Тест на простоту Миллера-Рабина.

$a^{p-1} \equiv 1 \bmod p$, p-простое (Тма Ферма).

$p-1 = 2^k \cdot q$, q-нечётное. Тогда для a т.ч. $p \nmid a$; либо

1) $a^q \equiv 1 \bmod p$, либо

2) одно из чисел $a^q, a^{2q}, \dots, a^{2^{k-1}q} \equiv -1 \bmod p$.

$a^q, a^{2q}, \dots, a^{2^{k-1}q}, a^{2^k q} \equiv 1 \bmod p$, все предыдущие числа в списке – квадраты друг друга

$a^{2^k q} \equiv 1 \bmod p$

Тогда либо первое число в списке, $a^q \equiv 1 \bmod p$ (и все остальные $\equiv 1 \bmod p$), либо найдётся b в списке т.ч. $b \neq 1$ и $b^2 \equiv 1 \bmod p$, т.е. $b \equiv -1 \bmod p$.

$\begin{cases} a^q \neq 1 \bmod p \\ a^{2^i q} \neq -1 \bmod p \text{ для } \forall i = 0 \dots k-1, \end{cases}$ выполняются, то

Если $\exists\, a$ т.ч. $\gcd(a, n) = 1$ и оба условия

a – "свидетель" того, что n-составное.

Miller-Rabin (n, a: $\gcd(a, n) = 1$) и

1. $n - 1 = 2^k q$, q-нечётное
2. $a := a^q \bmod n$
3. Если $a \equiv 1 \bmod n$
   вернуть "НЕ ЗНАЮ"
   ⊥
4. для $i = 0 \dots k-1$
   Если $a \equiv 1 \bmod n$
   вернуть ⊥
   $a := a^2 \bmod n$
5. Вернуть "n-составное"

Алгоритм повторяется k раз для случайно выбранных $a \in [2, n-2]$

Время работы: $O(k \lg^3 n)$, если исп. быстрое возведение в степень.

Вероятность ошибки (т.е. алгоритм вернул ⊥ для n-составного): 2^{-2k}

Лекция #~~8~~ 8

Тест на простоту, основанный на эллиптических кривых.

Задача: По данному (большому) числу p, определить, является ли p простым числом и, если да, вывести док-во ("сертификат") простоты p.

Самый быстрый на сегодняшний день **вероятностный** алгоритм предложен S. Goldwasser, J. Kilian "Primality testing using elliptic curves" '1986. С последующими улучшениями. Он работает за время $\text{poly}\lg p$, проверка сертификата простоты: $O(\lg^4 p)$

Детерминированные алгоритмы (Cohen, Lenstra "Primality testing & Jacobi Sums 1984) работают за квази-полиномиальное от $\lg p$ время: $(\lg p)^{O(\lg\lg p)}$

Т.е. детерминированные алгоритмы пригодны для небольших чисел p.

I. Предварительные сведения

Теорема 1 (О распределении порядков случайных эл. кривых, док-во в Lenstra "Factoring integers with elliptic curves")

$\exists p>5$ - простое, $S \subseteq \{p+1-L\sqrt{p}\rfloor, p+1+L\sqrt{p}\rfloor\}$, $|S|>\frac{2}{3}$. $\exists A, B \in \mathbb{F}_p$. Тогда $\exists c$ - константа ($c \in \Theta(1)$) т.ч.

$$\Pr\left[\#E_{A,B}(\mathbb{F}_p) \in S\right] > \frac{c}{\lg p} \cdot \frac{|S|-2}{2\lfloor L\sqrt{p}\rfloor+1},$$

где $\#E_{A,p}(\mathbb{F}_p)$ - число $\mathbb{F}_p$-рац. точек на кривой $E_{A,B}: y = x^3+Ax+B$.

Неформальная интерпретация теоремы: число точек на E_{AB} ведет себя как случайное число из интервала $[p+1-L\sqrt{p}\rfloor, p+1+L\sqrt{p}\rfloor]$.

Лемма 2 ~~(Лекция #3 доказ-во)~~

Пусть $n \in \mathbb{Z}$, $2,3 \nmid n$; $p>3$ - простой делитель n и $4A^3+27B^2 \not\equiv 0 \bmod p$. Для любого $x \in \mathbb{Z}/n\mathbb{Z}$ зададим $x_p := x \bmod p$ и для любой точки $L=(x,y) \in E_{A,B}(\mathbb{Z}/n\mathbb{Z})$ зададим $L_p=(x_p, y_p) \in E_{A,B}(\mathbb{F}_p)$, $\mathcal{O}_p = \mathcal{O}_* \in E_{A,B}(\mathbb{Z}/n\mathbb{Z})$. Тогда $\forall L, M \in E_{A,B}(\mathbb{Z}/n\mathbb{Z})$ если $L+M$ определено, то $(L+M)_p = L_p + M_p$ (↑ на $E_{A,B}(\mathbb{Z}/n\mathbb{Z})$, ↑ на $E_{AB}(\mathbb{F}_p)$).

Док-во: проверить ф-лы сложения ~~см. лекцию~~ для $E_{AB}(\mathbb{Z}/n\mathbb{Z})$, см. лекцию ~~#7~~

Теорема 3 (Критерий простоты)

$\exists n \in \mathbb{Z}$, $2,3 \nmid n$. Пусть далее $A, B \in \mathbb{Z}/n\mathbb{Z}$ т.ч. $\gcd(4A^3+27B^2, n) = 1$ и $L \neq 0$ на $E_{A,B}(\mathbb{Z}/n\mathbb{Z})$. Тогда если $\exists$ простое $q > (\sqrt[4]{n}+1)^2$ т.ч. $qL = 0$, то n - простое.

◁ От противного: $\exists n$ - составное $\Rightarrow \exists p > 3$ т.ч. $p \mid n$ и $p \leq \sqrt{n}$.

Заметим, $\gcd(4A^3+27B^2, p) \neq 0 \bmod p$ (иначе мы бы получили противоречие с условием $\gcd(4A^3+27B^2, n) = 1$). Тогда по лемме 2 $L_p \in E_{A,B}(\mathbb{F}_p)$ и

$q \cdot L_p = (qL)_p = 0_p = 0$. $\Rightarrow$ $\mathrm{ord}(L_p)$ должен делить q.

По Теореме Хассе, $\mathrm{ord}(L_p) \leq \#E_{A,B}(\mathbb{F}_p) \leq (\sqrt{p}+1)^2 \leq (\sqrt[4]{n}+1)^2 < q \Rightarrow$

($\#E_{A,B}(\mathbb{F}_p) \leq p+1+2\sqrt{p} = (\sqrt{p}+1)^2$)

Противоречие $\Rightarrow$ n - простое. ▷

основная

II Алгоритм: тестирование на простоту

основная идея: ~~сведем доказательство что (простое) p простое~~

Сведём док-во простоты p к док-ву простоты $q \leq \frac{p}{2} + o(p)$, рекурсивно применим алгоритм к q пока не получим достаточно малое значение q такое, что детерминированные тесты будут эффективны.

Для заданного p, построим кривую $E_{A,B}$ над $\mathbb{F}_p$ с точкой $L \in E_{A,B}(\mathbb{F}_p)$ порядка $q \approx p/2$.

Alg. 1. Gen_curve (p)

1. $A, B \xleftarrow{R} \mathbb{F}_p$ т.ч.: (a) $(4A^3+27B^2, p) = 1$
   (b) $\#E_{A,B}(\mathbb{F}_p) \in [\, p+1-\frac{1}{2}\lfloor\sqrt{p}\rfloor,\ p+1+\lfloor\sqrt{p}\rfloor \,]$ ← используют эффективные алгоритмы подсчёта точек на кривой, i.e. Алг. Схоофа
   (c) $\#E_{A,B}(\mathbb{F}_p)$ - чётно
2. $q = \#E_{A,B}(\mathbb{F}_p) / 2$
   Если $2 \mid q$ или $3 \mid q$, вернуться к шагу 1.
3. Запустить вероятностный алгоритм проверки q на простоту (алгоритм Миллера-Рабина) на $O(\lg p)$ шагов (т.е. чтобы вероятность ошибки была $\sim 2^{-\lg p}$.

Alg. 2 Find_point (p, q, A, B)

1. $X \xleftarrow{R} \mathbb{F}_p$ т.ч. X^3+AX+B - квадрат в $\mathbb{F}_p$.
2. $Y \xleftarrow{R} \{\pm\sqrt{X^3+AX+B}\}$, $L := (X, Y)$
3. Если $q \cdot L \neq 0$, вернуться к шагу 1
4. Вернуть L

Alg.3 Prove_prime (p)

LB = число бит в числе таком, что детерм. алгоритмы простоты эффективны для этого числа

1. $i = 0$
   $p_0 = p$
2. Пока $p_i > 2^{LB}$:
   2.1 (A_i, B_i), $p_{i+1} \leftarrow$ Gen_curve (p)
   2.2. $L_i \leftarrow$ Find-point (p_i, p_{i+1}, A, B)
   2.3 $i := i + 1$
   2.4. Если $i \geq (\lg p)^{\lg\lg p}$ V или $2 \mid p_i$, или $3 \mid p_i$, вернуться к шагу 1.
3. Проверить p_i на простоту детерминированным алгоритмом. ← в лабе: тривиальным делением на числа до $\sqrt{p_i}$
   Если p_i не док-но простым, вернуться к шагу 1.
4. Вернуть $C = ((A_0, B_0), L_0, p_1, \dots, (A_i, B_i), L_i, p_{i+1})$

Корректность:

- p – простое ⇒ выход C – сертификат – "свидетельство" простоты p. На шагах 2.1, 2.2. мы получаем кривую E_{A_i, B_i} и точку L_i порядка p_{i+1}, удовлетворяющие условиям Теоремы 3.
- p – составное ⇒ получим делители p на шаге 3 (или ранее) (2,3 | p)
  Алгоритма Find-point(), аналогично алгоритму факторизации.

Сложность:

Alg.1 самый затратный шаг: 1 (b) – подсчёт $\#E_{A,B}(F_p)$.
Алг. Скофа: $\tilde{O}(\log^8 p)$. В-ть того, что $\#E_{A,B}(F_p)$ лежит в нужном интервале – Теорема 1.

Alg.2 ——— // ——— Шаг 1: $X \not\equiv F_p$ – кв. вычет с вероятностью $O(1)$.

Шаг 4: Быстрое умножение на q:
$O(\lg q \cdot \lg^2 p) = O(\lg^3 p)$

Alg.3 В каждой итерации шага 2 p_i уменьшается на 2
⇒ ожидает $O(\lg p)$ итераций.
Доминирующий шаг: Шаг 1 (b) алгоритма Gen_curve()

⇒ Общее время работы: $O(\lg^9 p)$. # кривых $E_{A,B}$, не удовлетворяющих св-вам (a)–(c) шага 1 в Gen_curve
$= O(\lg^3 p)$ (эвристика).

ПРОВЕРКА СЕРТИФИКАТА

Alg 4 Check-Prime $(p_0, ((A_0, B_0), L_0, P_1), \dots, ((A_{i-1}, B_{i-1}), L_{i-1}, P_i))$

Выход: {Reject, Accept}

Для $j = 0 \dots i-1$:

(a) Assert $(2 \nmid p_j)$

(b) Assert $(3 \nmid p_j)$

(c) Assert $(4A_j^3 + 27B_j^2, p) = 1$

(d) Assert $(p_{j+1} > (\sqrt[4]{p_j} + 1)^2)$

(e) Assert $L_j \neq 0$

(f) Assert $p_{j+1} L_j = 0$

ВЕРНУТЬ Accept

КОРРЕКТНОСТЬ Если Check-Prime() возвращает Accept $\Rightarrow p_i$ – простое $\Rightarrow$ p_{i-1} простое по Теореме 3 ($\Rightarrow \dots \Rightarrow p_0$ – простое)

условия (a), (b) проверяются на шаге 2.4. Alg. 3 Prove-prime

(c) – шаг (1).(a) Alg 1 Gen-curve.

(d) Т-ма Хассе: $\#E_{A,B}(\mathbb{F}_{p_j}) \geq (\sqrt{p_j} - 1)^2 \Rightarrow$

$$p_{j+1} = \frac{\#E(\mathbb{F}_{p_j})}{2} \geq \frac{(\sqrt{p_j} - 1)^2}{2} > (\sqrt[4]{p_j} + 1)^2 \quad \forall p_j > 37$$

(для столь малых p_j проверка на простоту тривиальна).

(e), (f) проверяются в Find-Point шаг 3

КОНЕЦ

ВРЕМЯ РАБОТЫ: Проверка каждого p_j: $O(\lg^3 p)$ – шаг (f) самый затратный

Всего: $O(\lg p)$ различных p_j в сертификате C

$\Rightarrow O(\lg^4 p)$.