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

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

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

↑ "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

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

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

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;

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 ($\gcd(n, r) \neq 1$) 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.

SITUATION:

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

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

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

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

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

SITUATION:

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

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

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

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

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

SITUATION:

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

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

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

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

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

SITUATION:

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

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

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

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

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

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

p with $p|n$

(Comment: We really will work mod $(x^r - 1, p)$.)

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

$$\Downarrow$$

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

$$\Downarrow$$

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

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

$$\Uparrow$$

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

$$\Uparrow$$

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

SITUATION:

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

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

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

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

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

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

(Comment: We really will work mod $(x^r - 1, p)$.)

Situation:

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

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

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

How to Choose p:

SITUATION:

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

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

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

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

SITUATION:

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

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

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

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:

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

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

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

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:

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

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

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

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 $q|d$. Fix p such that

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

SITUATION:

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

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

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

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

SITUATION:

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

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

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

How do we choose $\boldsymbol{h}(\boldsymbol{x})$?

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* $f = ord_m(p)$. *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* $f = ord_m(p)$. *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 $f = ord_m(p)$. 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* $f = ord_m(p)$. *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* $f = ord_m(p)$*. 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* $f = ord_m(p)$*. 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.*

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

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* $f = ord_m(p)$. *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 $\text{ord}_r(p)$ 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* $f = ord_m(p)$*. 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 $\text{ord}_r(p)$ modulo p

$$h(x)$$

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

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

(Comment: We really will work mod $(x^r - 1, p)$.)

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

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

(Comment: We really will work mod $(x^r - 1, p)$.)

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

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

(Comment: We really will work mod $(x^r - 1, p)$.)

Situation:

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

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

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

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

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

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

(Comment: We really will work mod $(x^r - 1, p)$.)

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 $h(x), p$

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

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

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

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

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 $h(x), p$

$$n \text{ is composite}, \quad r \text{ is a prime}, \quad \ell = 2\sqrt{r}\log n$$
$$q \text{ is a prime}, \quad q \geq 4\sqrt{r}\log n$$
$$q \mid (r-1), \quad p \mid n, \quad q \mid \mathrm{ord}_r(p)$$
$$h(x) \text{ irreducible mod } p, \quad \deg h = \mathrm{ord}_r(p) \geq 2\ell$$

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 $> 2^\ell = 2^{2\sqrt{r}\log n}$

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.~~

SITUATION:

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

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

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

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

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

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

(Comment: We really will work mod $(x^r - 1, p)$.)

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 $|G| > n^{2\sqrt{r}}$.

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 $> 2^\ell = 2^{2\sqrt{r}\log n} = n^{2\sqrt{r}}$.

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

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

Note this is not $h(x)$.

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 $> 2^\ell = 2^{2\sqrt{r}\log n} = n^{2\sqrt{r}}$.

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

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

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 $m_1 \equiv m_2 \pmod{r}$

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

This is mod $(h(x), p)$.

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

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 $g(x)$

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 $> 2^\ell = 2^{2\sqrt{r}\log n} = n^{2\sqrt{r}}$.

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

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 $m_1 \equiv m_2 \pmod{r}$

  $\Longrightarrow m_1 \equiv m_2 \pmod{d}$ 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 $g(x)$

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

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

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 $g(x)$

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

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

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

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 $g(x)$

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

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

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

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

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 $g(x)$

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

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

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

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

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 $g(x)$

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

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

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

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

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 $m_1 \equiv m_2 \pmod{r}$

  $\Longrightarrow m_1 \equiv m_2 \pmod{d}$ 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 $\le r$ positive integers $\le d$ 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

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

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

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

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

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

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

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

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

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

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

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

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

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 $a \in \{1, 2, \ldots, \ell\}$,

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

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

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

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 $a \in \{1, 2, \ldots, \ell\}$,

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

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

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

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

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

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 $a \in \{1, 2, \ldots, \ell\}$,

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

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

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

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

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 $I_{g(x)}$.

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

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 $g(x)$

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

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

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

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

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 $g(x)$

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

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 $I_{g(x)}$.

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

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

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

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

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 $g(x)$

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 $> 2^\ell = 2^{2\sqrt{r}\log n} = n^{2\sqrt{r}}$.

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

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 $I_{g(x)}$.

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

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

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

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

$\blacksquare$