

Полиномиальный алгоритм проверки простоты числа

Комалёва Ольга



План семинара

- Постановка задачи
- Идея алгоритма
- Полиномиальный алгоритм
- Оценка времени работы алгоритма
- Доказательство корректности алгоритма

Постановка задачи

Дано натуральное число n .
Необходимо проверить является ли оно простым за полиномиальное время от длины числа n в бинарной форме.

План семинара

- Постановка задачи
- **Идея алгоритма**
- Полиномиальный алгоритм
- Оценка времени работы алгоритма
- Доказательство корректности алгоритма

Основная идея алгоритма

Лемма 1.1.

Пусть $a \in \mathbb{Z}$, $n \in \mathbb{N}$, $n \geq 2$, $a \in \mathbb{Z}_n^*$. Тогда

n - простое $\Leftrightarrow (X + a)^n \equiv X^n + a \pmod{n}$.

План семинара

- Постановка задачи
- Идея алгоритма
- Полиномиальный алгоритм
- Оценка времени работы алгоритма
- Доказательство корректности алгоритма

Алгоритм Agrawal

Input : integer $n > 1$

1. if $(\exists a, b > 1 : n = a^b)$ output COMPOSITE
2. $r = \min \{a : o_a(n) > \log^2 n\}$
3. if $(\exists a \leq r : 1 < \gcd(a, n) < n)$ output COMPOSITE
4. if $(n \leq r)$ output PRIME
5. for $a = 1$ to $\lfloor \sqrt{\phi(r)} \log n \rfloor$ do
 if $((X + a)^n \neq X^n + a \pmod{X^r - 1, n})$ output COMPOSITE
6. output PRIME

План семинара

- Постановка задачи
- Идея алгоритма
- Полиномиальный алгоритм
- Оценка времени работы алгоритма
- Доказательство корректности алгоритма

Время работы алгоритма

Лемма 2.1.

Пусть $LCM(m)$ - наименьшее общее кратное первых m чисел. Тогда, начиная с $m=7$, $LCM(m) \geq 2^m$.

Лемма 2.2.

Существует $r \leq \max(3, \lceil \log^5 n \rceil)$, и $o_r(n) > \log^2 n$.

Время работы алгоритма

Лемма 2.3.

Асимптотическая сложность алгоритма равна

$O\sim(\log^{21/2} n)$. Где $O\sim(t(n))$ равносильно $O(t(n)poly(\log(t(n))))$.

Доказательство:

Шаг 1: $O\sim(\log^3 n)$

Шаг 2-3: $O\sim(r(\log^2 n \log r + \log n)) = O\sim(\log^5 n)$

Шаг 4: $O\sim(\log n)$

Шаг 5: $O\sim((\sqrt{\varphi(r)} \log n) r \log^2 n) = O\sim(\log^{21/2} n)$

Так как каждая проверка равенства требует $O(\log n)$ умножений полиномов степени r с коэффициентами размером $O(\log n)$

Время работы алгоритма

Лемма 3.2.(Фоуври)

$P(n)$ - наибольший простой делитель n .

$\pi(x)$ - число простых чисел $p \leq x$, для которых

$P(p-1) > x^{2/3}$. Тогда $\exists c > 0, n_0 \in \mathbb{N} : \forall x \geq n_0 \quad \pi(x) \geq c \frac{x}{\log x}$.

Лемма 3.3.

Асимптотическая сложность алгоритма равна

$O^{\sim}(\log^{15/2} n)$.

План семинара

- Постановка задачи
- Идея алгоритма
- Полиномиальный алгоритм
- Оценка времени работы алгоритма
- Доказательство корректности алгоритма

Алгоритм Agrawal

Input : integer $n > 1$

1. if $(\exists a, b > 1 : n = a^b)$ output COMPOSITE
2. $r = \min \{a : o_a(n) > \log^2 n\}$
3. if $(\exists a \leq r : 1 < \gcd(a, n) < n)$ output COMPOSITE
4. if $(n \leq r)$ output PRIME
5. for $a = 1$ to $\lfloor \sqrt{\phi(r)} \log n \rfloor$ do
 if $((X + a)^n \neq X^n + a \pmod{X^r - 1, n})$ output COMPOSITE
6. output PRIME

Обозначения

$\varphi(r) = |Z_r^*|$ - ф. Эйлера

$o_m(n) = \min \{k : n^k \equiv 1 \pmod{m}\}$

$LCM(m)$ - НОК всех $i \leq m$

p - простое, $p|n$, $p > r$

$l = \lfloor \sqrt{\varphi(r)} \log n \rfloor$

$I = \left\{ \left(\frac{n}{p} \right)^i p^j : i, j \geq 0 \right\}$

$P = \left\{ \prod_{a=0}^l (X+a)^{e_a} : e_a \geq 0 \right\}$

G подгруппа Z_r^* ,
порожденная I ,

$t = |G| > \log^2 n$

$Q_r(X)$ - r -й циклотомический
многочлен над F_p

$h(X)$ - неприводимый множитель

$Q_r(X)$, $o_r(p) = \deg(h(X)) > 1$

$F = F_p[X]/(h(X))$ - кольцо вычетов
по модулю p и $h(X)$

Γ подгруппа F , порожденная P

Доказательство корректности

Теорема 3.1.

Алгоритм возвращает PRIME $\Leftrightarrow n$ – простое.

Лемма 3.2.

Если n – простое, то алгоритм возвращает PRIME.

Доказательство корректности

Определение 3.3.

Пусть $f(X)$ – полином, $m \in \mathbb{N}$.

m называется интроспективным к $f(X)$, если

$$[f(X)]^m = f(X^m) \pmod{X^r - 1, p}.$$

Лемма 3.4.

Если m_1 и m_2 интроспективные к $f(X)$ и $g(X)$, то

1. $m_1 m_2$ интроспективное к $f(X)$,
2. m_1 интроспективное к $f(X)g(X)$.

Доказательство корректности

Лемма 3.5. (Hendric Lenstra Jr.)

$$|\Gamma| \geq \binom{t+l}{t-1}$$

Лемма 3.6.

Если n не является степенью простого числа p ,

то $|\Gamma| \leq n^{\sqrt{t}}$

Лемма 3.7.

Если алгоритм возвращает PRIME, то n - простое.

Если не запомните ничего другого

- Существует полиномиальный алгоритм проверки простоты числа

- Идея алгоритма:

$$n \text{ - простое} \Leftrightarrow (X + a)^n \equiv X^n + a \pmod{n}$$

- Доказано, что алгоритм работает корректно и за время $O^{\sim}(\log^{15/2} n)$

ИСТОЧНИКИ

- М.Агравал, Н.Каял, Н.Сакхена «PRIMES is in P»
- А.Черемушкин «Лекции по арифметическим алгоритмам в криптографии»
- П.Ноден, К.Китте «Алгебраическая алгоритмика»
- Т.Кормен, Ч.Лейзерсон, Р.Ривест «Алгоритмы: построение и анализ»