Fermat's Little Theorem

Lecture 7

Justin Stevens

Outline

Statement

Theorem. If p is prime and a is an integer with $p \nmid a$, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Statement

Theorem. If p is prime and a is an integer with $p \nmid a$, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

Alternatively, for every integer a, $a^p \equiv a \pmod{p}$.

Challenge Problems

Example 1. (IMO 2005) Determine all positive integers relatively prime to all the terms of the infinite sequence $2^n + 3^n + 6^n - 1, n \geq 1$

Example 2. (NIMO) Let $p = 2017$ be a prime. Find the remainder when

$$\left\lfloor \frac{1^p}{p} \right\rfloor + \left\lfloor \frac{2^p}{p} \right\rfloor + \left\lfloor \frac{3^p}{p} \right\rfloor + \cdots + \left\lfloor \frac{2015^p}{p} \right\rfloor$$

is divided by p. Here $\lfloor \cdot \rfloor$ denotes the greatest integer function.

IMO Problem

Example. (IMO 2005) Determine all positive integers relatively prime to all the terms of the infinite sequence $2^n + 3^n + 6^n - 1, n \geq 1$

IMO Problem

Example. (IMO 2005) Determine all positive integers relatively prime to all the terms of the infinite sequence $2^n + 3^n + 6^n - 1, n \geq 1$

Solution. I claim the answer is 1, therefore, every prime p divides a term in the sequence.

IMO Problem

Example. (IMO 2005) Determine all positive integers relatively prime to all the terms of the infinite sequence $2^n + 3^n + 6^n - 1, n \geq 1$

Solution. I claim the answer is 1, therefore, every prime p divides a term in the sequence. For $p = 2$, $n = 1$ works and for $p = 3$, $n = 2$ works. By Fermat's Little Theorem for $n = p - 2$,

IMO Problem

Example. (IMO 2005) Determine all positive integers relatively prime to all the terms of the infinite sequence $2^n + 3^n + 6^n - 1, n \geq 1$

Solution. I claim the answer is 1, therefore, every prime p divides a term in the sequence. For $p = 2$, $n = 1$ works and for $p = 3$, $n = 2$ works. By Fermat's Little Theorem for $n = p - 2$,

$$6\left(2^{p-2} + 3^{p-2} + 6^{p-2} - 1\right) \equiv 3 \cdot 2^{p-1} + 2 \cdot 3^{p-1} + 6^{p-1} - 6$$

IMO Problem

Example. (IMO 2005) Determine all positive integers relatively prime to all the terms of the infinite sequence $2^n + 3^n + 6^n - 1, n \geq 1$

Solution. I claim the answer is 1, therefore, every prime p divides a term in the sequence. For $p = 2$, $n = 1$ works and for $p = 3$, $n = 2$ works. By Fermat's Little Theorem for $n = p - 2$,

$$\begin{aligned} 6\left(2^{p-2} + 3^{p-2} + 6^{p-2} - 1\right) &\equiv 3 \cdot 2^{p-1} + 2 \cdot 3^{p-1} + 6^{p-1} - 6 \\ &\equiv 3 + 2 + 1 - 6 \end{aligned}$$

IMO Problem

Example. (IMO 2005) Determine all positive integers relatively prime to all the terms of the infinite sequence $2^n + 3^n + 6^n - 1, n \geq 1$

Solution. I claim the answer is 1, therefore, every prime p divides a term in the sequence. For $p = 2$, $n = 1$ works and for $p = 3$, $n = 2$ works. By Fermat's Little Theorem for $n = p - 2$,

$$\begin{aligned} 6\left(2^{p-2} + 3^{p-2} + 6^{p-2} - 1\right) &\equiv 3 \cdot 2^{p-1} + 2 \cdot 3^{p-1} + 6^{p-1} - 6 \\ &\equiv 3 + 2 + 1 - 6 \\ &\equiv 0 \pmod{p}. \end{aligned}$$

IMO Problem

Example. (IMO 2005) Determine all positive integers relatively prime to all the terms of the infinite sequence $2^n + 3^n + 6^n - 1, n \geq 1$

Solution. I claim the answer is 1, therefore, every prime p divides a term in the sequence. For $p = 2$, $n = 1$ works and for $p = 3$, $n = 2$ works. By Fermat's Little Theorem for $n = p - 2$,

$$\begin{aligned} 6\left(2^{p-2} + 3^{p-2} + 6^{p-2} - 1\right) &\equiv 3 \cdot 2^{p-1} + 2 \cdot 3^{p-1} + 6^{p-1} - 6 \\ &\equiv 3 + 2 + 1 - 6 \\ &\equiv 0 \pmod{p}. \end{aligned}$$

Therefore, for $p \neq 2, 3$, when $n = p - 2$, we have $p \mid 2^n + 3^n + 6^n - 1$.

NIMO Sum

Example. (NIMO) Let $p = 2017$ be a prime. Find the remainder when

$$\left\lfloor \frac{1^p}{p} \right\rfloor + \left\lfloor \frac{2^p}{p} \right\rfloor + \left\lfloor \frac{3^p}{p} \right\rfloor + \cdots + \left\lfloor \frac{2015^p}{p} \right\rfloor$$

is divided by p. Here $\lfloor \cdot \rfloor$ denotes the greatest integer function.

Solution. By FLT, $n^p \equiv n \pmod{p}$, so $\lfloor \frac{n^p}{p} \rfloor = \frac{n^p - n}{p}$ and the sum is

NIMO Sum

Example. (NIMO) Let $p = 2017$ be a prime. Find the remainder when

$$\left\lfloor \frac{1^p}{p} \right\rfloor + \left\lfloor \frac{2^p}{p} \right\rfloor + \left\lfloor \frac{3^p}{p} \right\rfloor + \cdots + \left\lfloor \frac{2015^p}{p} \right\rfloor$$

is divided by p. Here $\lfloor \cdot \rfloor$ denotes the greatest integer function.

Solution. By FLT, $n^p \equiv n \pmod{p}$, so $\left\lfloor \frac{n^p}{p} \right\rfloor = \frac{n^p - n}{p}$ and the sum is

$$\sum_{k=1}^{p-2} \frac{k^p - k}{p} = \frac{1}{p} \sum_{k=1}^{p-2} (k^p - k).$$

NIMO Sum

Example. (NIMO) Let $p = 2017$ be a prime. Find the remainder when

$$\left\lfloor \frac{1^p}{p} \right\rfloor + \left\lfloor \frac{2^p}{p} \right\rfloor + \left\lfloor \frac{3^p}{p} \right\rfloor + \cdots + \left\lfloor \frac{2015^p}{p} \right\rfloor$$

is divided by p. Here $\lfloor \cdot \rfloor$ denotes the greatest integer function.

Solution. By FLT, $n^p \equiv n \pmod{p}$, so $\lfloor \frac{n^p}{p} \rfloor = \frac{n^p - n}{p}$ and the sum is

$$\sum_{k=1}^{p-2} \frac{k^p - k}{p} = \frac{1}{p} \sum_{k=1}^{p-2} (k^p - k).$$

From the Binomial Theorem, $j^p + (p-j)^p \equiv 0 \pmod{p^2}$ for all j, so

NIMO Sum

Example. (NIMO) Let $p = 2017$ be a prime. Find the remainder when

$$\left\lfloor \frac{1^p}{p} \right\rfloor + \left\lfloor \frac{2^p}{p} \right\rfloor + \left\lfloor \frac{3^p}{p} \right\rfloor + \cdots + \left\lfloor \frac{2015^p}{p} \right\rfloor$$

is divided by p. Here $\lfloor \cdot \rfloor$ denotes the greatest integer function.

Solution. By FLT, $n^p \equiv n \pmod{p}$, so $\left\lfloor \frac{n^p}{p} \right\rfloor = \frac{n^p - n}{p}$ and the sum is

$$\sum_{k=1}^{p-2} \frac{k^p - k}{p} = \frac{1}{p} \sum_{k=1}^{p-2} (k^p - k).$$

From the Binomial Theorem, $j^p + (p-j)^p \equiv 0 \pmod{p^2}$ for all j, so

$$\sum_{k=1}^{p-2} (k^p - k) \equiv 1^p - \sum_{k=1}^{p-2} k \equiv 1 - \frac{(p-2)(p-1)}{2} \equiv \frac{p(3-p)}{2} \pmod{p^2}.$$

NIMO Sum

Example. (NIMO) Let $p = 2017$ be a prime. Find the remainder when

$$\left\lfloor \frac{1^p}{p} \right\rfloor + \left\lfloor \frac{2^p}{p} \right\rfloor + \left\lfloor \frac{3^p}{p} \right\rfloor + \cdots + \left\lfloor \frac{2015^p}{p} \right\rfloor$$

is divided by p. Here $\lfloor \cdot \rfloor$ denotes the greatest integer function.

Solution. By FLT, $n^p \equiv n \pmod{p}$, so $\left\lfloor \frac{n^p}{p} \right\rfloor = \frac{n^p - n}{p}$ and the sum is

$$\sum_{k=1}^{p-2} \frac{k^p - k}{p} = \frac{1}{p} \sum_{k=1}^{p-2} (k^p - k).$$

From the Binomial Theorem, $j^p + (p-j)^p \equiv 0 \pmod{p^2}$ for all j, so

$$\sum_{k=1}^{p-2} (k^p - k) \equiv 1^p - \sum_{k=1}^{p-2} k \equiv 1 - \frac{(p-2)(p-1)}{2} \equiv \frac{p(3-p)}{2} \pmod{p^2}.$$

Substituting $p = 2017$, $\frac{3-p}{2} \equiv \frac{-2014}{2} \equiv -1007 \equiv \boxed{1010} \pmod{p}$.

Pseudoprimes

Over 25 centuries ago, Chinese mathematicians believed n is prime iff $2^n \equiv 2 \pmod{n}$. The counterexample $n = 341$ was discovered in 1819.

Pseudoprimes

Over 25 centuries ago, Chinese mathematicians believed n is prime iff $2^n \equiv 2 \pmod{n}$. The counterexample $n = 341$ was discovered in 1819.

Fermat's primality test says to pick a number a with $1 < a < p - 1$. If $a^{n-1} \not\equiv 1 \pmod{n}$, then we can conclude that a is composite. However, if the congruence holds, then we assign a high probability to n being prime.

Pseudoprimes

Over 25 centuries ago, Chinese mathematicians believed n is prime iff $2^n \equiv 2 \pmod{n}$. The counterexample $n = 341$ was discovered in 1819.

Fermat's primality test says to pick a number a with $1 < a < p - 1$. If $a^{n-1} \not\equiv 1 \pmod{n}$, then we can conclude that a is composite. However, if the congruence holds, then we assign a high probability to n being prime.

Composite n with $a^{n-1} \equiv 1 \pmod{n}$ are called **pseudoprimes** to base a.

Pseudoprimes

Over 25 centuries ago, Chinese mathematicians believed n is prime iff $2^n \equiv 2 \pmod{n}$. The counterexample $n = 341$ was discovered in 1819.

Fermat's primality test says to pick a number a with $1 < a < p - 1$. If $a^{n-1} \not\equiv 1 \pmod{n}$, then we can conclude that a is composite. However, if the congruence holds, then we assign a high probability to n being prime.

Composite n with $a^{n-1} \equiv 1 \pmod{n}$ are called **pseudoprimes** to base a.

Example. Prove that if n is a base-2 pseudoprime, then $M_n = 2^n - 1$ is a larger one.

Mersenne Pseudoprimes

Composite n with $a^{n-1} \equiv 1 \pmod{n}$ are called **pseudoprimes** to base a.

Example. If n is a base-2 pseudoprime, then $M_n = 2^n - 1$ is a larger one.

Mersenne Pseudoprimes

Composite n with $a^{n-1} \equiv 1 \pmod{n}$ are called **pseudoprimes** to base a.

Example. If n is a base-2 pseudoprime, then $M_n = 2^n - 1$ is a larger one.

Proof.

Since n is a base-2 pseudoprime, $2^{n-1} \equiv 1 \pmod{n}$, so $2^n \equiv 2 \pmod{n}$.

Mersenne Pseudoprimes

Composite n with $a^{n-1} \equiv 1 \pmod{n}$ are called **pseudoprimes** to base a.

Example. If n is a base-2 pseudoprime, then $M_n = 2^n - 1$ is a larger one.

Proof.

Since n is a base-2 pseudoprime, $2^{n-1} \equiv 1 \pmod{n}$, so $2^n \equiv 2 \pmod{n}$. Therefore, there exists an integer k with $2^n - 2 = kn$.

Mersenne Pseudoprimes

Composite n with $a^{n-1} \equiv 1 \pmod{n}$ are called **pseudoprimes** to base a.

Example. If n is a base-2 pseudoprime, then $M_n = 2^n - 1$ is a larger one.

Proof.

Since n is a base-2 pseudoprime, $2^{n-1} \equiv 1 \pmod{n}$, so $2^n \equiv 2 \pmod{n}$. Therefore, there exists an integer k with $2^n - 2 = kn$. Substituting, we have

Mersenne Pseudoprimes

Composite n with $a^{n-1} \equiv 1 \pmod{n}$ are called **pseudoprimes** to base a.

Example. If n is a base-2 pseudoprime, then $M_n = 2^n - 1$ is a larger one.

Proof.

Since n is a base-2 pseudoprime, $2^{n-1} \equiv 1 \pmod{n}$, so $2^n \equiv 2 \pmod{n}$. Therefore, there exists an integer k with $2^n - 2 = kn$. Substituting, we have

$$\begin{aligned} 2^{M_n - 1} - 1 &= 2^{kn} - 1 \\ &= (2^n - 1)\left(2^{n(k-1)} + 2^{n(k-2)} + \cdots + 2^n + 1\right) \\ &\equiv 0 \pmod{M_n}. \end{aligned}$$

Mersenne Pseudoprimes

Composite n with $a^{n-1} \equiv 1 \pmod{n}$ are called **pseudoprimes** to base a.

Example. If n is a base-2 pseudoprime, then $M_n = 2^n - 1$ is a larger one.

Proof.

Since n is a base-2 pseudoprime, $2^{n-1} \equiv 1 \pmod{n}$, so $2^n \equiv 2 \pmod{n}$. Therefore, there exists an integer k with $2^n - 2 = kn$. Substituting, we have

$$\begin{aligned} 2^{M_n - 1} - 1 &= 2^{kn} - 1 \\ &= (2^n - 1)\left(2^{n(k-1)} + 2^{n(k-2)} + \cdots + 2^n + 1\right) \\ &\equiv 0 \pmod{M_n}. \end{aligned}$$

Since n is composite, M_n is composite and the conclusion follows. □

Carmichael Numbers

A **Carmichael number** is an integer n that is a pseudoprime for every coprime base a. In other words, $a^{n-1} \equiv 1 \pmod{n}$ for every $\gcd(a, n) = 1$.

Example. Prove that 561 is a Carmichael number.

Proof. Factoring shows $561 = 3 \cdot 11 \cdot 17$. Therefore, for every a coprime to 3, 11, and 17, using Fermat's Little Theorem,

Carmichael Numbers

A **Carmichael number** is an integer n that is a pseudoprime for every coprime base a. In other words, $a^{n-1} \equiv 1 \pmod{n}$ for every $\gcd(a, n) = 1$.

Example. Prove that 561 is a Carmichael number.

Proof. Factoring shows $561 = 3 \cdot 11 \cdot 17$. Therefore, for every a coprime to 3, 11, and 17, using Fermat's Little Theorem,

$$a^2 \equiv 1 \pmod{3}, \quad a^{10} \equiv 1 \pmod{11}, \quad a^{16} \equiv 1 \pmod{17}.$$

Carmichael Numbers

A **Carmichael number** is an integer n that is a pseudoprime for every coprime base a. In other words, $a^{n-1} \equiv 1 \pmod{n}$ for every $\gcd(a, n) = 1$.

Example. Prove that 561 is a Carmichael number.

Proof. Factoring shows $561 = 3 \cdot 11 \cdot 17$. Therefore, for every a coprime to 3, 11, and 17, using Fermat's Little Theorem,

$$a^2 \equiv 1 \pmod{3}, \quad a^{10} \equiv 1 \pmod{11}, \quad a^{16} \equiv 1 \pmod{17}.$$

Using these congruences, we see that

$$a^{560} \equiv \left(a^2\right)^{280} \equiv 1 \pmod{3}$$

Carmichael Numbers

A **Carmichael number** is an integer n that is a pseudoprime for every coprime base a. In other words, $a^{n-1} \equiv 1 \pmod{n}$ for every $\gcd(a, n) = 1$.

Example. Prove that 561 is a Carmichael number.

Proof. Factoring shows $561 = 3 \cdot 11 \cdot 17$. Therefore, for every a coprime to 3, 11, and 17, using Fermat's Little Theorem,

$$a^2 \equiv 1 \pmod{3}, \quad a^{10} \equiv 1 \pmod{11}, \quad a^{16} \equiv 1 \pmod{17}.$$

Using these congruences, we see that

$$a^{560} \equiv \left(a^2\right)^{280} \equiv 1 \pmod{3}$$

$$a^{560} \equiv \left(a^{10}\right)^{56} \equiv 1 \pmod{11}$$

Carmichael Numbers

A **Carmichael number** is an integer n that is a pseudoprime for every coprime base a. In other words, $a^{n-1} \equiv 1 \pmod{n}$ for every $\gcd(a, n) = 1$.

Example. Prove that 561 is a Carmichael number.

Proof. Factoring shows $561 = 3 \cdot 11 \cdot 17$. Therefore, for every a coprime to 3, 11, and 17, using Fermat's Little Theorem,

$$a^2 \equiv 1 \pmod{3}, \quad a^{10} \equiv 1 \pmod{11}, \quad a^{16} \equiv 1 \pmod{17}.$$

Using these congruences, we see that

$$a^{560} \equiv \left(a^2\right)^{280} \equiv 1 \pmod{3}$$

$$a^{560} \equiv \left(a^{10}\right)^{56} \equiv 1 \pmod{11}$$

$$a^{560} \equiv \left(a^{16}\right)^{35} \equiv 1 \pmod{17}.$$

Carmichael Numbers

A **Carmichael number** is an integer n that is a pseudoprime for every coprime base a. In other words, $a^{n-1} \equiv 1 \pmod{n}$ for every $\gcd(a, n) = 1$.

Example. Prove that 561 is a Carmichael number.

Proof. Factoring shows $561 = 3 \cdot 11 \cdot 17$. Therefore, for every a coprime to 3, 11, and 17, using Fermat's Little Theorem,

$$a^2 \equiv 1 \pmod{3}, \quad a^{10} \equiv 1 \pmod{11}, \quad a^{16} \equiv 1 \pmod{17}.$$

Using these congruences, we see that

$$a^{560} \equiv \left(a^2\right)^{280} \equiv 1 \pmod{3}$$

$$a^{560} \equiv \left(a^{10}\right)^{56} \equiv 1 \pmod{11}$$

$$a^{560} \equiv \left(a^{16}\right)^{35} \equiv 1 \pmod{17}.$$

Therefore $a^{560} \equiv 1 \pmod{561}$ for all a relatively prime to 561.

Korselt's Criterion

The previous example establishes the intuition for the below theorem.

Theorem. (Korselt's Criterion) A number n is Carmichael if and only if $n = p_1 p_2 \cdots p_r$, where the p_i are distinct primes and $p_i - 1 \mid n - 1$ for every $1 \leq i \leq r$.

Wilson's Theorem

Theorem. (Wilson) $(p-1)! \equiv -1 \pmod{p}$ for all odd primes p.

Wilson's Theorem

Theorem. (Wilson) $(p-1)! \equiv -1 \pmod{p}$ for all odd primes p.

Solution. When $p = 7$, $6! = 720 \equiv -1 \pmod{7}$. Alternatively,

$$6! = 1 \cdot (2 \cdot 4)(3 \cdot 5) \cdot 6 \equiv 1 \cdot 1 \cdot 1 \cdot 6 \equiv -1 \pmod{7}.$$

Wilson's Theorem

Theorem. (Wilson) $(p-1)! \equiv -1 \pmod{p}$ for all odd primes p.

Solution. When $p = 7$, $6! = 720 \equiv -1 \pmod{7}$. Alternatively,

$$6! = 1 \cdot (2 \cdot 4)(3 \cdot 5) \cdot 6 \equiv 1 \cdot 1 \cdot 1 \cdot 6 \equiv -1 \pmod{7}.$$

We find groups of terms that multiply to 1 mod p. Observe that

$$x^2 \equiv 1 \mod p \iff (x-1)(x+1) \equiv 0 \mod p \iff x \equiv \pm 1 \mod p.$$

Wilson's Theorem

Theorem. (Wilson) $(p-1)! \equiv -1 \pmod{p}$ for all odd primes p.

Solution. When $p = 7$, $6! = 720 \equiv -1 \pmod{7}$. Alternatively,

$$6! = 1 \cdot (2 \cdot 4)(3 \cdot 5) \cdot 6 \equiv 1 \cdot 1 \cdot 1 \cdot 6 \equiv -1 \pmod{7}.$$

We find groups of terms that multiply to 1 mod p. Observe that

$$x^2 \equiv 1 \mod p \iff (x-1)(x+1) \equiv 0 \mod p \iff x \equiv \pm 1 \mod p.$$

Since p is odd, this implies we can pair the inverses off into $(p-3)/2$ pairs, say $(x_1, y_1), (x_2, y_2), (x_3, y_3), \cdots (x_{(p-3)/2}, y_{(p-3)/2})$. Therefore,

Wilson's Theorem

Theorem. (Wilson) $(p-1)! \equiv -1 \pmod{p}$ for all odd primes p.

Solution. When $p = 7$, $6! = 720 \equiv -1 \pmod{7}$. Alternatively,

$$6! = 1 \cdot (2 \cdot 4)(3 \cdot 5) \cdot 6 \equiv 1 \cdot 1 \cdot 1 \cdot 6 \equiv -1 \pmod{7}.$$

We find groups of terms that multiply to 1 mod p. Observe that

$$x^2 \equiv 1 \mod p \iff (x-1)(x+1) \equiv 0 \mod p \iff x \equiv \pm 1 \mod p.$$

Since p is odd, this implies we can pair the inverses off into $(p-3)/2$ pairs, say $(x_1, y_1), (x_2, y_2), (x_3, y_3), \cdots (x_{(p-3)/2}, y_{(p-3)/2})$. Therefore,

$$(p-1)! \equiv 1 \cdot (x_1 y_1)(x_2 y_2) \cdots \left[x_{(p-3)/2} y_{(p-3)/2}\right] \cdot (p-1) \pmod{p}$$

Wilson's Theorem

Theorem. (Wilson) $(p-1)! \equiv -1 \pmod{p}$ for all odd primes p.

Solution. When $p = 7$, $6! = 720 \equiv -1 \pmod{7}$. Alternatively,

$$6! = 1 \cdot (2 \cdot 4)(3 \cdot 5) \cdot 6 \equiv 1 \cdot 1 \cdot 1 \cdot 6 \equiv -1 \pmod{7}.$$

We find groups of terms that multiply to 1 mod p. Observe that

$$x^2 \equiv 1 \mod p \iff (x-1)(x+1) \equiv 0 \mod p \iff x \equiv \pm 1 \mod p.$$

Since p is odd, this implies we can pair the inverses off into $(p-3)/2$ pairs, say $(x_1, y_1), (x_2, y_2), (x_3, y_3), \cdots (x_{(p-3)/2}, y_{(p-3)/2})$. Therefore,

$$\begin{aligned}(p-1)! &\equiv 1 \cdot (x_1 y_1)(x_2 y_2) \cdots \left[x_{(p-3)/2} y_{(p-3)/2}\right] \cdot (p-1) \pmod{p} \\ &\equiv 1 \cdot 1 \cdot 1 \cdots 1 \cdot (p-1) \pmod{p}\end{aligned}$$

□

Wilson's Theorem

Theorem. (Wilson) $(p-1)! \equiv -1 \pmod{p}$ for all odd primes p.

Solution. When $p = 7$, $6! = 720 \equiv -1 \pmod{7}$. Alternatively,

$$6! = 1 \cdot (2 \cdot 4)(3 \cdot 5) \cdot 6 \equiv 1 \cdot 1 \cdot 1 \cdot 6 \equiv -1 \pmod{7}.$$

We find groups of terms that multiply to 1 mod p. Observe that

$$x^2 \equiv 1 \mod p \iff (x-1)(x+1) \equiv 0 \mod p \iff x \equiv \pm 1 \mod p.$$

Since p is odd, this implies we can pair the inverses off into $(p-3)/2$ pairs, say $(x_1, y_1), (x_2, y_2), (x_3, y_3), \cdots (x_{(p-3)/2}, y_{(p-3)/2})$. Therefore,

$$\begin{aligned}(p-1)! &\equiv 1 \cdot (x_1 y_1)(x_2 y_2) \cdots \left[x_{(p-3)/2} y_{(p-3)/2}\right] \cdot (p-1) \pmod{p} \\ &\equiv 1 \cdot 1 \cdot 1 \cdots 1 \cdot (p-1) \pmod{p} \\ &\equiv -1 \pmod{p}.\end{aligned}$$

□

Quadratic Residue

Theorem. For an odd prime p, $x^2 \equiv -1 \pmod{p}$ iff $p \equiv 1 \pmod{4}$.

Proof. If $x^2 \equiv -1 \pmod{p}$, then raising this to the power of $(p-1)/2$:

Quadratic Residue

Theorem. For an odd prime p, $x^2 \equiv -1 \pmod{p}$ iff $p \equiv 1 \pmod{4}$.

Proof. If $x^2 \equiv -1 \pmod{p}$, then raising this to the power of $(p-1)/2$:

$$\left(x^2\right)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \implies x^{p-1} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

Quadratic Residue

Theorem. For an odd prime p, $x^2 \equiv -1 \pmod{p}$ iff $p \equiv 1 \pmod{4}$.

Proof. If $x^2 \equiv -1 \pmod{p}$, then raising this to the power of $(p-1)/2$:

$$\left(x^2\right)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \implies x^{p-1} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

By Fermat's Little Theorem the LHS is 1, therefore $p \equiv 1 \pmod{4}$.

Quadratic Residue

Theorem. For an odd prime p, $x^2 \equiv -1 \pmod{p}$ iff $p \equiv 1 \pmod{4}$.

Proof. If $x^2 \equiv -1 \pmod{p}$, then raising this to the power of $(p-1)/2$:

$$\left(x^2\right)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \implies x^{p-1} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

By Fermat's Little Theorem the LHS is 1, therefore $p \equiv 1 \pmod{4}$.

By Wilson's Theorem, $(p-1)! \equiv -1 \pmod{p}$. Furthermore,

Quadratic Residue

Theorem. For an odd prime p, $x^2 \equiv -1 \pmod{p}$ iff $p \equiv 1 \pmod{4}$.

Proof. If $x^2 \equiv -1 \pmod{p}$, then raising this to the power of $(p-1)/2$:

$$\left(x^2\right)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \implies x^{p-1} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

By Fermat's Little Theorem the LHS is 1, therefore $p \equiv 1 \pmod{4}$.

By Wilson's Theorem, $(p-1)! \equiv -1 \pmod{p}$. Furthermore,

$$(p-1)! = [1 \cdot (p-1)]\,[2 \cdot (p-2)] \cdots [(p-1)/2 \cdot (p+1)/2]$$

Quadratic Residue

Theorem. For an odd prime p, $x^2 \equiv -1 \pmod{p}$ iff $p \equiv 1 \pmod{4}$.

Proof. If $x^2 \equiv -1 \pmod{p}$, then raising this to the power of $(p-1)/2$:

$$\left(x^2\right)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \implies x^{p-1} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

By Fermat's Little Theorem the LHS is 1, therefore $p \equiv 1 \pmod{4}$.

By Wilson's Theorem, $(p-1)! \equiv -1 \pmod{p}$. Furthermore,

$$\begin{aligned}(p-1)! &= [1 \cdot (p-1)]\,[2 \cdot (p-2)] \cdots [(p-1)/2 \cdot (p+1)/2] \\ &\equiv (1 \cdot -1)\,(2 \cdot -2) \cdots [(p-1)/2 \cdot (-(p-1)/2))] \pmod{p}\end{aligned}$$

Quadratic Residue

Theorem. For an odd prime p, $x^2 \equiv -1 \pmod{p}$ iff $p \equiv 1 \pmod{4}$.

Proof. If $x^2 \equiv -1 \pmod{p}$, then raising this to the power of $(p-1)/2$:

$$\left(x^2\right)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \implies x^{p-1} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

By Fermat's Little Theorem the LHS is 1, therefore $p \equiv 1 \pmod{4}$.

By Wilson's Theorem, $(p-1)! \equiv -1 \pmod{p}$. Furthermore,

$$\begin{aligned}(p-1)! &= [1 \cdot (p-1)]\,[2 \cdot (p-2)] \cdots [(p-1)/2 \cdot (p+1)/2] \\ &\equiv (1 \cdot -1)\,(2 \cdot -2) \cdots [(p-1)/2 \cdot (-(p-1)/2))] \pmod{p} \\ &\equiv (-1)^{\frac{p-1}{2}} \left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod{p}\end{aligned}$$

Quadratic Residue

Theorem. For an odd prime p, $x^2 \equiv -1 \pmod{p}$ iff $p \equiv 1 \pmod{4}$.

Proof. If $x^2 \equiv -1 \pmod{p}$, then raising this to the power of $(p-1)/2$:

$$\left(x^2\right)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \implies x^{p-1} \equiv (-1)^{\frac{p-1}{2}} \pmod{p}.$$

By Fermat's Little Theorem the LHS is 1, therefore $p \equiv 1 \pmod{4}$.

By Wilson's Theorem, $(p-1)! \equiv -1 \pmod{p}$. Furthermore,

$$\begin{aligned}(p-1)! &= [1 \cdot (p-1)]\,[2 \cdot (p-2)] \cdots [(p-1)/2 \cdot (p+1)/2] \\ &\equiv (1 \cdot -1)\,(2 \cdot -2) \cdots [(p-1)/2 \cdot (-(p-1)/2))] \pmod{p} \\ &\equiv (-1)^{\frac{p-1}{2}} \left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod{p}\end{aligned}$$

If $p \equiv 1 \pmod{4}$, then $x = \left(\frac{p-1}{2}\right)!$ solves $x^2 \equiv -1 \pmod{p}$.