Primes is in P 导读

郭嘉睿

ntguojiarui@pku.edu.cn

2021 年 3 月 26 日

摘要

Primes is in P 作为素性检验的经典论文, 提出了在对数时间内判断一个整数是否为素数的方法, 在此对文中的定理证明进行梳理, 并补全其证明内容. 证明过程中, 我们不假定读者具有相关的代数或数论知识, 有关的内容我们会在证明过程中补充出来.

Lemma 2.1. 设 $a \in \mathbb{Z}$, $n \in \mathbb{N}$, 且 $(a, n) = 1$, 那么 n 为素数当且仅当

$$(X + a)^n \equiv X^n + a (\mathrm{mod}\ n).$$

Proof. 对 $(X + a)^n$ 利用二项式定理展开得

$$(X + a)^n = X^n + \sum_{k=1}^{n-1} \binom{n}{k} a^{n-k} X^k + a^n.$$

若 n 为素数, 由 Fermat Little Theorem 可得 $a^n \equiv a (\mathrm{mod}\ n)$, 且组合数

$$\binom{n}{k} = \frac{n!}{(n-k)! \cdot k!} = n \frac{(n-1)!}{(n-k)! \cdot k!}$$

中, 分母的各项都不含因子 n, 相应的 $n | \binom{n}{k}$. 反过来, 若 n 为合数, 设素数 q 是 n 的一个因子, 且 $q^k || n$, 在组合数

$$\binom{n}{q} = \frac{n(n-1) \cdots (n-q+1)}{q(q-1) \cdots 1}$$

中, 由于分子中除了 n 都不能被 q 整除, 所以 $q^{k-1} || \binom{n}{q}$, 相应的在展开项中 x^q 次项不能被约去, 这就得到了矛盾. □

Additional Lemma 1. 设 $r \in \mathbb{N}$, $a \in \mathbb{Z}$, $(a, r) = 1$, a 模 r 的阶 $o_r(a)$ 定义为最小的正整数 k, s.t. $a^k \equiv 1 (\mathrm{mod}\ r)$, 那么 $o_r(a) | \varphi(r)$. 换言之, $a^{\varphi(r)} \equiv 1 (\mathrm{mod}\ r)$.

Proof. 对于 $m < r$, $(m, r) = 1$, 考虑下面 $o_r(a)$ 个元素

$$m, ma, ma^2, \cdots, ma^{o_r(a)-1},$$

易证它们模 r 两两不同余. 若不然, 存在 $i < j$, s.t. $ma^i \equiv ma^j (\mathrm{mod}\ r)$, 移项可得 $r | ma^i (a^{j-i} - 1)$, 再由 m, a 都与 r 互素可得 $a^{j-i} \equiv 1 (\mathrm{mod}\ r)$, 且 $0 < j - i < o_r(a)$, 这就得到了矛盾. 因此, 小于 r 且与 r 互素的元素总是 $o_r(a)$ 一组出现的, 这就证明了我们要的结论. □

关于以上证明的补充: 很显然这个定理的严格证明应当结合群论. 在群 $\mathbf{Z}_r^\times$ 中定义等价关系 $x \sim y$: 当且仅当 $x = ya^s$, $s \in \mathbf{N}$. 容易验证我们的定义满足自反, 对称, 传递性, 所以这确实是一个等价关系, 该等价关系划分出的陪集为 xH, 其中 $H = \{1, a, a^2, a^{o_r(a)-1}\}$, 群 $\mathbf{Z}_r^\times$ 的阶为 $\varphi(r)$, 每一个陪集的元素数目为 $o_r(a)$, 由 Lagrange 定理可得 $o_r(a) | \varphi(r)$.

Lemma 3.1. 用符号 LCM(m) 表示从 1 开始的 m 个整数的最小公倍数, 对于 $m \geq 7$, 成立

$$\mathrm{LCM}(m) \geq 2^m.$$

Proof. 论文引用的参考文献以及你可以找到的大部分资料都是用积分证明了一个组合恒等式, 我们直接归纳证明, 当然要求读者对组合数具有强大的功底. 对于正整数 $1 \leq m \leq n$, 定义代数式

$$I(m,n) = \sum_{k=0}^{n-m} \frac{(-1)^k \binom{n-m}{j}}{m+j},$$

我们对 $n-m$ 归纳证明

$$I(m,n) = \frac{1}{m\binom{n}{m}}.$$

$n-m=0$ 的情况是显而易见的, 请读者自行验证. 我们假设对于 $n-m=r$ 成立

$$I(m,m+r) = \frac{1}{m\binom{m}{m+r}},$$

以下考虑 $n-m=r+1$ 的情况, 首先我们给出一个引理:

$$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}.$$

该引理的证明是显然的, 事实上, 我们将组合数展开, 即有

$$\begin{aligned}\mathrm{LHS} &= \frac{n!}{(n-k)!\cdot k!} + \frac{n!}{(n-k+1)!\cdot(k-1)!} \\ &= \frac{n!\cdot(k-1+n-k+1)}{(n-k+1)!\cdot k!} = \binom{n+1}{k}.\end{aligned}$$

利用该性质对 $r+1$ 的情况进行化简:

$$\begin{aligned}I(m,m+r+1) &= \sum_{k=0}^{r+1} \frac{(-1)^k\binom{r+1}{k}}{m+k} \\ &= \sum_{k=0}^{r+1} \frac{(-1)^k\left(\binom{r}{k}+\binom{r}{k-1}\right)}{m+k} \\ &= \sum_{k=0}^{r} \frac{(-1)^k\binom{r}{k}}{m+k} - \sum_{k=1}^{r+1} \frac{(-1)^k\binom{r}{k-1}}{m+k} \\ &= \sum_{k=0}^{r} \frac{(-1)^k\binom{r}{k}}{m+k} - \sum_{k=0}^{r} \frac{(-1)^k\binom{r}{k}}{m+k+1} \\ &= I(m,m+r) - I(m+1,m+1+r) \\ &= \frac{1}{m\binom{m+r}{m}} - \frac{1}{(m+1)\binom{m+r+1}{m+1}} \\ &= \frac{(r+1)\cdot r!\cdot(m-1)!}{(m+r+1)!} = \frac{1}{m\binom{m+r+1}{m}},\end{aligned}$$

由数学归纳法原理我们即证明了我们要的结论. 注意到求和形式的 $I(m,n)$ 的分母取到了 m 到 n 之间的所有整数, 所以化简后 $I(m,n)$ 的分母一定能够整除 LCM(n), 从而

$$m\binom{n}{m} | \mathrm{LCM}(n).$$

进而我们得到了以下两个式子:

$$n\binom{2n}{n}|\mathrm{LCM}(2n)|\mathrm{LCM}(2n+1),$$

$$(n+1)\binom{2n+1}{n+1}=(2n+1)\binom{2n}{n}|\mathrm{LCM}(2n+1).$$

注意到 n 与 $2n+1$ 是互素的, 进而

$$n(2n+1)\binom{2n}{n}|\mathrm{LCM}(2n+1).$$

注意到 $\binom{2n}{n}$ 是二项式系数中最大的, 我们有

$$\mathrm{LCM}(2n+1)\geq n\cdot 2^{2n}\geq 2^{2n+1}(n\geq 2),$$

$$\mathrm{LCM}(2n+2)\geq \mathrm{LCM}(2n+1)\geq n\cdot 2^{2n}\geq 2^{2n+2}(n\geq 4).$$

以上事实表明对于 $m\geq 9$, $\mathrm{LCM}(m)\geq 2^m$. 简单验证可知对于 $m=7,8$ 也满足. □

Algorithm AKS 素性检测

Input: Integer $n>1$.

1: **if** $n=a^b$, $a\in\mathbf{N}$, $b>1$ **then**
2: **return** COMPOSITE
3: **end if**
4: Find the smallest r such that $o_r(n)>\log^2 n$
5: **if** $1<(a,n)<n$ for some $a<r$ **then**
6: **return** COMPOSITE
7: **end if**
8: **if** $n<r$ **then**
9: **return** PRIME
10: **end if**
11: **for** $a=1$ **to** $\lfloor\sqrt{\varphi(r)}\log n\rfloor$ **do**
12: **if** $(X+a)^n\not\equiv X^n+a(\mathrm{mod}\ X^r-1,n)$ **then**
13: **return** COMPOSITE
14: **end if**
15: **end for**
16: **return** PRIME

Lemma 4.2. 若 n 为素数, 以上算法输出 PRIME.

Proof. 若 n 为素数, 以上算法在第 1, 3, 5 步都不可能输出 COMPOSITE, 所以一定在第 4 步或者第 6 步输出了 PRIME. □

Lemma 4.3. 存在某一个 $r<\max\{3,\lceil\log^5 n\rceil\}$, s.t. $o_r(n)>\log^2 n$.

实际上, 论文中的证明是有问题的. 这是因为, $o_r(n)$ 仅对 $(r,n)=1$ 的情况进行了定义, 在 (r,n) 不为 1 的时候, 由于在任何情况下都不可能有 $n^k\equiv 1(\mathrm{mod}\ r)$, 实际上 $o_r(n)=\infty$. 在 $o_r(n)=\infty$ 的情况下, 讨论该算法是没有意义的. 举一个例子, 不妨取 $n=6$, 此时正整数

$s=4$ 当然满足条件 (首先, 6 在 $\mathbf{Z}_4$ 中不可逆, 其次, 4 也不能整除 6). 但是, 最后取出来的 $r=\dfrac{4}{2}=2$ 在所属的集合中.

可以看到论文中的问题主要在两方面: 首先, $o_r(n)$ 有可能不是有限值; 其次, 对 s 约去 (s,n) 并不能保证它和 n 互素. 但实际上, 这并不表示该定理是错误的, 我们可以用其他方法来证明它, 而且, 以下的证明也依赖于论文中的证明思路.

Proof. $n=2$ 的情形是显然的, 下设 $n\geq 3$, 此时 $B=\lceil \log^5 n\rceil > 10$. 考虑乘积式

$$S=n^{\lfloor \log B\rfloor}\prod_{i=1}^{\lfloor \log^2 n\rfloor}(n^i-1),$$

设 s 是最小的不能整除它的正整数. 若 $s>B$, 那么 $1\leq m\leq B$ 的整数都能被 S 整除, 由 **Lemma3.1.** 可知 $S\geq 2^B$. 但是

$$S<n^{\lfloor \log B\rfloor}\prod_{i=1}^{\lfloor \log^2 n\rfloor}n^i<n^{\log^4 n}\leq 2^{\lceil \log^5 n\rceil}=2^B.$$

这说明了一定有 $s\leq B$. 取

$$r=\frac{s}{(s,n^{\lfloor \log B\rfloor})}\triangleq\frac{s}{c}.$$

注意到 $c|n^{\lfloor \log B\rfloor}$, 若

$$r|\prod_{i=1}^{\lfloor \log^2 n\rfloor}(n^i-1),$$

相乘可得 $s=rc|S$, 这与我们的假设不符, 所以

$$r\nmid\prod_{i=1}^{\lfloor \log^2 n\rfloor}(n^i-1),$$

换言之, 对于所有的 $i\leq\lfloor \log^2 n\rfloor$, $n^i\not\equiv 1(\mathrm{mod}\ r)$, 且注意到对于所有的大于 1 的正整数 m, 均有 $m^{\lfloor \log B\rfloor+1}>B\geq s\geq r$, 表明每一个素因子在 s 中最多出现 $\lfloor \log B\rfloor$ 重, 因此我们对 s 处理得到 r 之后, 所有重因子一定全部被约去了, 剩下来的 r 一定是和 n 互素的, 即 $(r,n)=1$, 这就得到了我们的结论. □

Additional Lemma 2. 如果对于 $0\leq a\leq l$, 以下两式均成立:

$$(x+a)^n\equiv x^n+a(\mathrm{mod}\ x^r-1,p),$$

$$(x+a)^p\equiv x^p+a(\mathrm{mod}\ x^r-1,p),$$

且 $p|n$, 那么

$$(x+a)^{\frac{n}{p}}=x^{\frac{n}{p}}+a(\mathrm{mod}\ x^r-1,p).$$

Proof. 相当于证明自省性 (introspective) 对于除法封闭. 我们有

$$(x+a)^n=[(x+a)^p]^{\frac{n}{p}}\equiv(x^p+a)^{\frac{n}{p}}\equiv x^n+a(\mathrm{mod}\ x^r-1,n).$$

在上式中用 x 替代 x^p, 即有

$$(x+a)^{\frac{n}{p}}\equiv x^{\frac{n}{p}}+a(\mathrm{mod}\ x^r-1,n).$$

□

Lemma 4.5. 自省数对乘法封闭, 即若 m, m' 都是 $f(x)$ 的自省数, 那么 mm' 也是. 这里, 说 $m \in \mathbf{N}$ 是 $f(x)$ 的自省数, 如果

$$[f(x)]^m \equiv f(x^m)(\text{mod } x^r - 1, p).$$

Proof. 根据自省数的定义,

$$[f(x)]^{mm'} \equiv [f(x^m)]^{m'}(\text{mod } x^r - 1, p).$$

另外,

$$[f(x^m)]^{m'} \equiv f(x^{mm'})(\text{mod } x^{mr} - 1, p).$$

最后再注意到 $x^r - 1 | x^{mr-1}$ 即可. □

Lemma 4.6. 自省数的性质对多项式的乘法也是封闭的, 也就是说, 若 m 是多项式 $f(x)$ 和 $g(x)$ 的自省数, 那么它也是多项式 $f(x)g(x)$ 的自省数.

Proof. 事实上,

$$[f(x)g(x)]^m \equiv [f(x)]^m[g(x)]^m \equiv f(x^m)g(x^m)(\text{mod } x^r - 1, p).$$

□

Lemma 4.5. 和 **Lemma 4.6.** 自然的构造出了两个集合, 分别是是自然数的集合

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

和多项式的集合

$$P = \left\{ \prod_{a=0}^{l} (x+a)^{e_a} \middle| e_a \geq 0 \right\}.$$

在我们进行接下来的证明之前, 有必要向读者介绍一些基本的抽象代数知识.

Additional Lemma 3. 对于整数集模 p 构成的剩余类, 可以自然的定义一个循环群 $\mathbf{Z}_p = \{0, 1, \cdots, p-1\}$. 用 $\mathbf{Z}_p^\times$ 表示这一个加法群中所有的乘法可逆元, 那么 $x \in \mathbf{Z}_p^\times$ 当且仅当 $(x, p) = 1$.

Proof. 充分性: 若 $(x, p) = 1$, 则存在正整数 a, b, s.t.

$$ax + bp = 1.$$

两边模 p, 即有 $ax \equiv 1(\text{mod } p)$, 表明 a 即为 x 的逆元.
必要性: 设 x 的逆元为 a, 则 $ax \equiv 1(\text{mod } p)$, 表明 $ax = bp + 1$, 移项可得

$$ax - bp = 1,$$

这就表明了 $(x, p) = 1$. □

Additional Lemma 4. 群 $\mathbf{Z}_p^\times$ 的阶 $t > \log^2 n$.

Proof. 考虑 $1, n, n^2, n^3, \cdots, n^{o_r(n)-1}$, 它们都在群 $\mathbf{Z}_p^\times$ 中, 而 $o_r(n) > \log^2 n$, 所以 $t \geq o_r(n) > \log^2 n$. □

第二个群的构造要用到更多的代数知识, 主要是分圆多项式, 而这些理论又以域扩张理论和 Galois 理论为基础, 我们给出以下结论, 有兴趣的读者可以自行了解.

我们已经很自然的知道域 (field) 的定义了: 如果一个交换幺环中的每一个非零元素都有逆元, 且满足乘法交换律, 那么就称这个它是一个域. 可以看到, 域的性质非常好, 满足了我们要的几乎所有条件, 因此, 我们主要研究域的扩张. 在此之前, 我们先介绍有限域的概念:

对于素数 p 以及模 p 的剩余类 $\{0, 1, 2, \cdots, p-1\}$, 易知除了 0 以外所有元素均可逆, 所以它构成一个域, 我们把它叫做 Galois 域, 即为 $GF(p)$. 那么问题来了, 假如 n 不是素数, 那么是否存在 n 个元素的域呢?

Additional Lemma 5. 对于素数 p 和正整数 n, 存在 p^n 元有限域 $GF(p^n)$, 且在同构意义下这样的域是唯一的.

Proof. 考虑多项式 $f(x) = x^{p^n} - x$, 注意到 $f'(x) = p^n x^{p^n-1} - 1 = -1 \neq 0$, 所以 $f(x)$ 无重根, 一共有 p^n 个根, 这些根的集合为 F, 我们证明 F 作为 $GF(p)$ 的一个域扩张构成了一个域 (注意到 $\mathrm{char}(F) = p$): 对于 $a, b \in P$, 利用二项式定理展开有

$$(a+b)^{p^n} = a^{p^n} + b^{p^n} = a + b,$$

$$(a-b)^{p^n} = a^{p^n} + (-b)^{p^n},$$

若 $p \neq 2$, 则 p^n 为奇数, 从而 $(-b)^{p^n} = -b^{p^n}$; 若 $p = 2$, 依然有 $(-b)^{p^n} = b^{p^n} = -b^{p^n}$, 总而言之,

$$(a-b)^{p^n} = a^{p^n} - b^{p^n} = a - b.$$

对于乘除法 (除法要求分母不为 0),

$$(ab)^{p^n} = a^{p^n} b^{p^n} = ab,$$

$$\left(\frac{a}{b}\right)^{p^n} = \frac{a^{p^n}}{b^{p^n}} = \frac{a}{b},$$

表明 $a+b, a-b, ab, \dfrac{a}{b}$ 依然在 F 中, 所以 F 确实是一个域, 同构是显然的. □

Additional Lemma 6. $GF(p^n)^*$ 关于乘法构成 $p^n - 1$ 阶循环群.

Proof. 对于任意 $m \in \mathbf{N}$, 方程 $x^m - 1 = 0$ 在 $GF(p^n)^*$ 内至多有 m 个根, 所以 $GF(p^n)^*$ 关于乘法构成循环群. □

有了以上定义, 我们准备开始介绍有关分圆多项式的内容了. 对于素域 P, 多项式 $x^n - 1$ 称为 n 次分圆多项式. 对于有理数域 $\mathbf{Q}$, 并不是 n 次分圆多项式的所有根都在 $\mathbf{Q}$ 里 (比如, $x^3 - 1$ 的根 $\omega = \dfrac{-1+\sqrt{-3}}{2} \notin \mathbf{Q}$), 由此我们考虑 n 次分圆多项式在素域 P 上的分裂域, 定义域扩张 E/F 的扩张指数为 n, 如果在 E 中存在 n 个线性无关的数, 但不存在 $n+1$ 个线性无关的数, 记为 $[E : F] = n$. 问题是, n 次分圆多项式的扩张指数是多少?

对于有理数域 $\mathbf{Q}$, 不加证明地给出以下结论:

Theorem. n 次分圆多项式在有理数域 $\mathbf{Q}$ 上的分裂域的扩张指数为 $\varphi(n)$.

我们终于快要得到最后的结论了, 对于有限域 $GF(p)$, 有以下定理:

Additional Lemma 7. n 次分圆多项式在有限域 $GF(p)$ 上的分裂域的扩张指数为 $o_n(p)$.

Proof. 记 n 次分圆多项式在有限域 $GF(p)$ 上的分裂域为 $F = GF(p)(\alpha)$, 并记 $[F : GF(p)] = s$, $o_n(p) = e$, 我们证明 $s = e$.

首先, 由 $[F:GF(p)]=s$ 可知 $|F|=p^s$, 而 n 次分圆多项式的单位根构成的 n 阶群 G 是乘法群 F^* 的子群, 由 Lagrange 定理可得 $n|p^s-1$, 由 e 的最小性可得 $e\le s$;
此外, 由于 $n|p^e-1$, $GF(p^e)$ 包含一个 n 阶乘法子群, 实际上就是 n 阶单位根群 G, G 中的元素线性组合可以得到 $GF(p)(\alpha)=GF(p^s)$, 它一定包含于 $GF(p^e)$, 所以 $s\le e$, 我们就证明了 $s=e$. □

我们开始定义第二个群: 对于 r 次分圆多项式 x^r-1, 找一个次数为 $o_r(p)$ 的不可约多项式 $h(x)$ 整除 x^r-1, 那么 $h(x)$ 的次数大于 1 (由于 $o_r(p)>1$), 考虑 P 中元素模 $h(x)$ 构成的群 $\mathcal{G}$, 它是 $F=GF(p)[x]/(h(x))$ 的一个子群, 且是由 $x,x+1,x+2,\cdots,x+l$ 中的元素进行若干次乘法生成的. [1]

Lemma 4.7. 群 $\mathcal{G}$ 的阶

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

Proof. 首先证明: P 中两个次数低于 t 的多项式会映到两个不同的像. 若不然, 假设存在两个不同的多项式 $f(x),g(x)$, s.t.$f(x)=g(x)$, 在 I 中取正整数 m, 由自省性可得 (以下所有的运算都是按照域 F 的运算法则, 即在 $GF(p)$ 中模 $h(x)$; 观察到 $h(x)|x^r-1$, 所以两个数对 x^r-1 同余也一定对 $h(x)$ 同余):

$$f(x^m)-g(x^m)=[f(x)]^m-[g(x)]^m=0,$$

表明对于所有 G 中的元素 m, x^m 是方程 $Q(y)=f(y)-g(y)=0$ 的根. 而 $(m,r)=1$, 所以这些 x^m 是互不相同的, 这就说明了 $Q(y)$ 至少有 t 个根, 而 $Q(y)$ 次数是小于 t 的, 这就得到了矛盾.
注意到

$$1\le l=\lfloor\sqrt{\varphi(r)}\log n\rfloor\le\sqrt{r}\log n<\sqrt{rt}\le r,$$

所以 $x,x+1,\cdots,x+l$ 是互不相同的, 所以 $\mathcal{G}$ 中至少有 $l+1$ 个一次多项式. 从 $l+1$ 个多项式中选择 k 个, 有 $\binom{l+1+k-1}{k}=\binom{l+k}{k}$ 种选法, 所以次数小于 t 的多项式至少有

$$\sum_{i=0}^{t-1}\binom{l+i}{i}=\binom{t+l}{t-1}$$

种选法, 所以

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

□

Lemma 4.8. 若 n 不是 p 的幂, 那么 $|\mathcal{G}|\le n^{\sqrt{t}}$.

Proof. 考虑 I 的以下子集:

$$\hat{I}=\left\{\left(\frac{n}{p}\right)^i\cdot p^j\,\middle|\,0\le i,j\le\lfloor\sqrt{t}\rfloor\right\},$$

假如 n 不是 p 的幂, 那么 $|\hat{I}|=(\lfloor\sqrt{t}\rfloor+1)^2>t$, 而 $|G|=t$, 所以 $\hat{I}$ 中至少两个元素模 r 同余 (这是由于 $\hat{I}$ 中的元素都是 $\mathbf{Z}_r$ 中的可逆元), 不妨设 $m_1>m_2$, 进而由 $r|m_1-m_2$ 可得

$$x^{m_1}\equiv x^{m_2}(\text{mod } x^r-1,p).$$

[1] 这样的定义是为了保证 F 是一个域 (利用到了一个最基本的定理: $F/(f(x))$ 是域当且仅当 $f(x)$ 在 F 中不可约).

对于 $f(x) \in P$, 有

$$[f(x)]^{m_1} \equiv f(x^{m_1}) \equiv f(x^{m_2}) \equiv [f(x)]^{m_2} \pmod{x^r - 1, p},$$

说明对于 $\forall f(x) \in \mathcal{G}$, $f(x)$ 都是方程

$$Q(y) = y^{m_1} - y^{m_2}$$

的根, 因此 $Q(y)$ 在 $F = GF(p)[x]/(h(x))$ 中至少有 $|\mathcal{G}|$ 个根, 而 $Q(y)$ 的次数

$$m_1 \leq \left(\frac{n}{p}\right)^{\sqrt{t}} \cdot p^{\sqrt{t}} = n^{\sqrt{t}},$$

所以 $|\mathcal{G}| \leq n^{\sqrt{t}}$. □

Lemma 4.9. 若以上算法输出 PRIME, 则 n 为素数.

Proof. 若算法返回 PRIME, 那么

$$\begin{aligned}
|\mathcal{G}| &\geq \binom{t+l}{t-1} = \binom{t+l}{l+1} \\
&\geq \binom{l+1+\lfloor\sqrt{t}\log n\rfloor}{l+1} = \binom{l+1+\lfloor\sqrt{t}\log n\rfloor}{\lfloor\sqrt{t}\log n\rfloor} \\
&\geq \binom{2\lfloor\sqrt{t}\log n\rfloor+1}{\lfloor\sqrt{t}\log n\rfloor} \\
&> 2^{\lfloor\sqrt{t}\log n\rfloor+1} \\
&\geq n^{\sqrt{t}},
\end{aligned}$$

这里, 第一个不等号是 **Lemma 4.7.**, 第二, 第三和第五个不等号是由于 **Additional Lemma 4.**(由于 $t > \log^2 n$ 以及 $t \geq \varphi(r)$), 第四个不等号是利用

$$\binom{2n+3}{n+1} = 3\binom{2n+1}{n} + \binom{2n+1}{n-1} > 2\binom{2n+1}{n},$$

归纳可得.
但是, **Lemma 4.8.** 表明在 n 不是素数的幂的时候 $|\mathcal{G}| \leq n^{\sqrt{t}}$, 因此 n 一定是 $n = p^k$ 的形式, 算法的第一步已经排除了 $n = a^b$ 的情形, 所以这时候 $k = 1$, p 一定是素数. □

参考文献

[1] Manindra Agrawal and Neeraj Kayal and Nitin Saxena. PRIMES Is in P[J]. Annals of Mathematics, 2004, 160(2) : 781-793.

[2] Errata: PRIMES is in P[J]. Annals of Mathematics, 2019, 189(1) : 317-318.

[3] 聂灵沼, 丁石孙. 代数学引论. 北京, 高等教育出版社, 2000.

[4] 何依波. https://blog.csdn.net/weixin_39800875/article/details/111708866.

[5] https://blog.csdn.net/weixin_43902708/article/details/89854566.