PRIMALITY TESTING IN POLYNOMIAL TIME

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

PRIMALITY TESTING IN POLYNOMIAL TIME

CAUTION: This is a theoretical result.

Primality Testing in Polynomial Time

Caution: This is a theoretical result. We will describe an algorithm that determines whether a number n is prime in $\mathcal{O}((\log n)^{12+\varepsilon})$ steps

Primality Testing in Polynomial Time

Caution: This is a theoretical result. We will describe an algorithm that determines whether a number n is prime in $\mathcal{O}((\log n)^{12+\varepsilon})$ steps, a truly remarkable result.

PRIMALITY TESTING IN POLYNOMIAL TIME

CAUTION: This is a theoretical result. We will describe an algorithm that determines whether a number n is prime in $\mathcal{O}((\log n)^{12+\varepsilon})$ steps, a truly remarkable result. There is, however, no claim that if $n < 10^{1000}$, then the algorithm takes less than n steps.

Primality Testing in Polynomial Time

Another Caution:

ANOTHER CAUTION:

$$\log x = \log_2 x$$

Simple Idea: Suppose that a and n are coprime integers. Then n is a prime if and only if

$$(x - a)^n \equiv x^n - a \pmod{n}.$$

Simple Idea: Suppose that a and n are coprime integers. Then n is a prime if and only if

$$(x - a)^n \equiv x^n - a \pmod{n}.$$

Comments: Verifying the congruence requires too much running time as the LHS contains $n + 1$ non-zero terms.

Simple Idea: Suppose that a and n are coprime integers. Then n is a prime if and only if

$$(x - a)^n \equiv x^n - a \pmod{n}.$$

Comments: Verifying the congruence requires too much running time as the LHS contains $n + 1$ non-zero terms.

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

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

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

What does this mean?

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

What does this mean?

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

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

What does this mean?

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

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

  in MAPLE.

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

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

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

big-oh

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

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

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:

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 $k_1 < k_2 < \cdots < k_t$.

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.

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 $x^{n \bmod r} - (a \bmod n)$.

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

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

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

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

n prime $\Longrightarrow$ $(*)$ holds

$(*)$ holds $\Longrightarrow$ n prime

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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. $\pi(x) = \big|\{p : p \text{ prime} \le x\}\big|$

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

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

$\uparrow$

"s" as in s*pecial*

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

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

$\uparrow$ "s" as in s*pecial*

$P(n)$ 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

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

$$\uparrow$$

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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 $\text{ord}_r(n)$.

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

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

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 $\text{ord}_r(n)$. Note that if $q \nmid \text{ord}_r(n)$, then

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

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

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

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 $\text{ord}_r(n)$. Note that if $q \nmid \text{ord}_r(n)$, then

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

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 $\operatorname{ord}_r(n)$. Note that if $q \nmid \operatorname{ord}_r(n)$, then

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

Hence, r divides

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

If there are k primes dividing the product, then

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

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

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

If there are k primes dividing the product, then

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

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

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 $\operatorname{ord}_r(n)$. Note that if $q \nmid \operatorname{ord}_r(n)$, then

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

Hence, r divides

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

If there are k primes dividing the product, then

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

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

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

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

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

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

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;

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 ($\underbrace{n^{(r-1)/q} \not\equiv 1 \pmod{r}}_{\uparrow \; q | \mathrm{ord}_r(n)}$)
            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;
$r = 2$;
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;
$r = 2$;
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;
    $r \to r + 1$;
$\}$
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;
    $r \rightarrow r + 1$; Note that, after the while loop, $r = n$ is possible.
$\}$
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;
    $r \rightarrow r + 1$;
$\}$
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, after the while loop, $r = n$ is possible. Then n is prime, and the algorithm indicates it is.

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

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

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;
$r = 2$;
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;

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;
$r = 2$;
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;
```

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

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;

    $r \rightarrow r + 1$;   **Problem :** What's up with that?

$\}$

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;

SITUATION:

n is composite, $\quad$ r is a prime

SITUATION:

n is composite, r is a prime

q is a prime, $q \geq 4\sqrt{r}\log n$

SITUATION:

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

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

$$q|(r-1), \quad q|\mathrm{ord}_r(n)$$

SITUATION:

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

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

$$q|(r-1), \quad q|\mathrm{ord}_r(n)$$

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

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

SITUATION:

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

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

$$q|(r-1), \quad q|\text{ord}_r(n)$$

WANT: There is an integer a with $1 \leq a \leq \underbrace{2\sqrt{r}\log n}_{\ell}$ such that

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

SITUATION:

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

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

$$q|(r-1), \quad q|\text{ord}_r(n)$$

WANT: There is an integer a with $1 \leq a \leq \underbrace{2\sqrt{r}\log n}_{\ell}$ such that

$$(x-a)^n \not\equiv (x^n - a) \pmod{x^r - 1, \underbrace{n}_{p \text{ with } p|n}}.$$

SITUATION:

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

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

$$q|(r-1), \quad q|\mathrm{ord}_r(n)$$

WANT: There is an integer a with $1 \leq a \leq \underbrace{2\sqrt{r}\log n}_{\ell}$ such that

$$(x-a)^n \not\equiv (x^n - a) \pmod{\underbrace{x^r - 1}_{h(x)}, \underbrace{n}_{p}}.$$

$h(x)$ monic, where $h(x)|(x^r - 1) \bmod p$

p with $p|n$

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

$$\Downarrow$$

$$\mathrm{Rem}((x-a)^n-(x^n-a),x^r-1,x) \bmod p = 0$$

$$\Downarrow$$

$$\mathrm{Rem}((x-a)^n-(x^n-a),h(x),x) \bmod p = 0$$

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

$$\Downarrow$$

$$\mathtt{Rem}\left((x-a)^n-(x^n-a),x^r-1,x\right)\ \mathtt{mod}\ \mathtt{p} = 0$$

$$\Downarrow\ ?$$

$$\mathtt{Rem}\left((x-a)^n-(x^n-a),h(x),x\right)\ \mathtt{mod}\ \mathtt{p} = 0$$

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

$$\Downarrow$$

$$\mathtt{Rem}((x-a)^n-(x^n-a),x^r-1,x) \bmod p = 0$$

$$\Downarrow$$

$$\mathtt{Rem}((x-a)^n-(x^n-a),h(x),x) \bmod p = 0$$

$$(x-a)^n-(x^n-a)=(x^r-1)Q(x)+R(x)$$

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

$$\Downarrow$$

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

$$\Downarrow$$

$$\mathtt{Rem}((x-a)^n-(x^n-a), h(x), x) \ \mathtt{mod}\ p = 0$$

$$\begin{aligned}(x-a)^n-(x^n-a) &= (x^r-1)Q(x)+R(x)\\ &= h(x)u(x)Q(x)+pv(x)Q(x)+R(x)\end{aligned}$$

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

$$\Downarrow$$

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

$$\Downarrow$$

$$\texttt{Rem}((\mathtt{x}-\mathtt{a})^{\mathtt{n}}-(\mathtt{x}^{\mathtt{n}}-\mathtt{a}),\mathtt{h}(\mathtt{x}),\mathtt{x})\ \texttt{mod p = 0}$$

$$\begin{aligned}(x-a)^n-(x^n-a) &= (x^r-1)Q(x)+R(x)\\ &= h(x)u(x)Q(x)+pv(x)Q(x)+R(x)\\ &= h(x)w(x)+R(x)+pR_0(x)\end{aligned}$$

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

$$\Downarrow$$

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

$$\Downarrow$$

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

$$\begin{aligned}(x-a)^n-(x^n-a) &= (x^r-1)Q(x)+R(x)\\ &= h(x)u(x)Q(x)+pv(x)Q(x)+R(x)\\ &= h(x)w(x)+R(x)+pR_0(x)\end{aligned}$$

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

$$\Downarrow$$

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

$$\Downarrow \ \checkmark$$

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

$$\begin{aligned}
(x - a)^n - (x^n - a) &= (x^r - 1)Q(x) + R(x) \\
&= h(x)u(x)Q(x) + pv(x)Q(x) + R(x) \\
&= h(x)w(x) + R(x) + pR_0(x)
\end{aligned}$$

Situation:

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

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

$$q|(r-1), \quad q|\text{ord}_r(n)$$

Want: There is an integer a with $1 \leq a \leq 2\sqrt{r}\log n$ such that

$$(x-a)^n \not\equiv (x^n - a) \pmod{h(x), p},$$

where p is a prime dividing n and $h(x)$ is a monic factor of $x^r - 1$ modulo p.

SITUATION:

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

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

$$q|(r-1), \quad q|\text{ord}_r(n)$$

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

$$(x-a)^n \not\equiv \left(x^n - a\right) \pmod{h(x), p},$$

where p is a prime dividing n and $h(x)$ is a monic factor of $x^r - 1$ modulo p (both of our choosing).

SITUATION:

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

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

$$q|(r-1), \quad q|\mathrm{ord}_r(n)$$

HOW TO CHOOSE p:

SITUATION:

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

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

$$q|(r-1), \quad q|\text{ord}_r(n)$$

HOW TO CHOOSE p: If $n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$, then

SITUATION:

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

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

$$q|(r-1), \quad q|\mathrm{ord}_r(n)$$

HOW TO CHOOSE p: If $n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}$, then

$$d = \mathrm{ord}_r(p_1) \cdots \mathrm{ord}_r(p_t) \implies n^d \equiv 1 \pmod{r}.$$

SITUATION:

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

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

$$q|(r-1), \quad q|\mathrm{ord}_r(n)$$

HOW TO CHOOSE p: If $n = p_1^{e_1}p_2^{e_2}\cdots p_t^{e_t}$, then

$$d = \mathrm{ord}_r(p_1)\cdots\mathrm{ord}_r(p_t) \implies n^d \equiv 1 \pmod{r}.$$

We deduce $q|d$.

SITUATION:

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

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

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

HOW TO CHOOSE $\boldsymbol{p}$: If $\boldsymbol{n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t}}$, then

$$\boldsymbol{d} = \mathrm{ord}_{\boldsymbol{r}}(\boldsymbol{p_1}) \cdots \mathrm{ord}_{\boldsymbol{r}}(\boldsymbol{p_t}) \implies \boldsymbol{n^d \equiv 1 \pmod{r}}.$$

We deduce $\boldsymbol{q|d}$. Fix $\boldsymbol{p}$ such that

$$\boldsymbol{p|n} \quad \text{and} \quad \boldsymbol{q} | \mathrm{ord}_{\boldsymbol{r}}(\boldsymbol{p}).$$

SITUATION:

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

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

$$q|(r-1), \quad p|n, \quad q|\mathrm{ord}_r(p)$$

SITUATION:

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

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

$$q|(r-1), \quad p|n, \quad q|\mathrm{ord}_r(p)$$

How do we choose $h(x)$?

The Factorization of Cyclotomic Polynomials Modulo a Prime

The Factorization of Cyclotomic Polynomials Modulo a Prime

Let r be a positive integer, and let p be a prime. Write $r = p^k m$ where $p \nmid m$. Let $f = \text{ord}_m(p)$. Then the r^{th} cyclotomic polynomial $\Phi_r(x)$ factors as a product of $\phi(m)/f$ incongruent irreducible polynomials modulo p of degree f each raised to the $\phi(p^k)$ power.

The Factorization of Cyclotomic Polynomials Modulo a Prime

Let r be a positive integer, and let p be a prime. Write $r = p^k m$ where $p \nmid m$. Let $f = \text{ord}_m(p)$. Then the r^{th} cyclotomic polynomial $\Phi_r(x)$ factors as a product of $\phi(m)/f$ incongruent irreducible polynomials modulo p of degree f each raised to the $\phi(p^k)$ power.

The Factorization of Cyclotomic Polynomials Modulo a Prime

Let r be a positive integer, and let p be a prime. Write $r = p^k m$ where $p \nmid m$. Let $f = \text{ord}_m(p)$. Then the r^{th} cyclotomic polynomial $\Phi_r(x)$ factors as a product of $\phi(m)/f$ incongruent irreducible polynomials modulo p of degree f each raised to the $\phi(p^k)$ power.

r prime,

The Factorization of Cyclotomic Polynomials Modulo a Prime

Let r be a positive integer, and let p be a prime. Write $r = p^k m$ where $p \nmid m$. Let $f = \text{ord}_m(p)$. Then the r^{th} cyclotomic polynomial $\Phi_r(x)$ factors as a product of $\phi(m)/f$ incongruent irreducible polynomials modulo p of degree f each raised to the $\phi(p^k)$ power.

r prime, $k = 0$,

The Factorization of Cyclotomic Polynomials Modulo a Prime

Let r be a positive integer, and let p be a prime. Write $r = p^k m$ where $p \nmid m$. Let $f = \text{ord}_m(p)$. Then the r^{th} cyclotomic polynomial $\Phi_r(x)$ factors as a product of $\phi(m)/f$ incongruent irreducible polynomials modulo p of degree f each raised to the $\phi(p^k)$ power.

r prime, $\;k = 0,\;\; m = r,$

The Factorization of Cyclotomic Polynomials Modulo a Prime

Let r be a positive integer, and let p be a prime. Write $r = p^k m$ where $p \nmid m$. Let $f = \text{ord}_m(p)$. Then the r^{th} cyclotomic polynomial $\Phi_r(x)$ factors as a product of $\phi(m)/f$ incongruent irreducible polynomials modulo p of degree f each raised to the $\phi(p^k)$ power.

$$r \text{ prime}, \quad k = 0, \quad m = r, \quad \Phi_r(x) = \frac{x^r - 1}{x - 1}$$

The Factorization of Cyclotomic Polynomials Modulo a Prime

Let r be a positive integer, and let p be a prime. Write $r = p^k m$ where $p \nmid m$. Let $f = \mathrm{ord}_m(p)$. Then the r^{th} cyclotomic polynomial $\Phi_r(x)$ factors as a product of $\phi(m)/f$ incongruent irreducible polynomials modulo p of degree f each raised to the $\phi(p^k)$ power.

$x^r - 1$ has a factor of degree $\mathrm{ord}_r(p)$ modulo p

The Factorization of Cyclotomic Polynomials Modulo a Prime

Let r be a positive integer, and let p be a prime. Write $r = p^k m$ where $p \nmid m$. Let $f = \text{ord}_m(p)$. Then the r^{th} cyclotomic polynomial $\Phi_r(x)$ factors as a product of $\phi(m)/f$ incongruent irreducible polynomials modulo p of degree f each raised to the $\phi(p^k)$ power.

$h(x)$

$x^r - 1$ has a factor of degree $\text{ord}_r(p)$ modulo p

SITUATION:

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

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

$$q|(r-1), \quad p|n, \quad q|\mathrm{ord}_r(p)$$

$$h(x) \text{ irreducible mod } p, \quad \deg h = \mathrm{ord}_r(p)$$

SITUATION:

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

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

$$q|(r-1), \quad p|n, \quad q|\mathrm{ord}_r(p)$$

$$h(x) \text{ irreducible mod } p, \quad \deg h = \mathrm{ord}_r(p)$$

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

$$(x-a)^n \not\equiv (x^n - a) \pmod{h(x), p}.$$

SITUATION:

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

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

$$q|(r-1), \quad p|n, \quad q|\mathrm{ord}_r(p)$$

$$h(x) \text{ irreducible mod } p, \quad \deg h = \mathrm{ord}_r(p)$$

WANT: There is an integer a with $1 \leq a \leq \underbrace{2\sqrt{r}\log n}_{\ell}$ such that

$$(x-a)^n \not\equiv (x^n - a) \pmod{h(x), p}.$$

SITUATION:

$$n \text{ is composite,} \quad r \text{ is a prime,} \quad \ell = 2\sqrt{r}\log n$$

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

$$q|(r-1), \quad p|n, \quad q|\text{ord}_r(p)$$

$$h(x) \text{ irreducible mod } p, \quad \deg h = \text{ord}_r(p)$$

WANT: There is an integer a with $1 \leq a \leq \ell$ such that

$$(x-a)^n \not\equiv x^n - a \pmod{h(x), p}.$$

SITUATION:

$$n \text{ is composite,} \quad r \text{ is a prime,} \quad \ell = 2\sqrt{r}\log n$$

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

$$q|(r-1), \quad p|n, \quad q|\text{ord}_r(p)$$

$$h(x) \text{ irreducible mod } p, \quad \deg h = \text{ord}_r(p) \geq 2\ell$$

WANT: There is an integer a with $1 \leq a \leq \ell$ such that

$$(x-a)^n \not\equiv \; x^n - a \pmod{h(x), p}.$$

SITUATION:

$$n \text{ is composite}, \quad r \text{ is a prime}, \quad \ell = 2\sqrt{r}\log n$$

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

$$q|(r-1), \quad p|n, \quad q|\mathrm{ord}_r(p)$$

$$h(x) \text{ irreducible mod } p, \quad \deg h = \mathrm{ord}_r(p) \geq 2\ell$$

Not really, but it sounds good.

WANT: There is an integer a with $1 \leq a \leq \ell$ such that

$$(x-a)^n \not\equiv x^n - a \pmod{h(x), p}.$$

Arithmetic Modulo $h(x)$, p

ARITHMETIC MODULO $h(x), p$

Well-Known: Arithmetic modulo $h(x), p$ forms a field F with $p^{\deg h}$ elements which can be represented by the polynomials of degree $< \deg h$ with coefficients from $\{0, 1, \ldots, p-1\}$.

ARITHMETIC MODULO $h(x), p$

Well-Known: Arithmetic modulo $h(x), p$ forms a field F with $p^{\deg h}$ elements which can be represented by the polynomials of degree $< \deg h$ with coefficients from $\{0, 1, \ldots, p-1\}$. As with any finite field, the non-zero elements form a cyclic group under multiplication.

ARITHMETIC MODULO $h(x), p$

Well-Known: Arithmetic modulo $h(x), p$ forms a field F with $p^{\deg h}$ elements which can be represented by the polynomials of degree $< \deg h$ with coefficients from $\{0, 1, \ldots, p-1\}$. As with any finite field, the non-zero elements form a cyclic group under multiplication.

Main Lemma: The set

$$G = \{(x-1)^{e_1}(x-2)^{e_2} \cdots (x-\ell)^{e_\ell} : e_j \geq 0\}$$

forms a subgroup of the multiplicative group of non-zero elements of F (which necessarily is cyclic).

Arithmetic Modulo $h(x), p$

Well-Known: Arithmetic modulo $h(x), p$ forms a field F with $p^{\deg h}$ elements which can be represented by the polynomials of degree $< \deg h$ with coefficients from $\{0, 1, \ldots, p-1\}$. As with any finite field, the non-zero elements form a cyclic group under multiplication.

Main Lemma: The set

$$G = \{(x-1)^{e_1}(x-2)^{e_2} \cdots (x-\ell)^{e_\ell} : e_j \geq 0\}$$

forms a subgroup of the multiplicative group of non-zero elements of F (which necessarily is cyclic) of size $> 2^\ell$

ARITHMETIC MODULO $h(x), p$

Well-Known: Arithmetic modulo $h(x), p$ forms a field F with $p^{\deg h}$ elements which can be represented by the polynomials of degree $< \deg h$ with coefficients from $\{0, 1, \ldots, p-1\}$. As with any finite field, the non-zero elements form a cyclic group under multiplication.

Main Lemma: The set

$$G = \{(x-1)^{e_1}(x-2)^{e_2} \cdots (x-\ell)^{e_\ell} : e_j \geq 0\}$$

forms a subgroup of the multiplicative group of non-zero elements of F (which necessarily is cyclic) of size $> 2^\ell = 2^{2\sqrt{r}\log n}$

Arithmetic Modulo $h(x), p$

Well-Known: Arithmetic modulo $h(x), p$ forms a field F with $p^{\deg h}$ elements which can be represented by the polynomials of degree $< \deg h$ with coefficients from $\{0, 1, \ldots, p-1\}$. As with any finite field, the non-zero elements form a cyclic group under multiplication.

Main Lemma: The set

$$G = \{(x-1)^{e_1}(x-2)^{e_2} \cdots (x-\ell)^{e_\ell} : e_j \geq 0\}$$

forms a subgroup of the multiplicative group of non-zero elements of F (which necessarily is cyclic) of size $> 2^\ell = 2^{2\sqrt{r}\log n} = n^{2\sqrt{r}}$.

Main Lemma: The set

$$G = \{(x-1)^{e_1}(x-2)^{e_2}\cdots(x-\ell)^{e_\ell} : e_j \geq 0\}$$

forms a subgroup of the multiplicative group of non-zero elements of F (which necessarily is cyclic) of size $> 2^\ell = 2^{2\sqrt{r}\log n} = n^{2\sqrt{r}}$.

Main Lemma: The set

$$G = \{(x-1)^{e_1}(x-2)^{e_2} \cdots (x-\ell)^{e_\ell} : e_j \geq 0\}$$

forms a subgroup of the multiplicative group of non-zero elements of F (which necessarily is cyclic) of size $> 2^\ell = 2^{2\sqrt{r}\log n} = n^{2\sqrt{r}}$.

We explain why this main lemma gives us what we want

Main Lemma: The set

$$G = \{(x-1)^{e_1}(x-2)^{e_2}\cdots(x-\ell)^{e_\ell} : e_j \geq 0\}$$

forms a subgroup of the multiplicative group of non-zero elements of F (which necessarily is cyclic) of size $> 2^\ell = 2^{2\sqrt{r}\log n} = n^{2\sqrt{r}}$.

We explain why this main lemma gives us what we want and then discuss why it is true.

Notation:

Notation: Since G is cyclic, there is an element

$$g(x) = (x-1)^{e_1}(x-2)^{e_2}\cdots(x-\ell)^{e_\ell}$$

in G (and, hence, in F) of order $|G| > n^{2\sqrt{r}}$.

Notation: Since G is cyclic, there is an element

$$g(x) = (x-1)^{e_1}(x-2)^{e_2} \cdots (x-\ell)^{e_\ell}$$

in G (and, hence, in F) of order $|G| > n^{2\sqrt{r}}$. Define

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r-1, p}\}.$$

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

PROPERTIES OF $I_{g(x)}$:

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

Properties of $I_{g(x)}$:

- $m_1, m_2 \in I_{g(x)} \implies m_1 m_2 \in I_{g(x)}$

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

PROPERTIES OF $I_{g(x)}$:

- $m_1, m_2 \in I_{g(x)} \implies m_1 m_2 \in I_{g(x)}$

$$g(x)^{m_2} \equiv g(x^{m_2}) \pmod{x^r - 1, p}$$

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

PROPERTIES OF $I_{g(x)}$:

- $m_1, m_2 \in I_{g(x)} \implies m_1 m_2 \in I_{g(x)}$

$$g(x)^{m_2} \equiv g(x^{m_2}) \pmod{x^r - 1, p}$$

$$\implies g(x^{m_1})^{m_2} \equiv g(x^{m_1 m_2}) \pmod{x^{m_1 r} - 1, p}$$

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

PROPERTIES OF $I_{g(x)}$:

- $m_1, m_2 \in I_{g(x)} \implies m_1 m_2 \in I_{g(x)}$

$$g(x)^{m_2} \equiv g(x^{m_2}) \pmod{x^r - 1, p}$$

$$\implies g(x^{m_1})^{m_2} \equiv g(x^{m_1 m_2}) \pmod{x^{m_1 r} - 1, p}$$

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

Properties of $I_{g(x)}$:

- $m_1, m_2 \in I_{g(x)} \implies m_1 m_2 \in I_{g(x)}$

$$g(x)^{m_2} \equiv g(x^{m_2}) \pmod{x^r - 1, p}$$

$$\implies g(x^{m_1})^{m_2} \equiv g(x^{m_1 m_2}) \pmod{x^r \quad - 1, p}$$

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

PROPERTIES OF $I_{g(x)}$:

- $m_1, m_2 \in I_{g(x)} \implies m_1 m_2 \in I_{g(x)}$

$$g(x)^{m_2} \equiv g(x^{m_2}) \pmod{x^r - 1, p}$$

$$\implies g(x^{m_1})^{m_2} \equiv g(x^{m_1 m_2}) \pmod{x^r - 1, p}$$

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

Properties of $I_{g(x)}$:

- $m_1, m_2 \in I_{g(x)} \implies m_1 m_2 \in I_{g(x)}$

$$g(x)^{m_2} \equiv g(x^{m_2}) \pmod{x^r - 1, p}$$

$$\implies g(x^{m_1})^{m_2} \equiv g(x^{m_1 m_2}) \pmod{x^r - 1, p}$$

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

Properties of $I_{g(x)}$:

- $m_1, m_2 \in I_{g(x)} \implies m_1 m_2 \in I_{g(x)}$

$$g(x)^{m_2} \equiv g(x^{m_2}) \pmod{x^r - 1, p}$$

$$\implies g(x^{m_1})^{m_2} \equiv g(x^{m_1 m_2}) \pmod{x^r - 1, p}$$

$$g(x^{m_1}) \equiv g(x)^{m_1} \pmod{x^r - 1, p}$$

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

PROPERTIES OF $I_{g(x)}$:

- $m_1, m_2 \in I_{g(x)} \implies m_1 m_2 \in I_{g(x)}$

$$g(x)^{m_2} \equiv g(x^{m_2}) \pmod{x^r - 1, p}$$

$$\implies g(x^{m_1})^{m_2} \equiv g(x^{m_1 m_2}) \pmod{x^r - 1, p}$$

$$g(x^{m_1}) \equiv g(x)^{m_1} \pmod{x^r - 1, p}$$

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

Properties of $I_{g(x)}$:

- $m_1, m_2 \in I_{g(x)} \implies m_1 m_2 \in I_{g(x)}$

$$g(x)^{m_2} \equiv g(x^{m_2}) \pmod{x^r - 1, p}$$

$$\implies g(x)^{m_1 m_2} \equiv g(x^{m_1 m_2}) \pmod{x^r - 1, p}$$

$$g(x^{m_1}) \equiv g(x)^{m_1} \pmod{x^r - 1, p}$$

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

Properties of $I_{g(x)}$:

- $m_1, m_2 \in I_{g(x)} \implies m_1 m_2 \in I_{g(x)}$

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

PROPERTIES OF $I_{g(x)}$:

- $m_1, m_2 \in I_{g(x)} \implies m_1 m_2 \in I_{g(x)}$
- $m_1, m_2 \in I_{g(x)}$ and $m_1 \equiv m_2 \pmod{r}$

  $\Longrightarrow m_1 \equiv m_2 \pmod{d}$ where $d =$ order of $g(x)$

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

PROPERTIES OF $I_{g(x)}$:

- $m_1, m_2 \in I_{g(x)} \implies m_1 m_2 \in I_{g(x)}$
- $m_1, m_2 \in I_{g(x)}$ and $m_1 \equiv m_2 \pmod{r}$

  $\implies m_1 \equiv m_2 \pmod{d}$ where d = order of $g(x)$

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

Properties of $I_{g(x)}$:

- $m_1, m_2 \in I_{g(x)} \implies m_1 m_2 \in I_{g(x)}$
- $m_1, m_2 \in I_{g(x)}$ and $m_1 \equiv m_2 \pmod{r}$
  $\implies m_1 \equiv m_2 \pmod{d}$ where d = order of $g(x)$

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

PROPERTIES OF $I_{g(x)}$:

- $m_1, m_2 \in I_{g(x)} \implies m_1 m_2 \in I_{g(x)}$
- $m_1, m_2 \in I_{g(x)}$ and $m_1 \equiv m_2 \pmod{r}$

  $\implies m_1 \equiv m_2 \pmod{d}$ where $d =$ order of $g(x)$

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

Properties of $I_{g(x)}$:

- $m_1, m_2 \in I_{g(x)} \implies m_1 m_2 \in I_{g(x)}$
- $m_1, m_2 \in I_{g(x)}$ and $m_1 \equiv m_2 \pmod{r}$

  $\implies m_1 \equiv m_2 \pmod{d}$ where $d =$ order of $g(x)$

$$x^{m_2 j} - x^{m_1 j} = x^{m_1 j}\left(x^{(m_2 - m_1) j} - 1\right)$$

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

Properties of $I_{g(x)}$:

- $m_1, m_2 \in I_{g(x)} \implies m_1 m_2 \in I_{g(x)}$
- $m_1, m_2 \in I_{g(x)}$ and $m_1 \equiv m_2 \pmod{r}$

  $\implies m_1 \equiv m_2 \pmod{d}$ where $d =$ order of $g(x)$

$$x^{m_2 j} - x^{m_1 j} = x^{m_1 j}\left(x^{(m_2 - m_1)j} - 1\right)$$

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

Properties of $I_{g(x)}$:

- $m_1, m_2 \in I_{g(x)} \implies m_1 m_2 \in I_{g(x)}$
- $m_1, m_2 \in I_{g(x)}$ and $m_1 \equiv m_2 \pmod{r}$
  $\implies m_1 \equiv m_2 \pmod{d}$ where $d =$ order of $g(x)$

$$\begin{aligned} x^{m_2 j} - x^{m_1 j} &= x^{m_1 j}\left(x^{(m_2 - m_1)j} - 1\right) \\ &= x^{m_1 j}\left(x^r - 1\right)\left(\cdots\right) \end{aligned}$$

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

PROPERTIES OF $I_{g(x)}$:

- $m_1, m_2 \in I_{g(x)} \implies m_1 m_2 \in I_{g(x)}$
- $m_1, m_2 \in I_{g(x)}$ and $m_1 \equiv m_2 \pmod{r}$
  $\implies m_1 \equiv m_2 \pmod{d}$ where $d =$ order of $g(x)$

$$\begin{aligned} x^{m_2 j} - x^{m_1 j} &= x^{m_1 j}\left(x^{(m_2 - m_1)j} - 1\right) \\ &= x^{m_1 j}\left(x^r - 1\right)\left(\cdots\right) \end{aligned}$$

$$\implies \quad x^{m_2 j} \equiv x^{m_1 j} \pmod{x^r - 1, p}$$

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

PROPERTIES OF $I_{g(x)}$:

- $m_1, m_2 \in I_{g(x)} \implies m_1 m_2 \in I_{g(x)}$
- $m_1, m_2 \in I_{g(x)}$ and $m_1 \equiv m_2 \pmod{r}$

  $\implies m_1 \equiv m_2 \pmod{d}$ where $d =$ order of $g(x)$

$$\begin{aligned} x^{m_2 j} - x^{m_1 j} &= x^{m_1 j}\left(x^{(m_2 - m_1)j} - 1\right) \\ &= x^{m_1 j}\left(x^r - 1\right)\left(\cdots\right) \end{aligned}$$

$$\begin{aligned} \implies \quad & x^{m_2 j} \equiv x^{m_1 j} \pmod{x^r - 1, p} \\ \implies \quad & g(x^{m_2}) \equiv g(x^{m_1}) \pmod{x^r - 1, p} \end{aligned}$$

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

PROPERTIES OF $I_{g(x)}$:

- $m_1, m_2 \in I_{g(x)} \implies m_1 m_2 \in I_{g(x)}$
- $m_1, m_2 \in I_{g(x)}$ and $m_1 \equiv m_2 \pmod{r}$

  $\implies m_1 \equiv m_2 \pmod{d}$ where $d =$ order of $g(x)$

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

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

PROPERTIES OF $I_{g(x)}$:

- $m_1, m_2 \in I_{g(x)} \implies m_1 m_2 \in I_{g(x)}$
- $m_1, m_2 \in I_{g(x)}$ and $m_1 \equiv m_2 \pmod{r}$

  $\implies m_1 \equiv m_2 \pmod{d}$ where $d =$ order of $g(x)$

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

$$\implies g(x)^{m_2} \equiv g(x)^{m_1} \pmod{x^r - 1, p}$$

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

PROPERTIES OF $I_{g(x)}$:

- $m_1, m_2 \in I_{g(x)} \implies m_1 m_2 \in I_{g(x)}$
- $m_1, m_2 \in I_{g(x)}$ and $m_1 \equiv m_2 \pmod{r}$

  $\implies m_1 \equiv m_2 \pmod{d}$ where $d =$ order of $g(x)$

$$\begin{aligned} g(x^{m_2}) \equiv g(x^{m_1}) &\pmod{x^r - 1, p} \\ \implies g(x)^{m_2} \equiv g(x)^{m_1} &\pmod{x^r - 1, p} \\ \implies g(x)^{m_2 - m_1} \equiv 1 &\pmod{x^r - 1, p} \end{aligned}$$

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

Properties of $I_{g(x)}$:

- $m_1, m_2 \in I_{g(x)} \implies m_1 m_2 \in I_{g(x)}$
- $m_1, m_2 \in I_{g(x)}$ and $m_1 \equiv m_2 \pmod{r}$

  $\implies m_1 \equiv m_2 \pmod{d}$ where $d =$ order of $g(x)$

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

$$\implies g(x)^{m_2} \equiv g(x)^{m_1} \pmod{x^r - 1, p}$$

$$\implies g(x)^{m_2 - m_1} \equiv 1 \pmod{x^r - 1, p}$$

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

PROPERTIES OF $I_{g(x)}$:

- $m_1, m_2 \in I_{g(x)} \implies m_1 m_2 \in I_{g(x)}$
- $m_1, m_2 \in I_{g(x)}$ and $m_1 \equiv m_2 \pmod{r}$

  $\implies m_1 \equiv m_2 \pmod{d}$ where $d =$ order of $g(x)$

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

PROPERTIES OF $I_{g(x)}$:

- $m_1, m_2 \in I_{g(x)} \implies m_1 m_2 \in I_{g(x)}$
- $m_1, m_2 \in I_{g(x)}$ and $m_1 \equiv m_2 \pmod{r}$

  $\implies m_1 \equiv m_2 \pmod{d}$ where $d =$ order of $g(x)$

MORAL:

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

PROPERTIES OF $I_{g(x)}$:

- $m_1, m_2 \in I_{g(x)} \implies m_1 m_2 \in I_{g(x)}$
- $m_1, m_2 \in I_{g(x)}$ and $m_1 \equiv m_2 \pmod{r}$

  $\implies m_1 \equiv m_2 \pmod{d}$ where $d =$ order of $g(x)$

MORAL: There are $\leq r$ positive integers $\leq d$ in $I_{g(x)}$.

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

Moral: There are $\leq r$ positive integers $\leq d$ in $I_{g(x)}$.

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

Moral: There are $\leq r$ positive integers $\leq d$ in $I_{g(x)}$.

Want: There is an integer a with $1 \leq a \leq \ell$ such that

$$(x-a)^n \not\equiv \left(x^n - a\right) \pmod{h(x)\ \ , p}.$$

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

MORAL: There are $\leq r$ positive integers $\leq d$ in $I_{g(x)}$.

WANT: There is an integer a with $1 \leq a \leq \ell$ such that

$$(x - a)^n \not\equiv \left(x^n - a\right) \pmod{x^r - 1, p}.$$

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

Moral: There are $\leq r$ positive integers $\leq d$ in $I_{g(x)}$.

Want: There is an integer a with $1 \leq a \leq \ell$ such that

$$(x - a)^n \not\equiv \left(x^n - a\right) \pmod{x^r - 1, p}.$$

Assume otherwise.

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

Moral: There are $\leq r$ positive integers $\leq d$ in $I_{g(x)}$.

Want: There is an integer a with $1 \leq a \leq \ell$ such that

$$(x - a)^n \not\equiv \left(x^n - a\right) \pmod{x^r - 1, p}.$$

Assume otherwise. Then, for all $a \in \{1, 2, \ldots, \ell\}$,

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

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

Moral: There are $\leq r$ positive integers $\leq d$ in $I_{g(x)}$.

Want: There is an integer a with $1 \leq a \leq \ell$ such that

$$(x - a)^n \not\equiv \left(x^n - a\right) \pmod{x^r - 1, p}.$$

Assume otherwise. Then, for all $a \in \{1, 2, \ldots, \ell\}$,

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

$$g(x) = (x - 1)^{e_1}(x - 2)^{e_2} \cdots (x - \ell)^{e_\ell}$$

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

Moral: There are $\leq r$ positive integers $\leq d$ in $I_{g(x)}$.

Want: There is an integer a with $1 \leq a \leq \ell$ such that

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

Assume otherwise. Then, for all $a \in \{1, 2, \ldots, \ell\}$,

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

$$g(x) = (x-1)^{e_1}(x-2)^{e_2} \cdots (x-\ell)^{e_\ell}$$
$$\implies g(x)^n \equiv g(x^n) \pmod{x^r - 1, p}$$

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

Moral: There are $\leq r$ positive integers $\leq d$ in $I_{g(x)}$.

Want: There is an integer a with $1 \leq a \leq \ell$ such that

$$(x-a)^n \not\equiv \left(x^n - a\right) \pmod{x^r - 1, p}.$$

Assume otherwise. Then, for all $a \in \{1, 2, \ldots, \ell\}$,

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

$$g(x) = (x-1)^{e_1}(x-2)^{e_2} \cdots (x-\ell)^{e_\ell}$$

$$\Longrightarrow g(x)^n \equiv g(x^n) \pmod{x^r - 1, p}$$

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

Moral: There are $\leq r$ positive integers $\leq d$ in $I_{g(x)}$.

$$n \in I_{g(x)}$$

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

Moral: There are $\leq r$ positive integers $\leq d$ in $I_{g(x)}$.

$$n \in I_{g(x)}$$

$$g(x)^p \equiv g(x^p) \pmod{p}$$

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

Moral: There are $\leq r$ positive integers $\leq d$ in $I_{g(x)}$.

$$n \in I_{g(x)}$$

$$g(x)^p \equiv g(x^p) \pmod{x^r - 1, p}$$

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

Moral: There are $\leq r$ positive integers $\leq d$ in $I_{g(x)}$.

$$n \in I_{g(x)}$$

$$g(x)^p \equiv g(x^p) \pmod{x^r - 1, p}$$

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

Moral: There are $\leq r$ positive integers $\leq d$ in $I_{g(x)}$.

$$n \in I_{g(x)}, \quad p \in I_{g(x)}$$

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

Moral: There are $\leq r$ positive integers $\leq d$ in $I_{g(x)}$.

$$n \in I_{g(x)}, \quad p \in I_{g(x)}$$

$$n^i p^j \in I_{g(x)} \quad \text{for } 0 \leq i, j \leq [\sqrt{r}]$$

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

MORAL: There are $\leq r$ positive integers $\leq d$ in $I_{g(x)}$.

$$n \in I_{g(x)}, \quad p \in I_{g(x)}$$

$$n^i p^j \in I_{g(x)} \quad \text{for } 0 \leq i, j \leq [\sqrt{r}]$$

$$1 \leq n^i p^j$$

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

Moral: There are $\leq r$ positive integers $\leq d$ in $I_{g(x)}$.

$$n \in I_{g(x)}, \quad p \in I_{g(x)}$$

$$n^i p^j \in I_{g(x)} \quad \text{for } 0 \leq i, j \leq [\sqrt{r}]$$

$$1 \leq n^i p^j \leq n^{i+j}$$

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

Moral: There are $\leq r$ positive integers $\leq d$ in $I_{g(x)}$.

$$n \in I_{g(x)}, \quad p \in I_{g(x)}$$

$$n^i p^j \in I_{g(x)} \quad \text{for } 0 \leq i, j \leq [\sqrt{r}]$$

$$1 \leq n^i p^j \leq n^{i+j} \leq n^{2\sqrt{r}}$$

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

Moral: There are $\leq r$ positive integers $\leq d$ in $I_{g(x)}$.

$$n \in I_{g(x)}, \quad p \in I_{g(x)}$$

$$n^i p^j \in I_{g(x)} \quad \text{for } 0 \leq i, j \leq [\sqrt{r}]$$

$$1 \leq n^i p^j \leq n^{i+j} \leq n^{2\sqrt{r}} \leq d$$

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

MORAL: There are $\leq r$ positive integers $\leq d$ in $I_{g(x)}$.

$$n \in I_{g(x)}, \quad p \in I_{g(x)}$$

$$n^i p^j \in I_{g(x)} \quad \text{for } 0 \leq i, j \leq [\sqrt{r}]$$

$$1 \leq n^i p^j \leq n^{i+j} \leq n^{2\sqrt{r}} \leq d$$

$$n^{i_1} p^{j_1} = n^{i_2} p^{j_2}$$

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

Moral: There are $\leq r$ positive integers $\leq d$ in $I_{g(x)}$.

$$n \in I_{g(x)}, \quad p \in I_{g(x)}$$

$$n^i p^j \in I_{g(x)} \quad \text{for } 0 \leq i, j \leq [\sqrt{r}]$$

$$1 \leq n^i p^j \leq n^{i+j} \leq n^{2\sqrt{r}} \leq d$$

$$n^{i_1} p^{j_1} = n^{i_2} p^{j_2} \implies n = p^k$$

$$I_{g(x)} = \{m : g(x)^m \equiv g(x^m) \pmod{x^r - 1, p}\}$$

MORAL: There are $\leq r$ positive integers $\leq d$ in $I_{g(x)}$.

$$n \in I_{g(x)}, \quad p \in I_{g(x)}$$

$$n^i p^j \in I_{g(x)} \quad \text{for } 0 \leq i, j \leq [\sqrt{r}]$$

$$1 \leq n^i p^j \leq n^{i+j} \leq n^{2\sqrt{r}} \leq d$$

$$n^{i_1} p^{j_1} = n^{i_2} p^{j_2} \implies n = p^k$$

It remains to justify the ...

Main Lemma: The set

$$G = \{(x-1)^{e_1}(x-2)^{e_2}\cdots(x-\ell)^{e_\ell} : e_j \geq 0\}$$

forms a subgroup of the multiplicative group of non-zero elements of F (which necessarily is cyclic) of size $> 2^\ell = 2^{2\sqrt{r}\log n} = n^{2\sqrt{r}}$.

Main Lemma: The set

$$G = \{(x-1)^{e_1}(x-2)^{e_2} \cdots (x-\ell)^{e_\ell} : e_j \geq 0\}$$

forms a subgroup of the multiplicative group of non-zero elements of F (which necessarily is cyclic) of size $> 2^\ell = 2^{2\sqrt{r}\log n} = n^{2\sqrt{r}}$.

F is the field of p^d elements

Main Lemma: The set

$$G = \{(x-1)^{e_1}(x-2)^{e_2}\cdots(x-\ell)^{e_\ell} : e_j \geq 0\}$$

forms a subgroup of the multiplicative group of non-zero elements of F (which necessarily is cyclic) of size $> 2^\ell = 2^{2\sqrt{r}\log n} = n^{2\sqrt{r}}$.

Change in Notation

F is the field of p^d elements

Main Lemma: The set

$$G = \{(x-1)^{e_1}(x-2)^{e_2}\cdots(x-\ell)^{e_\ell} : e_j \geq 0\}$$

forms a subgroup of the multiplicative group of non-zero elements of F (which necessarily is cyclic) of size $> 2^\ell = 2^{2\sqrt{r}\log n} = n^{2\sqrt{r}}$.

F is the field of p^d elements

which we represent using arithmetic mod $h(x), p$

Main Lemma: The set

$$G = \{(x-1)^{e_1}(x-2)^{e_2}\cdots(x-\ell)^{e_\ell} : e_j \geq 0\}$$

forms a subgroup of the multiplicative group of non-zero elements of F (which necessarily is cyclic) of size $> 2^\ell = 2^{2\sqrt{r}\log n} = n^{2\sqrt{r}}$.

F is the field of p^d elements

which we represent using arithmetic mod $h(x), p$

where $h(x)$ is monic, of degree d, and irreducible mod p

Main Lemma: The set

$$G = \{(x-1)^{e_1}(x-2)^{e_2}\cdots(x-\ell)^{e_\ell} : e_j \geq 0\}$$

forms a subgroup of the multiplicative group of non-zero elements of F (which necessarily is cyclic) of size $> 2^\ell = 2^{2\sqrt{r}\log n} = n^{2\sqrt{r}}$.

n is composite, $\quad r$ is a prime, $\quad \ell = 2\sqrt{r}\log n$

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

$q|(r-1), \quad p|n, \quad q|\mathrm{ord}_r(p)$

$h(x)$ irreducible mod p, $\quad \deg h = \mathrm{ord}_r(p) \geq 2\ell$

Main Lemma: The set

$$G = \{(x-1)^{e_1}(x-2)^{e_2}\cdots(x-\ell)^{e_\ell} : e_j \geq 0\}$$

forms a subgroup of the multiplicative group of non-zero elements of F (which necessarily is cyclic) of size $> 2^\ell = 2^{2\sqrt{r}\log n} = n^{2\sqrt{r}}$.

$$n \text{ is composite,} \quad r \text{ is a prime,} \quad \ell = 2\sqrt{r}\log n$$

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

$$q|(r-1), \quad p|n, \quad q|\text{ord}_r(p)$$

$$h(x) \text{ irreducible mod } p, \quad \underbrace{\deg h = \text{ord}_r(p) \geq 2\ell}_{d \geq 2\ell}$$

Main Lemma: The set

$$G = \{(x-1)^{e_1}(x-2)^{e_2}\cdots(x-\ell)^{e_\ell} : e_j \geq 0\}$$

forms a subgroup of the multiplicative group of non-zero elements of F (which necessarily is cyclic) of size $> 2^\ell = 2^{2\sqrt{r}\log n} = n^{2\sqrt{r}}$.

$$n \text{ is composite,} \quad r \text{ is a prime,} \quad \ell = 2\sqrt{r}\log n$$

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

$$q|(r-1), \quad p|n, \quad q|\mathrm{ord}_r(p)$$

$$h(x) \text{ irreducible mod } p, \quad \underbrace{\deg h = \mathrm{ord}_r(p) \geq 2\ell}_{d/\ell \geq 2}$$

Main Lemma: The set

$$G = \{(x-1)^{e_1}(x-2)^{e_2}\cdots(x-\ell)^{e_\ell} : e_j \geq 0\}$$

forms a subgroup of the multiplicative group of non-zero elements of F (which necessarily is cyclic) of size $> 2^\ell = 2^{2\sqrt{r}\log n} = n^{2\sqrt{r}}$.

$$n \text{ is composite,} \quad r \text{ is a prime,} \quad \ell = 2\sqrt{r}\log n$$

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

$$q|(r-1), \quad p|n, \quad q|\mathrm{ord}_r(p)$$

$$h(x) \text{ irreducible mod } p, \quad \underbrace{\deg h = \mathrm{ord}_r(p) \geq 2\ell}_{d/\ell \geq 2}$$

Remember Me → $d/\ell \geq 2$

Main Lemma: The set

$$G = \{(x-1)^{e_1}(x-2)^{e_2} \cdots (x-\ell)^{e_\ell} : e_j \geq 0\}$$

forms a subgroup of the multiplicative group of non-zero elements of F (which necessarily is cyclic) of size $> 2^\ell = 2^{2\sqrt{r}\log n} = n^{2\sqrt{r}}$.

n is composite, r is a prime, $\ell = 2\sqrt{r}\log n$

q is a prime, $q \geq 4\sqrt{r}\log n$

$q|(r-1)$, $p|n$, $q|\text{ord}_r(p)$

$h(x)$ irreducible mod p, $\deg h = \text{ord}_r(p) \geq 2\ell$

Main Lemma: The set

$$G = \{(x-1)^{e_1}(x-2)^{e_2}\cdots(x-\ell)^{e_\ell} : e_j \geq 0\}$$

forms a subgroup of the multiplicative group of non-zero elements of F (which necessarily is cyclic) of size $> 2^\ell = 2^{2\sqrt{r}\log n} = n^{2\sqrt{r}}$.

$$q|(r-1), \quad q \geq 4\sqrt{r}\log n, \quad \ell = 2\sqrt{r}\log n$$

Main Lemma: The set

$$G = \{(x-1)^{e_1}(x-2)^{e_2}\cdots(x-\ell)^{e_\ell} : e_j \geq 0\}$$

forms a subgroup of the multiplicative group of non-zero elements of F (which necessarily is cyclic) of size $> 2^\ell = 2^{2\sqrt{r}\log n} = n^{2\sqrt{r}}$.

$$q|(r-1), \quad q \geq 4\sqrt{r}\log n, \quad \ell = 2\sqrt{r}\log n$$

Main Lemma: The set

$$G = \{(x-1)^{e_1}(x-2)^{e_2}\cdots(x-\ell)^{e_\ell} : e_j \geq 0\}$$

forms a subgroup of the multiplicative group of non-zero elements of F (which necessarily is cyclic) of size $> 2^\ell = 2^{2\sqrt{r}\log n} = n^{2\sqrt{r}}$.

$$q|(r-1), \quad q \geq 4\sqrt{r}\log n, \quad \ell = 2\sqrt{r}\log n$$

each prime $\leq r$ does not divide n

Main Lemma: The set

$$G = \{(x-1)^{e_1}(x-2)^{e_2} \cdots (x-\ell)^{e_\ell} : e_j \geq 0\}$$

forms a subgroup of the multiplicative group of non-zero elements of F (which necessarily is cyclic) of size $> 2^\ell = 2^{2\sqrt{r}\log n} = n^{2\sqrt{r}}$.

$$q|(r-1), \quad q \geq 4\sqrt{r}\log n, \quad \ell = 2\sqrt{r}\log n$$

each prime $\leq r$ does not divide n

$$p > r$$

Main Lemma: The set

$$G = \{(x-1)^{e_1}(x-2)^{e_2}\cdots(x-\ell)^{e_\ell} : e_j \geq 0\}$$

forms a subgroup of the multiplicative group of non-zero elements of F (which necessarily is cyclic) of size $> 2^\ell = 2^{2\sqrt{r}\log n} = n^{2\sqrt{r}}$.

$$q|(r-1), \quad q \geq 4\sqrt{r}\log n, \quad \ell = 2\sqrt{r}\log n$$

each prime $\leq r$ does not divide n

$$p > r > q$$

Main Lemma: The set

$$G = \{(x-1)^{e_1}(x-2)^{e_2}\cdots(x-\ell)^{e_\ell} : e_j \geq 0\}$$

forms a subgroup of the multiplicative group of non-zero elements of F (which necessarily is cyclic) of size $> 2^\ell = 2^{2\sqrt{r}\log n} = n^{2\sqrt{r}}$.

$$q|(r-1), \quad q \geq 4\sqrt{r}\log n, \quad \ell = 2\sqrt{r}\log n$$

each prime $\leq r$ does not divide n

$$p > r > q \geq 4\sqrt{r}\log n$$

Main Lemma: The set

$$G = \{(x-1)^{e_1}(x-2)^{e_2}\cdots(x-\ell)^{e_\ell} : e_j \geq 0\}$$

forms a subgroup of the multiplicative group of non-zero elements of F (which necessarily is cyclic) of size $> 2^\ell = 2^{2\sqrt{r}\log n} = n^{2\sqrt{r}}$.

$$q|(r-1), \quad q \geq 4\sqrt{r}\log n, \quad \ell = 2\sqrt{r}\log n$$

each prime $\leq r$ does not divide n

$$p > r > q \geq 4\sqrt{r}\log n > \ell$$

Main Lemma: The set

$$G = \{(x-1)^{e_1}(x-2)^{e_2}\cdots(x-\ell)^{e_\ell} : e_j \geq 0\}$$

forms a subgroup of the multiplicative group of non-zero elements of F (which necessarily is cyclic) of size $> 2^\ell = 2^{2\sqrt{r}\log n} = n^{2\sqrt{r}}$.

$$p > r > q \geq 4\sqrt{r}\log n > \ell$$

Main Lemma: The set

$$G = \{(x-1)^{e_1}(x-2)^{e_2} \cdots (x-\ell)^{e_\ell} : e_j \geq 0\}$$

forms a subgroup of the multiplicative group of non-zero elements of F (which necessarily is cyclic) of size $> 2^\ell = 2^{2\sqrt{r}\log n} = n^{2\sqrt{r}}$.

$$p > r > q \geq 4\sqrt{r}\log n > \ell$$

$$0, 1, \ldots, \ell \text{ are distinct modulo } p$$

Main Lemma: The set

$$G = \{(x-1)^{e_1}(x-2)^{e_2}\cdots(x-\ell)^{e_\ell} : e_j \geq 0\}$$

forms a subgroup of the multiplicative group of non-zero elements of F (which necessarily is cyclic) of size $> 2^\ell = 2^{2\sqrt{r}\log n} = n^{2\sqrt{r}}$.

$$p > r > q \geq 4\sqrt{r}\log n > \ell$$

$0, 1, \ldots, \ell$ are distinct modulo p

$\Longrightarrow$ the elements of G with $e_1 + \cdots + e_\ell < d$ are distinct modulo $h(x), p$

Main Lemma: The set

$$G = \{(x-1)^{e_1}(x-2)^{e_2}\cdots(x-\ell)^{e_\ell} : e_j \geq 0\}$$

forms a subgroup of the multiplicative group of non-zero elements of F (which necessarily is cyclic) of size $> 2^\ell = 2^{2\sqrt{r}\log n} = n^{2\sqrt{r}}$.

the elements of G with $e_1 + \cdots + e_\ell < d$ are distinct

Main Lemma: The set

$$G = \{(x-1)^{e_1}(x-2)^{e_2}\cdots(x-\ell)^{e_\ell} : e_j \geq 0\}$$

forms a subgroup of the multiplicative group of non-zero elements of F (which necessarily is cyclic) of size $> 2^\ell = 2^{2\sqrt{r}\log n} = n^{2\sqrt{r}}$.

the elements of G with $e_1 + \cdots + e_\ell < d$ are distinct

the number of solutions of $e_1 + \cdots + e_\ell < d$ is

the number of ways of choosing ℓ objects from $\ell + d - 1$

Main Lemma: The set

$$G = \{(x-1)^{e_1}(x-2)^{e_2}\cdots(x-\ell)^{e_\ell} : e_j \geq 0\}$$

forms a subgroup of the multiplicative group of non-zero elements of F (which necessarily is cyclic) of size $> 2^\ell = 2^{2\sqrt{r}\log n} = n^{2\sqrt{r}}$.

the elements of G with $e_1 + \cdots + e_\ell < d$ are distinct

$$|G| \geq \binom{\ell + d - 1}{\ell}$$

Main Lemma: The set

$$G = \{(x-1)^{e_1}(x-2)^{e_2}\cdots(x-\ell)^{e_\ell} : e_j \geq 0\}$$

forms a subgroup of the multiplicative group of non-zero elements of F (which necessarily is cyclic) of size $> 2^\ell = 2^{2\sqrt{r}\log n} = n^{2\sqrt{r}}$.

the elements of G with $e_1 + \cdots + e_\ell < d$ are distinct

$$|G| \geq \binom{\ell+d-1}{\ell}$$

$$= \frac{(\ell+d-1)(\ell+d-2)\cdots d}{\ell!}$$

Main Lemma: The set

$$G = \{(x-1)^{e_1}(x-2)^{e_2}\cdots(x-\ell)^{e_\ell} : e_j \geq 0\}$$

forms a subgroup of the multiplicative group of non-zero elements of F (which necessarily is cyclic) of size $> 2^\ell = 2^{2\sqrt{r}\log n} = n^{2\sqrt{r}}$.

the elements of G with $e_1 + \cdots + e_\ell < d$ are distinct

$$|G| \geq \binom{\ell + d - 1}{\ell}$$

$$= \frac{(\ell + d - 1)(\ell + d - 2)\cdots d}{\ell!} > \quad -$$

Main Lemma: The set

$$G = \{(x-1)^{e_1}(x-2)^{e_2}\cdots(x-\ell)^{e_\ell} : e_j \geq 0\}$$

forms a subgroup of the multiplicative group of non-zero elements of F (which necessarily is cyclic) of size $> 2^\ell = 2^{2\sqrt{r}\log n} = n^{2\sqrt{r}}$.

the elements of G with $e_1 + \cdots + e_\ell < d$ are distinct

$$|G| \geq \binom{\ell + d - 1}{\ell}$$

$$= \frac{(\ell+d-1)(\ell+d-2)\cdots d}{\ell!} > \frac{\quad}{\ell^\ell}$$

Main Lemma: The set

$$G = \{(x-1)^{e_1}(x-2)^{e_2} \cdots (x-\ell)^{e_\ell} : e_j \geq 0\}$$

forms a subgroup of the multiplicative group of non-zero elements of F (which necessarily is cyclic) of size $> 2^\ell = 2^{2\sqrt{r}\log n} = n^{2\sqrt{r}}$.

the elements of G with $e_1 + \cdots + e_\ell < d$ are distinct

$$|G| \geq \binom{\ell + d - 1}{\ell}$$

$$= \frac{(\ell + d - 1)(\ell + d - 2)\cdots d}{\ell!} > \left(\frac{}{\ell}\right)^\ell$$

Main Lemma: The set

$$G = \{(x-1)^{e_1}(x-2)^{e_2}\cdots(x-\ell)^{e_\ell} : e_j \geq 0\}$$

forms a subgroup of the multiplicative group of non-zero elements of F (which necessarily is cyclic) of size $> 2^\ell = 2^{2\sqrt{r}\log n} = n^{2\sqrt{r}}$.

the elements of G with $e_1 + \cdots + e_\ell < d$ are distinct

$$|G| \geq \binom{\ell+d-1}{\ell}$$

$$= \frac{(\ell+d-1)(\ell+d-2)\cdots d}{\ell!} > \left(\frac{d}{\ell}\right)^\ell$$

Main Lemma: The set

$$G = \{(x-1)^{e_1}(x-2)^{e_2}\cdots(x-\ell)^{e_\ell} : e_j \geq 0\}$$

forms a subgroup of the multiplicative group of non-zero elements of F (which necessarily is cyclic) of size $> 2^\ell = 2^{2\sqrt{r}\log n} = n^{2\sqrt{r}}$.

the elements of G with $e_1 + \cdots + e_\ell < d$ are distinct

$$|G| \geq \binom{\ell + d - 1}{\ell}$$

$$= \frac{(\ell + d - 1)(\ell + d - 2)\cdots d}{\ell!} > \left(\frac{d}{\ell}\right)^\ell$$

Main Lemma: The set

$$G = \{(x-1)^{e_1}(x-2)^{e_2}\cdots(x-\ell)^{e_\ell} : e_j \geq 0\}$$

forms a subgroup of the multiplicative group of non-zero elements of F (which necessarily is cyclic) of size $> 2^\ell = 2^{2\sqrt{r}\log n} = n^{2\sqrt{r}}$.

the elements of G with $e_1 + \cdots + e_\ell < d$ are distinct

$$|G| \geq \binom{\ell+d-1}{\ell}$$

$$= \frac{(\ell+d-1)(\ell+d-2)\cdots d}{\ell!} > 2^\ell$$