $n - 1 = p_2(p_1 - 1) + p_2 - 1$, $p_2 < p_1$), следовательно $(a_1 a_2)^{n-1} \not\equiv 1 \pmod{n}$, а значит $a_1 a_2$ — третий лжесвидетель.

$k \geq 3 : a_1 a_2 \equiv 1 \pmod{\frac{n}{p_1 p_2}} \Rightarrow \forall j \in N : (a_1 a_2)^j \equiv 1 \pmod{\frac{n}{p_1 p_2}} \Rightarrow \forall j \in N : (a_1 a_2)^j \not\equiv -1 \pmod{n}$, а значит $a_1 a_2$ — снова третий лжесвидетель.

Итак, у нас есть три различных лжесвидетеля, применим лемму 3: группы B, Ba_1, Ba_2 и $Ba_1 a_2$ попарно различны, равномощны, попарно не пересекаются и целиком содержатся в Z_n^* , а значит:

$$|B \cup Ba_1 \cup Ba_2 \cup Ba_1 a_2| = 4|B| \leq Z_n^* = \phi(n) \quad (17)$$

т. е. $|B| \leq \frac{\phi(n)}{4}$ что и требовалось доказать. $\square$