《PRIMES is in **P**》论文精讲

陈威宇 黄兆鋆 周书予

信息科学技术学院

March 11, 2022



Introduction

$$\text{PRIMES} = \{w | w \text{ is binary representation of a prime number}\}$$

PRIMES 属于以下复杂度类:

- **EXP**, 比如众所周知的有 *Sieve of Eratosthenes*.
- **coNP**, 因为 $\overline{\text{PRIMES}} = \text{COMPOSITES} \in \mathbf{NP}$.
- **NP**, [?].
- **BPP**, [?].
- **P**, [?].

[?]: Every Prime Has a Succinct Certificate

Lucas Primality Test

正整数 $n \geqslant 3$ 是质数当且仅当存在整数 $1 < a < n$ 满足 $a^{n-1} \equiv 1 \mod 1$ 且对于 $n-1$ 的每个质因子 p 都有 $a^{(n-1)/p} \not\equiv 1 \bmod n$.

证明.

$\Leftarrow$: 考虑 $\mathrm{ord}_n(a)$. $\Rightarrow$: 取 n 的原根作为 a. □

想验证 p 是质数, 只需要给出满足条件的 a 以及 $p-1$ 的质因数分解 $p-1 = \prod_{i=1}^{k} p_i$, **同时**进一步验证 p_i 都是质数.

可以归纳证明验证 p 时所需的 certificate 长度为 $O(\mathrm{poly}(\log p))$, 从而说明了 PRIMES $\in$ **NP**.

Generalization of Fermat's Little Theorem

Theorem

正整数 $n \geqslant 2$ 是质数当且仅当存在与 n 互质的整数 a, 满足

$$(x+a)^n \equiv x^n + a \mod n$$

上述定理中的等式常被称为 freshman's dream.

证明.

n 是质数 $\Rightarrow n|\binom{n}{k}$ $(\forall 1 \leqslant k < n)$, $(x+a)^n - x^n - a^n$ 系数全为 0.
n 不是质数 $\Rightarrow$ 若 $p^k \| n$, 则 $p^k \nmid \binom{n}{p} = \frac{n \times (n-1) \times \cdots \times (n-p+1)}{1 \times 2 \times \cdots \times p}$, p 次项系数非零. □

[?]: PRIMES is in **BPP**

前述结论用于素数测试的一大障碍在于需要计算的多项式次数太大了.

所以可以考虑随机选取一个模数多项式 $r(x) \in \mathbb{Z}[x]$, 然后检验 $(x+a)^n \equiv x^n + a \bmod (r(x), n)$ 是否成立.

Theorem

设 n 是一个含有质因子 $p \geqslant 17$ 的非质数, 且不是某个质数的整数次幂. 在 $\mathbb{Z}[x]$ 中随机选取一个 $l = \lceil \log n \rceil$ 次首一多项式 $r(x)$, 则有至少 60% 的概率, $(x+1)^n \neq x^n + 1 \bmod (r(x), n)$.

[?]: PRIMES is in **BPP**

令 $P_n(x) = (x+1)^n - 1 - x^n$. 当 n 不是质数时, $P_n(x) \neq 0 \bmod p$, 这是因为 $[x^{p^k}]P_n(x) = \binom{n}{p^k} = \frac{n\times(n-1)\times\cdots\times(n-p^k+1)}{(p^k)!} \neq 0 \bmod p$, 其中 $p^k \| n$, 这里要求了 $n \neq p^k$.

于是我们在 $\mathbb{Z}_p[x]$ 下考虑问题. 注意到 $\mathbb{Z}_p[x]$ 下存在唯一分解, 不可约因式的概念, 记 $I(d)$ 表示其中 d 次不可约首一多项式的数量, 可以估计其下界[1]

$$I(d) = \frac{1}{d}\sum_{e|d}\mu(e)p^{d/e} \geqslant \frac{1}{d}\left(p^d - \sum_{e<d, e|d} p^{d/e}\right) \geqslant \frac{p^d}{d} - p^{d/2}$$

[1] 这个结论不太初等, 就不在此过多阐述了, 可详细参考 [?].

[?]: PRIMES is in **BPP**

记 $\mathcal{C}$ 表示 $\mathbb{Z}_p[x]$ 中含有 $> \frac{l}{2}$ 次不可约因式的 l 次首一多项式集合.
同样对 $|\mathcal{C}|$ 估计下界

$$|\mathcal{C}| = \sum_{k=\lfloor \frac{l}{2} \rfloor + 1}^{l} I(k) p^{l-k} \geqslant \sum_{k=\lfloor \frac{l}{2} \rfloor + 1}^{l} p^l \left(\frac{1}{k} - \frac{1}{p^{k/2}} \right) \geqslant \left(\ln 2 - \frac{1}{48} \right) p^l$$

(其中利用了 $p \geqslant 17$.)
注意一个 l 次多项式中不可能包含超过一个 $> \frac{l}{2}$ 次不可约因式.

[?]: PRIMES is in **BPP**

因为 $\deg P_n(x) < n$, $P_n(x)$ 只有不超过 $\frac{2n}{l}$ 个 $> \frac{l}{2}$ 次不可约因式, 从而 $\mathcal{C}$ 中只有不超过 $\frac{2n}{l} \cdot p^{\frac{l}{2}-1}$ 个多项式可能是 $P_n(x)$ 的因式.

$$\begin{aligned}
\mathbb{P}\left(r \text{ doesn't divide } P_n\right) &\geqslant \mathbb{P}\left(r \in \mathcal{C} \wedge r \text{ doesn't divide } P_n\right) \\
&= \mathbb{P}\left(r \in \mathcal{C}\right) - \mathbb{P}\left(r \in \mathcal{C} \wedge r \text{ divides } P_n\right) \\
&\geqslant \left(\ln 2 - \frac{1}{48}\right) - \frac{2n}{l} \cdot p^{\frac{l}{2}-1}/p^l \\
&\geqslant \ln 2 - \frac{1}{48} - \frac{2n}{l4^{\frac{l}{2}+1}} > \frac{3}{5}
\end{aligned}$$

(注意到 $n > p \geqslant 17, l = \lceil \log n \rceil \geqslant 5$.)

Notations & Preliminaries

在这一部分我们引入一些记号.

当 $\gcd(a, r) = 1$ 时, 满足 $a^k \equiv 1 \bmod r$ 的正整数 k 是一定存在的, 称其中最小的为 a 模 r 的阶, 记作 $\mathrm{ord}_r(a)$. 用欧拉函数 $\varphi(r)$ 表示比 r 小的与 r 互质的数的数量, 容易验证 $\mathrm{ord}_r(a) | \varphi(r)$.

当 p 是素数, $h(x)$ 是 $\mathbb{Z}_p[x]$ 中不可约多项式时, $\mathbb{Z}_p[x]/h(x)$ 是有限域. 之后我们会用记号 $f(x) \equiv g(x) \bmod (h(x), p)$ 来表示 $f(x)$ 和 $g(x)$ 在 $\mathbb{F} \triangleq \mathbb{Z}_p[x]/h(x)$ 中相等.

$\tilde{O}(f(n)) = O(f(n)\ \mathrm{poly}(\log f(n))) = O(f^{1+\varepsilon}(n))$ 表示忽略对数因子.

Natural Language Description

算法分为如下五个步骤:

1. 第一步检查 n 是否是“整数幂”形式的非素数.
2. 第二步求出最小的满足 $\mathrm{ord}_r(n) > \log^2 n$ 的正整数 r.
3. 第三步检查 n 是否有不超过 r 的非平凡因子.
4. 第四步是平凡的: 如果 $n \leqslant r$ 没有不超过 r 的非平凡因子, 此时 n 一定是质数.
5. 第五步对于 $a = 1, \cdots, \lfloor \sqrt{\varphi(r)} \log n \rfloor$, 检查 $(x+a)^n \equiv x^n + a \bmod (x^r - 1, n)$ 是否成立, 若存在不满足则 n 不是质数, **否则 n 是质数**.

只有最后一句话的正确性是非平凡的.

Pseodocode

1: **function** AKS_PRIMALITY_TESTING(n)
2: **if** $n = a^b$ for $a \in \mathbb{N}$ and $b > 1$ **then**
3: **return** COMPOSITE
4: $r \leftarrow \min\{m \in \mathbb{N} | \mathrm{ord}_m(n) > \log^2 n\}$
5: **if** $1 < \gcd(a, n) < n$ for some $a \leqslant r$ **then**
6: **return** COMPOSITE
7: **if** $n \leqslant r$ **then**
8: **return** PRIME
9: **for** $a = 1 \rightarrow \lfloor \sqrt{\varphi(r) \log n} \rfloor$ **do**
10: **if** $(x + a)^n \not\equiv x^n + a \bmod (x^r - 1, n)$ **then**
11: **return** COMPOSITE
12: **return** PRIME

正确性证明中, 非平凡的部分只有“证明通过第五步测试的 n 是质数”.

任取这样的 n 的一个满足 $\mathrm{ord}_r(p) > 1$ 的质因子 p, 注意到有 $p > r$.

根据有限域上分圆多项式那套理论, $x^r - 1$ 在 $\mathbb{Z}_p$ 下有一个 $\mathrm{ord}_r(p)$ 次不可约多项式因子 $h(x)$. 以下记 $\mathbb{F} = \mathbb{Z}_p[x]/h(x)$. 事实上我们没有显式地给出 p 和 $h(x)$ 的具体值, 只是考虑在 $\mathrm{mod}(x^r - 1, n)$ 下做运算, 是因为 $f(x) \equiv g(x) \bmod (x^r - 1, n) \Rightarrow f(x) \equiv g(x) \bmod (h(x), p)$.

注意到前述算法中我们只限制了 $\mathrm{ord}_r(n)$ $(> \log^2 n)$, 而没有限制 $\mathrm{ord}_r(p)$. 原作者在 2002 年的预印版论文[2]中使用了一些解析数论手段来限制 $\mathrm{ord}_r(p)$, 但后来 Hendrik Lenstra Jr. 的工作简化了证明.

谢谢你, Hendrik Lenstra Jr. !

[2] 这里有下载链接

Introspectivity: Generalization of Freshman's Dream

对于 $a = 0, 1, \cdots, l \triangleq \lfloor \sqrt{\varphi(r)} \log n \rfloor$, $(x+a)^m \equiv x^m + a \bmod (x^r - 1, p)$ 对于 $m = n$ (由第五步验证) 和 $m = p$ (由扩展费马小) 均成立.

我们指出它对于 $m = \frac{n}{p}$ 也成立, 这是因为

$$(x^p + a)^{\frac{n}{p}} \equiv \left[(x+a)^p\right]^{\frac{n}{p}} \equiv (x+a)^n \equiv x^n + a \equiv \left(x^p\right)^{\frac{n}{p}} + a$$

用 x 替代[3] x^p 即可. 我们可以从中抽象出这样的概念:

定义 (内省)

如果 $m \in \mathbb{N}$ 和多项式 $f \in \mathbb{Z}[x]$ 满足 $f(x^m) \equiv f^m(x) \bmod (x^r - 1, p)$, 则称 m 对 f 内省 (introspective).

惊喜地发现内省性对数乘和多项式乘都是封闭的.

[3] 为什么可以替代呢?

Introspectivity: Generalization of Freshman's Dream

引理 (数乘封闭性)

如果 m_1 和 m_2 都对 f 内省, 则 $m_1 m_2$ 对 f 内省.

证明.

$f(x^{m_1 m_2}) \equiv [f(x^{m_1})]^{m_2} \equiv [f^{m_1}(x)]^{m_2} \equiv f^{m_1 m_2}(x)$, 其中第一个 $\equiv$ 在 $\bmod(x^{m_1 r} - 1, p)$ 下成立, 但这比在 $\bmod(x^r - 1, p)$ 下要强. □

引理 (多项式乘封闭性)

如果 m 对 f_1 和 f_2 都内省, 则 m 对 $f_1 f_2$ 内省.

证明.

$[f_1(x) f_2(x)]^m \equiv f_1^m(x) f_2^m(x) \equiv f_1(x^m) f_2(x^m) \equiv f_1 f_2(x^m)$ □

Introspectivity: Generalization of Freshman's Dream

由于 $p, \frac{n}{p}$ 对 $x, x+1, \cdots, x+l$ 分别内省, 两边分别作为生成元得到集合 $I = \left\{ p^i \left(\frac{n}{p}\right)^j \middle| i, j \leqslant 0 \right\}$ 和 $P = \left\{ \prod_{a=0}^{l} (x+a)^{e_a} \middle| e_a \geqslant 0 \right\}$ 也两两内省.

因为模 $x^r - 1$ 下 x^{kr+b} 和 x^b 是一样的, 考虑对 I 中元素模 r 得到 $\mathbb{Z}_r^*$ 的子群 G. 记 $|G| = t$, 注意到 $\langle n \rangle \leqslant G$, 故 $t \geqslant \mathrm{ord}_r(n) > \log^2 n$.

类似的, 把 P 中元素映到 $\mathbb{F}$ 上得到 $\mathbb{F}$ 的乘法子群 $\mathcal{G}$.

接下来的工作就是给出 $\mathcal{G}$ 大小的上下界, 并从中归谬得出 "n 是质数" 的结论.

lowerbound of $|\mathcal{G}|$

引理 (Hendrik Lenstra Jr.)

$|\mathcal{G}| \geqslant \binom{t+l}{t-1}$.

考虑证明 P 中任意两个不同的小于 t 次多项式映到 $\mathbb{F}$ 上仍不同. 反证, 假设 $f, g \in P$ 映到 $\mathbb{F}$ 上相同, 那么根据内省性, $d \triangleq f - g$ 代入所有 x^m 后映到 $\mathbb{F}$ 上都是 $\mathbf{0}$, 其中 $m \in G, x^m \in \mathbb{F}$. 这说明如果我们把 d 看成 $\mathbb{F}[y]$ 的元素, d 在 $\mathbb{F}$ 上就有至少 t 个根[4], 而 $\deg(d) < t$ 产生了矛盾.

P 中小于 t 次多项式个数是 $\binom{t+l}{t-1}$, 这是不定方程 $\sum_{a=0}^{l} e_a < t$ 的解数.

在 Hendrik Lenstra Jr. 之前, 一个平凡的结论是 $|\mathcal{G}| \geqslant \binom{\mathrm{ord}_r(p)+l}{\mathrm{ord}_r(p)-1}$.

[4] 这里有赖于 x^m 在 $\mathbb{F}$ 中两两不同, 即所谓“x 是 $\mathbb{F}$ 的 r 次本原根”.

upperbound of $|\mathcal{G}|$

引理

如果 n 不是 p 的整数次幂, 那么 $|\mathcal{G}| \leqslant n^{\lfloor\sqrt{t}\rfloor}$.

考虑集合 $\hat{I} = \left\{ p^i \left(\frac{n}{p}\right)^j \middle| 0 \leqslant i, j \leqslant \lfloor\sqrt{t}\rfloor \right\}$, 如果 n 不是 p 的整数次幂, 那么 $\hat{I}$ 中有 $(\lfloor\sqrt{t}\rfloor + 1)^2 > t$ 个互异元素, 且一定存在两个数之差是 r 的倍数.

不妨设为 $m_1, m_2 \in \hat{I}$, 满足 $x^{m_1} \equiv x^{m_2} \bmod (x^r - 1, p)$. 任取 $f \in \mathcal{G}$, 由于 $f^{m_1}(x) \equiv f(x^{m_1}) \equiv f(x^{m_2}) \equiv f^{m_2}(x)$, 故 $Q(Y) = Y^{m_1} - Y^{m_2} \in \mathbb{F}[Y]$ 以 $\mathcal{G}$ 中任意元素为根, 从而 $|\mathcal{G}| \leqslant \deg Q = m_1 \leqslant (p \cdot \frac{n}{p})^{\lfloor\sqrt{t}\rfloor} = n^{\lfloor\sqrt{t}\rfloor}$.

sufficiency for AKS Prime Testing

$$
\begin{aligned}
|\mathcal{G}| &\geqslant \binom{t+l}{t-1} = \binom{t+l}{l+1} \\
&\geqslant \binom{\lfloor\sqrt{t}\log n\rfloor + 1 + l}{l+1} && \text{since } t > \log^2 n \Rightarrow t \geqslant \lfloor\sqrt{t}\log n\rfloor \\
&= \binom{\lfloor\sqrt{t}\log n\rfloor + 1 + l}{\lfloor\sqrt{t}\log n\rfloor} \\
&\geqslant \binom{2\lfloor\sqrt{t}\log n\rfloor + 1}{\lfloor\sqrt{t}\log n\rfloor} && \text{since } G \leqslant \mathbb{Z}_r^* \Rightarrow t \leqslant \varphi(r) \\
&> 2^{\lfloor\sqrt{t}\log n\rfloor} + 1 && \text{since } \binom{2k+1}{k} > 2^{k+1} \text{ for } k > 1 \\
&\geqslant n^{\lfloor\sqrt{t}\rfloor}
\end{aligned}
$$

sufficiency for AKS Prime Testing

上下界的矛盾导致了 n 只能是 p 的整数次幂, 而由第一步, 这个幂次不能大于 1, 所以 $n = p$ 是质数.

在算法的第五步中, 我们取了 $l = \lfloor \sqrt{\varphi(r)} \log n \rfloor$ 以保证 $|\mathcal{G}|$ 足够大. 能不能减小一点呢?
如果以下猜想成立, 复杂度就可以被优化至 $\tilde{O}(\log^3 n)$.

Conjecture

如果 r 是与 n 互质的质数, 且满足 $(x-1)^n \equiv x^n - 1 \bmod (x^r - 1, n)$, 则要么 n 是质数, 要么 $n^2 \equiv 1 \bmod r$.

做法是找到一个不整除 $n^2 - 1$ 的质数 r, 并判定 $(x-1)^n \equiv x^n - 1 \bmod (x^r - 1, n)$ 是否成立, 若成立则根据猜想 n 是质数, 否则 n 一定不是质数.
上述要求的 r 是一定存在, 且不超过 $2 \ln n$ 的, 这是因为根据 [?], 不超过 x 的质数乘积至少是 e^x, 故不超过 $2 \ln n$ 的质数乘积至少是 $\mathrm{e}^{2 \ln n} = n^2$, 它们不可能都是 $n^2 - 1$ 的因子.
[?] 验证了该猜想在 $r \leqslant 100, n \leqslant 10^{10}$ 时是成立的.

Reference I

Q. & A.