# PRIMALITY TESTING IN POLYNOMIAL TIME

A Theorem of

M. AGRAWAL, N. KAYAL, AND N. SAXENA
Department of Computer Science & Engineering
Indian Institute of Technology in Kanpur

$$(x-a)^n \equiv x^n - a \pmod{x^r - 1, n}$$

## What does this mean?

- The difference $(x-a)^n - (x^n - a)$ is an element in the ideal $(x^r - 1, n)$ in the ring $\mathbb{Z}[x]$.
- It is the same as the assertion

  $\texttt{Rem}((\texttt{x}-\texttt{a})^{\texttt{n}} - (\texttt{x}^{\texttt{n}} - \texttt{a}), \texttt{x}^{\texttt{r}} - 1, \texttt{x})\ \texttt{mod n = 0}$

  in MAPLE.

```
> Rem((x-2)^15-(x^15-2),x^3-1,x) mod 15
```

$$12\,x^2 + 9\,x + 9$$

$r$ denotes a prime of size $\ll \log n$

$$(x-a)^n \equiv x^n - a \pmod{x^r - 1, n}$$

**Idea for Checking this Congruence:**

- Write $n = 2^{k_1} + 2^{k_2} + \cdots + 2^{k_{t-1}} + 2^{k_t}$, where $k_1 < k_2 < \cdots < k_t$.
- Compute $f_j(x) = (x-a)^{2^j} \pmod{x^r - 1, n}$ for $j \in \{0, 1, \ldots, k_t\}$ successively by squaring.
- Compute $\prod_{j=1}^{t} f_{k_j} \pmod{x^r - 1, n}$ and compare to $x^{n \bmod r} - (a \bmod n)$.

**Conjecture:** Suppose $r$ does not divide $n(n^2 - 1)$ where $r$ is prime. Then $n$ is a prime if and only if

$$(*) \qquad (x-1)^n \equiv x^n - 1 \pmod{x^r - 1, n}.$$

$$n \text{ prime} \quad \overset{\checkmark}{\Longrightarrow} \quad (*) \text{ holds}$$

$$(*) \text{ holds} \quad \overset{?}{\Longrightarrow} \quad n \text{ prime}$$

**Conjecture:** Suppose $r$ does not divide $n(n^2-1)$ where $r$ is prime. Then $n$ is a prime if and only if

$$(*) \qquad (x-1)^n \equiv x^n - 1 \pmod{x^r - 1, n}.$$

**Idea for an Algorithm Assuming Conjecture:**

**Conjecture:** Suppose $r$ does not divide $n(n^2-1)$ where $r$ is prime. Then $n$ is a prime if and only if

$$(*) \qquad (x-1)^n \equiv x^n - 1 \pmod{x^r - 1, n}.$$

**Idea for an Algorithm Assuming Conjecture:** Suppose $n$ is large.

**Conjecture:** Suppose $r$ does not divide $n(n^2-1)$ where $r$ is prime. Then $n$ is a prime if and only if

$$(*) \qquad (x-1)^n \equiv x^n - 1 \pmod{x^r - 1, n}.$$

**Idea for an Algorithm Assuming Conjecture:** Suppose $n$ is large. Since

$$\prod_{p \le x} p \ge e^{0.8x} \quad \text{for } x \ge 67,$$

there is a prime $r \in [2, 5\log n]$ not dividing $n^2 - 1$.

**Conjecture:** Suppose $r$ does not divide $n(n^2-1)$ where $r$ is prime. Then $n$ is a prime if and only if

$$(*) \qquad (x-1)^n \equiv x^n - 1 \pmod{x^r - 1, n}.$$

**Idea for an Algorithm Assuming Conjecture:** Suppose $n$ is large. Since

$$\prod_{p \le x} p \ge e^{0.8x} \quad \text{for } x \ge 67,$$

there is a prime $r \in [2, 5\log n]$ not dividing $n^2-1$. If $r$ divides $n$, then $n$ is composite.

**Conjecture:** Suppose $r$ does not divide $n(n^2-1)$ where $r$ is prime. Then $n$ is a prime if and only if

$$(*) \qquad (x-1)^n \equiv x^n - 1 \pmod{x^r - 1, n}.$$

**Idea for an Algorithm Assuming Conjecture:** Suppose $n$ is large. Since

$$\prod_{p \le x} p \ge e^{0.8x} \quad \text{for } x \ge 67,$$

there is a prime $r \in [2, 5\log n]$ not dividing $n^2-1$. If $r$ divides $n$, then $n$ is composite. Otherwise, check if $(*)$ holds to determine whether $n$ is a prime.

**Conjecture:** Suppose $r$ does not divide $n(n^2-1)$ where $r$ is prime. Then $n$ is a prime if and only if

$$(*) \qquad (x-1)^n \equiv x^n - 1 \pmod{x^r - 1, n}.$$

**What if the Conjecture is not true?**

# Two Important Papers in the Literature:

**Two Important Papers in the Literature:**

- Etienne Fouvry, *Théorèm de Brun-Titchmarsh, application au théorèm de Fermat*, Invent. Math **79** (1985), 383–407.
- Leonard Adleman and D. Roger Heath-Brown, *The first case of Fermat's Last Theorem*, Invent. Math **79** (1985), 409–416.

**Two Important Papers in the Literature:**

- Etienne Fouvry, *Théorèm de Brun-Titchmarsh, application au théorèm de Fermat*, Invent. Math **79** (1985), 383–407.
- Leonard Adleman and D. Roger Heath-Brown, *The first case of Fermat's Last Theorem*, Invent. Math **79** (1985), 409–416.

**Two Important Papers in the Literature:**

- Etienne Fouvry, *Théorèm de Brun-Titchmarsh, application au théorèm de Fermat*, Invent. Math **79** (1985), 383–407.
- Leonard Adleman and D. Roger Heath-Brown, *The first case of Fermat's Last Theorem*, Invent. Math **79** (1985), 409–416.

**Two Important Papers in the Literature:**

- Etienne Fouvry, *Théorèm de Brun-Titchmarsh, application au théorèm de Fermat*, Invent. Math **79** (1985), 383–407.
- Leonard Adleman and D. Roger Heath-Brown, *The first case of Fermat's Last Theorem*, Invent. Math **79** (1985), 409–416.

Adleman and Heath-Brown, using Fouvry's result, showed for the first time that the first case of Fermat's Last Theorem holds for infinitely many prime exponents.

## Two Important Papers in the Literature:

- Etienne Fouvry, *Théorèm de Brun-Titchmarsh, application au théorèm de Fermat*, Invent. Math **79** (1985), 383–407.
- Leonard Adleman and D. Roger Heath-Brown, *The first case of Fermat's Last Theorem*, Invent. Math **79** (1985), 409–416.

Fouvry showed that there are infinitely many primes $p$ for which the largest prime factor of $p - 1$ exceeds $p^{2/3}$.

## Two Important Papers in the Literature:

- Etienne Fouvry, *Théorèm de Brun-Titchmarsh, application au théorèm de Fermat*, Invent. Math **79** (1985), 383–407.
- Leonard Adleman and D. Roger Heath-Brown, *The first case of Fermat's Last Theorem*, Invent. Math **79** (1985), 409–416.

Fouvry showed that there are infinitely many primes $p$ for which the largest prime factor of $p - 1$ exceeds $p^{2/3}$. More precisely, he showed . . .

**Two Important Papers in the Literature:**

- Etienne Fouvry, *Théorèm de Brun-Titchmarsh, application au théorèm de Fermat*, Invent. Math **79** (1985), 383–407.
- Leonard Adleman and D. Roger Heath-Brown, *The first case of Fermat's Last Theorem*, Invent. Math **79** (1985), 409–416.

**Notation.**

**Two Important Papers in the Literature:**

- Etienne Fouvry, *Théorèm de Brun-Titchmarsh, application au théorèm de Fermat*, Invent. Math **79** (1985), 383–407.
- Leonard Adleman and D. Roger Heath-Brown, *The first case of Fermat's Last Theorem*, Invent. Math **79** (1985), 409–416.

**Notation.** $$\pi(x) = \left|\{p : p \text{ prime} \le x\}\right|$$

**Two Important Papers in the Literature:**

- Etienne Fouvry, *Théorèm de Brun-Titchmarsh, application au théorèm de Fermat*, Invent. Math **79** (1985), 383–407.
- Leonard Adleman and D. Roger Heath-Brown, *The first case of Fermat's Last Theorem*, Invent. Math **79** (1985), 409–416.

**Notation.** $$\pi(x) = \left|\{p : p \text{ prime} \leq x\}\right|$$

$$\pi_s(x) = \left|\{p : p \text{ prime} \leq x, P(p-1) > p^{2/3}\}\right|$$

**Two Important Papers in the Literature:**

- Etienne Fouvry, *Théorèm de Brun-Titchmarsh, application au théorèm de Fermat*, Invent. Math **79** (1985), 383–407.
- Leonard Adleman and D. Roger Heath-Brown, *The first case of Fermat's Last Theorem*, Invent. Math **79** (1985), 409–416.

**Notation.** $$\pi(x) = \left|\{p : p \text{ prime} \le x\}\right|$$

$$\underset{\substack{\uparrow\\ \text{“s” as in } special}}{\pi_s}(x) = \left|\{p : p \text{ prime} \le x, P(p-1) > p^{2/3}\}\right|$$

## Two Important Papers in the Literature:

- Etienne Fouvry, *Théorèm de Brun-Titchmarsh, application au théorèm de Fermat*, Invent. Math **79** (1985), 383–407.
- Leonard Adleman and D. Roger Heath-Brown, *The first case of Fermat's Last Theorem*, Invent. Math **79** (1985), 409–416.

**Notation.** $\pi(x) = \left|\{p : p \text{ prime} \le x\}\right|$

$$\pi_s(x) = \left|\{p : p \text{ prime} \le x, \underbrace{P(p-1)} > p^{2/3}\}\right|$$

"s" as in *special*

$P(n)$ is the largest prime factor of $n$

**Two Important Papers in the Literature:**

- Etienne Fouvry, *Théorèm de Brun-Titchmarsh, application au théorèm de Fermat*, Invent. Math **79** (1985), 383–407.
- Leonard Adleman and D. Roger Heath-Brown, *The first case of Fermat's Last Theorem*, Invent. Math **79** (1985), 409–416.

**Lemma 1.** There is a constant $c > 0$ and $x_0$ such that

$$\pi_s(x) \geq c\frac{x}{\log x} \quad \text{for all } x \geq x_0.$$

**Two Important Papers in the Literature:**

- Etienne Fouvry, *Théorèm de Brun-Titchmarsh, application au théorèm de Fermat*, Invent. Math **79** (1985), 383–407.
- Leonard Adleman and D. Roger Heath-Brown, *The first case of Fermat's Last Theorem*, Invent. Math **79** (1985), 409–416.

**Classical.** $\pi(x) \le \dfrac{2x}{\log x}$ for $x$ large

## Two Important Papers in the Literature:

- Etienne Fouvry, *Théorèm de Brun-Titchmarsh, application au théorèm de Fermat*, Invent. Math **79** (1985), 383–407.
- Leonard Adleman and D. Roger Heath-Brown, *The first case of Fermat's Last Theorem*, Invent. Math **79** (1985), 409–416.

**Lemma 1.** $\pi_s(x) \geq \dfrac{cx}{\log x}$ for $x$ large

**Lemma 2.** There are positive constants $c_1$ and $c_2$ such that the interval $I = (c_1(\log n)^6, c_2(\log n)^6]$ contains a prime $r$ with $r - 1$ having a prime factor $q$ satisfying

$$q \geq 4\sqrt{r}\log n \quad \text{and} \quad q|\mathrm{ord}_r(n).$$

**Lemma 2.** There are positive constants $c_1$ and $c_2$ such that the interval $I = (c_1(\log n)^6, c_2(\log n)^6]$ contains a prime $r$ with $r - 1$ having a prime factor $q$ satisfying

$$q \geq 4\sqrt{r}\log n \quad \text{and} \quad q | \underbrace{\mathrm{ord}_r(n)}.$$

$$n^s \equiv 1 \pmod{r} \implies q|s$$

**Lemma 2.** There are positive constants $c_1$ and $c_2$ such that the interval $I = (c_1(\log n)^6, c_2(\log n)^6]$ contains a prime $r$ with $r - 1$ having a prime factor $q$ satisfying

$$q \geq 4\sqrt{r}\log n \quad \text{and} \quad q|\mathrm{ord}_r(n).$$

**Lemma 2.** There are positive constants $c_1$ and $c_2$ such that the interval $I = (c_1(\log n)^6, c_2(\log n)^6]$ contains a prime $r$ with $r - 1$ having a prime factor $q$ satisfying

$$q \geq 4\sqrt{r}\log n \quad \text{and} \quad q|\mathrm{ord}_r(n).$$

**Proof.**

**Lemma 2.** There are positive constants $c_1$ and $c_2$ such that the interval $I = (c_1(\log n)^6, c_2(\log n)^6]$ contains a prime $r$ with $r - 1$ having a prime factor $q$ satisfying

$$q \geq 4\sqrt{r}\log n \quad \text{and} \quad q | \mathrm{ord}_r(n).$$

**Proof.** We may suppose that $n$ is large.

**Lemma 2.** There are positive constants $c_1$ and $c_2$ such that the interval $I = (c_1(\log n)^6, c_2(\log n)^6]$ contains a prime $r$ with $r - 1$ having a prime factor $q$ satisfying

$$q \geq 4\sqrt{r}\log n \quad \text{and} \quad q|\text{ord}_r(n).$$

**Proof.** We may suppose that $n$ is large. By Lemma 1, the number of special primes in $I$ is at least

**Lemma 2.** There are positive constants $c_1$ and $c_2$ such that the interval $I = (c_1(\log n)^6, c_2(\log n)^6]$ contains a prime $r$ with $r - 1$ having a prime factor $q$ satisfying

$$q \geq 4\sqrt{r}\log n \quad \text{and} \quad q|\mathrm{ord}_r(n).$$

**Proof.** We may suppose that $n$ is large. By Lemma 1, the number of special primes in $I$ is at least

$$\pi_s(c_2(\log n)^6) - \pi_s(c_1(\log n)^6)$$

**Lemma 2.** There are positive constants $c_1$ and $c_2$ such that the interval $I = (c_1(\log n)^6, c_2(\log n)^6]$ contains a prime $r$ with $r - 1$ having a prime factor $q$ satisfying

$$q \geq 4\sqrt{r}\log n \quad \text{and} \quad q|\mathrm{ord}_r(n).$$

**Proof.** We may suppose that $n$ is large. By Lemma 1, the number of special primes in $I$ is at least

$$\begin{aligned}\pi_s(c_2(\log n)^6) &- \pi_s(c_1(\log n)^6) \\ &\geq \pi_s(c_2(\log n)^6) - \pi(c_1(\log n)^6)\end{aligned}$$

**Classical.** $\pi(x) \leq \dfrac{2x}{\log x}$ for $x$ large

**Lemma 2.** There are positive constants $c_1$ and $c_2$ such that the interval $I = (c_1(\log n)^6, c_2(\log n)^6]$ contains a prime $r$ with $r - 1$ having a prime factor $q$ satisfying

$$q \geq 4\sqrt{r}\log n \quad \text{and} \quad q|\mathrm{ord}_r(n).$$

**Proof.** We may suppose that $n$ is large. By Lemma 1, the number of special primes in $I$ is at least

$$\begin{aligned}
\pi_s(c_2(\log n)^6) - \pi_s(c_1(\log n)^6) \\
&\geq \pi_s(c_2(\log n)^6) - \pi(c_1(\log n)^6) \\
&\geq \frac{cc_2(\log n)^6}{7\log\log n}
\end{aligned}$$

**Lemma 2.** There are positive constants $c_1$ and $c_2$ such that the interval $I = (c_1(\log n)^6, c_2(\log n)^6]$ contains a prime $r$ with $r - 1$ having a prime factor $q$ satisfying

$$q \geq 4\sqrt{r}\log n \quad \text{and} \quad q|\mathrm{ord}_r(n).$$

**Proof.** We may suppose that $n$ is large. By Lemma 1, the number of special primes in $I$ is at least

$$\begin{aligned}
\pi_s(c_2(\log n)^6) &- \pi_s(c_1(\log n)^6) \\
&\geq \pi_s(c_2(\log n)^6) - \pi(c_1(\log n)^6) \\
&\geq \frac{cc_2(\log n)^6}{7\log\log n} - \frac{c_1(\log n)^6}{3\log\log n}
\end{aligned}$$

**Lemma 2.** There are positive constants $c_1$ and $c_2$ such that the interval $I = (c_1(\log n)^6, c_2(\log n)^6]$ contains a prime $r$ with $r - 1$ having a prime factor $q$ satisfying

$$q \geq 4\sqrt{r}\log n \quad \text{and} \quad q|\mathrm{ord}_r(n).$$

**Proof.** We may suppose that $n$ is large. By Lemma 1, the number of special primes in $I$ is at least

$$\begin{aligned} \pi_s(c_2(\log n)^6) - \pi_s(c_1(\log n)^6) \\ &\geq \pi_s(c_2(\log n)^6) - \pi(c_1(\log n)^6) \\ &\geq \left(\frac{cc_2}{7} - \frac{c_1}{3}\right)\frac{(\log n)^6}{\log\log n} \end{aligned}$$

**Lemma 2.** There are positive constants $c_1$ and $c_2$ such that the interval $I = (c_1(\log n)^6, c_2(\log n)^6]$ contains a prime $r$ with $r - 1$ having a prime factor $q$ satisfying

$$q \geq 4\sqrt{r}\log n \quad \text{and} \quad q|\mathrm{ord}_r(n).$$

**Proof.** We may suppose that $n$ is large. By Lemma 1, the number of special primes in $I$ is at least

$$\begin{aligned}
&\pi_s(c_2(\log n)^6) - \pi_s(c_1(\log n)^6) \\
&\qquad \geq \pi_s(c_2(\log n)^6) - \pi(c_1(\log n)^6) \\
&\qquad \geq \quad c' \quad \frac{(\log n)^6}{\log\log n}.
\end{aligned}$$

**Lemma 2.** There are positive constants $c_1$ and $c_2$ such that the interval $I = (c_1(\log n)^6, c_2(\log n)^6]$ contains a prime $r$ with $r-1$ having a prime factor $q$ satisfying

$$q \geq 4\sqrt{r}\log n \quad \text{and} \quad q|\mathrm{ord}_r(n).$$

**Proof.** We may suppose that $n$ is large. By Lemma 1, the number of special primes in $I$ is at least

$$\pi_s(c_2(\log n)^6) - \pi_s(c_1(\log n)^6) \geq \frac{c'(\log n)^6}{\log\log n}.$$

**Lemma 2.** There are positive constants $c_1$ and $c_2$ such that the interval $I = (c_1(\log n)^6, c_2(\log n)^6]$ contains a prime $r$ with $r - 1$ having a prime factor $q$ satisfying

$$q \geq 4\sqrt{r}\log n \quad \text{and} \quad q|\mathrm{ord}_r(n).$$

**Proof.** We may suppose that $n$ is large. By Lemma 1, the number of special primes in $I$ is at least

$$\pi_s(c_2(\log n)^6) - \pi_s(c_1(\log n)^6) \geq \frac{c'(\log n)^6}{\log\log n}.$$

If $r$ is a special prime in $I$, then $r - 1$ has a prime factor $q$ satisfying

$$q \geq r^{2/3}$$

**Lemma 2.** There are positive constants $c_1$ and $c_2$ such that the interval $I = (c_1(\log n)^6, c_2(\log n)^6]$ contains a prime $r$ with $r - 1$ having a prime factor $q$ satisfying

$$q \geq 4\sqrt{r}\log n \quad \text{and} \quad q|\mathrm{ord}_r(n).$$

**Proof.** We may suppose that $n$ is large. By Lemma 1, the number of special primes in $I$ is at least

$$\pi_s\big(c_2(\log n)^6\big) - \pi_s\big(c_1(\log n)^6\big) \geq \frac{c'(\log n)^6}{\log\log n}.$$

If $r$ is a special prime in $I$, then $r - 1$ has a prime factor $q$ satisfying

$$q \geq r^{2/3} = \sqrt{r}\, r^{1/6}$$

**Lemma 2.** There are positive constants $c_1$ and $c_2$ such that the interval $I = (c_1(\log n)^6, c_2(\log n)^6]$ contains a prime $r$ with $r - 1$ having a prime factor $q$ satisfying

$$q \geq 4\sqrt{r}\log n \quad \text{and} \quad q | \mathrm{ord}_r(n).$$

**Proof.** We may suppose that $n$ is large. By Lemma 1, the number of special primes in $I$ is at least

$$\pi_s(c_2(\log n)^6) - \pi_s(c_1(\log n)^6) \geq \frac{c'(\log n)^6}{\log\log n}.$$

If $r$ is a special prime in $I$, then $r - 1$ has a prime factor $q$ satisfying

$$q \geq r^{2/3} = \sqrt{r}\, r^{1/6} \geq 4\sqrt{r}\log n.$$

**Lemma 2.** There are positive constants $c_1$ and $c_2$ such that the interval $I = (c_1(\log n)^6, c_2(\log n)^6]$ contains a prime $r$ with $r - 1$ having a prime factor $q$ satisfying

$$q \geq 4\sqrt{r}\log n \quad \text{and} \quad q | \mathrm{ord}_r(n).$$

**Proof.** There are $\geq c'(\log n)^6/\log\log n$ primes $r$ in $I$ with $r-1$ having a prime factor $q \geq r^{2/3} \geq 4\sqrt{r}\log n$.

**Lemma 2.** There are positive constants $c_1$ and $c_2$ such that the interval $I = (c_1(\log n)^6, c_2(\log n)^6]$ contains a prime $r$ with $r - 1$ having a prime factor $q$ satisfying

$$q \geq 4\sqrt{r}\log n \quad \text{and} \quad q|\mathrm{ord}_r(n).$$

**Proof.** There are $\geq c'(\log n)^6/\log\log n$ primes $r$ in $I$ with $r-1$ having a prime factor $q \geq r^{2/3} \geq 4\sqrt{r}\log n$. We want at least one such $q$ to divide $\mathrm{ord}_r(n)$.

**Lemma 2.** There are positive constants $c_1$ and $c_2$ such that the interval $I = (c_1(\log n)^6, c_2(\log n)^6]$ contains a prime $r$ with $r - 1$ having a prime factor $q$ satisfying

$$q \geq 4\sqrt{r} \log n \quad \text{and} \quad q | \mathrm{ord}_r(n).$$

**Proof.** There are $\geq c'(\log n)^6 / \log\log n$ primes $r$ in $I$ with $r-1$ having a prime factor $q \geq r^{2/3} \geq 4\sqrt{r}\log n$. We want at least one such $q$ to divide $\mathrm{ord}_r(n)$. Note that if $q \nmid \mathrm{ord}_r(n)$, then

$$\mathrm{ord}_r(n) \leq r^{1/3} \leq M \quad \text{where} \quad M = c_2^{1/3}(\log n)^2.$$

**Proof.** There are $\geq c'(\log n)^6 / \log\log n$ primes $r$ in $I$ with $r-1$ having a prime factor $q \geq r^{2/3} \geq 4\sqrt{r}\log n$. We want at least one such $q$ to divide $\mathrm{ord}_r(n)$. Note that if $q \nmid \mathrm{ord}_r(n)$, then

$$\mathrm{ord}_r(n) \leq r^{1/3} \leq M \quad \text{where } M = c_2^{1/3}(\log n)^2.$$

**Proof.** There are $\geq c'(\log n)^6/\log\log n$ primes $r$ in $I$ with $r-1$ having a prime factor $q \geq r^{2/3} \geq 4\sqrt{r}\log n$. We want at least one such $q$ to divide $\mathrm{ord}_r(n)$. Note that if $q \nmid \mathrm{ord}_r(n)$, then

$$\mathrm{ord}_r(n) \leq r^{1/3} \leq M \quad \text{where } M = c_2^{1/3}(\log n)^2.$$

Hence, $r$ divides

$$\prod_{1\leq j\leq M} (n^j - 1) \leq n^{M^2}.$$

**Proof.** There are $\geq c'(\log n)^6 / \log\log n$ primes $r$ in $I$ with $r-1$ having a prime factor $q \geq r^{2/3} \geq 4\sqrt{r}\log n$. We want at least one such $q$ to divide $\mathrm{ord}_r(n)$. Note that if $q \nmid \mathrm{ord}_r(n)$, then

$$\mathrm{ord}_r(n) \leq r^{1/3} \leq M \quad \text{where } \; M = c_2^{1/3}(\log n)^2.$$

Hence, $r$ divides

$$\prod_{1\leq j\leq M} (n^j - 1) \leq n^{M^2}.$$

If there are $k$ primes dividing the product, then

$2^k \leq n^{M^2}$

**Proof.** There are $\geq c'(\log n)^6/\log\log n$ primes $r$ in $I$ with $r-1$ having a prime factor $q \geq r^{2/3} \geq 4\sqrt{r}\log n$. We want at least one such $q$ to divide $\mathrm{ord}_r(n)$. Note that if $q \nmid \mathrm{ord}_r(n)$, then

$$\mathrm{ord}_r(n) \leq r^{1/3} \leq M \quad \text{where } M = c_2^{1/3}(\log n)^2.$$

Hence, $r$ divides

$$\prod_{1\leq j\leq M}(n^j - 1) \leq n^{M^2}.$$

If there are $k$ primes dividing the product, then

$$2^k \leq n^{M^2} \implies k = \mathcal{O}(M^2 \log n) = \mathcal{O}((\log n)^5).$$

**Proof.** There are $\geq c'(\log n)^6/\log\log n$ primes $r$ in $I$ with $r-1$ having a prime factor $q \geq r^{2/3} \geq 4\sqrt{r}\log n$. We want at least one such $q$ to divide $\mathrm{ord}_r(n)$. Note that if $q \nmid \mathrm{ord}_r(n)$, then

$$\mathrm{ord}_r(n) \leq r^{1/3} \leq M \quad \text{where} \quad M = c_2^{1/3}(\log n)^2.$$

Hence, $r$ divides

$$\prod_{1\leq j\leq M} (n^j - 1) \leq n^{M^2}.$$

If there are $k$ primes dividing the product, then

$$2^k \leq n^{M^2} \implies k = \mathcal{O}(M^2 \log n) = \mathcal{O}((\log n)^5).$$

Hence, for at least one prime $r \in I$ as above . . . . ∎

**Lemma 2.** There are positive constants $c_1$ and $c_2$ such that the interval $I = (c_1(\log n)^6, c_2(\log n)^6]$ contains a prime $r$ with $r - 1$ having a prime factor $q$ satisfying

$$q \geq 4\sqrt{r}\log n \quad \text{and} \quad q|\mathrm{ord}_r(n).$$

**Lemma 2.** There are positive constants $c_1$ and $c_2$ such that the interval $I = (c_1(\log n)^6, c_2(\log n)^6]$ contains a prime $r$ with $r - 1$ having a prime factor $q$ satisfying

$$q \geq 4\sqrt{r}\log n \quad \text{and} \quad q|\mathrm{ord}_r(n).$$

**So what's the algorithm?**

Input: integer $n > 1$

if ( $n$ is of the form $a^b$, $b > 1$ ) output COMPOSITE;

$r = 2$;

while ( $r < n$ ) $\{$

    if ( $\gcd(n, r) \neq 1$ ) output COMPOSITE;

    if ( $r$ is prime )

        let $q$ be the largest prime factor of $r - 1$;

        if ( $q \geq 4\sqrt{r}\log n$ ) and ( $n^{(r-1)/q} \not\equiv 1 \pmod{r}$ )

            break;

    $r \rightarrow r + 1$;

$\}$

for $a = 1$ to $2\sqrt{r}\log n$

    if ( $(x - a)^n \not\equiv x^n - a \pmod{x^r - 1, n}$ ) output COMPOSITE;

output PRIME;

**Lemma 2.** There are positive constants $c_1$ and $c_2$ such that the interval $I = (c_1(\log n)^6, c_2(\log n)^6]$ contains a prime $r$ with $r-1$ having a prime factor $q$ satisfying

$$q \geq 4\sqrt{r}\log n \quad \text{and} \quad q|\text{ord}_r(n).$$

```
    if ( gcd(n,r) ≠ 1 ) output COMPOSITE;
    if ( r is prime )
        let q be the largest prime factor of r − 1;
        if ( q ≥ 4√r log n ) and ( n^((r−1)/q) ≢ 1 (mod r) )
            break;
    r → r + 1;
}
for a = 1 to 2√r log n
    if ( (x − a)^n ≢ x^n − a (mod x^r − 1, n) ) output COMPOSITE;
output PRIME;
```

$\underbrace{n^{(r-1)/q} \not\equiv 1 \pmod r}_{\uparrow \; q|\text{ord}_r(n)}$

Input: integer $n > 1$

if ( $n$ is of the form $a^b$, $b > 1$ ) output COMPOSITE;
$r = 2$;
while ( $r < n$ ) $\{$
    if ( $\gcd(n, r) \neq 1$ ) output COMPOSITE;
    if ( $r$ is prime )
        let $q$ be the largest prime factor of $r - 1$;
        if ( $q \geq 4\sqrt{r}\log n$ ) and ( $n^{(r-1)/q} \not\equiv 1 \pmod{r}$ )
            break;
    $r \longrightarrow r + 1$;
$\}$
for $a = 1$ to $2\sqrt{r}\log n$
    if ( $(x - a)^n \not\equiv x^n - a \pmod{x^r - 1, n}$ ) output COMPOSITE;
output PRIME;

Input: integer $n > 1$

if ( $n$ is of the form $a^b$, $b > 1$ ) output COMPOSITE;

$r = 2$;

while ( $r < n$ ) { Lemma 2 $\Longrightarrow$ loop ends with $r \ll (\log n)^6$

    if ( $\gcd(n, r) \neq 1$ ) output COMPOSITE;

    if ( $r$ is prime )

        let $q$ be the largest prime factor of $r - 1$;

        if ( $q \geq 4\sqrt{r}\log n$ ) and ( $n^{(r-1)/q} \not\equiv 1 \pmod{r}$ )

            break;

ITE;

**Lemma 2.** There are positive constants $c_1$ and $c_2$ such that the interval $I = (c_1(\log n)^6, c_2(\log n)^6]$ contains a prime $r$ with $r - 1$ having a prime factor $q$ satisfying

$$q \geq 4\sqrt{r}\log n \quad \text{and} \quad q \mid \mathrm{ord}_r(n).$$

Input: integer $n > 1$

if ( $n$ is of the form $a^b$, $b > 1$ ) output COMPOSITE;<br>
$r = 2$;<br>
while ( $r < n$ ) {      Lemma 2 $\Longrightarrow$ loop ends with $r \ll (\log n)^6$<br>
    if ( $\gcd(n, r) \neq 1$ ) output COMPOSITE;<br>
    if ( $r$ is prime )<br>
        let $q$ be the largest prime factor of $r - 1$;<br>
        if ( $q \geq 4\sqrt{r}\log n$ ) and ( $n^{(r-1)/q} \not\equiv 1 \pmod{r}$ )<br>
            break;<br>
    $r \rightarrow r + 1$;      Note that, after the while loop, $r = n$ is possible.<br>
}<br>
for $a = 1$ to $2\sqrt{r}\log n$<br>
    if ( $(x-a)^n \not\equiv x^n - a \pmod{x^r - 1, n}$ ) output COMPOSITE;<br>
output PRIME;

Input: integer $n > 1$

if ( $n$ is of the form $a^b$, $b > 1$ ) output COMPOSITE;

$r = 2$;

while ( $r < n$ ) { Lemma 2 $\Longrightarrow$ loop ends with $r \ll (\log n)^6$

    if ( $\gcd(n, r) \neq 1$ ) output COMPOSITE;

    if ( $r$ is prime )

        let $q$ be the largest prime factor of $r - 1$;

        if ( $q \geq 4\sqrt{r}\log n$ ) and ( $n^{(r-1)/q} \not\equiv 1 \pmod{r}$ )

            break;

    $r \rightarrow r + 1$; Note that, after the while loop, $r = n$ is possible.

} Then $n$ is prime, and the algorithm indicates it is.

for $a = 1$ to $2\sqrt{r}\log n$

    if ( $(x - a)^n \not\equiv x^n - a \pmod{x^r - 1, n}$ ) output COMPOSITE;

output PRIME;

Input: integer $n > 1$

if ( $n$ is of the form $a^b$, $b > 1$ ) output COMPOSITE;

$r = 2$;

while ( $r < n$ ) { Lemma 2 $\Longrightarrow$ loop ends with $r \ll (\log n)^6$

if ( $\gcd(n, r) \neq 1$ ) output COMPOSITE;

if ( $r$ is prime )

let $q$ be the largest prime factor of $r - 1$;

if ( $q \geq 4\sqrt{r}\log n$ ) and ( $n^{(r-1)/q} \not\equiv 1 \pmod{r}$ )

break;

$r \rightarrow r + 1$; **IMPORTANT:**

}

for $a = 1$ to $2\sqrt{r}\log n$

if ( $(x-a)^n \not\equiv x^n - a \pmod{x^r - 1, n}$ ) output COMPOSITE;

output PRIME;

Input: integer $n > 1$

if ( $n$ is of the form $a^b$, $b > 1$ ) output COMPOSITE;
$r = 2$;
while ( $r < n$ ) {

Lemma 2 $\Longrightarrow$ loop ends with $r \ll (\log n)^6$

    if ( $\gcd(n, r) \neq 1$ ) output COMPOSITE;
    if ( $r$ is prime )
        let $q$ be the largest prime factor of $r - 1$;
        if ( $q \geq 4\sqrt{r}\log n$ ) and ( $n^{(r-1)/q} \not\equiv 1 \pmod r$ )
            break;
    $r \to r + 1$;

**IMPORTANT:** In general, if $n$ is a prime, then the algorithm indicates it is.

}
for $a = 1$ to $2\sqrt{r}\log n$
    if ( $(x - a)^n \not\equiv x^n - a \pmod{x^r - 1, n}$ ) output COMPOSITE;
output PRIME;

Input: integer $n > 1$

if ( $n$ is of the form $a^b$, $b > 1$ ) output COMPOSITE;

$r = 2$;

while ( $r < n$ ) $\{$

  if ( $\gcd(n, r) \neq 1$ ) output COMPOSITE;

  if ( $r$ is prime )

    let $q$ be the largest prime factor of $r - 1$;

    if ( $q \geq 4\sqrt{r}\log n$ ) and ( $n^{(r-1)/q} \not\equiv 1 \pmod{r}$ )

      break;

  $r \rightarrow r + 1$;

$\}$

for $a = 1$ to $2\sqrt{r}\log n$

  if ( $(x - a)^n \not\equiv x^n - a \pmod{x^r - 1, n}$ ) output COMPOSITE;

output PRIME;

Input: integer $n > 1$

if ( $n$ is of the form $a^b$, $b > 1$ ) output COMPOSITE;<br>
$r = 2$;<br>
while ( $r < n$ ) {<br>
    if ( $\gcd(n, r) \neq 1$ ) output COMPOSITE;<br>
    if ( $r$ is prime )<br>
        let $q$ be the largest prime factor of $r - 1$;<br>
        if ( $q \geq 4\sqrt{r}\log n$ ) and ( $n^{(r-1)/q} \not\equiv 1 \pmod{r}$ )<br>
            break;<br>
    $r \rightarrow r + 1$;<br>
}<br>
for $a = 1$ to $2\sqrt{r}\log n$<br>
    if ( $(x - a)^n \not\equiv x^n - a \pmod{x^r - 1, n}$ ) output COMPOSITE;<br>
output PRIME;

Since the while loop ends with $r \ll (\log n)^6$, the running time is polynomial in $\log n$.

Input: integer $n > 1$

if ( $n$ is of the form $a^b$, $b > 1$ ) output COMPOSITE;<br>
$r = 2$;<br>
while ( $r < n$ ) $\{$<br>
    if ( $\gcd(n, r) \neq 1$ ) output COMPOSITE;<br>
    if ( $r$ is prime )<br>
        let $q$ be the largest prime factor of $r - 1$;<br>
        if ( $q \geq 4\sqrt{r} \log n$ ) and ( $n^{(r-1)/q} \not\equiv 1 \pmod{r}$ )<br>
            break;<br>
    $r \rightarrow r + 1$;<br>
$\}$<br>
for $a = 1$ to $2\sqrt{r} \log n$<br>
    if ( $(x - a)^n \not\equiv x^n - a \pmod{x^r - 1, n}$ ) output COMPOSITE;<br>
output PRIME;

Input: integer $n > 1$

if ( $n$ is of the form $a^b$, $b > 1$ ) output COMPOSITE;

$r = 2$;

while ( $r < n$ ) $\{$

    if ( $\gcd(n, r) \neq 1$ ) output COMPOSITE;

    if ( $r$ is prime )

        let $q$ be the largest prime factor of $r - 1$;

        if ( $q \geq 4\sqrt{r}\log n$ ) and ( $n^{(r-1)/q} \not\equiv 1 \pmod{r}$ )

            break;

    $r \to r + 1$;

$\}$

for $a = 1$ to $2\sqrt{r}\log n$

    if ( $(x - a)^n \not\equiv x^n - a \pmod{x^r - 1, n}$ ) output COMPOSITE;

output PRIME;

**Note that $n$ does not have any prime divisors $\leq r$.**

```
Input:  integer n > 1

if ( n is of the form a^b, b > 1 ) output COMPOSITE;
r = 2;
while ( r < n ) {
    if ( gcd(n,r) ≠ 1 ) output COMPOSITE;
    if ( r is prime )
        let q be the largest prime factor of r − 1;
        if ( q ≥ 4√r log n ) and ( n^((r−1)/q) ≢ 1 (mod r) )
            break;
    r → r + 1;
}
for a = 1 to 2√r log n
    if ( (x − a)^n ≢ x^n − a (mod x^r − 1, n) ) output COMPOSITE;
output PRIME;
```

**PROBLEM :** Show that if $n$ is composite, then the algorithm indicates it is.

**SITUATION:**

$$\boldsymbol{n} \text{ is composite,} \quad \boldsymbol{r} \text{ is a prime}$$

$$\boldsymbol{q} \text{ is a prime,} \quad \boldsymbol{q} \geq \mathbf{4}\sqrt{\boldsymbol{r}}\,\log \boldsymbol{n}$$

$$\boldsymbol{q} \nmid \boldsymbol{n}, \quad \boldsymbol{q} | (\boldsymbol{r} - \mathbf{1}), \quad \boldsymbol{q} | \mathbf{ord}_{\boldsymbol{r}}(\boldsymbol{n})$$

**WANT:** There is an integer $\boldsymbol{a}$ with $\mathbf{1} \leq \boldsymbol{a} \leq \mathbf{2}\sqrt{\boldsymbol{r}}\,\log \boldsymbol{n}$ such that

$$(\boldsymbol{x} - \boldsymbol{a})^{\boldsymbol{n}} \not\equiv (\boldsymbol{x}^{\boldsymbol{n}} - \boldsymbol{a}) \pmod{\boldsymbol{x}^{\boldsymbol{r}} - \mathbf{1},\ \boldsymbol{n}}.$$