# Генерация простых чисел

Как проверить число на простоту?

① „В лоб"

Переберём все числа x от 2 до $\sqrt{N}$
и проверим $N \vdots x$

Сложность $O(n^2\sqrt{N}) = O(n^2 2^{n/2})$

$|N| = \log N = n$

② Th. Ферма

$a^{p-1} \equiv 1 \mod p$

p - простое
$a \not\vdots p$

Th. Эйлера

$a^{\varphi(n)} \equiv 1 \mod n$

## Тест Ферма

Вход: N
Выбираем случайное $a \in [2, N-1]$
и проверяем

$$a^{N-1} \equiv 1 \mod N$$

правда ↙ ↘ неправда

„Не знаю", но N - простое

N - составное

Утв: $\exists$ N - составное и $\exists$ a: $a^{N-1} \not\equiv 1 \mod N$

НОД(a, N) = 1

свидетель не простоты

⇒ Как минимум половина чисел 2.. N-1 тоже являются свидетелями непростоты.

$\exists\ b: \quad b^{N-1} \equiv 1 \mod N$

↑ плохое число, число Ферма

$\forall\ c = a \cdot b \quad c^{N-1} = \underbrace{a^{N-1}}_{\neq 1} \cdot \underbrace{b^{N-1}}_{1} \not\equiv 1 \mod N$

Ферма # "лжеца" $b$ $\exists$ "свидетель" $c$.

$b_1$ и $b_2$ — "плохие"

$ab_1 \not\equiv ab_2 \mod N$, т.к. $a$ обратимо

$c_1'' \qquad c_2''$

$\Rightarrow \forall\ b_i \ \exists\ c_i \Rightarrow |\{b_i\}| \leq \frac{1}{2}(N-1)$

$\Rightarrow$ Вероятность того, что случайное $a$ будет "лжецом" $\leq \frac{1}{2}$.

Следствие:

Если мы запустим тест Ферма для $k$ случайных $a_1 .. a_k \in [2, N-1]$, то они ошибётся с вер-ю $\leq 1/2^k$.

Числа Кармайкла

Числа, у которых нет свидетелей:

$N$ — составное

Первое = 561 = 3·11·17

$\forall\ a = 2 \ldots N-1$, НОД$(a,N)=1$ $\quad a^{N-1} \equiv 1 \mod N$

Тест Миллера - Рабина

Выбираем $a$.

1. Проверяем $a^{N-1} \equiv 1 \mod N$
2. $N-1 = 2^s \cdot d$, $d$ — нечётное

Вычислим: $a^d \bmod N = \ldots$ ?

$a^{2d} \bmod N = \ldots \neq 1$

$\vdots$

$a^{2^s d} \bmod N = 1$

- Если все эти числа = 1 $\Rightarrow$ всё ОК, $N$ - простое
- Если среди этих чисел есть не 1, то посмотрим на последнее такое число. Если оно не равно $-1$ $\Rightarrow$ нам нашли нетривиальный корень из 1 $\Rightarrow$ $N$ - составное.
- По Т. Рабина этот тест ошибётся с вер-ю $\leq \frac{1}{4}$

Следствие:

Если повторить тест Р-М $k$ раз $\Rightarrow$ получим ошибку с вер-ю $\leq \frac{1}{4^k}$

Как сгенерировать простое число?

Возьмём случайное и проверим.

$\#$ простых чисел $\leq N \approx \frac{N}{\log N}$

Случайное $n$-битовое число будет простым с вер-ю $1/n$

$\Rightarrow$ В среднем нам потребуется сделать $n$ попыток

# Хороши ли вероятностные алгоритмы?

1. Если мы взяли числа от $1..10^9$ и проверили их с $a=2$, то мы получим 0.002 % ошибок.

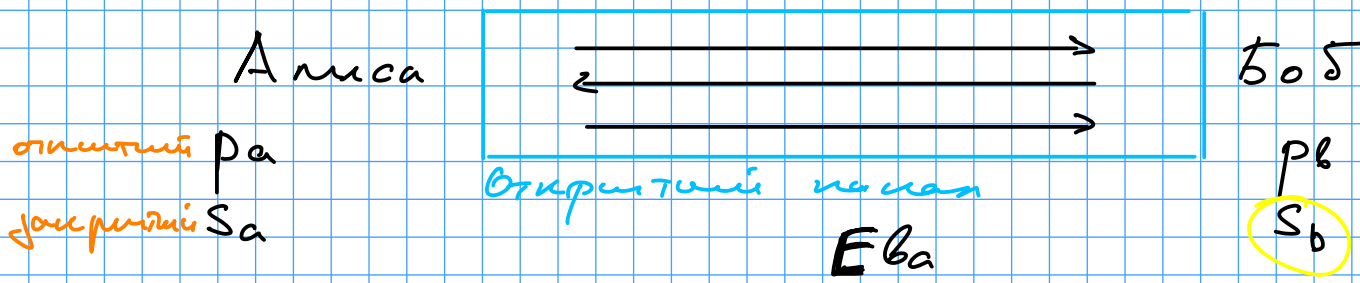
   $\Rightarrow$ "индустриальные простые числа"

2. Э детерминированный алгоритм (Агравал – ... – – ...) 2002
   Алгоритм был $O(n^{12})$
   Сейчас $O(n^4)$

NB: Проверка на простоту не даёт разложение на множители

Эту задачу быстро решать не умеют.

## RSA




$E(m, p_a)$ – шифрование

$D(E(m, p_a), S_a) \to m$ дешифрование

- Действия Алисы: Послать: $C = E(m, p_b)$
- Действия Боба: $D(C, S_b) \to m$

- Предположение: невозможно восстановить $m$ по $E(m, pb)$ и $pb$

↑

Шифрование с открытым ключом

Схема RSA

$p, q \in P$

$n = p \cdot q$

$\exists e: НОД(e, (p-1)(q-1)) = 1$

Возьмём $d$: $d \cdot e \equiv 1 \mod (p-1)(q-1)$

(из алгоритма Евклида)

Утв: $(m^e)^d \equiv m \mod N$

$d \cdot e \equiv 1 \mod \underbrace{(p-1)(q-1)}_{= \varphi(n)} \Rightarrow de - 1 : \varphi(n)$

$\forall m < n,\ m^{e \cdot d} \equiv m^{k\varphi(n)} \cdot m \mod N$

$m^{k\varphi(n)} \equiv 1$

Открытый ключ: $(n, e)$

Закрытый ключ: $(d)$

$E(m, (n, e)) \to m^e \mod n$

$D(c, (d)) \to c^d \mod n$

Предположение: по $n, e, m^e \mod n$ нельзя восстановить $m$ за "разумное" время

Замечания:

1. На самом деле в RSA шифруют ключ для шифрования с закрытым ключом
2. Схема работает только для пассивного противника
3. Можно использовать RSA для цифровой подписи