АЛГОРИТМ МИЛЛЕРА-РАБИНА

Лекция А.И. Галочкина

Теорема 1. *Пусть n – нечетное натуральное число, имеющее $r \geq 1$ простых делителей, t – нечетное натуральное число; $M(n,\, t)$ – множество натуральных чисел x $(1 \leq x < n, \quad (x,\, n) = 1)$, для которых выполняется хотя бы одно из сравнений*

$$x^t \equiv 1 \mod n \tag{1}$$

$$x^{2^k t} \equiv -1 \mod n\,, \quad k = 0\,, 1\,, 2\,, \ldots\,. \tag{2}$$

Тогда количество чисел в множестве $M(n,\, t)$

$$\# M(n,\, t) \leq \frac{\varphi(n)}{2^{\,r-1}}\,. \tag{3}$$

Пусть разложение числа n на простые сомножители имеет вид

$$n = p_1^{s_1} \cdots p_r^{s_r}\,, \quad d = \min_{j=\overline{1,\,r}} \nu_2(p_j - 1) \geq 1\,. \tag{4}$$

Лемма 1. *При $k \geq d$ сравнение (2) не имеет решений.*

Доказательство. Допустим противное: x_0 – решение сравнения (2) при $k \geq d$. Из (4) следует, что существует такое простое число $p \mid n$, что $\nu_2(p-1) = d \geq 1\,, \quad p - 1 = 2^{\,d} l$, где l – нечетное число. Мы имеем:

$$x_0^{2^k t} \equiv -1 \mod p\,, \quad x_0^{2^k t l} \equiv -1 \mod p\,, \quad x_0^{(p-1)2^{k-d} t} \equiv -1 \mod p\,,$$

что противоречит малой теореме Ферма. □

Доказательство теоремы 1. При каждом $j, \quad 1 \leq j \leq r$, сравнение

$$x^t \equiv 1 \mod p_j^{s_j}$$

имеет не более

$$\big(\,t,\, \varphi(p_j^{s_j})\big) \leq \frac{\varphi(p_j^{s_j})}{2^{\,d}} \tag{5}$$

решений. По китайской теореме об остатках сравнение (1) имеет не более

$$\prod_{j=1}^{r} \frac{\varphi(p_j^{s_j})}{2^{\,d}} = \frac{\varphi(n)}{2^{\,dr}}$$

Поскольку $(ab,\, c) \le (ab,\, ac) = a(b,\, c)$, то сравнение

$$x^{2^k t} \equiv -1 \mod p_j^{s_j}$$

имеет не более

$$\left(\, 2^{\,k}t,\, \varphi(p_j^{s_j})\right) \le 2^{\,k} \frac{\varphi(p_j^{s_j})}{2^{\,d}} \tag{6}$$

решений, а сравнение (2) – не более, чем $2^{\,kr}\dfrac{\varphi(n)}{2^{\,dr}}$ решений. Следовательно, по лемме 1

$$\#M(n,\, t) \le \frac{\varphi(n)}{2^{\,dr}} \left(1 + \sum_{k=0}^{d-1} 2^{kr} \right) = \varphi(n) \left(\frac{1}{2^{\,r}-1} + \frac{2^{\,r}-2}{(2^{\,r}-1)\, 2^{\,dr}} \right)\,, \tag{7}$$

а, так как $d \ge 1$, то получаем оценку (3). □

Дальнейшие рассуждения основываются на следующей лемме

Лемма 2. *Пусть n – нечетное число, для которого имеют место равенства (4), t – нечетное число, а число $u > 1$. Пусть далее для некоторого $j \quad (1 \le j \le r)$ выполняется неравенство*

$$\left(\, t,\, \varphi(p_j^{s_j})\right) \le \frac{\varphi(p_j^{s_j})}{u2^{\,d}} \tag{8}$$

Тогда

$$\#M(n,\, t) \le \frac{\varphi(n)}{u2^{\,r-1}}\,. \tag{9}$$

Доказательство леммы почти дословно повторяет доказательство теоремы 1. Одно из неравенств (5) заменится на неравенство (8). Соответствующее неравенство (6) заменится на оценку

$$\left(\, 2^{\,k}t,\, \varphi(p_j^{s_j})\right) \le 2^{\,k} \frac{\varphi(p_j^{s_j})}{u2^{\,d}}\,,$$

в результате чего в оценке (7) множитель $\dfrac{\varphi(n)}{2^{\,dr}}$ заменится на $\dfrac{\varphi(n)}{u2^{\,dr}}$ и, вместо оценки (3), получим (9).

Лемма 3. *Пусть p – простое число, $p^2 \mid n, \quad p \nmid t$, тогда*

$$\#M(n,\,t) \le \frac{\varphi(n)}{p2^{\,r-1}}\,.$$

Доказательство. Пусть $n = p^{\,s}p_2^{s_2}\cdots p_r^{s_r}\,, \quad s \ge 2$. Тогда $p \mid \varphi(n)\,, \quad p \nmid t$ и

$$\big(\,t,\,\varphi(p_j^{s_j})\big) \le \frac{\varphi(p^{\,s})}{p2^{\,d}}$$

и осталось воспользоваться леммой 2. □

Алгоритм Миллера-Рабина отсеивания составных чисел

Задано нечетное число n. Требуется установить, является ли это число составным.

Пусть $n-1 = 2^{\,s}t\,, \quad t$ нечетно. Выбираем случайным образом натуральное число $x \quad (1 < x < n)$.

1) Если $(x,\,n) > 1$, то n – составное число. СТОП.

2) Если $(x,\,n) = 1$ и не выполняется ни одно из сравнений (1) и (2) при $0 \le k < s$, то n – составное число. СТОП.

В противном случае выбираем другое число x.

Обозначим: $M(n) = M(n,\,t)$.

Теорема 2. *Пусть составное число n не делится ни на 2, ни на 3. Тогда*

$$\#M(n) \le \frac{\varphi(n)}{4}\,.$$

Доказательство. Из теоремы 1 и леммы 3 следует, что для завершения доказательства теоремы осталось разобрать только случай $n = p_1p_2$, где p_1 и p_2 – различные нечетные простые числа. Из теоремы 1 следует, что $\#M(n) \le \frac{\varphi(n)}{2}$, но учитывая специфику выбора t, эту оценку можно усилить. Пусть

$$p_j - 1 = 2^{\,s_j}l_j\,, \quad 2 \nmid l_j\,, \quad 1 \le s_1 \le s_2\,, \quad d = s_1\,, \quad j = 1,\,2\,. \tag{10}$$

Если при $j = 1$ или 2 число $l_j \nmid t$, то существует нечетное простое число q, такое, что $\nu_q(l_j) > \nu_q(t)$, поэтому

$$(t,\,p_j - 1) \le \frac{\varphi(p_j)}{q2^{\,d}}$$

и по лемме 2 при $r = 2$

$$\#M(n) \le \frac{\varphi(n)}{2q} \le \frac{\varphi(n)}{6}\,,$$

то есть в этом случае теорема доказана.

Осталось рассмотреть случай $l_1 \mid t\,,\quad l_2 \mid t$, а значит $l_1 \mid (n-1)\,,$ $l_2 \mid (n-1)$. Из (10) и равенства

$$n - 1 = p_1p_2 - 1 = (p_1 - 1)(p_2 - 1) + (p_1 - 1) + (p_2 - 1)$$

следует, что $l_1 \mid (p_2 - 1)\,,\quad l_2 \mid (p_1 - 1)$, а так как l_1 и l_2 – нечетные числа, то из (10) следует, что $l_1 \mid l_2$ и $l_2 \mid l_1$, значит $l_1 = l_2$. Обозначим: $l = l_1 = l_2$. Равенства (10) принимают вид:

$$p_1 - 1 = 2^{s_1} l\,,\quad p_2 - 1 = 2^{s_2} l\,,\quad d = s_1 < s_2$$

(при $s_1 = s_2 \qquad p_1 = p_2$, что исключено). Следовательно,

$$(t,\, p_2 - 1) = (t,\, \varphi(p_2)) \le \frac{\varphi(p_2)}{2^{s_2}} \le \frac{\varphi(p_2)}{2 \cdot 2^{d}}$$

и утверждение теоремы следует из леммы 2 и неравенства $d \ge 1$. $\square$

ЗАМЕЧАНИЕ. При помощи теоремы 1 можно привести быстрый вероятностный алгоритм, позволяющий по известным открытом и секретном ключам в алгоритме RSA разлагать n в произведение двух простых множителей.