Lecture 10

A Curious Connection with the Odd Covering Problem

Coverings of the Integers:

A *covering of the integers* is a system of congruences

$$x \equiv a_j \pmod{m_j}$$

having the property that every integer satisfies at least one of the congruences.

Coverings of the Integers:

A *covering of the integers* is a system of congruences

$$x \equiv a_j \pmod{m_j}$$

having the property that every integer satisfies at least one of the congruences.

Example 1:

$$x \equiv 0 \pmod{2}$$
$$x \equiv 1 \pmod{2}$$

Example 2:

$$\begin{aligned}
x &\equiv 0 \pmod{2} \\
x &\equiv 2 \pmod{3} \\
x &\equiv 1 \pmod{4} \\
x &\equiv 1 \pmod{6} \\
x &\equiv 3 \pmod{12}
\end{aligned}$$

Example 2:

$$
\begin{aligned}
x &\equiv 0 \pmod{2}\\
x &\equiv 2 \pmod{3}\\
x &\equiv 1 \pmod{4}\\
x &\equiv 1 \pmod{6}\\
x &\equiv 3 \pmod{12}
\end{aligned}
$$

0	1	2	3	4	5	6	7	8	9	10	11

Open Problem:

Does there exist an “odd covering” of the integers, a covering consisting of distinct odd moduli > 1?

Open Problem:

Does there exist an "odd covering" of the integers, a covering consisting of distinct odd moduli > 1?

Erdős: \$25 (for proof none exists)

Open Problem:

Does there exist an “odd covering” of the integers, a covering consisting of distinct odd moduli > 1?

Erdős: $25 (for proof none exists)

Selfridge: $2000 (for explicit example)

Sierpinski's Application:

There exist infinitely many (even a positive proportion of) positive integers k such that $k \times 2^n + 1$ is composite for all non-negative integers n.

Sierpinski's Application:

There exist infinitely many (even a positive proportion of) positive integers $\boldsymbol{k}$ such that $\boldsymbol{k \times 2^n + 1}$ is composite for all non-negative integers $\boldsymbol{n}$.

Selfridge's Example: $\boldsymbol{k = 78557}$

(smallest odd known)

Sierpinski's Application:

There exist infinitely many (even a positive proportion of) positive integers k such that $k \times 2^n + 1$ is composite for all non-negative integers n.

Selfridge's Example: $k = 78557$

(smallest odd known)

Polynomial Question: Does there exist $f(x) \in \mathbb{Z}[x]$ such that $f(x)x^n + 1$ is reducible for all non-negative integers n?

Sierpinski's Application:

There exist infinitely many (even a positive proportion of) positive integers k such that $k \times 2^n + 1$ is composite for all non-negative integers n.

Selfridge's Example: $k = 78557$
(smallest odd known)

Polynomial Question: Does there exist $f(x) \in \mathbb{Z}[x]$ such that $f(x)x^n + 1$ is reducible for all non-negative integers n?

Require: $f(1) \neq -1$

Sierpinski's Application:

There exist infinitely many (even a positive proportion of) positive integers k such that $k \times 2^n + 1$ is composite for all non-negative integers n.

Selfridge's Example: $k = 78557$
(smallest odd known)

Polynomial Question: Does there exist $f(x) \in \mathbb{Z}[x]$ such that $f(1) \neq -1$ and $f(x)x^n + 1$ is reducible for all non-negative integers n?

Sierpinski's Application:

There exist infinitely many (even a positive proportion of) positive integers k such that $k \times 2^n + 1$ is composite for all non-negative integers n.

Selfridge's Example: $k = 78557$
(smallest odd known)

Polynomial Question: Does there exist $f(x) \in \mathbb{Z}[x]$ such that $f(1) \neq -1$ and $f(x)x^n + 1$ is reducible for all non-negative integers n?

Answer: Nobody knows.

Schinzel's Example:

$$(5x^9+6x^8+3x^6+8x^5+9x^3+6x^2+8x+3)x^n+12$$

is reducible for all non-negative integers n

Schinzel's Example:

$$(5x^9+6x^8+3x^6+8x^5+9x^3+6x^2+8x+3)x^n+12$$

is reducible for all non-negative integers n

Comment: For each n, the above polynomial is divisible by at least one of

$$\Phi_k(x) \quad \text{where } k \in \{2,3,4,6,12\}.$$

Schinzel's Example:

$$(5x^9+6x^8+3x^6+8x^5+9x^3+6x^2+8x+3)x^n+12$$

is reducible for all non-negative integers n

Comment: For each n, the above polynomial is divisible by at least one of

$$\Phi_k(x) \quad \text{where } k \in \{2, 3, 4, 6, 12\}.$$

$$n \equiv 0 \pmod 2 \implies f(x)x^n + 12 \equiv 0 \pmod{x+1}$$

Schinzel's Example:

$$(5x^9+6x^8+3x^6+8x^5+9x^3+6x^2+8x+3)x^n+12$$

is reducible for all non-negative integers n

Comment: For each n, the above polynomial is divisible by at least one of

$$\Phi_k(x) \quad \text{where } k \in \{2, 3, 4, 6, 12\}.$$

$$n \equiv 0 \pmod 2 \implies f(x)x^n + 12 \equiv 0 \pmod{x+1}$$
$$n \equiv 2 \pmod 3 \implies f(x)x^n + 12 \equiv 0 \pmod{x^2+x+1}$$

Schinzel's Example:

$$(5x^9+6x^8+3x^6+8x^5+9x^3+6x^2+8x+3)x^n+12$$

is reducible for all non-negative integers n

Comment: For each n, the above polynomial is divisible by at least one of

$$\Phi_k(x) \quad \text{where } k \in \{2, 3, 4, 6, 12\}.$$

$$n \equiv 0 \pmod 2 \implies f(x)x^n + 12 \equiv 0 \pmod{x+1}$$
$$n \equiv 2 \pmod 3 \implies f(x)x^n + 12 \equiv 0 \pmod{x^2+x+1}$$
$$n \equiv 1 \pmod 4 \implies f(x)x^n + 12 \equiv 0 \pmod{x^2+1}$$

Schinzel's Example:

$$(5x^9+6x^8+3x^6+8x^5+9x^3+6x^2+8x+3)x^n+12$$

is reducible for all non-negative integers n

Comment: For each n, the above polynomial is divisible by at least one of

$$\Phi_k(x) \quad \text{where } k \in \{2,3,4,6,12\}.$$

$$n \equiv 0 \pmod 2 \implies f(x)x^n + 12 \equiv 0 \pmod{x+1}$$
$$n \equiv 2 \pmod 3 \implies f(x)x^n + 12 \equiv 0 \pmod{x^2+x+1}$$
$$n \equiv 1 \pmod 4 \implies f(x)x^n + 12 \equiv 0 \pmod{x^2+1}$$
$$n \equiv 1 \pmod 6 \implies f(x)x^n + 12 \equiv 0 \pmod{x^2-x+1}$$

Schinzel's Example:

$$(5x^9+6x^8+3x^6+8x^5+9x^3+6x^2+8x+3)x^n+12$$

is reducible for all non-negative integers n

Comment: For each n, the above polynomial is divisible by at least one of

$$\Phi_k(x) \quad \text{where } k \in \{2, 3, 4, 6, 12\}.$$

$$\begin{aligned}
n \equiv 0 \pmod{2} &\implies f(x)x^n + 12 \equiv 0 \pmod{x+1} \\
n \equiv 2 \pmod{3} &\implies f(x)x^n + 12 \equiv 0 \pmod{x^2+x+1} \\
n \equiv 1 \pmod{4} &\implies f(x)x^n + 12 \equiv 0 \pmod{x^2+1} \\
n \equiv 1 \pmod{6} &\implies f(x)x^n + 12 \equiv 0 \pmod{x^2-x+1} \\
n \equiv 3 \pmod{12} &\implies f(x)x^n + 12 \equiv 0 \pmod{x^4-x^2+1}
\end{aligned}$$

Schinzel's Example:

$$(5x^9 + 6x^8 + 3x^6 + 8x^5 + 9x^3 + 6x^2 + 8x + 3)x^n + 12$$

is reducible for all non-negative integers n

Theorem. There exists an $f(x) \in \mathbb{Z}[x]$ with non-negative coefficients such that $f(x)x^n + 4$ is reducible for all non-negative integers n.

Schinzel's Example:

$$(5x^9 + 6x^8 + 3x^6 + 8x^5 + 9x^3 + 6x^2 + 8x + 3)x^n + 12$$

is reducible for all non-negative integers n

Theorem. There exists an $f(x) \in \mathbb{Z}[x]$ with non-negative coefficients such that $f(x)x^n + 4$ is reducible for all non-negative integers n.

Schinzel's Example:

$$(5x^9+6x^8+3x^6+8x^5+9x^3+6x^2+8x+3)x^n+12$$

is reducible for all non-negative integers n

Theorem. There exists an $f(x) \in \mathbb{Z}[x]$ with non-negative coefficients such that $f(x)x^n + 4$ is reducible for all non-negative integers n.

Schinzel's Example:

$$(5x^9+6x^8+3x^6+8x^5+9x^3+6x^2+8x+3)x^n+12$$

is reducible for all non-negative integers n

Theorem. There exists an $f(x) \in \mathbb{Z}[x]$ with non-negative coefficients such that $f(x)x^n + 4$ is reducible for all non-negative integers n.

Comment: For each n, the first polynomial is divisible by at least one $\Phi_k(x)$ where k divides 12.

Schinzel's Example:

$$(5x^9+6x^8+3x^6+8x^5+9x^3+6x^2+8x+3)x^n+12$$

is reducible for all non-negative integers n

Theorem. There exists an $f(x) \in \mathbb{Z}[x]$ with non-negative coefficients such that $f(x)x^n+4$ is reducible for all non-negative integers n.

Comment: For each n, the second polynomial is divisible by at least one $\Phi_k(x)$ where k divides some integer N having more than 10^{17} digits.

Schinzel's Example:

$$(5x^9+6x^8+3x^6+8x^5+9x^3+6x^2+8x+3)x^n+12$$

is reducible for all non-negative integers n

Theorem. There exists an $f(x) \in \mathbb{Z}[x]$ with non-negative coefficients such that $f(x)x^n+4$ is reducible for all non-negative integers n.

Comment: For each n, the second polynomial is divisible by at least one $\Phi_k(x)$ where k divides

$$2^{4367503340863488 00}3^{41}5^{31}7^{37}11^{29}13^{23}17^{16}19^{18}23^{23}29^{29}31^{31}37^{37}41^{41}.$$

Schinzel's Theorem: If there is an $f(x) \in \mathbb{Z}[x]$ such that $f(1) \neq -1$ and $f(x)x^n + 1$ is reducible for all non-negative integers n, then there is an odd covering of the integers.

Theorem (F., Ford, Konyagin). Let $u(x)$ and $v(x)$ be in $\mathbb{Z}[x]$ with

$$u(0) \neq 0,\ v(0) \neq 0, \text{ and } \gcd(u(x), v(x)) = 1.$$

Let r_1 and r_2 denote the number of non-zero terms in $u(x)$ and $v(x)$, respectively. If

$$m \geq \max\left\{2 \times 5^{2N-1}, 2\max\{\deg u, \deg v\}\left(5^{N-1} + \frac{1}{4}\right)\right\}$$

where $N = 2\,\|u\|^2 + 2\,\|v\|^2 + 2r_1 + 2r_2 - 7$, then the non-reciprocal part of $u(x)x^m + v(x)$ is irreducible unless one of the following holds:

(i) The polynomial $-u(x)v(x)$ is a pth power for some prime p dividing m.

(ii) One of $\pm u(x)$ or $\pm v(x)$ is a 4th power, the other is 4 times a 4th power, and $4|m$.

Theorem (F., Ford, Konyagin). When m is large, either $u(x)x^m + v(x)$ has an obvious factorization or the non-reciprocal part of $u(x)x^m + v(x)$ is irreducible.

Theorem (F., Ford, Konyagin). When m is large, either $u(x)x^m + v(x)$ has an obvious factorization or the non-reciprocal part of $u(x)x^m + v(x)$ is irreducible.

Comment: Schinzel essentially proved this with a different understanding of what "m is large" means.

Theorem (F., Ford, Konyagin). When m is large, either $u(x)x^m + v(x)$ has an obvious factorization or the non-reciprocal part of $u(x)x^m + v(x)$ is irreducible.

Lemma (Schinzel). Let $f(x) \in \mathbb{Z}[x]$. Suppose that n is sufficiently large (depending on f). Then the non-reciprocal part of $f(x)x^n + 1$ is irreducible over $\mathbb{Q}$ or identically ± 1 unless one of the following holds:

(i) $-f(x)$ is a pth power in $\mathbb{Q}[x]$ for some prime p dividing n.

(ii) $f(x)$ is 4 times a 4th power in $\mathbb{Q}[x]$ and n is divisible by 4.

Lemma 2 (Apostol). Let n and m be positive integers with $n > m$. The resultant of $\Phi_n(x)$ and $\Phi_m(x)$ is divisible by a prime p if and only if n/m is a power of p.

Step 1. Suppose we almost have a covering in that every integer $n \geq n_0$ (for some n_0) satisfies at least one of the congruences

$$x \equiv a_1 \pmod{m_1}, \dots, \; x \equiv a_r \pmod{m_r}$$

where the a_j's and m_j's are integers with each $m_j > 0$.

Step 1. Suppose we almost have a covering in that every integer $n \geq n_0$ (for some n_0) satisfies at least one of the congruences

$$x \equiv a_1 \pmod{m_1}, \ldots, \ x \equiv a_r \pmod{m_r}$$

where the a_j's and m_j's are integers with each $m_j > 0$. Let $n \in \mathbb{Z}$.

Step 1. Suppose we almost have a covering in that every integer $n \geq n_0$ (for some n_0) satisfies at least one of the congruences

$$x \equiv a_1 \pmod{m_1}, \ldots, \; x \equiv a_r \pmod{m_r}$$

where the a_j's and m_j's are integers with each $m_j > 0$. Let $n \in \mathbb{Z}$. We claim that n satisfies at least one of the congruences above.

Step 1. Suppose we almost have a covering in that every integer $n \geq n_0$ (for some n_0) satisfies at least one of the congruences

$$x \equiv a_1 \pmod{m_1}, \ldots, \; x \equiv a_r \pmod{m_r}$$

where the a_j's and m_j's are integers with each $m_j > 0$. Let $n \in \mathbb{Z}$. We claim that n satisfies at least one of the congruences above (so the congruences form a covering).

Step 1. Suppose we almost have a covering in that every integer $n \geq n_0$ (for some n_0) satisfies at least one of the congruences

$$x \equiv a_1 \pmod{m_1}, \dots, \; x \equiv a_r \pmod{m_r}$$

where the a_j's and m_j's are integers with each $m_j > 0$. Let $n \in \mathbb{Z}$. We claim that n satisfies at least one of the congruences above (so the congruences form a covering).

Let $k \in \mathbb{Z}$ with

$$n + k\, m_1 m_2 \cdots m_r \geq n_0.$$

Step 1. Suppose we almost have a covering in that every integer $n \geq n_0$ (for some n_0) satisfies at least one of the congruences

$$x \equiv a_1 \pmod{m_1}, \dots, \; x \equiv a_r \pmod{m_r}$$

where the a_j's and m_j's are integers with each $m_j > 0$. Let $n \in \mathbb{Z}$. We claim that n satisfies at least one of the congruences above (so the congruences form a covering).

Let $k \in \mathbb{Z}$ with

$$n + k\, m_1 m_2 \cdots m_r \geq n_0.$$

Then, for some $j \in \{1, 2, \dots, r\}$,

$$n + k\, m_1 m_2 \cdots m_r \equiv a_j \pmod{m_j}.$$

Step 1. Suppose we almost have a covering in that every integer $n \geq n_0$ (for some n_0) satisfies at least one of the congruences

$$x \equiv a_1 \pmod{m_1}, \ldots, \; x \equiv a_r \pmod{m_r}$$

where the a_j's and m_j's are integers with each $m_j > 0$. Let $n \in \mathbb{Z}$. We claim that n satisfies at least one of the congruences above (so the congruences form a covering).

Let $k \in \mathbb{Z}$ with

$$n + k\, m_1 m_2 \cdots m_r \geq n_0.$$

Then, for some $j \in \{1, 2, \ldots, r\}$,

$$n \equiv n + k\, m_1 m_2 \cdots m_r \equiv a_j \pmod{m_j}.$$

Step 2. $f(0) \neq 0$ and $f(x) \not\equiv 1$.

Step 2. $f(0) \neq 0$ and $f(x) \not\equiv 1$.

Step 2. $\boldsymbol{f(0) \neq 0}$ and $\boldsymbol{f(x) \not\equiv 1}$.

We will show that if $\boldsymbol{f(x)x^n + 1}$ is reducible for all $\boldsymbol{n \geq N}$ (where $\boldsymbol{N}$ is arbitrary), then there is an odd covering of the integers.

Step 2. $f(0) \neq 0$ and $f(x) \not\equiv 1$.

We will show that if $f(x)x^n + 1$ is reducible for all $n \geq N$ (where N is arbitrary), then there is an odd covering of the integers. If $f(x) = g(x)x^k$, then

$$f(x)x^n+1 \text{ is reducible} \iff g(x)x^{n+k}+1 \text{ is reducible.}$$

Step 2. $f(0) \neq 0$ and $f(x) \not\equiv 1$.

We will show that if $f(x)x^n + 1$ is reducible for all $n \geq N$ (where N is arbitrary), then there is an odd covering of the integers. If $f(x) = g(x)x^k$, then

$$f(x)x^n+1 \text{ is reducible} \iff g(x)x^{n+k}+1 \text{ is reducible},$$

so one can replace $f(x)$ with $g(x)$.

Step 2. $f(0) \neq 0$ and $f(x) \not\equiv 1$.

Step 2. $f(0) \neq 0$ and $f(x) \not\equiv 1$.

Henceforth, assume $F(x) = f(x)x^n + 1$
is reducible for all large n.

We want to show there is an odd covering.

Step 2. $f(0) \neq 0$ and $f(x) \not\equiv 1$.

Step 2. $\boldsymbol{f(0) \neq 0}$ and $\boldsymbol{f(x) \not\equiv 1}$.

Is $\boldsymbol{x^n + 1}$ reducible for every $\boldsymbol{n} \in \mathbb{Z}^+$?

Step 2. $f(0) \neq 0$ and $f(x) \not\equiv 1$.

Is $x^n + 1$ reducible for every $n \in \mathbb{Z}^+$?

$$x^{2^t} + 1 = \Phi_{2^{t+1}}(x) \text{ is irreducible for every } t \in \mathbb{Z}^+$$

Step 3. Let p be a prime, and let m be a positive integer such that p divides m. Then $x^p = \zeta_m$ has no solutions $x \in \mathbb{Q}(\zeta_m)$.

Step 3. Let p be a prime, and let m be a positive integer such that p divides m. Then $x^p = \underset{\substack{\uparrow \\ e^{2\pi \mathrm{i}/m}}}{\zeta_m}$ has no solutions $x \in \mathbb{Q}(\zeta_m)$.

Step 3. Let p be a prime, and let m be a positive integer such that p divides m. Then $x^p = \underset{\substack{\uparrow \\ e^{2\pi \mathrm{i}/m}}}{\zeta_m}$ has no solutions $x \in \mathbb{Q}(\zeta_m)$.

Since

$$\zeta_p = e^{2\pi \mathrm{i}/p} \quad \text{and} \quad \zeta_{pm} = e^{2\pi \mathrm{i}/(pm)},$$

we deduce that, for $j \in \{0, 1, \ldots, p-1\}$,

$$\left(\zeta_p^j \zeta_{pm}\right)^p = \zeta_p^{pj} \zeta_{pm}^p = \zeta_{pm}^p = \zeta_m.$$

Step 3. Let p be a prime, and let m be a positive integer such that p divides m. Then $x^p = \underset{\substack{\uparrow \\ e^{2\pi \mathrm{i}/m}}}{\zeta_m}$ has no solutions $x \in \mathbb{Q}(\zeta_m)$.

Since

$$\zeta_p = e^{2\pi \mathrm{i}/p} \quad \text{and} \quad \zeta_{pm} = e^{2\pi \mathrm{i}/(pm)},$$

we deduce that, for $j \in \{0, 1, \ldots, p-1\}$,

$$\left(\zeta_p^j \zeta_{pm}\right)^p = \zeta_p^{pj} \zeta_{pm}^p = \zeta_{pm}^p = \zeta_m.$$

The roots of $x^p = \zeta_m$ are $\zeta_p^j \zeta_{pm}$ $(0 \le j \le p-1)$.

Step 3. Let p be a prime, and let m be a positive integer such that p divides m. Then $x^p = \underset{\substack{\uparrow \\ e^{2\pi \mathrm{i}/m}}}{\zeta_m}$ has no solutions $x \in \mathbb{Q}(\zeta_m)$.

The roots of $x^p = \zeta_m$ are $\zeta_p^j \zeta_{pm}$ $(0 \leq j \leq p-1)$.

Step 3. Let p be a prime, and let m be a positive integer such that p divides m. Then $x^p = \underset{\substack{\uparrow \\ e^{2\pi \mathrm{i}/m}}}{\zeta_m}$ has no solutions $x \in \mathbb{Q}(\zeta_m)$.

The roots of $x^p = \zeta_m$ are $\zeta_p^j \zeta_{pm}$ $(0 \leq j \leq p-1)$. Assume one of these is in $\mathbb{Q}(\zeta_m)$.

Step 3. Let p be a prime, and let m be a positive integer such that p divides m. Then $x^p = \underset{\substack{\uparrow \\ e^{2\pi \mathrm{i}/m}}}{\zeta_m}$ has no solutions $x \in \mathbb{Q}(\zeta_m)$.

The roots of $x^p = \zeta_m$ are $\zeta_p^j \zeta_{pm}$ $(0 \leq j \leq p-1)$. Assume one of these is in $\mathbb{Q}(\zeta_m)$. Then

$$\zeta_p = \zeta_m^{m/p} \in \mathbb{Q}(\zeta_m)$$

Step 3. Let p be a prime, and let m be a positive integer such that p divides m. Then $x^p = \zeta_m$ has no solutions $x \in \mathbb{Q}(\zeta_m)$.

$$\uparrow$$
$$e^{2\pi \mathrm{i}/m}$$

The roots of $x^p = \zeta_m$ are $\zeta_p^j \zeta_{pm}$ $(0 \leq j \leq p-1)$. Assume one of these is in $\mathbb{Q}(\zeta_m)$. Then

$$\zeta_p = \zeta_m^{m/p} \in \mathbb{Q}(\zeta_m) \implies \zeta_{pm} \in \mathbb{Q}(\zeta_m).$$

Step 3. Let p be a prime, and let m be a positive integer such that p divides m. Then $x^p = \underset{\substack{\uparrow \\ e^{2\pi \mathrm{i}/m}}}{\zeta_m}$ has no solutions $x \in \mathbb{Q}(\zeta_m)$.

The roots of $x^p = \zeta_m$ are $\zeta_p^j \zeta_{pm}$ $(0 \le j \le p-1)$. Assume one of these is in $\mathbb{Q}(\zeta_m)$. Then

$$\zeta_p = \zeta_m^{m/p} \in \mathbb{Q}(\zeta_m) \implies \zeta_{pm} \in \mathbb{Q}(\zeta_m).$$

This contradicts, for example, that the minimal polynomial for ζ_{pm} is $\Phi_{pm}(x)$ which has degree $\phi(pm) > \phi(m)$.

Step 4. Each reciprocal factor of $F(x) = f(x)x^n + 1$ divides $f(x)\tilde{f}(x) - x^{\deg f}$.

Step 4. Each reciprocal factor of $F(x) = f(x)x^n + 1$ divides $f(x)\tilde{f}(x) - x^{\deg f}$. Hence, there is a finite list of irreducible reciprocal factors that can divide $f(x)x^n + 1$ as n varies.

Step 4. Each reciprocal factor of $F(x) = f(x)x^n + 1$ divides $f(x)\tilde{f}(x) - x^{\deg f}$. Hence, there is a finite list of irreducible reciprocal factors that can divide $f(x)x^n + 1$ as n varies.

Since

$$\widetilde{F}(x) = x^{n+\deg f} + \tilde{f}(x),$$

Step 4. Each reciprocal factor of $F(x) = f(x)x^n + 1$ divides $f(x)\tilde{f}(x) - x^{\deg f}$. Hence, there is a finite list of irreducible reciprocal factors that can divide $f(x)x^n + 1$ as n varies.

Since

$$\widetilde{F}(x) = x^{n+\deg f} + \tilde{f}(x),$$

each reciprocal factor of F divides

$$f(x)\widetilde{F}(x) - x^{\deg f}F(x)$$

Step 4. Each reciprocal factor of $F(x) = f(x)x^n + 1$ divides $f(x)\tilde{f}(x) - x^{\deg f}$. Hence, there is a finite list of irreducible reciprocal factors that can divide $f(x)x^n + 1$ as n varies.

Since

$$\widetilde{F}(x) = x^{n+\deg f} + \tilde{f}(x),$$

each reciprocal factor of F divides

$$f(x)\widetilde{F}(x) - x^{\deg f}F(x) = f(x)\tilde{f}(x) - x^{\deg f}.$$

Step 4. There is a finite list of irreducible reciprocal factors that can divide $F(x) = f(x)x^n + 1$ as n varies.

Step 4. There is a finite list of irreducible reciprocal factors that can divide $F(x) = f(x)x^n + 1$ as n varies.

Step 5. There is an n_0 such that if $n \geq n_0$, then every irreducible reciprocal factor of $F(x)$ is cyclotomic.

Step 4. There is a finite list of irreducible reciprocal factors that can divide $F(x) = f(x)x^n + 1$ as n varies.

Step 5. There is an n_0 such that if $n \geq n_0$, then every irreducible reciprocal factor of $F(x)$ is cyclotomic.

Suppose $g(x)$ is an irreducible reciprocal polynomial that divides $f(x)x^n + 1$ and $f(x)x^m + 1$ where $n > m$.

Step 4. There is a finite list of irreducible reciprocal factors that can divide $F(x) = f(x)x^n + 1$ as n varies.

Step 5. There is an n_0 such that if $n \geq n_0$, then every irreducible reciprocal factor of $F(x)$ is cyclotomic.

Suppose $g(x)$ is an irreducible reciprocal polynomial that divides $f(x)x^n + 1$ and $f(x)x^m + 1$ where $n > m$. Then $g(x)$ divides

$$x^{n-m}\big(f(x)x^m+1\big)-\big(f(x)x^n+1\big)$$

Step 4. There is a finite list of irreducible reciprocal factors that can divide $F(x) = f(x)x^n + 1$ as n varies.

Step 5. There is an n_0 such that if $n \geq n_0$, then every irreducible reciprocal factor of $F(x)$ is cyclotomic.

Suppose $g(x)$ is an irreducible reciprocal polynomial that divides $f(x)x^n + 1$ and $f(x)x^m + 1$ where $n > m$. Then $g(x)$ divides

$$x^{n-m}\big(f(x)x^m+1\big)-\big(f(x)x^n+1\big) = x^{n-m} - 1.$$

Step 4. There is a finite list of irreducible reciprocal factors that can divide $F(x) = f(x)x^n + 1$ as n varies.

Step 5. There is an n_0 such that if $n \geq n_0$, then every irreducible reciprocal factor of $F(x)$ is cyclotomic.

Suppose $g(x)$ is an irreducible reciprocal polynomial that divides $f(x)x^n + 1$ and $f(x)x^m + 1$ where $n > m$. Then $g(x)$ divides

$$x^{n-m}\big(f(x)x^m+1\big)-\big(f(x)x^n+1\big) = x^{n-m} - 1.$$

Therefore, each irreducible reciprocal polynomial that is a factor of $F(x)$ for more than one n is cyclotomic.

Step 4. There is a finite list of irreducible reciprocal factors that can divide $F(x) = f(x)x^n + 1$ as n varies.

Step 5. There is an n_0 such that if $n \geq n_0$, then every irreducible reciprocal factor of $F(x)$ is cyclotomic.

Suppose $g(x)$ is an irreducible reciprocal polynomial that divides $f(x)x^n + 1$ and $f(x)x^m + 1$ where $n > m$. Then $g(x)$ divides

$$x^{n-m}\big(f(x)x^m+1\big)-\big(f(x)x^n+1\big) = x^{n-m} - 1.$$

Therefore, each irreducible reciprocal polynomial that is a factor of $F(x)$ for more than one n is cyclotomic. Apply the result of Step 4.

Lemma (Schinzel). Let $f(x) \in \mathbb{Z}[x]$. Suppose that n is sufficiently large (depending on f). Then the non-reciprocal part of $F(x) = f(x)x^n + 1$ is irreducible over $\mathbb{Q}$ or identically ± 1 unless one of the following holds:

(i) $-f(x)$ is a pth power in $\mathbb{Q}[x]$ for some prime p dividing n.

(ii) $f(x)$ is 4 times a 4th power in $\mathbb{Q}[x]$ and n is divisible by 4.

Lemma (Schinzel). Let $f(x) \in \mathbb{Z}[x]$. Suppose that n is sufficiently large (depending on f). Then the non-reciprocal part of $F(x) = f(x)x^n + 1$ is irreducible over $\mathbb{Q}$ or identically ± 1 unless one of the following holds:

(i) $-f(x)$ is a pth power in $\mathbb{Q}[x]$ for some prime p dividing n.

(ii) $f(x)$ is 4 times a 4th power in $\mathbb{Q}[x]$ and n is divisible by 4.

Step 6. Suppose (i) and (ii) do not hold for $F(x)$ and n is large. Then $F(x)$ is divisible by a cyclotomic polynomial.

Step 6. Suppose (i) and (ii) do not hold for $F(x) = f(x)x^n + 1$ and n is large. Then $F(x)$ is divisible by a cyclotomic polynomial.

(i) $-f(x)$ is a pth power and $p|n$

(ii) $f(x)$ is 4 times a 4th power and $4|n$

Step 6. Suppose (i) and (ii) do not hold for $F(x) = f(x)x^n + 1$ and n is large. Then $F(x)$ is divisible by a cyclotomic polynomial.

(i) $-f(x)$ is a pth power and $p|n$

(ii) $f(x)$ is 4 times a 4th power and $4|n$

Claim: $f(x)$ is not 4 times a 4th power

Step 6. Suppose (i) and (ii) do not hold for $F(x) = f(x)x^n + 1$ and n is large. Then $F(x)$ is divisible by a cyclotomic polynomial.

(i) $-f(x)$ is a pth power and $p|n$
(ii) $f(x)$ is 4 times a 4th power and $4|n$

Claim: $f(x)$ is not 4 times a 4th power

Proof. Assume otherwise.

Step 6. Suppose (i) and (ii) do not hold for $F(x) = f(x)x^n + 1$ and n is large. Then $F(x)$ is divisible by a cyclotomic polynomial.

(i) $-f(x)$ is a pth power and $p|n$
(ii) $f(x)$ is 4 times a 4th power and $4|n$

Claim: $f(x)$ is not 4 times a 4th power

Proof. Assume otherwise. Consider $n = q$ where q is a large odd prime.

Step 6. Suppose (i) and (ii) do not hold for $F(x) = f(x)x^n + 1$ and n is large. Then $F(x)$ is divisible by a cyclotomic polynomial.

(i) $-f(x)$ is a pth power and $p|n$
(ii) $f(x)$ is 4 times a 4th power and $4|n$

Claim: $f(x)$ is not 4 times a 4th power

Proof. Assume otherwise. Consider $n = q$ where q is a large odd prime, so large that $-f(x)$ is not a qth power.

Step 6. Suppose (i) and (ii) do not hold for $F(x) = f(x)x^n + 1$ and n is large. Then $F(x)$ is divisible by a cyclotomic polynomial.

(i) $-f(x)$ is a pth power and $p|n$

(ii) $f(x)$ is 4 times a 4th power and $4|n$

Claim: $f(x)$ is not 4 times a 4th power

Proof. Assume otherwise. Consider $n = q$ where q is a large odd prime, so large that $-f(x)$ is not a qth power. Note that $4 \nmid n$.

Step 6. Suppose (i) and (ii) do not hold for $F(x) = f(x)x^n + 1$ and n is large. Then $F(x)$ is divisible by a cyclotomic polynomial.

(i) $-f(x)$ is a pth power and $p|n$

(ii) $f(x)$ is 4 times a 4th power and $4|n$

Claim: $f(x)$ is not 4 times a 4th power

Proof. Assume otherwise. Consider $n = q$ where q is a large odd prime, so large that $-f(x)$ is not a qth power. Note that $4 \nmid n$. Hence, (i) and (ii) do not hold.

Step 6. Suppose (i) and (ii) do not hold for $F(x) = f(x)x^n + 1$ and n is large. Then $F(x)$ is divisible by a cyclotomic polynomial.

$$\text{(i) } -f(x) \text{ is a } p\text{th power and } p|n$$
$$\text{(ii) } f(x) \text{ is } 4 \text{ times a } 4\text{th power and } 4|n$$

Claim: $f(x)$ is not 4 times a 4th power

Proof. Assume otherwise. Consider $n = q$ where q is a large odd prime, so large that $-f(x)$ is not a qth power. Note that $4 \nmid n$. Hence, (i) and (ii) do not hold. By Step 6, $F(x)$ is divisible by $\Phi_m(x)$ for some positive integer m.

Step 6. Suppose (i) and (ii) do not hold for $F(x) = f(x)x^n + 1$ and n is large. Then $F(x)$ is divisible by a cyclotomic polynomial.

Claim: $f(x)$ is not 4 times a 4th power

Proof. Assume otherwise. Consider $n = q$ where q is a large odd prime, so large that $-f(x)$ is not a qth power. Note that $4 \nmid n$. Hence, (i) and (ii) do not hold. By Step 6, $F(x)$ is divisible by $\Phi_m(x)$ for some positive integer m.

Step 6. Suppose (i) and (ii) do not hold for $F(x) = f(x)x^n + 1$ and n is large. Then $F(x)$ is divisible by a cyclotomic polynomial.

Claim: $f(x)$ is not 4 times a 4th power

Proof. Assume otherwise. Consider $n = q$ where q is a large odd prime, so large that $-f(x)$ is not a qth power. Note that $4 \nmid n$. Hence, (i) and (ii) do not hold. By Step 6, $F(x)$ is divisible by $\Phi_m(x)$ for some positive integer m. Let $\zeta = \zeta_m$ so that $F(\zeta) = 0$.

Step 6. Suppose (i) and (ii) do not hold for $F(x) = f(x)x^n + 1$ and n is large. Then $F(x)$ is divisible by a cyclotomic polynomial.

Claim: $f(x)$ is not 4 times a 4th power

Proof. Assume otherwise. Consider $n = q$ where q is a large odd prime, so large that $-f(x)$ is not a qth power. Note that $4 \nmid n$. Hence, (i) and (ii) do not hold. By Step 6, $F(x)$ is divisible by $\Phi_m(x)$ for some positive integer m. Let $\zeta = \zeta_m$ so that $F(\zeta) = 0$. Then $f(\zeta)\zeta^n = -1$.

Step 6. Suppose (i) and (ii) do not hold for $F(x) = f(x)x^n + 1$ and n is large. Then $F(x)$ is divisible by a cyclotomic polynomial.

Claim: $f(x)$ is not 4 times a 4th power

Proof. Assume otherwise. Consider $n = q$ where q is a large odd prime, so large that $-f(x)$ is not a qth power. Note that $4 \nmid n$. Hence, (i) and (ii) do not hold. By Step 6, $F(x)$ is divisible by $\Phi_m(x)$ for some positive integer m. Let $\zeta = \zeta_m$ so that $F(\zeta) = 0$. Then $f(\zeta)\zeta^n = -1$. By the assumption, $-1/4$ is a rational number that is an algebraic integer, giving a contradiction.

Step 6. Suppose (i) and (ii) do not hold for $F(x) = f(x)x^n + 1$ and n is large. Then $F(x)$ is divisible by a cyclotomic polynomial.

Claim: $f(x)$ is not 4 times a 4th power

Proof. Assume otherwise. Consider $n = q$ where q is a large odd prime, so large that $-f(x)$ is not a qth power. Note that $4 \nmid n$. Hence, (i) and (ii) do not hold. By Step 6, $F(x)$ is divisible by $\Phi_m(x)$ for some positive integer m. Let $\zeta = \zeta_m$ so that $F(\zeta) = 0$. Then $f(\zeta)\zeta^n = -1$. By the assumption, $-1/4$ is a rational number that is an algebraic integer, giving a contradiction. ■

Step 6. Suppose (i) and (ii) do not hold for $F(x) = f(x)x^n + 1$ and n is large. Then $F(x)$ is divisible by a cyclotomic polynomial.

Claim: $f(x)$ is not 4 times a 4th power

Step 6. Suppose (i) and (ii) do not hold for $F(x) = f(x)x^n + 1$ and n is large. Then $F(x)$ is divisible by a cyclotomic polynomial.

Claim: $f(x)$ is not 4 times a 4th power

Step 6. Suppose (i) does not hold for $F(x)$ and n is large. Then $F(x)$ is divisible by a cyclotomic polynomial.

Step 1. A covering of all large integers is a covering.

Step 1. A covering of all large integers is a covering.

Step 2. $\boldsymbol{f(0) \neq 0}$ and $\boldsymbol{f(x) \not\equiv 1}$.

Step 1. A covering of all large integers is a covering.

Step 2. $f(0) \neq 0$ and $f(x) \not\equiv 1$.

Step 3. $p|m \implies x^p = \zeta_m$ has no solutions $x \in \mathbb{Q}(\zeta_m)$.

Step 1. A covering of all large integers is a covering.

Step 2. $\boldsymbol{f(0) \neq 0}$ and $\boldsymbol{f(x) \not\equiv 1}$.

Step 3. $\boldsymbol{p|m \implies x^p \neq \zeta_m}$ for $\boldsymbol{x \in \mathbb{Q}(\zeta_m)}$.

Step 1. A covering of all large integers is a covering.

Step 2. $f(0) \neq 0$ and $f(x) \not\equiv 1$.

Step 3. $p|m \implies x^p \neq \zeta_m$ for $x \in \mathbb{Q}(\zeta_m)$.

Step 6. Suppose (i) does not hold for $F(x)$ and n is large. Then $F(x)$ is divisible by a cyclotomic polynomial.

(i) $-f(x)$ is a pth power and $p|n$

Step 6. Suppose (i) does not hold for $F(x)$ and n is large. Then $F(x)$ is divisible by a cyclotomic polynomial.

$$\text{(i) } -f(x) \text{ is a } p\text{th power and } p|n$$

Step 6. Suppose (i) does not hold for $F(x)$ and n is large. Then $F(x)$ is divisible by a cyclotomic polynomial.

$$\text{(i) } -f(x) \text{ is a } p\text{th power and } p|n$$

Let $m_1, m_2, \ldots, m_r$ be such that if $n \geq n_0$ and (i) does not hold, then $\Phi_{m_j}(x) | \big(f(x)x^n + 1 \big)$ for some j.

Step 6. Suppose (i) does not hold for $F(x)$ and n is large. Then $F(x)$ is divisible by a cyclotomic polynomial.

$$\text{(i) } -f(x) \text{ is a } p\text{th power and } p|n$$

Let $m_1, m_2, \dots, m_r$ be such that if $n \geq n_0$ and (i) does not hold, then $\Phi_{m_j}(x) | \big(f(x)x^n + 1\big)$ for some j.

Why is r finite?

Step 6. Suppose (i) does not hold for $F(x)$ and n is large. Then $F(x)$ is divisible by a cyclotomic polynomial.

$$\text{(i) } -f(x) \text{ is a } p\text{th power and } p|n$$

Let $m_1, m_2, \ldots, m_r$ be such that if $n \geq n_0$ and (i) does not hold, then $\Phi_{m_j}(x) | \big(f(x)x^n + 1\big)$ for some j.

Why is r finite?

Each reciprocal factor must divide $f(x)\tilde{f}(x) - x^{\deg f}$.

Step 6. Suppose (i) does not hold for $F(x)$ and n is large. Then $F(x)$ is divisible by a cyclotomic polynomial.

$$\text{(i) } -f(x) \text{ is a } p\text{th power and } p|n$$

Let $m_1, m_2, \ldots, m_r$ be such that if $n \geq n_0$ and (i) does not hold, then $\Phi_{m_j}(x) | \big(f(x)x^n + 1\big)$ for some j.

Step 6. Suppose (i) does not hold for $F(x)$ and n is large. Then $F(x)$ is divisible by a cyclotomic polynomial.

$$\text{(i) } -f(x) \text{ is a } p\text{th power and } p|n$$

Let $m_1, m_2, \ldots, m_r$ be such that if $n \geq n_0$ and (i) does not hold, then $\Phi_{m_j}(x)|\big(f(x)x^n + 1\big)$ for some j. For each $j \in \{1, 2, \ldots, r\}$, we may suppose that there is an a_j such that $\Phi_{m_j}(x)|\big(f(x)x^{a_j} + 1\big)$.

Step 6. Suppose (i) does not hold for $F(x)$ and n is large. Then $F(x)$ is divisible by a cyclotomic polynomial.

$$\text{(i) } -f(x) \text{ is a } p\text{th power and } p|n$$

Let $m_1, m_2, \dots, m_r$ be such that if $n \ge n_0$ and (i) does not hold, then $\Phi_{m_j}(x) | \big(f(x)x^n + 1\big)$ for some j. For each $j \in \{1, 2, \dots, r\}$, we may suppose that there is an a_j such that $\Phi_{m_j}(x) | \big(f(x)x^{a_j} + 1\big)$. Let $\mathcal{P}$ be the set of primes p for which $f(x)$ is minus a pth power.

Step 6. Suppose (i) does not hold for $F(x)$ and n is large. Then $F(x)$ is divisible by a cyclotomic polynomial.

$$\text{(i) } -f(x) \text{ is a } p\text{th power and } p|n$$

Let $m_1, m_2, \ldots, m_r$ be such that if $n \geq n_0$ and (i) does not hold, then $\Phi_{m_j}(x) | \big(f(x)x^n + 1\big)$ for some j. For each $j \in \{1, 2, \ldots, r\}$, we may suppose that there is an a_j such that $\Phi_{m_j}(x) | \big(f(x)x^{a_j} + 1\big)$. Let $\mathcal{P}$ be the set of primes p for which $f(x)$ is minus a pth power.

$$n \geq n_0 \implies \begin{cases} n \equiv a_j \pmod{m_j} \quad \text{(some } j\text{)} \\ \text{or} \\ n \equiv 0 \pmod{p} \quad \text{(some } p \in \mathcal{P}\text{)} \end{cases}$$

$$n \geq n_0 \implies \begin{cases} n \equiv a_j \pmod{m_j} \quad \text{(some } j\text{)} \\ \text{or} \\ n \equiv 0 \pmod{p} \quad \text{(some } p \in \mathcal{P}\text{)} \end{cases}$$

$$n \geq n_0 \implies \begin{cases} n \equiv a_j \pmod{m_j} \quad \text{(some } j\text{)} \\ \text{or} \\ n \equiv 0 \pmod{p} \quad \text{(some } p \in \mathcal{P}\text{)} \end{cases}$$

Suppose $\Phi_m(x) \mid (f(x)x^n + 1)$ and $p \mid m$ for some $p \in \mathcal{P}$.

$$
n \geq n_0 \implies \begin{cases} n \equiv a_j \pmod{m_j} \quad \text{(some } j\text{)} \\ \text{or} \\ n \equiv 0 \pmod{p} \quad \text{(some } p \in \mathcal{P}\text{)} \end{cases}
$$

Suppose $\Phi_m(x) | (f(x)x^n+1)$ and $p|m$ for some $p \in \mathcal{P}$.

We claim that $n \equiv 0 \pmod{p}$.

$$n \geq n_0 \implies \begin{cases} n \equiv a_j \pmod{m_j} \quad \text{(some } j\text{)} \\ \text{or} \\ n \equiv 0 \pmod{p} \quad \text{(some } p \in \mathcal{P}\text{)} \end{cases}$$

Suppose $\Phi_m(x) | (f(x)x^n+1)$ and $p|m$ for some $p \in \mathcal{P}$.

We claim that $n \equiv 0 \pmod{p}$.

Then we can remove m_j divisible by primes in $\mathcal{P}$
and still have a covering of the integers.

Step 3. $p|m \implies x^p \neq \zeta_m$ for $x \in \mathbb{Q}(\zeta_m)$.

Step 3. $p|m \implies x^p \neq \zeta_m$ for $x \in \mathbb{Q}(\zeta_m)$.

Suppose $\Phi_m(x)|(f(x)x^n+1)$ and $p|m$ for some $p \in \mathcal{P}$.

Step 3. $p|m \implies x^p \neq \zeta_m$ for $x \in \mathbb{Q}(\zeta_m)$.

Suppose $\Phi_m(x)|(f(x)x^n+1)$ and $p|m$ for some $p \in \mathcal{P}$. Then

$$-f(x) = g(x)^p$$

Step 3. $p|m \implies x^p \neq \zeta_m$ for $x \in \mathbb{Q}(\zeta_m)$.

Suppose $\Phi_m(x)|(f(x)x^n+1)$ and $p|m$ for some $p \in \mathcal{P}$. Then

$$-f(x) = g(x)^p \quad \text{and} \quad g(\zeta)^p\zeta^n = 1$$

for some $g(x) \in \mathbb{Z}[x]$ and for $\zeta = \zeta_m$.

Step 3. $p|m \Longrightarrow x^p \neq \zeta_m$ for $x \in \mathbb{Q}(\zeta_m)$.

Suppose $\Phi_m(x)|(f(x)x^n+1)$ and $p|m$ for some $p \in \mathcal{P}$. Then

$$-f(x) = g(x)^p \quad \text{and} \quad g(\zeta)^p\zeta^n = 1$$

for some $g(x) \in \mathbb{Z}[x]$ and for $\zeta = \zeta_m$. Fix integers u and v such that $-nu + pv = 1$.

Step 3. $p|m \Longrightarrow x^p \neq \zeta_m$ for $x \in \mathbb{Q}(\zeta_m)$.

Suppose $\Phi_m(x)|(f(x)x^n+1)$ and $p|m$ for some $p \in \mathcal{P}$. Then

$$-f(x) = g(x)^p \quad \text{and} \quad g(\zeta)^p \zeta^n = 1$$

for some $g(x) \in \mathbb{Z}[x]$ and for $\zeta = \zeta_m$. Fix integers u and v such that $-nu + pv = 1$. Then

$$g(\zeta)^p = \zeta^{-n}$$

Step 3. $p|m \implies x^p \neq \zeta_m$ for $x \in \mathbb{Q}(\zeta_m)$.

Suppose $\Phi_m(x) | (f(x)x^n+1)$ and $p|m$ for some $p \in \mathcal{P}$. Then

$$-f(x) = g(x)^p \quad \text{and} \quad g(\zeta)^p \zeta^n = 1$$

for some $g(x) \in \mathbb{Z}[x]$ and for $\zeta = \zeta_m$. Fix integers u and v such that $-nu + pv = 1$. Then

$$g(\zeta)^p = \zeta^{-n} \implies g(\zeta)^{pu} = \zeta^{-nu} = \zeta^{1-pv}$$

Step 3. $p|m \implies x^p \neq \zeta_m$ for $x \in \mathbb{Q}(\zeta_m)$.

Suppose $\Phi_m(x)|(f(x)x^n+1)$ and $p|m$ for some $p \in \mathcal{P}$. Then

$$-f(x) = g(x)^p \quad \text{and} \quad g(\zeta)^p \zeta^n = 1$$

for some $g(x) \in \mathbb{Z}[x]$ and for $\zeta = \zeta_m$. Fix integers u and v such that $-nu + pv = 1$. Then

$$\begin{aligned} g(\zeta)^p = \zeta^{-n} &\implies g(\zeta)^{pu} = \zeta^{-nu} = \zeta^{1-pv} \\ &\implies \left(g(\zeta)^u \zeta^v\right)^p = \zeta \end{aligned}$$

Step 3. $p|m \implies x^p \neq \zeta_m$ for $x \in \mathbb{Q}(\zeta_m)$.

Suppose $\Phi_m(x)|(f(x)x^n+1)$ and $p|m$ for some $p \in \mathcal{P}$. Then

$$-f(x) = g(x)^p \quad \text{and} \quad g(\zeta)^p\zeta^n = 1$$

for some $g(x) \in \mathbb{Z}[x]$ and for $\zeta = \zeta_m$. Fix integers u and v such that $-nu + pv = 1$. Then

$$\begin{aligned} g(\zeta)^p = \zeta^{-n} &\implies g(\zeta)^{pu} = \zeta^{-nu} = \zeta^{1-pv} \\ &\implies \left(g(\zeta)^u\zeta^v\right)^p = \zeta \end{aligned}$$

Step 3. $p|m \implies x^p \neq \zeta_m$ for $x \in \mathbb{Q}(\zeta_m)$.

Suppose $\Phi_m(x)|(f(x)x^n+1)$ and $p|m$ for some $p \in \mathcal{P}$. Then

$$-f(x) = g(x)^p \quad \text{and} \quad g(\zeta)^p \zeta^n = 1$$

for some $g(x) \in \mathbb{Z}[x]$ and for $\zeta = \zeta_m$. Fix integers u and v such that $-nu + pv = 1$. Then

$$\begin{aligned} g(\zeta)^p = \zeta^{-n} \implies & \ g(\zeta)^{pu} = \zeta^{-nu} = \zeta^{1-pv} \\ \implies & \ \left(g(\zeta)^u \zeta^v\right)^p = \zeta \end{aligned}$$

Step 3. $p|m \implies x^p \neq \zeta_m$ for $x \in \mathbb{Q}(\zeta_m)$.

Suppose $\Phi_m(x) | (f(x)x^n+1)$ and $p|m$ for some $p \in \mathcal{P}$. Then

$$-f(x) = g(x)^p \quad \text{and} \quad g(\zeta)^p \zeta^n = 1$$

for some $g(x) \in \mathbb{Z}[x]$ and for $\zeta = \zeta_m$. Fix integers u and v such that $-nu + pv = 1$. Then

$$\begin{aligned} g(\zeta)^p = \zeta^{-n} &\implies g(\zeta)^{pu} = \zeta^{-nu} = \zeta^{1-pv} \\ &\implies \left(g(\zeta)^u \zeta^v\right)^p = \zeta \end{aligned}$$

Step 3. $p|m \implies x^p \neq \zeta_m$ for $x \in \mathbb{Q}(\zeta_m)$.

Suppose $\Phi_m(x)|(f(x)x^n+1)$ and $p|m$ for some $p \in \mathcal{P}$. Then

$$-f(x) = g(x)^p \quad \text{and} \quad g(\zeta)^p\zeta^n = 1$$

for some $g(x) \in \mathbb{Z}[x]$ and for $\zeta = \zeta_m$. Fix integers u and v such that $-nu + pv = 1$. Then

$$\begin{aligned} g(\zeta)^p = \zeta^{-n} &\implies g(\zeta)^{pu} = \zeta^{-nu} = \zeta^{1-pv} \\ &\implies \left(g(\zeta)^u\zeta^v\right)^p = \zeta \end{aligned}$$

Step 3. $p|m \implies x^p \neq \zeta_m$ for $x \in \mathbb{Q}(\zeta_m)$.

Suppose $\Phi_m(x)|(f(x)x^n+1)$ and $p|m$ for some $p \in \mathcal{P}$. Then

$$-f(x) = g(x)^p \quad \text{and} \quad g(\zeta)^p\zeta^n = 1$$

for some $g(x) \in \mathbb{Z}[x]$ and for $\zeta = \zeta_m$. Fix integers u and v such that $-nu + pv = 1$. Then

$$\begin{aligned} g(\zeta)^p = \zeta^{-n} &\implies g(\zeta)^{pu} = \zeta^{-nu} = \zeta^{1-pv} \\ &\implies \left(g(\zeta)^u\zeta^v\right)^p = \zeta, \end{aligned}$$

a contradiction.

Step 3. $p|m \implies x^p \neq \zeta_m$ for $x \in \mathbb{Q}(\zeta_m)$.

Suppose $\Phi_m(x) | (f(x)x^n + 1)$ and $p|m$ for some $p \in \mathcal{P}$. Then

$$-f(x) = g(x)^p \quad \text{and} \quad g(\zeta)^p \zeta^n = 1$$

for some $g(x) \in \mathbb{Z}[x]$ and for $\zeta = \zeta_m$. Fix integers u and v such that $-nu + pv = 1$. Then

$$\begin{aligned} g(\zeta)^p = \zeta^{-n} &\implies g(\zeta)^{pu} = \zeta^{-nu} = \zeta^{1-pv} \\ &\implies \left(g(\zeta)^u \zeta^v\right)^p = \zeta, \end{aligned}$$

a contradiction.

Step 3. $p|m \implies x^p \neq \zeta_m$ for $x \in \mathbb{Q}(\zeta_m)$.

Suppose $\Phi_m(x)|(f(x)x^n+1)$ and $p|m$ for some $p \in \mathcal{P}$. Then

$$-f(x) = g(x)^p \quad \text{and} \quad g(\zeta)^p\zeta^n = 1$$

for some $g(x) \in \mathbb{Z}[x]$ and for $\zeta = \zeta_m$. Fix integers u and v such that $-nu + pv = 1$. Then

$$\begin{aligned} g(\zeta)^p = \zeta^{-n} &\implies g(\zeta)^{pu} = \zeta^{-nu} = \zeta^{1-pv} \\ &\implies \left(g(\zeta)^u\zeta^v\right)^p = \zeta, \end{aligned}$$

a contradiction. We deduce then that $p|n$.

Step 3. $p|m \implies x^p \neq \zeta_m$ for $x \in \mathbb{Q}(\zeta_m)$.

Suppose $\Phi_m(x)|(f(x)x^n+1)$ and $p|m$ for some $p \in \mathcal{P}$. Then

$$-f(x) = g(x)^p \quad \text{and} \quad g(\zeta)^p \zeta^n = 1$$

for some $g(x) \in \mathbb{Z}[x]$ and for $\zeta = \zeta_m$. Fix integers u and v such that $-nu + pv = 1$. Then

$$\begin{aligned} g(\zeta)^p = \zeta^{-n} \implies & g(\zeta)^{pu} = \zeta^{-nu} = \zeta^{1-pv} \\ \implies & \left(g(\zeta)^u \zeta^v\right)^p = \zeta, \end{aligned}$$

a contradiction. We deduce then that $p|n$.

$$n \geq n_0 \implies \begin{cases} n \equiv a_j \pmod{m_j} \quad \text{(some } j\text{)} \\ \text{or} \\ n \equiv 0 \pmod{p} \quad \text{(some } p \in \mathcal{P}\text{)} \end{cases}$$

Suppose $\Phi_m(x) | (f(x)x^n + 1)$ and $p | m$ for some $p \in \mathcal{P}$.

We claim that $n \equiv 0 \pmod{p}$.

Then we can remove m_j divisible by primes in $\mathcal{P}$ and still have a covering of the integers.

Covering:

$$
\begin{array}{ll}
n \equiv a_j \pmod{m_j} & (1 \le j \le r) \\
n \equiv 0 \pmod{p} & (p \in \mathcal{P})
\end{array}
$$

Covering:
$$\begin{aligned} n &\equiv a_j \pmod{m_j} \quad (1 \le j \le r) \\ n &\equiv 0 \pmod{p} \qquad\qquad (p \in \mathcal{P}) \end{aligned}$$

$p \nmid m_j$ for all $p \in \mathcal{P}$ and all $j \in \{1, 2, \dots, r\}$

Covering:

$$\begin{aligned} x &\equiv a_j \pmod{m_j} \quad & (1 \le j \le r) \\ x &\equiv 0 \pmod{p} \quad & (p \in \mathcal{P}) \end{aligned}$$

$p \nmid m_j$ for all $p \in \mathcal{P}$ and all $j \in \{1, 2, \ldots, r\}$

Covering:

$$\begin{aligned} x &\equiv a_j \pmod{m_j} \quad && (1 \leq j \leq r) \\ x &\equiv 0 \pmod{p} && (p \in \mathcal{P}) \end{aligned}$$

$$p \nmid m_j \text{ for all } p \in \mathcal{P} \text{ and all } j \in \{1, 2, \ldots, r\}$$

Claim: Suppose $m_j = 2^t m_0$ and $m_i = 2^s m_0$, where m_0 is an odd integer > 1, and t and s are integers with $t > s \geq 0$. Then $a_j \equiv a_i \pmod{m_0}$.

Covering:
$$x \equiv a_j \pmod{m_j} \quad (1 \le j \le r)$$
$$x \equiv 0 \pmod{p} \quad (p \in \mathcal{P})$$

$p \nmid m_j$ for all $p \in \mathcal{P}$ and all $j \in \{1, 2, \ldots, r\}$

Claim: Suppose $m_j = 2^t m_0$ and $m_i = 2^s m_0$, where m_0 is an odd integer > 1, and t and s are integers with $t > s \ge 0$. Then $a_j \equiv a_i \pmod{m_0}$.

Why?

Covering:
$$\begin{aligned} x &\equiv a_j \pmod{m_j} \quad && (1 \le j \le r) \\ x &\equiv 0 \pmod{p} && (p \in \mathcal{P}) \end{aligned}$$

$$p \nmid m_j \text{ for all } p \in \mathcal{P} \text{ and all } j \in \{1, 2, \ldots, r\}$$

Claim: Suppose $m_j = 2^t m_0$ and $m_i = 2^s m_0$, where m_0 is an odd integer > 1, and t and s are integers with $t > s \ge 0$. Then $a_j \equiv a_i \pmod{m_0}$.

Why?

Not why is this true, but why do we care?

Covering:

$$x \equiv a_j \pmod{m_j} \quad (1 \le j \le r)$$
$$x \equiv 0 \pmod{p} \qquad (p \in \mathcal{P})$$

$p \nmid m_j$ for all $p \in \mathcal{P}$ and all $j \in \{1, 2, \ldots, r\}$

Claim: Suppose $m_j = 2^t m_0$ and $m_i = 2^s m_0$, where m_0 is an odd integer > 1, and t and s are integers with $t > s \ge 0$. Then $a_j \equiv a_i \pmod{m_0}$.

Why?

Not why is this true, but why do I care?

Covering:
$$x \equiv a_j \pmod{m_j} \quad (1 \le j \le r)$$
$$x \equiv 0 \pmod{p} \qquad (p \in \mathcal{P})$$

$p \nmid m_j$ for all $p \in \mathcal{P}$ and all $j \in \{1, 2, \ldots, r\}$

Claim: Suppose $m_j = 2^t m_0$ and $m_i = 2^s m_0$, where m_0 is an odd integer > 1, and t and s are integers with $t > s \ge 0$. Then $a_j \equiv a_i \pmod{m_0}$.

Replace $x \equiv a_j \pmod{m_j}$ and $x \equiv a_i \pmod{m_i}$ with $x \equiv a_j \pmod{m_0}$.

Covering: $$\begin{aligned} &x \equiv a_j \pmod{m_j} \quad (1 \leq j \leq r) \\ &x \equiv 0 \pmod{p} \qquad\qquad (p \in \mathcal{P}) \end{aligned}$$

$$p \nmid m_j \text{ for all } p \in \mathcal{P} \text{ and all } j \in \{1, 2, \ldots, r\}$$

Claim: Suppose $m_j = 2^t m_0$ and $m_i = 2^s m_0$, where m_0 is an odd integer > 1, and t and s are integers with $t > s \geq 0$. Then $a_j \equiv a_i \pmod{m_0}$.

Replace $x \equiv a_j \pmod{m_j}$ and $x \equiv a_i \pmod{m_i}$ with $x \equiv a_j \pmod{m_0}$. If for some j there is no i, still replace $x \equiv a_j \pmod{m_j}$ with $x \equiv a_j \pmod{m_0}$.

Covering: $$\begin{array}{ll} x \equiv a_j \pmod{m_j} & (1 \le j \le r) \\ x \equiv 0 \pmod{p} & (p \in \mathcal{P}) \end{array}$$

$p \nmid m_j$ for all $p \in \mathcal{P}$ and all $j \in \{1, 2, \ldots, r\}$

Claim: Suppose $m_j = 2^t m_0$ and $m_i = 2^s m_0$, where m_0 is an odd integer > 1, and t and s are integers with $t > s \ge 0$. Then $a_j \equiv a_i \pmod{m_0}$.

Replace $x \equiv a_j \pmod{m_j}$ and $x \equiv a_i \pmod{m_i}$ with $x \equiv a_j \pmod{m_0}$. If for some j there is no i, still replace $x \equiv a_j \pmod{m_j}$ with $x \equiv a_j \pmod{m_0}$. Then there is a covering with moduli that are distinct odd numbers together with possibly powers of 2.

$\exists$ a covering with distinct odd moduli and powers of $\mathbf{2}$

$\exists$ a covering with distinct odd moduli and powers of $\mathbf{2}$

Suppose the complete list of moduli that are powers of $\mathbf{2}$ are from the set $\{\mathbf{2}, \mathbf{2}^{\mathbf{2}}, \dots, \mathbf{2}^{\boldsymbol{k}}\}$.

$\exists$ a covering with distinct odd moduli and powers of $\mathbf{2}$

Suppose the complete list of moduli that are powers of $\mathbf{2}$ are from the set $\{\mathbf{2}, \mathbf{2^2}, \ldots, \mathbf{2^k}\}$.

A congruence mod $\mathbf{2}$ "covers" $\mathbf{2^{k-1}}$ classes mod $\mathbf{2^k}$.

$\exists$ a covering with distinct odd moduli and powers of $\mathbf{2}$

Suppose the complete list of moduli that are powers of $\mathbf{2}$ are from the set $\{\mathbf{2}, \mathbf{2}^{\mathbf{2}}, \ldots, \mathbf{2}^{k}\}$.

A congruence mod $\mathbf{2}$ "covers" $\mathbf{2}^{k-1}$ classes mod $\mathbf{2}^{k}$.
A congruence mod $\mathbf{2}^{\mathbf{2}}$ "covers" $\mathbf{2}^{k-2}$ classes mod $\mathbf{2}^{k}$.

$\exists$ a covering with distinct odd moduli and powers of $\mathbf{2}$

Suppose the complete list of moduli that are powers of $\mathbf{2}$ are from the set $\{\mathbf{2}, \mathbf{2}^{\mathbf{2}}, \ldots, \mathbf{2}^{\boldsymbol{k}}\}$.

A congruence mod $\mathbf{2}$ "covers" $\mathbf{2}^{\boldsymbol{k}-\mathbf{1}}$ classes mod $\mathbf{2}^{\boldsymbol{k}}$.
A congruence mod $\mathbf{2}^{\mathbf{2}}$ "covers" $\mathbf{2}^{\boldsymbol{k}-\mathbf{2}}$ classes mod $\mathbf{2}^{\boldsymbol{k}}$.

$$\vdots \qquad\qquad \vdots \qquad\qquad \vdots$$

A congruence mod $\mathbf{2}^{\boldsymbol{k}}$ "covers" $\mathbf{2}^{\mathbf{0}}$ classes mod $\mathbf{2}^{\boldsymbol{k}}$.

$\exists$ a covering with distinct odd moduli and powers of 2

Suppose the complete list of moduli that are powers of 2 are from the set $\{2, 2^2, \dots, 2^k\}$.

A congruence mod 2 "covers" 2^{k-1} classes mod 2^k.
A congruence mod 2^2 "covers" 2^{k-2} classes mod 2^k.

$$\vdots \qquad\qquad \vdots \qquad\qquad \vdots$$

A congruence mod 2^k "covers" 2^0 classes mod 2^k.

$\exists$ a covering with distinct odd moduli and powers of 2

Suppose the complete list of moduli that are powers of 2 are from the set $\{2, 2^2, \ldots, 2^k\}$.

A congruence mod 2 "covers" 2^{k-1} classes mod 2^k.
A congruence mod 2^2 "covers" 2^{k-2} classes mod 2^k.

$$\vdots \qquad\qquad \vdots \qquad\qquad \vdots$$

A congruence mod 2^k "covers" 2^0 classes mod 2^k.

No integer satisfying $x \equiv a \pmod{2^k}$ satisfies one of the congruences in our covering with moduli a power of 2.

$\exists$ a covering with distinct odd moduli and powers of $\mathbf{2}$

No integer satisfying $\boldsymbol{x \equiv a \pmod{2^k}}$ satisfies one of the congruences in our covering with moduli a power of $\mathbf{2}$.

$\exists$ a covering with distinct odd moduli and powers of $\mathbf{2}$

No integer satisfying $x \equiv a \pmod{2^k}$ satisfies one of the congruences in our covering with moduli a power of $\mathbf{2}$. Let $x \equiv a'_j \pmod{m'_j}$ be the congruences with m'_j odd.

$\exists$ a covering with distinct odd moduli and powers of $\mathbf{2}$

No integer satisfying $x \equiv a \pmod{2^k}$ satisfies one of the congruences in our covering with moduli a power of $\mathbf{2}$. Let $x \equiv a'_j \pmod{m'_j}$ be the congruences with m'_j odd.

$2^k u + v\Big(\prod m'_j\Big) = 1$ for some $u \in \mathbb{Z}$ and $v \in \mathbb{Z}$

$\exists$ a covering with distinct odd moduli and powers of $\mathbf{2}$

No integer satisfying $x \equiv a \pmod{2^k}$ satisfies one of the congruences in our covering with moduli a power of $\mathbf{2}$. Let $x \equiv a'_j \pmod{m'_j}$ be the congruences with m'_j odd.

$$2^k u + v\Big(\prod m'_j\Big) = 1 \quad \text{for some } u \in \mathbb{Z} \text{ and } v \in \mathbb{Z}$$

Let $n \in \mathbb{Z}$.

$\exists$ a covering with distinct odd moduli and powers of $\mathbf{2}$

No integer satisfying $x \equiv a \pmod{2^k}$ satisfies one of the congruences in our covering with moduli a power of 2. Let $x \equiv a'_j \pmod{m'_j}$ be the congruences with m'_j odd.

$$2^k u + v\Big(\prod m'_j\Big) = 1 \quad \text{for some } u \in \mathbb{Z} \text{ and } v \in \mathbb{Z}$$

Let $n \in \mathbb{Z}$. Consider $m = a + 2^k u(n - a)$.

$\exists$ a covering with distinct odd moduli and powers of 2

No integer satisfying $x \equiv a \pmod{2^k}$ satisfies one of the congruences in our covering with moduli a power of 2. Let $x \equiv a'_j \pmod{m'_j}$ be the congruences with m'_j odd.

$$2^k u + v\Big(\prod m'_j\Big) = 1 \quad \text{for some } u \in \mathbb{Z} \text{ and } v \in \mathbb{Z}$$

Let $n \in \mathbb{Z}$. Consider $m = a + 2^k u(n - a)$. Then

$$m \equiv a \pmod{2^k} \implies m \equiv a'_j \pmod{m'_j}$$

for some j.

$\exists$ a covering with distinct odd moduli and powers of $\mathbf{2}$

No integer satisfying $x \equiv a \pmod{2^k}$ satisfies one of the congruences in our covering with moduli a power of $\mathbf{2}$. Let $x \equiv a'_j \pmod{m'_j}$ be the congruences with m'_j odd.

$$2^k u + v\Big(\prod m'_j\Big) = 1 \quad \text{for some } u \in \mathbb{Z} \text{ and } v \in \mathbb{Z}$$

Let $n \in \mathbb{Z}$. Consider $m = a + 2^k u(n - a)$. Then

$$m \equiv a \pmod{2^k} \implies m \equiv a'_j \pmod{m'_j}$$

for some j.

$\exists$ a covering with distinct odd moduli and powers of $\mathbf{2}$

No integer satisfying $x \equiv a \pmod{2^k}$ satisfies one of the congruences in our covering with moduli a power of $\mathbf{2}$. Let $x \equiv a'_j \pmod{m'_j}$ be the congruences with m'_j odd.

$$2^k u + v\left(\prod m'_j\right) = 1 \quad \text{for some } u \in \mathbb{Z} \text{ and } v \in \mathbb{Z}$$

Let $n \in \mathbb{Z}$. Consider $m = a + 2^k u(n - a)$. Then

$$m \equiv a \pmod{2^k} \implies m \equiv a'_j \pmod{m'_j}$$

for some j.

$\exists$ a covering with distinct odd moduli and powers of 2

No integer satisfying $x \equiv a \pmod{2^k}$ satisfies one of the congruences in our covering with moduli a power of 2. Let $x \equiv a'_j \pmod{m'_j}$ be the congruences with m'_j odd.

$$2^k u + v\Big(\prod m'_j\Big) = 1 \implies 2^k u \equiv 1 \pmod{m'_j}$$

Let $n \in \mathbb{Z}$. Consider $m = a + 2^k u(n - a)$. Then

$$m \equiv a \pmod{2^k} \implies m \equiv a'_j \pmod{m'_j}$$

for some j.

$\exists$ a covering with distinct odd moduli and powers of 2

No integer satisfying $x \equiv a \pmod{2^k}$ satisfies one of the congruences in our covering with moduli a power of 2. Let $x \equiv a'_j \pmod{m'_j}$ be the congruences with m'_j odd.

$$2^k u + v\Big(\prod m'_j\Big) = 1 \implies 2^k u \equiv 1 \pmod{m'_j}$$

Let $n \in \mathbb{Z}$. Consider $m = a + 2^k u(n-a)$. Then

$$m \equiv a \pmod{2^k} \implies m \equiv a'_j \pmod{m'_j}$$

for some j. Thus,

$$n \equiv m \pmod{m'_j}.$$

$\exists$ a covering with distinct odd moduli and powers of $\mathbf{2}$

No integer satisfying $x \equiv a \pmod{2^k}$ satisfies one of the congruences in our covering with moduli a power of 2. Let $x \equiv a'_j \pmod{m'_j}$ be the congruences with m'_j odd.

$$2^k u + v\Big(\prod m'_j\Big) = 1 \implies 2^k u \equiv 1 \pmod{m'_j}$$

Let $n \in \mathbb{Z}$. Consider $m = a + 2^k u(n-a)$. Then

$$m \equiv a \pmod{2^k} \implies m \equiv a'_j \pmod{m'_j}$$

for some j. Thus,

$$n \equiv m \pmod{m'_j}.$$

$\exists$ a covering with distinct odd moduli and powers of 2

No integer satisfying $x \equiv a \pmod{2^k}$ satisfies one of the congruences in our covering with moduli a power of 2. Let $x \equiv a'_j \pmod{m'_j}$ be the congruences with m'_j odd.

$$2^k u + v\Big(\prod m'_j\Big) = 1 \implies 2^k u \equiv 1 \pmod{m'_j}$$

Let $n \in \mathbb{Z}$. Consider $m = a + 2^k u(n - a)$. Then

$$m \equiv a \pmod{2^k} \implies m \equiv a'_j \pmod{m'_j}$$

for some j. Thus,

$$n \equiv m \equiv a'_j \pmod{m'_j}.$$

$\exists$ a covering with distinct odd moduli

No integer satisfying $x \equiv a \pmod{2^k}$ satisfies one of the congruences in our covering with moduli a power of 2. Let $x \equiv a'_j \pmod{m'_j}$ be the congruences with m'_j odd.

$$2^k u + v\Big(\prod m'_j\Big) = 1 \implies 2^k u \equiv 1 \pmod{m'_j}$$

Let $n \in \mathbb{Z}$. Consider $m = a + 2^k u(n - a)$. Then

$$m \equiv a \pmod{2^k} \implies m \equiv a'_j \pmod{m'_j}$$

for some j. Thus,

$$n \equiv m \equiv a'_j \pmod{m'_j}.$$

Covering:
$$\begin{aligned} x &\equiv a_j \pmod{m_j} \quad (1 \le j \le r) \\ x &\equiv 0 \pmod{p} \qquad\qquad (p \in \mathcal{P}) \end{aligned}$$

$$p \nmid m_j \text{ for all } p \in \mathcal{P} \text{ and all } j \in \{1, 2, \ldots, r\}$$

Claim: Suppose $m_j = 2^t m_0$ and $m_i = 2^s m_0$, where m_0 is an odd integer > 1, and t and s are integers with $t > s \ge 0$. Then $a_j \equiv a_i \pmod{m_0}$.

Covering:
$$\begin{aligned} x &\equiv a_j \pmod{m_j} \quad && (1 \le j \le r) \\ x &\equiv 0 \pmod{p} \quad && (p \in \mathcal{P}) \end{aligned}$$

$$p \nmid m_j \text{ for all } p \in \mathcal{P} \text{ and all } j \in \{1, 2, \ldots, r\}$$

Claim: Suppose $m_j = 2^t m_0$ and $m_i = 2^s m_0$, where m_0 is an odd integer > 1, and t and s are integers with $t > s \ge 0$. Then $a_j \equiv a_i \pmod{m_0}$.

Lemma 2 (Apostol). Let n and m be positive integers with $n > m$. The resultant of $\Phi_n(x)$ and $\Phi_m(x)$ is divisible by a prime p if and only if n/m is a power of p.

Covering:
$$\begin{aligned} x &\equiv a_j \pmod{m_j} \quad (1 \le j \le r) \\ x &\equiv 0 \pmod{p} \quad (p \in \mathcal{P}) \end{aligned}$$

$p \nmid m_j$ for all $p \in \mathcal{P}$ and all $j \in \{1, 2, \ldots, r\}$

Claim: Suppose $m_j = 2^t m_0$ and $m_i = 2^s m_0$, where m_0 is an odd integer > 1, and t and s are integers with $t > s \geq 0$. Then $a_j \equiv a_i \pmod{m_0}$.

Covering:
$$\begin{aligned} x &\equiv a_j \pmod{m_j} \quad (1 \le j \le r) \\ x &\equiv 0 \pmod{p} \quad (p \in \mathcal{P}) \end{aligned}$$

Claim: Suppose $m_j = 2^t m_0$ and $m_i = 2^s m_0$, where m_0 is an odd integer > 1, and t and s are integers with $t > s \ge 0$. Then $a_j \equiv a_i \pmod{m_0}$.

Covering:
$$\begin{aligned} &x \equiv a_j \pmod{m_j} \quad (1 \le j \le r) \\ &x \equiv 0 \pmod{p} \qquad\qquad (p \in \mathcal{P}) \end{aligned}$$

Claim: Suppose $m_j = 2^t m_0$ and $m_i = 2^s m_0$, where m_0 is an odd integer > 1, and t and s are integers with $t > s \ge 0$. Then $a_j \equiv a_i \pmod{m_0}$.

$$m_j = 2^t m_0,\ m_i = 2^s m_0 \implies a_j \equiv a_i \pmod{m_0}$$

Covering:

$$\begin{aligned} x &\equiv a_j \pmod{m_j} \quad (1 \le j \le r) \\ x &\equiv 0 \pmod{p} \qquad\qquad (p \in \mathcal{P}) \end{aligned}$$

Claim: Suppose $m_j = 2^t m_0$ and $m_i = 2^s m_0$, where m_0 is an odd integer > 1, and t and s are integers with $t > s \ge 0$. Then $a_j \equiv a_i \pmod{m_0}$.

$$m_j = 2^t m_0,\ m_i = 2^s m_0 \implies a_j \equiv a_i \pmod{m_0}$$

Covering:

$$x \equiv a_j \pmod{m_j} \quad (1 \le j \le r)$$
$$x \equiv 0 \pmod{p} \qquad (p \in \mathcal{P})$$

Claim: Suppose $m_j = 2^t m_0$ and $m_i = 2^s m_0$, where m_0 is an odd integer > 1, and t and s are integers with $t > s \ge 0$. Then $a_j \equiv a_i \pmod{m_0}$.

$$m_j = 2^t m_0,\ m_i = 2^s m_0 \implies a_j \equiv a_i \pmod{m_0}$$

$$m_j = 2^t m_0,\ m_i = 2^s m_0 \implies a_j \equiv a_i \pmod{m_0}$$

$$m_j = 2^t m_0,\ m_i = 2^s m_0 \implies a_j \equiv a_i \pmod{m_0}$$

$$\Phi_{pn}(x) = \begin{cases} & \text{if } p | n \\ & \text{if } p \nmid n \end{cases}$$

$$m_j = 2^t m_0,\ m_i = 2^s m_0 \implies a_j \equiv a_i \pmod{m_0}$$

$$\Phi_{pn}(x) = \begin{cases} \Phi_n(x^p) & \text{if } p \mid n \\ & \text{if } p \nmid n \end{cases}$$

$$m_j = 2^t m_0,\ m_i = 2^s m_0 \implies a_j \equiv a_i \pmod{m_0}$$

$$\Phi_{pn}(x) = \begin{cases} \Phi_n(x^p) & \text{if } p|n \\ \Phi_n(x^p)/\Phi_n(x) & \text{if } p \nmid n \end{cases}$$

$$m_j = 2^t m_0,\ m_i = 2^s m_0 \implies a_j \equiv a_i \pmod{m_0}$$

$$\Phi_{pn}(x) = \begin{cases} \Phi_n(x^p) & \text{if } p \mid n \\ \Phi_n(x^p)/\Phi_n(x) & \text{if } p \nmid n \end{cases}$$

$$\Phi_{2n}(x) = \Phi_n(-x) \quad \text{for } n > 1 \text{ odd}$$

$$m_j = 2^t m_0,\ m_i = 2^s m_0 \implies a_j \equiv a_i \pmod{m_0}$$

$$\Phi_{pn}(x) = \begin{cases} \Phi_n(x^p) & \text{if } p \mid n \\ \Phi_n(x^p)/\Phi_n(x) & \text{if } p \nmid n \end{cases}$$

$$\Phi_{2n}(x) = \Phi_n(-x) \quad \text{for } n > 1 \text{ odd}$$

$$\Phi_{2^t m_0}(x)$$

$$m_j = 2^t m_0,\ m_i = 2^s m_0 \implies a_j \equiv a_i \pmod{m_0}$$

$$\Phi_{pn}(x) = \begin{cases} \Phi_n(x^p) & \text{if } p|n \\ \Phi_n(x^p)/\Phi_n(x) & \text{if } p \nmid n \end{cases}$$

$$\Phi_{2n}(x) = \Phi_n(-x) \quad \text{for } n > 1 \text{ odd}$$

$$\Phi_{2^t m_0}(x) = \Phi_{2^{t-1} m_0}(x^2)$$

$$m_j = 2^t m_0,\ m_i = 2^s m_0 \implies a_j \equiv a_i \pmod{m_0}$$

$$\Phi_{pn}(x) = \begin{cases} \Phi_n(x^p) & \text{if } p | n \\ \Phi_n(x^p)/\Phi_n(x) & \text{if } p \nmid n \end{cases}$$

$$\Phi_{2n}(x) = \Phi_n(-x) \quad \text{for } n > 1 \text{ odd}$$

$$\Phi_{2^t m_0}(x) = \Phi_{2^{t-1} m_0}(x^2) = \Phi_{2^{t-2} m_0}(x^{2^2})$$

$$m_j = 2^t m_0,\ m_i = 2^s m_0 \implies a_j \equiv a_i \pmod{m_0}$$

$$\Phi_{pn}(x) = \begin{cases} \Phi_n(x^p) & \text{if } p|n \\ \Phi_n(x^p)/\Phi_n(x) & \text{if } p \nmid n \end{cases}$$

$$\Phi_{2n}(x) = \Phi_n(-x) \quad \text{for } n > 1 \text{ odd}$$

$$\begin{aligned} \Phi_{2^t m_0}(x) &= \Phi_{2^{t-1} m_0}(x^2) = \Phi_{2^{t-2} m_0}(x^{2^2}) \\ &= \Phi_{2^{t-3} m_0}(x^{2^3}) = \cdots = \Phi_{2m_0}(x^{2^{t-1}}) \end{aligned}$$

$$m_j = 2^t m_0,\ m_i = 2^s m_0 \implies a_j \equiv a_i \pmod{m_0}$$

$$\Phi_{pn}(x) = \begin{cases} \Phi_n(x^p) & \text{if } p \mid n \\ \Phi_n(x^p)/\Phi_n(x) & \text{if } p \nmid n \end{cases}$$

$$\Phi_{2n}(x) = \Phi_n(-x) \quad \text{for } n > 1 \text{ odd}$$

$$\begin{aligned} \Phi_{2^t m_0}(x) &= \Phi_{2^{t-1} m_0}(x^2) = \Phi_{2^{t-2} m_0}(x^{2^2}) \\ &= \Phi_{2^{t-3} m_0}(x^{2^3}) = \cdots = \Phi_{2 m_0}(x^{2^{t-1}}) \\ &\equiv \Phi_{m_0}(x^{2^{t-1}}) \pmod{2} \end{aligned}$$

$$m_j = 2^t m_0,\ m_i = 2^s m_0 \implies a_j \equiv a_i \pmod{m_0}$$

$$\Phi_{pn}(x) = \begin{cases} \Phi_n(x^p) & \text{if } p|n \\ \Phi_n(x^p)/\Phi_n(x) & \text{if } p \nmid n. \end{cases}$$

$$\Phi_{2n}(x) = \Phi_n(-x) \quad \text{for } n > 1 \text{ odd.}$$

$$\begin{aligned} \Phi_{2^t m_0}(x) &= \Phi_{2^{t-1}m_0}(x^2) = \Phi_{2^{t-2}m_0}(x^{2^2}) \\ &= \Phi_{2^{t-3}m_0}(x^{2^3}) = \cdots = \Phi_{2m_0}(x^{2^{t-1}}) \\ &\equiv \Phi_{m_0}(x^{2^{t-1}}) \equiv \Phi_{m_0}(x)^{2^{t-1}} \pmod{2} \end{aligned}$$

$$m_j = 2^t m_0,\ m_i = 2^s m_0 \implies a_j \equiv a_i \pmod{m_0}$$

$$\Phi_{pn}(x) = \begin{cases} \Phi_n(x^p) & \text{if } p|n \\ \Phi_n(x^p)/\Phi_n(x) & \text{if } p \nmid n. \end{cases}$$

$$\Phi_{2n}(x) = \Phi_n(-x) \quad \text{for } n > 1 \text{ odd.}$$

$$\begin{aligned} \Phi_{2^t m_0}(x) &= \Phi_{2^{t-1} m_0}(x^2) = \Phi_{2^{t-2} m_0}(x^{2^2}) \\ &= \Phi_{2^{t-3} m_0}(x^{2^3}) = \cdots = \Phi_{2m_0}(x^{2^{t-1}}) \\ &\equiv \Phi_{m_0}(x^{2^{t-1}}) \equiv \Phi_{m_0}(x)^{2^{t-1}} \pmod{2} \end{aligned}$$

$\Phi_{m_0}(x)$ divides both $\Phi_{2^t m_0}(x)$ and $\Phi_{2^s m_0}(x)$ mod 2

$$m_j = 2^t m_0,\ m_i = 2^s m_0 \implies a_j \equiv a_i \pmod{m_0}$$

$$m_j = 2^t m_0,\ m_i = 2^s m_0 \implies a_j \equiv a_i \pmod{m_0}$$

$$a_i + (k-1)m_i < a_j \le a_i + km_i$$

$$m_j = 2^t m_0,\; m_i = 2^s m_0 \implies a_j \equiv a_i \pmod{m_0}$$

$$a_i + (k-1)m_i < a_j \leq a_i + km_i$$

$$\ell = a_i + km_i - a_j$$

$$m_j = 2^t m_0,\ m_i = 2^s m_0 \implies a_j \equiv a_i \pmod{m_0}$$

$$a_i + (k-1)m_i < a_j \le a_i + km_i$$

$$\ell = a_i + km_i - a_j \in [0, m_i)$$

$$m_j = 2^t m_0,\ m_i = 2^s m_0 \implies a_j \equiv a_i \pmod{m_0}$$

$$a_i + (k-1)m_i < a_j \le a_i + km_i$$

$$\ell = a_i + km_i - a_j \in [0, m_i)$$

$$\Phi_{m_i}(x) \big| \big(\, f(x)x^{a_i} + 1 \,\big)$$

$$m_j = 2^t m_0,\ m_i = 2^s m_0 \implies a_j \equiv a_i \pmod{m_0}$$

$$a_i + (k-1)m_i < a_j \leq a_i + km_i$$

$$\ell = a_i + km_i - a_j \in [0, m_i)$$

$$\Phi_{m_i}(x) \Big| \Big(\underbrace{f(x)x^{a_i} + 1}_{\substack{\uparrow \\ \text{add } f(x)x^{a_i}(x^{km_i} - 1)}} \Big)$$

$$m_j = 2^t m_0,\ m_i = 2^s m_0 \implies a_j \equiv a_i \pmod{m_0}$$

$$a_i + (k-1)m_i < a_j \le a_i + km_i$$

$$\ell = a_i + km_i - a_j \in [0, m_i)$$

$$\Phi_{m_i}(x) \,\Big|\, \Big(\underbrace{f(x)x^{a_i} + 1} \Big)$$

$$\uparrow$$

add $f(x)x^{a_i}(x^{km_i} - 1)$

get $f(x)x^{a_i+km_i} + 1$

$$m_j = 2^t m_0,\ m_i = 2^s m_0 \implies a_j \equiv a_i \pmod{m_0}$$

$$a_i + (k-1)m_i < a_j \leq a_i + km_i$$
$$\ell = a_i + km_i - a_j \in [0, m_i)$$

$$\Phi_{m_i}(x) \Big| \left(f(x)x^{a_i+km_i} + 1\right)$$

$$m_j = 2^t m_0,\ m_i = 2^s m_0 \implies a_j \equiv a_i \pmod{m_0}$$

$$a_i + (k-1)m_i < a_j \le a_i + km_i$$

$$\ell = a_i + km_i - a_j \in [0, m_i)$$

$$\Phi_{m_i}(x) \Big| \Big(f(x)x^{a_i+km_i} + 1\Big)$$

$$\Phi_{m_j}(x) \Big| \Big(f(x)x^{a_j} + 1\Big)$$

$$m_j = 2^t m_0,\ m_i = 2^s m_0 \implies a_j \equiv a_i \pmod{m_0}$$

$$a_i + (k-1)m_i < a_j \leq a_i + km_i$$
$$\ell = a_i + km_i - a_j \in [0, m_i)$$

$$\Phi_{m_i}(x) \big| \big(f(x)x^{a_i+km_i} + 1\big)$$
$$\Phi_{m_j}(x) \big| \big(f(x)x^{a_j+\ell} + x^{\ell}\big)$$

$$m_j = 2^t m_0,\ m_i = 2^s m_0 \implies a_j \equiv a_i \pmod{m_0}$$

$$a_i + (k-1)m_i < a_j \le a_i + km_i$$

$$\ell = a_i + km_i - a_j \in [0, m_i)$$

$$\Phi_{m_i}(x) \Big| \left(f(x)x^{a_i+km_i} + 1\right)$$

$$\Phi_{m_j}(x) \Big| \left(f(x)x^{a_j+\ell} + x^\ell\right)$$

$$m_j = 2^t m_0,\ m_i = 2^s m_0 \implies a_j \equiv a_i \pmod{m_0}$$

$$a_i + (k-1)m_i < a_j \le a_i + km_i$$

$$\ell = a_i + km_i - a_j \in [0, m_i)$$

$$\Phi_{m_i}(x) \,\Big|\, \left(f(x)x^{a_i+km_i} + 1\right)$$

$$\Phi_{m_j}(x) \,\Big|\, \left(f(x)x^{a_j+\ell} + x^{\ell}\right)$$

$$m_j = 2^t m_0,\ m_i = 2^s m_0 \implies a_j \equiv a_i \pmod{m_0}$$

$$a_i + (k-1)m_i < a_j \leq a_i + km_i$$
$$\ell = a_i + km_i - a_j \in [0, m_i)$$

$$\Phi_{m_i}(x) \big| \big(f(x)x^{a_i+km_i} + 1\big)$$
$$\Phi_{m_j}(x) \big| \big(f(x)x^{a_i+km_i} + x^{\ell}\big)$$

$$m_j = 2^t m_0,\ m_i = 2^s m_0 \implies a_j \equiv a_i \pmod{m_0}$$

$$a_i + (k-1)m_i < a_j \leq a_i + km_i$$
$$\ell = a_i + km_i - a_j \in [0, m_i)$$

$$\Phi_{m_i}(x) \big| \big(f(x)x^{a_i+km_i} + 1\big)$$
$$\Phi_{m_j}(x) \big| \big(f(x)x^{a_i+km_i} + x^{\ell}\big)$$

$$\Phi_{m_i}(x)u(x) + \Phi_{m_j}(x)v(x) = x^{\ell} - 1$$

$$m_j = 2^t m_0,\ m_i = 2^s m_0 \implies a_j \equiv a_i \pmod{m_0}$$

$$a_i + (k-1)m_i < a_j \leq a_i + km_i$$

$$\ell = a_i + km_i - a_j \in [0, m_i)$$

$$\Phi_{m_i}(x)u(x) + \Phi_{m_j}(x)v(x) = x^\ell - 1$$

$$m_j = 2^t m_0,\ m_i = 2^s m_0 \implies a_j \equiv a_i \pmod{m_0}$$

$$a_i + (k-1)m_i < a_j \le a_i + k m_i$$

$$\ell = a_i + k m_i - a_j \in [0, m_i)$$

$$\Phi_{m_i}(x)u(x) + \Phi_{m_j}(x)v(x) = x^\ell - 1$$

$\Phi_{m_0}(x)$ divides $x^\ell - 1$ modulo 2

$$m_j = 2^t m_0,\ m_i = 2^s m_0 \implies a_j \equiv a_i \pmod{m_0}$$

$$a_i + (k-1)m_i < a_j \leq a_i + km_i$$

$$\ell = a_i + km_i - a_j \in [0, m_i)$$

$$\Phi_{m_i}(x)u(x) + \Phi_{m_j}(x)v(x) = x^\ell - 1$$

$\Phi_{m_0}(x)$ divides $x^\ell - 1$ modulo 2

Some divisor $\Phi_{\ell'}(x)$ of $x^\ell - 1$ and $\Phi_{m_0}(x)$ have a factor in common modulo 2.

$$m_j = 2^t m_0,\ m_i = 2^s m_0 \implies a_j \equiv a_i \pmod{m_0}$$

$$\ell = a_i + k m_i - a_j \in [0, m_i)$$

Some divisor $\Phi_{\ell'}(x)$ of $x^\ell - 1$ and $\Phi_{m_0}(x)$ have a factor in common modulo 2.

$$m_j = 2^t m_0,\ m_i = 2^s m_0 \implies a_j \equiv a_i \pmod{m_0}$$

$$\ell = a_i + k m_i - a_j \in [0, m_i)$$

Some divisor $\Phi_{\ell'}(x)$ of $x^\ell - 1$ and $\Phi_{m_0}(x)$
have a factor in common modulo 2
$\implies$ resultant of $\Phi_{\ell'}(x)$ and $\Phi_{m_0}(x)$ is even.

$$m_j = 2^t m_0,\ m_i = 2^s m_0 \implies a_j \equiv a_i \pmod{m_0}$$

$$\ell = a_i + k m_i - a_j \in [0, m_i)$$

Some divisor $\Phi_{\ell'}(x)$ of $x^\ell - 1$ and $\Phi_{m_0}(x)$

have a factor in common modulo 2

$\implies$ resultant of $\Phi_{\ell'}(x)$ and $\Phi_{m_0}(x)$ is even.

$$\Phi_{\ell'}(x) \equiv u(x)w(x) \pmod{2}$$
$$\Phi_{m_0}(x) \equiv v(x)w(x) \pmod{2}$$

$$m_j = 2^t m_0,\ m_i = 2^s m_0 \implies a_j \equiv a_i \pmod{m_0}$$

$$\ell = a_i + k m_i - a_j \in [0, m_i)$$

Some divisor $\Phi_{\ell'}(x)$ of $x^\ell - 1$ and $\Phi_{m_0}(x)$
have a factor in common modulo 2

$\implies$ resultant of $\Phi_{\ell'}(x)$ and $\Phi_{m_0}(x)$ is even.

Lemma 2 (Apostol). Let n and m be positive integers with $n > m$. The resultant of $\Phi_n(x)$ and $\Phi_m(x)$ is divisible by a prime p if and only if n/m is a power of p.

$$m_j = 2^t m_0,\ m_i = 2^s m_0 \implies a_j \equiv a_i \pmod{m_0}$$

$$\ell = a_i + k m_i - a_j \in [0, m_i)$$

Some divisor $\Phi_{\ell'}(x)$ of $x^\ell - 1$ and $\Phi_{m_0}(x)$

have a factor in common modulo 2

$\implies$ resultant of $\Phi_{\ell'}(x)$ and $\Phi_{m_0}(x)$ is even.

Lemma 2 (Apostol). Let n and m be positive integers with $n > m$. The resultant of $\Phi_n(x)$ and $\Phi_m(x)$ is divisible by a prime p if and only if n/m is a power of p.

$2 \nmid m_0$

$$m_j = 2^t m_0,\ m_i = 2^s m_0 \implies a_j \equiv a_i \pmod{m_0}$$

$$\ell = a_i + k m_i - a_j \in [0, m_i)$$

Some divisor $\Phi_{\ell'}(x)$ of $x^\ell - 1$ and $\Phi_{m_0}(x)$

have a factor in common modulo 2

$\implies$ resultant of $\Phi_{\ell'}(x)$ and $\Phi_{m_0}(x)$ is even.

Lemma 2 (Apostol). Let n and m be positive integers with $n > m$. The resultant of $\Phi_n(x)$ and $\Phi_m(x)$ is divisible by a prime p if and only if n/m is a power of p.

$2 \nmid m_0 \implies m_0 | \ell'$

$$m_j = 2^t m_0,\ m_i = 2^s m_0 \implies a_j \equiv a_i \pmod{m_0}$$

$$\ell = a_i + k m_i - a_j \in [0, m_i)$$

Some divisor $\Phi_{\ell'}(x)$ of $x^\ell - 1$ and $\Phi_{m_0}(x)$
have a factor in common modulo 2
$\implies$ resultant of $\Phi_{\ell'}(x)$ and $\Phi_{m_0}(x)$ is even.

Lemma 2 (Apostol). Let n and m be positive integers with $n > m$. The resultant of $\Phi_n(x)$ and $\Phi_m(x)$ is divisible by a prime p if and only if n/m is a power of p.

$$2 \nmid m_0 \implies m_0 | \ell' \implies m_0 | \ell$$

$$m_j = 2^t m_0,\ m_i = 2^s m_0 \implies a_j \equiv a_i \pmod{m_0}$$

$$\ell = a_i + km_i - a_j \in [0, m_i)$$

Some divisor $\Phi_{\ell'}(x)$ of $x^\ell - 1$ and $\Phi_{m_0}(x)$
have a factor in common modulo 2
$\implies$ resultant of $\Phi_{\ell'}(x)$ and $\Phi_{m_0}(x)$ is even.

Lemma 2 (Apostol). Let n and m be positive integers with $n > m$. The resultant of $\Phi_n(x)$ and $\Phi_m(x)$ is divisible by a prime p if and only if n/m is a power of p.

$$2 \nmid m_0 \implies m_0 | \ell' \implies m_0 | \ell \implies a_j \equiv a_i \pmod{m_0}$$