A Randomized Algorithm for Primality

Piotr Wojciechowski[1]

[1]Lane Department of Computer Science and Electrical Engineering
West Virginia University

Outline

Outline

Outline

Goal

Want to show that there is a polynomial time algorithm for testing Primality

Attempt at a simple algorithm

1. Pick a random residue $a \mod N$
2. If $a^{N-1} \not\equiv 1 mod N$ answer N is composite
3. Otherwise answer N is probably prime.

Cases of Algorithm failure

However this algorithm fails due to numbers like $N = 561$ which have the property that for all residues $r \in \Phi(N)$, $r^{N-1} \equiv 1 \mod N$. Such numbers are referred to as *Carmichael Numbers*. The Carmichael numbers have this property is because for all primes $p|N$, $p - 1|N - 1$.

Example

For $N = 591$ we have that $561 = 3 \cdot 11 \cdot 17$ and $560 = 2 \cdot 280$, $560 = 10 \cdot 56$, and $560 = 16 \cdot 35$.

Goal

Want to show that there is a polynomial time algorithm for testing Primality

Attempt at a simple algorithm

1. Pick a random residue $a \mod N$
2. If $a^{N-1} \not\equiv 1 mod N$ answer N is composite
3. Otherwise answer N is probably prime.

Cases of Algorithm failure

However this algorithm fails due to numbers like $N = 561$ which have the property that for all residues $r \in \Phi(N)$, $r^{N-1} \equiv 1 \mod N$. Such numbers are referred to as *Carmichael Numbers*. The Carmichael numbers have this property is because for all primes $p|N$, $p - 1|N - 1$.

Example

For $N = 591$ we have that $561 = 3 \cdot 11 \cdot 17$ and $560 = 2 \cdot 280$, $560 = 10 \cdot 56$, and $560 = 16 \cdot 35$.

Goal

Want to show that there is a polynomial time algorithm for testing Primality

Attempt at a simple algorithm

1. Pick a random residue $a \mod N$
2. If $a^{N-1} \not\equiv 1 mod N$ answer N is composite
3. Otherwise answer N is probably prime.

Cases of Algorithm failure

However this algorithm fails due to numbers like $N = 561$ which have the property that for all residues $r \in \Phi(N)$, $r^{N-1} \equiv 1 \mod N$. Such numbers are referred to as *Carmichael Numbers*. The Carmichael numbers have this property is because for all primes $p|N$, $p - 1|N - 1$.

Example

For $N = 591$ we have that $561 = 3 \cdot 11 \cdot 17$ and $560 = 2 \cdot 280$, $560 = 10 \cdot 56$, and $560 = 16 \cdot 35$.

Goal

Want to show that there is a polynomial time algorithm for testing Primality

Attempt at a simple algorithm

1. Pick a random residue $a \mod N$
2. If $a^{N-1} \not\equiv 1 mod N$ answer N is composite
3. Otherwise answer N is probably prime.

Cases of Algorithm failure

However this algorithm fails due to numbers like $N = 561$ which have the property that for all residues $r \in \Phi(N)$, $r^{N-1} \equiv 1 \mod N$. Such numbers are referred to as *Carmichael Numbers*. The Carmichael numbers have this property is because for all primes $p|N$, $p - 1|N - 1$.

Example

For $N = 591$ we have that $561 = 3 \cdot 11 \cdot 17$ and $560 = 2 \cdot 280$, $560 = 10 \cdot 56$, and $560 = 16 \cdot 35$.

Goal

Want to show that there is a polynomial time algorithm for testing Primality

Attempt at a simple algorithm

1. Pick a random residue $a \mod N$
2. If $a^{N-1} \not\equiv 1 mod N$ answer N is composite
3. Otherwise answer N is probably prime.

Cases of Algorithm failure

However this algorithm fails due to numbers like $N = 561$ which have the property that for all residues $r \in \Phi(N)$, $r^{N-1} \equiv 1 \mod N$. Such numbers are referred to as *Carmichael Numbers*. The Carmichael numbers have this property is because for all primes $p|N$, $p - 1|N - 1$.

Example

For $N = 591$ we have that $561 = 3 \cdot 11 \cdot 17$ and $560 = 2 \cdot 280$, $560 = 10 \cdot 56$, and $560 = 16 \cdot 35$.

Goal

Want to show that there is a polynomial time algorithm for testing Primality

Attempt at a simple algorithm

1. Pick a random residue $a \mod N$
2. If $a^{N-1} \not\equiv 1 mod N$ answer N is composite
3. Otherwise answer N is probably prime.

Cases of Algorithm failure

However this algorithm fails due to numbers like $N = 561$ which have the property that for all residues $r \in \Phi(N)$, $r^{N-1} \equiv 1 \mod N$. Such numbers are referred to as *Carmichael Numbers*. The Carmichael numbers have this property is because for all primes $p|N, p-1|N-1$.

Example

For $N = 591$ we have that $561 = 3 \cdot 11 \cdot 17$ and $560 = 2 \cdot 280$, $560 = 10 \cdot 56$, and $560 = 16 \cdot 35$.

Goal

Want to show that there is a polynomial time algorithm for testing Primality

Attempt at a simple algorithm

1. Pick a random residue $a \mod N$
2. If $a^{N-1} \not\equiv 1 mod N$ answer N is composite
3. Otherwise answer N is probably prime.

Cases of Algorithm failure

However this algorithm fails due to numbers like $N = 561$ which have the property that for all residues $r \in \Phi(N)$, $r^{N-1} \equiv 1 \mod N$. Such numbers are referred to as *Carmichael Numbers*. The Carmichael numbers have this property is because for all primes $p|N$, $p - 1|N - 1$.

Example

For $N = 591$ we have that $561 = 3 \cdot 11 \cdot 17$ and $560 = 2 \cdot 280$, $560 = 10 \cdot 56$, and $560 = 16 \cdot 35$.

Outline

Goal

Want to show that the equation $x^2 \equiv a \mod p$ where p is a prime and $a \not\equiv 0 \mod p$ has 0 or 2 solutions.

Theorem

Let p be a prime, if $a^{\frac{p-1}{2}} \equiv 1 \mod p$ then the equation $x^2 \equiv a \mod p$ has two roots. If $a^{\frac{p-1}{2}} \not\equiv 1 \mod p$ (and $a \not\equiv 0 \mod p$) then $a^{\frac{p-1}{2}} \equiv -1 \mod p$ and the equation $x^2 \equiv a \mod p$ has no roots.

Proof.

As p is prime then it has a primitive root r. Thus $a \equiv r^i \mod p$ for some $i < p-1$. There are two cases.

If, $i = 2 * j$ is even, then $a^{\frac{p-1}{2}} \equiv r^{j(p-1)} \equiv 1 \mod p$ and a has two square roots, r^j and $r^{j+\frac{p-1}{2}}$.

This accounts for half of the residues mod p and since each already has two square roots none of the remaining residues have any. So, if $i = 2j+1$ is odd then then r^i has no square roots p, and $a^{\frac{p-1}{2}} \equiv r^{\frac{p-1}{2}} \mod p$. We have that the latter number is a square root of $1 \mod p$ and is not $1 \mod p$ thus $a^{\frac{p-1}{2}} \equiv -1 \mod p$. □

Goal

Want to show that the equation $x^2 \equiv a \mod p$ where p is a prime and $a \not\equiv 0 \mod p$ has 0 or 2 solutions.

Theorem

Let p be a prime, if $a^{\frac{p-1}{2}} \equiv 1 \mod p$ then the equation $x^2 \equiv a \mod p$ has two roots. If $a^{\frac{p-1}{2}} \not\equiv 1 \mod p$ (and $a \not\equiv 0 \mod p$) then $a^{\frac{p-1}{2}} \equiv -1 \mod p$ and the equation $x^2 \equiv a \mod p$ has no roots.

Proof.

As p is prime then it has a primitive root r. Thus $a \equiv r^i \mod p$ for some $i < p-1$. There are two cases.

If, $i = 2 * j$ is even, then $a^{\frac{p-1}{2}} \equiv r^{j(p-1)} \equiv 1 \mod p$ and a has two square roots, r^j and $r^{j+\frac{p-1}{2}}$.

This accounts for half of the residues mod p and since each already has two square roots none of the remaining residues have any. So, if $i = 2j+1$ is odd then then r^i has no square roots p, and $a^{\frac{p-1}{2}} \equiv r^{\frac{p-1}{2}} \mod p$. We have that the latter number is a square root of $1 \mod p$ and is not $1 \mod p$ thus $a^{\frac{p-1}{2}} \equiv -1 \mod p$. □

Goal

Want to show that the equation $x^2 \equiv a \mod p$ where p is a prime and $a \not\equiv 0 \mod p$ has 0 or 2 solutions.

Theorem

Let p be a prime, if $a^{\frac{p-1}{2}} \equiv 1 \mod p$ then the equation $x^2 \equiv a \mod p$ has two roots. If $a^{\frac{p-1}{2}} \not\equiv 1 \mod p$ (and $a \not\equiv 0 \mod p$) then $a^{\frac{p-1}{2}} \equiv -1 \mod p$ and the equation $x^2 \equiv a \mod p$ has no roots.

Proof.

As p is prime then it has a primitive root r. Thus $a \equiv r^i \mod p$ for some $i < p - 1$.
There are two cases.
If, $i = 2 * j$ is even, then $a^{\frac{p-1}{2}} \equiv r^{j(p-1)} \equiv 1 \mod p$ and a has two square roots, r^j and $r^{j+\frac{p-1}{2}}$.
This accounts for half of the residues mod p and since each already has two square roots none of the remaining residues have any. So, if $i = 2j + 1$ is odd then then r^i has no square roots p, and $a^{\frac{p-1}{2}} \equiv r^{\frac{p-1}{2}} \mod p$. We have that the latter number is a square root of $1 \mod p$ and is not $1 \mod p$ thus $a^{\frac{p-1}{2}} \equiv -1 \mod p$. □

Goal

Want to show that the equation $x^2 \equiv a \mod p$ where p is a prime and $a \not\equiv 0 \mod p$ has 0 or 2 solutions.

Theorem

Let p be a prime, if $a^{\frac{p-1}{2}} \equiv 1 \mod p$ then the equation $x^2 \equiv a \mod p$ has two roots. If $a^{\frac{p-1}{2}} \not\equiv 1 \mod p$ (and $a \not\equiv 0 \mod p$) then $a^{\frac{p-1}{2}} \equiv -1 \mod p$ and the equation $x^2 \equiv a \mod p$ has no roots.

Proof.

As p is prime then it has a primitive root r. Thus $a \equiv r^i \mod p$ for some $i < p-1$. There are two cases.

If, $i = 2 * j$ is even, then $a^{\frac{p-1}{2}} \equiv r^{j(p-1)} \equiv 1 \mod p$ and a has two square roots, r^j and $r^{j+\frac{p-1}{2}}$.

This accounts for half of the residues mod p and since each already has two square roots none of the remaining residues have any. So, if $i = 2j+1$ is odd then then r^i has no square roots p, and $a^{\frac{p-1}{2}} \equiv r^{\frac{p-1}{2}} \mod p$. We have that the latter number is a square root of $1 \mod p$ and is not $1 \mod p$ thus $a^{\frac{p-1}{2}} \equiv -1 \mod p$. □

Goal

Want to show that the equation $x^2 \equiv a \mod p$ where p is a prime and $a \not\equiv 0 \mod p$ has 0 or 2 solutions.

Theorem

Let p be a prime, if $a^{\frac{p-1}{2}} \equiv 1 \mod p$ then the equation $x^2 \equiv a \mod p$ has two roots. If $a^{\frac{p-1}{2}} \not\equiv 1 \mod p$ (and $a \not\equiv 0 \mod p$) then $a^{\frac{p-1}{2}} \equiv -1 \mod p$ and the equation $x^2 \equiv a \mod p$ has no roots.

Proof.

As p is prime then it has a primitive root r. Thus $a \equiv r^i \mod p$ for some $i < p-1$. There are two cases.

If, $i = 2 * j$ is even, then $a^{\frac{p-1}{2}} \equiv r^{j(p-1)} \equiv 1 \mod p$ and a has two square roots, r^j and $r^{j+\frac{p-1}{2}}$.

This accounts for half of the residues mod p and since each already has two square roots none of the remaining residues have any. So, if $i = 2j+1$ is odd then then r^i has no square roots p, and $a^{\frac{p-1}{2}} \equiv r^{\frac{p-1}{2}} \mod p$. We have that the latter number is a square root of $1 \mod p$ and is not $1 \mod p$ thus $a^{\frac{p-1}{2}} \equiv -1 \mod p$. □

Goal

Want to show that the equation $x^2 \equiv a \mod p$ where p is a prime and $a \not\equiv 0 \mod p$ has 0 or 2 solutions.

Theorem

Let p be a prime, if $a^{\frac{p-1}{2}} \equiv 1 \mod p$ then the equation $x^2 \equiv a \mod p$ has two roots. If $a^{\frac{p-1}{2}} \not\equiv 1 \mod p$ (and $a \not\equiv 0 \mod p$) then $a^{\frac{p-1}{2}} \equiv -1 \mod p$ and the equation $x^2 \equiv a \mod p$ has no roots.

Proof.

As p is prime then it has a primitive root r. Thus $a \equiv r^i \mod p$ for some $i < p-1$. There are two cases.

If, $i = 2 * j$ is even, then $a^{\frac{p-1}{2}} \equiv r^{j(p-1)} \equiv 1 \mod p$ and a has two square roots, r^j and $r^{j+\frac{p-1}{2}}$.

This accounts for half of the residues mod p and since each already has two square roots none of the remaining residues have any. So, if $i = 2j+1$ is odd then then r^i has no square roots p, and $a^{\frac{p-1}{2}} \equiv r^{\frac{p-1}{2}} \mod p$. We have that the latter number is a square root of 1 mod p and is not 1 mod p thus $a^{\frac{p-1}{2}} \equiv -1 \mod p$. □

Goal

Want to show that the equation $x^2 \equiv a \mod p$ where p is a prime and $a \not\equiv 0 \mod p$ has 0 or 2 solutions.

Theorem

Let p be a prime, if $a^{\frac{p-1}{2}} \equiv 1 \mod p$ then the equation $x^2 \equiv a \mod p$ has two roots. If $a^{\frac{p-1}{2}} \not\equiv 1 \mod p$ (and $a \not\equiv 0 \mod p$) then $a^{\frac{p-1}{2}} \equiv -1 \mod p$ and the equation $x^2 \equiv a \mod p$ has no roots.

Proof.

As p is prime then it has a primitive root r. Thus $a \equiv r^i \mod p$ for some $i < p-1$. There are two cases.

If, $i = 2 * j$ is even, then $a^{\frac{p-1}{2}} \equiv r^{j(p-1)} \equiv 1 \mod p$ and a has two square roots, r^j and $r^{j+\frac{p-1}{2}}$.

This accounts for half of the residues mod p and since each already has two square roots none of the remaining residues have any. So, if $i = 2j+1$ is odd then then r^i has no square roots p, and $a^{\frac{p-1}{2}} \equiv r^{\frac{p-1}{2}} \mod p$. We have that the latter number is a square root of $1 \mod p$ and is not $1 \mod p$ thus $a^{\frac{p-1}{2}} \equiv -1 \mod p$. □

Goal

Want to show that the equation $x^2 \equiv a \mod p$ where p is a prime and $a \not\equiv 0 \mod p$ has 0 or 2 solutions.

Theorem

Let p be a prime, if $a^{\frac{p-1}{2}} \equiv 1 \mod p$ then the equation $x^2 \equiv a \mod p$ has two roots. If $a^{\frac{p-1}{2}} \not\equiv 1 \mod p$ (and $a \not\equiv 0 \mod p$) then $a^{\frac{p-1}{2}} \equiv -1 \mod p$ and the equation $x^2 \equiv a \mod p$ has no roots.

Proof.

As p is prime then it has a primitive root r. Thus $a \equiv r^i \mod p$ for some $i < p-1$. There are two cases.

If, $i = 2 * j$ is even, then $a^{\frac{p-1}{2}} \equiv r^{j(p-1)} \equiv 1 \mod p$ and a has two square roots, r^j and $r^{j+\frac{p-1}{2}}$.

This accounts for half of the residues mod p and since each already has two square roots none of the remaining residues have any. So, if $i = 2j+1$ is odd then then r^i has no square roots p, and $a^{\frac{p-1}{2}} \equiv r^{\frac{p-1}{2}} \mod p$. We have that the latter number is a square root of $1 \mod p$ and is not $1 \mod p$ thus $a^{\frac{p-1}{2}} \equiv -1 \mod p$. □

Example

Let $p = 5$ and $r = 2$, as $3 \equiv 2^3 \mod 5$ we have that $3^2 \equiv -1 \mod 5$ and 3 has no square roots mod 5.
As $4 \equiv 2^2 \mod 5$ we have that $4^2 \equiv 1 \mod 5$ and 4 has two square roots, 2 and 3, mod 5.

Outline

Definition (Legendre Symbol)

Let $p \neq 2$ be a prime and $a \not\equiv 0 \mod p$, the *Legendre Symbol* of a and p, denoted $(a|p)$ is simply the value, 1 or -1, of $a^{\frac{p-1}{2}} \mod p$

Theorem (Gauss's Lemma)

Let p be a prime, $(p|q) = (-1)^m$ where m is the number of residues in the set $R = \{q \mod p, 2q \mod p, \ldots, \frac{p-1}{2}q \mod p\}$ that are greater than $\frac{p-1}{2}$.

Gauss's Lemma.

First all residues in R are distinct and no two elements in R add up to $0 \mod p$. Let R' be the set of residues that result from R if each of the m elements $a \in R$ such that $a \geq \frac{p-1}{2}$ are replaced by $p - a$. So all elements in R' are no more than $\frac{p-1}{2}$, and, actually, $R' = \{1, 2, \ldots, \frac{p-1}{2}\}$. We also have that $R' = \{\pm q \mod p, \pm 2q \mod p, \ldots, \pm\frac{p-1}{2}q \mod p\}$ where exactly m elements are negated. Taking the product of all the elements in each of these two sets yields that $\frac{p-1}{2}! \equiv (-1)^m q^{\frac{p-1}{2}} \frac{p-1}{2}! \mod p$ and the lemma follows. □

Definition (Legendre Symbol)

Let $p \neq 2$ be a prime and $a \not\equiv 0 \mod p$, the *Legendre Symbol* of a and p, denoted $(a|p)$ is simply the value, 1 or -1, of $a^{\frac{p-1}{2}} \mod p$

Theorem (Gauss's Lemma)

Let p be a prime, $(p|q) = (-1)^m$ where m is the number of residues in the set $R = \{q \mod p, 2q \mod p, \ldots, \frac{p-1}{2}q \mod p\}$ that are greater than $\frac{p-1}{2}$.

Gauss's Lemma.

First all residues in R are distinct and no two elements in R add up to $0 \mod p$. Let R' be the set of residues that result from R if each of the m elements $a \in R$ such that $a \geq \frac{p-1}{2}$ are replaced by $p - a$. So all elements in R' are no more than $\frac{p-1}{2}$, and, actually, $R' = \{1, 2, \ldots, \frac{p-1}{2}\}$. We also have that $R' = \{\pm q \mod p, \pm 2q \mod p, \ldots, \pm\frac{p-1}{2}q \mod p\}$ where exactly m elements are negated. Taking the product of all the elements in each of these two sets yields that $\frac{p-1}{2}! \equiv (-1)^m q^{\frac{p-1}{2}} \frac{p-1}{2}! \mod p$ and the lemma follows. □

Definition (Legendre Symbol)

Let $p \neq 2$ be a prime and $a \not\equiv 0 \mod p$, the *Legendre Symbol* of a and p, denoted $(a|p)$ is simply the value, 1 or -1, of $a^{\frac{p-1}{2}} \mod p$

Theorem (Gauss's Lemma)

Let p be a prime, $(p|q) = (-1)^m$ where m is the number of residues in the set $R = \{q \mod p, 2q \mod p, \ldots, \frac{p-1}{2}q \mod p\}$ that are greater than $\frac{p-1}{2}$.

Gauss's Lemma.

First all residues in R are distinct and no two elements in R add up to $0 \mod p$. Let R' be the set of residues that result from R if each of the m elements $a \in R$ such that $a \geq \frac{p-1}{2}$ are replaced by $p - a$. So all elements in R' are no more than $\frac{p-1}{2}$, and, actually, $R' = \{1, 2, \ldots, \frac{p-1}{2}\}$. We also have that $R' = \{\pm q \mod p, \pm 2q \mod p, \ldots, \pm\frac{p-1}{2}q \mod p\}$ where exactly m elements are negated. Taking the product of all the elements in each of these two sets yields that $\frac{p-1}{2}! \equiv (-1)^m q^{\frac{p-1}{2}} \frac{p-1}{2}! \mod p$ and the lemma follows. □

Definition (Legendre Symbol)

Let $p \neq 2$ be a prime and $a \not\equiv 0 \mod p$, the *Legendre Symbol* of a and p, denoted $(a|p)$ is simply the value, 1 or -1, of $a^{\frac{p-1}{2}} \mod p$

Theorem (Gauss's Lemma)

Let p be a prime, $(p|q) = (-1)^m$ where m is the number of residues in the set $R = \{q \mod p, 2q \mod p, \ldots, \frac{p-1}{2}q \mod p\}$ that are greater than $\frac{p-1}{2}$.

Gauss's Lemma.

First all residues in R are distinct and no two elements in R add up to $0 \mod p$. Let R' be the set of residues that result from R if each of the m elements $a \in R$ such that $a \geq \frac{p-1}{2}$ are replaced by $p - a$. So all elements in R' are no more than $\frac{p-1}{2}$, and, actually, $R' = \{1, 2, \ldots, \frac{p-1}{2}\}$. We also have that $R' = \{\pm q \mod p, \pm 2q \mod p, \ldots, \pm\frac{p-1}{2}q \mod p\}$ where exactly m elements are negated. Taking the product of all the elements in each of these two sets yields that $\frac{p-1}{2}! \equiv (-1)^m q^{\frac{p-1}{2}} \frac{p-1}{2}! \mod p$ and the lemma follows. □

Definition (Legendre Symbol)

Let $p \neq 2$ be a prime and $a \not\equiv 0 \mod p$, the *Legendre Symbol* of a and p, denoted $(a|p)$ is simply the value, 1 or -1, of $a^{\frac{p-1}{2}} \mod p$

Theorem (Gauss's Lemma)

Let p be a prime, $(p|q) = (-1)^m$ where m is the number of residues in the set $R = \{q \mod p, 2q \mod p, \ldots, \frac{p-1}{2}q \mod p\}$ that are greater than $\frac{p-1}{2}$.

Gauss's Lemma.

First all residues in R are distinct and no two elements in R add up to $0 \mod p$. Let R' be the set of residues that result from R if each of the m elements $a \in R$ such that $a \geq \frac{p-1}{2}$ are replaced by $p - a$. So all elements in R' are no more than $\frac{p-1}{2}$, and, actually, $R' = \{1, 2, \ldots, \frac{p-1}{2}\}$. We also have that $R' = \{\pm q \mod p, \pm 2q \mod p, \ldots, \pm\frac{p-1}{2}q \mod p\}$ where exactly m elements are negated. Taking the product of all the elements in each of these two sets yields that $\frac{p-1}{2}! \equiv (-1)^m q^{\frac{p-1}{2}} \frac{p-1}{2}! \mod p$ and the lemma follows. □

Definition (Legendre Symbol)

Let $p \neq 2$ be a prime and $a \not\equiv 0 \mod p$, the *Legendre Symbol* of a and p, denoted $(a|p)$ is simply the value, 1 or -1, of $a^{\frac{p-1}{2}} \mod p$

Theorem (Gauss's Lemma)

Let p be a prime, $(p|q) = (-1)^m$ *where m is the number of residues in the set* $R = \{q \mod p, 2q \mod p, \ldots, \frac{p-1}{2}q \mod p\}$ *that are greater than* $\frac{p-1}{2}$.

Gauss's Lemma.

First all residues in R are distinct and no two elements in R add up to $0 \mod p$. Let R' be the set of residues that result from R if each of the m elements $a \in R$ such that $a \geq \frac{p-1}{2}$ are replaced by $p - a$. So all elements in R' are no more than $\frac{p-1}{2}$, and, actually, $R' = \{1, 2, \ldots, \frac{p-1}{2}\}$. We also have that $R' = \{\pm q \mod p, \pm 2q \mod p, \ldots, \pm\frac{p-1}{2}q \mod p\}$ where exactly m elements are negated. Taking the product of all the elements in each of these two sets yields that $\frac{p-1}{2}! \equiv (-1)^m q^{\frac{p-1}{2}} \frac{p-1}{2}! \mod p$ and the lemma follows. □

Definition (Legendre Symbol)

Let $p \neq 2$ be a prime and $a \not\equiv 0 \mod p$, the *Legendre Symbol* of a and p, denoted $(a|p)$ is simply the value, 1 or -1, of $a^{\frac{p-1}{2}} \mod p$

Theorem (Gauss's Lemma)

Let p be a prime, $(p|q) = (-1)^m$ *where m is the number of residues in the set* $R = \{q \mod p, 2q \mod p, \ldots, \frac{p-1}{2}q \mod p\}$ *that are greater than* $\frac{p-1}{2}$.

Gauss's Lemma.

First all residues in R are distinct and no two elements in R add up to $0 \mod p$. Let R' be the set of residues that result from R if each of the m elements $a \in R$ such that $a \geq \frac{p-1}{2}$ are replaced by $p - a$. So all elements in R' are no more than $\frac{p-1}{2}$, and, actually, $R' = \{1, 2, \ldots, \frac{p-1}{2}\}$. We also have that $R' = \{\pm q \mod p, \pm 2q \mod p, \ldots, \pm\frac{p-1}{2}q \mod p\}$ where exactly m elements are negated. Taking the product of all the elements in each of these two sets yields that $\frac{p-1}{2}! \equiv (-1)^m q^{\frac{p-1}{2}} \frac{p-1}{2}! \mod p$ and the lemma follows. □

Example

$(4,5) = 1 = 1^2$ and $R = \{4 \mod 5, 2 * 4 \mod 5\} = \{4,3\}$ which has two elements greater than 2.

Outline

Theorem (Legendre's Law of Quadratic Reciprocity)

Let $p \neq 2$ and $q \neq 2$ be primes, then $(p|q) \cdot (q|p) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Legendre's Law of Quadratic Reciprocity.

First we calculate $(q|p)$. Let us look at the set R' from the previous proof, and consider the sum of its elements $\mod 2$. As $R' = 1, 2, \ldots, \frac{p-1}{2}$ then this sum is simply $\sum_{i=1}^{\frac{p-1}{2}} i \mod 2$. But if we look at how R' was derived we get that the sum is $q\sum_{i=1}^{\frac{p-1}{2}} i - p\sum_{i=1}^{\frac{p-1}{2}} \lfloor \frac{iq}{p} \rfloor + m_p p \mod 2$. The first term is simply sum of the original $\{q, 2q, \ldots, \frac{p-1}{2}q\}$. The second term accounts for taking the residues $\mod p$. The third term accounts for replacing m_p elements a with $p - a$. Thus equating these two sums and simplifying we get that $m_p = \sum_{i=1}^{\frac{p-1}{2}} \lfloor \frac{iq}{p} \rfloor$. Similarly $m_q = \sum_{i=1}^{\frac{q-1}{2}} \lfloor \frac{ip}{q} \rfloor$. □

Theorem (Legendre's Law of Quadratic Reciprocity)

Let $p \neq 2$ and $q \neq 2$ be primes, then $(p|q) \cdot (q|p) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Legendre's Law of Quadratic Reciprocity.

First we calculate $(q|p)$. Let us look at the set R' from the previous proof, and consider the sum of its elements $\mod 2$. As $R' = 1, 2, \ldots, \frac{p-1}{2}$ then this sum is simply $\sum_{i=1}^{\frac{p-1}{2}} i \mod 2$. But if we look at how R' was derived we get that the sum is $q\sum_{i=1}^{\frac{p-1}{2}} i - p\sum_{i=1}^{\frac{p-1}{2}} \lfloor \frac{iq}{p} \rfloor + m_p p \mod 2$. The first term is simply sum of the original $\{q, 2q, \ldots, \frac{p-1}{2}q\}$. The second term accounts for taking the residues $\mod p$. The third term accounts for replacing m_p elements a with $p - a$. Thus equating these two sums and simplifying we get that $m_p = \sum_{i=1}^{\frac{p-1}{2}} \lfloor \frac{iq}{p} \rfloor$. Similarly $m_q = \sum_{i=1}^{\frac{q-1}{2}} \lfloor \frac{ip}{q} \rfloor$. $\square$

Theorem (Legendre's Law of Quadratic Reciprocity)

Let $p \neq 2$ and $q \neq 2$ be primes, then $(p|q) \cdot (q|p) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Legendre's Law of Quadratic Reciprocity.

First we calculate $(q|p)$. Let us look at the set R' from the previous proof, and consider the sum of its elements $\mod 2$. As $R' = 1, 2, \ldots, \frac{p-1}{2}$ then this sum is simply $\sum_{i=1}^{\frac{p-1}{2}} i \mod 2$. But if we look at how R' was derived we get that the sum is $q\sum_{i=1}^{\frac{p-1}{2}} i - p\sum_{i=1}^{\frac{p-1}{2}} \lfloor \frac{iq}{p} \rfloor + m_p p \mod 2$. The first term is simply sum of the original $\{q, 2q, \ldots, \frac{p-1}{2}q\}$. The second term accounts for taking the residues $\mod p$. The third term accounts for replacing m_p elements a with $p - a$. Thus equating these two sums and simplifying we get that $m_p = \sum_{i=1}^{\frac{p-1}{2}} \lfloor \frac{iq}{p} \rfloor$. Similarly $m_q = \sum_{i=1}^{\frac{q-1}{2}} \lfloor \frac{ip}{q} \rfloor$. □

Theorem (Legendre's Law of Quadratic Reciprocity)

Let $p \neq 2$ and $q \neq 2$ be primes, then $(p|q) \cdot (q|p) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Legendre's Law of Quadratic Reciprocity.

First we calculate $(q|p)$. Let us look at the set R' from the previous proof, and consider the sum of its elements $\mod 2$. As $R' = 1, 2, \ldots, \frac{p-1}{2}$ then this sum is simply $\sum_{i=1}^{\frac{p-1}{2}} i \mod 2$. But if we look at how R' was derived we get that the sum is $q\sum_{i=1}^{\frac{p-1}{2}} i - p\sum_{i=1}^{\frac{p-1}{2}} \lfloor \frac{iq}{p} \rfloor + m_p p \mod 2$. The first term is simply sum of the original $\{q, 2q, \ldots, \frac{p-1}{2}q\}$. The second term accounts for taking the residues $\mod p$. The third term accounts for replacing m_p elements a with $p - a$. Thus equating these two sums and simplifying we get that $m_p = \sum_{i=1}^{\frac{p-1}{2}} \lfloor \frac{iq}{p} \rfloor$. Similarly $m_q = \sum_{i=1}^{\frac{q-1}{2}} \lfloor \frac{ip}{q} \rfloor$. □

Theorem (Legendre's Law of Quadratic Reciprocity)

Let $p \neq 2$ and $q \neq 2$ be primes, then $(p|q) \cdot (q|p) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Legendre's Law of Quadratic Reciprocity.

First we calculate $(q|p)$. Let us look at the set R' from the previous proof, and consider the sum of its elements $\mod 2$. As $R' = 1, 2, \ldots, \frac{p-1}{2}$ then this sum is simply $\sum_{i=1}^{\frac{p-1}{2}} i \mod 2$. But if we look at how R' was derived we get that the sum is $q\sum_{i=1}^{\frac{p-1}{2}} i - p\sum_{i=1}^{\frac{p-1}{2}} \lfloor \frac{iq}{p} \rfloor + m_p p \mod 2$. The first term is simply sum of the original $\{q, 2q, \ldots, \frac{p-1}{2}q\}$. The second term accounts for taking the residues $\mod p$. The third term accounts for replacing m_p elements a with $p - a$. Thus equating these two sums and simplifying we get that $m_p = \sum_{i=1}^{\frac{p-1}{2}} \lfloor \frac{iq}{p} \rfloor$. Similarly $m_q = \sum_{i=1}^{\frac{q-1}{2}} \lfloor \frac{ip}{q} \rfloor$. □

Theorem (Legendre's Law of Quadratic Reciprocity)

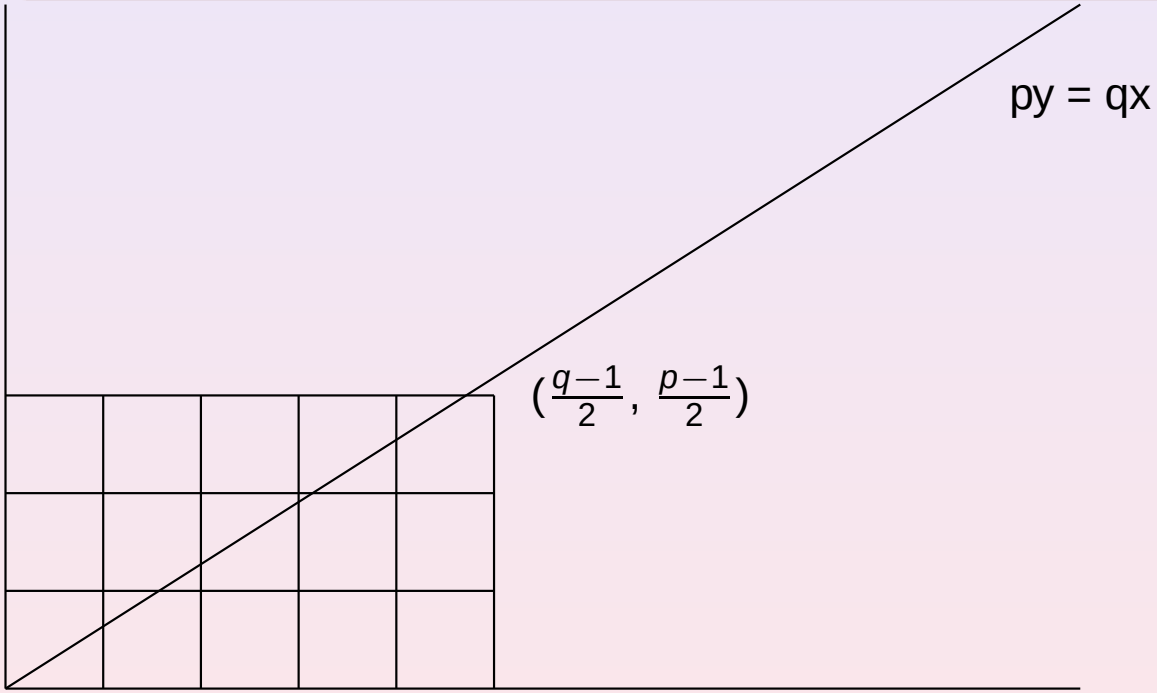
Let $p \neq 2$ and $q \neq 2$ be primes, then $(p|q) \cdot (q|p) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

Legendre's Law of Quadratic Reciprocity.

First we calculate $(q|p)$. Let us look at the set R' from the previous proof, and consider the sum of its elements $\mod 2$. As $R' = 1, 2, \ldots, \frac{p-1}{2}$ then this sum is simply $\sum_{i=1}^{\frac{p-1}{2}} i \mod 2$. But if we look at how R' was derived we get that the sum is $q\sum_{i=1}^{\frac{p-1}{2}} i - p\sum_{i=1}^{\frac{p-1}{2}} \lfloor \frac{iq}{p} \rfloor + m_p p \mod 2$. The first term is simply sum of the original $\{q, 2q, \ldots, \frac{p-1}{2}q\}$. The second term accounts for taking the residues $\mod p$. The third term accounts for replacing m_p elements a with $p - a$. Thus equating these two sums and simplifying we get that $m_p = \sum_{i=1}^{\frac{p-1}{2}} \lfloor \frac{iq}{p} \rfloor$. Similarly $m_q = \sum_{i=1}^{\frac{q-1}{2}} \lfloor \frac{ip}{q} \rfloor$. □

Proof (cont.)

It we look at the values of m_p and m_q geometrically we see that m_p is the *number of positive integer points in the* $\frac{p-1}{2} \times \frac{q-1}{2}$ *rectangle bellow the line* $py = qx$ and m_q is the number of these points above that line. □



Proof.

Thus $(p|q) \cdot (q|p) = (-1)^{m_p + m_q} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$. □

Goal

We will now extend the Legendre Symbol to cover non-prime numbers.

Definition (Legendre Symbol)

Let $N = q_1 q_2 \dots q_n$ where the q_is are odd primes. We define $(M|N) = \prod_{i=1}^{n} (M|q_i)$

Example

$(4|15) = (4|3)(4|5) = (4 \mod 3) \cdot (4^2 \mod 5) = 1$

Goal

We will now extend the Legendre Symbol to cover non-prime numbers.

Definition (Legendre Symbol)

Let $N = q_1 q_2 \dots q_n$ where the q_is are odd primes. We define $(M|N) = \prod_{i=1}^{n} (M|q_i)$

Example

$(4|15) = (4|3)(4|5) = (4 \mod 3) \cdot (4^2 \mod 5) = 1$

Goal

We will now extend the Legendre Symbol to cover non-prime numbers.

Definition (Legendre Symbol)

Let $N = q_1 q_2 \dots q_n$ where the q_is are odd primes. We define $(M|N) = \prod_{i=1}^{n} (M|q_i)$

Example

$(4|15) = (4|3)(4|5) = (4 \mod 3) \cdot (4^2 \mod 5) = 1$

Theorem

1. $(M_1M_2|N) = (M_1|N)(M_2|N)$
2. $(M+N|N) = (M|N)$
3. $(M|N)(N|M) = (-1)^{\frac{M-1}{2}\frac{N-1}{2}}$

Proof.

Let $N = q_1 \dots q_n$ be the prime factorization of N and $M = p_1 \dots p_m$ be the prime factorization of M.

1. $(M_1M_2|N) = \prod_{i=1}^{n}(M_1M_2|q_i) = \prod_{i=1}^{n}(M_1|q_i)(M_2|q_i) = (M_1|N)(M_2|N)$
2. $(M+N|N) = \prod_{i=1}^{n}(M+N|q_i) = \prod_{i=1}^{n}(M|q_i) = (M|N)$
3. $(M|N)(N|M) = \prod_{i=1}^{n}\prod_{j=1}^{m}(p_j|q_i)(q_i|p_j) = (-1)^{\sum_{i=1}^{n}\sum_{j=1}^{m}\frac{p_j-1}{2}\frac{q_i-1}{2}} = (-1)^{\sum_{i=1}^{n}\frac{q_i-1}{2}\sum_{j=1}^{m}\frac{p_j-1}{2}} = (-1)^{\frac{M-1}{2}\frac{N-1}{2}}$

The final step for the third part holds because if a and b are odd then $\frac{a-1}{2} + \frac{b-1}{2} = \frac{ab-1}{2} \mod 2$

□

Theorem

1. $(M_1M_2|N) = (M_1|N)(M_2|N)$
2. $(M+N|N) = (M|N)$
3. $(M|N)(N|M) = (-1)^{\frac{M-1}{2}\frac{N-1}{2}}$

Proof.

Let $N = q_1 \dots q_n$ be the prime factorization of N and $M = p_1 \dots p_m$ be the prime factorization of M.

1. $(M_1M_2|N) = \prod_{i=1}^{n}(M_1M_2|q_i) = \prod_{i=1}^{n}(M_1|q_i)(M_2|q_i) = (M_1|N)(M_2|N)$
2. $(M+N|N) = \prod_{i=1}^{n}(M+N|q_i) = \prod_{i=1}^{n}(M|q_i) = (M|N)$
3. $(M|N)(N|M) = \prod_{i=1}^{n}\prod_{j=1}^{m}(p_j|q_i)(q_i|p_j) = (-1)^{\sum_{i=1}^{n}\sum_{j=1}^{m}\frac{p_j-1}{2}\frac{q_i-1}{2}} = (-1)^{\sum_{i=1}^{n}\frac{q_i-1}{2}\sum_{j=1}^{m}\frac{p_j-1}{2}} = (-1)^{\frac{M-1}{2}\frac{N-1}{2}}$

The final step for the third part holds because if a and b are odd then $\frac{a-1}{2} + \frac{b-1}{2} = \frac{ab-1}{2} \mod 2$

□

Theorem

1. $(M_1M_2|N) = (M_1|N)(M_2|N)$
2. $(M+N|N) = (M|N)$
3. $(M|N)(N|M) = (-1)^{\frac{M-1}{2}\frac{N-1}{2}}$

Proof.

Let $N = q_1 \dots q_n$ be the prime factorization of N and $M = p_1 \dots p_m$ be the prime factorization of M.

1. $(M_1M_2|N) = \prod_{i=1}^{n}(M_1M_2|q_i) = \prod_{i=1}^{n}(M_1|q_i)(M_2|q_i) = (M_1|N)(M_2|N)$
2. $(M+N|N) = \prod_{i=1}^{n}(M+N|q_i) = \prod_{i=1}^{n}(M|q_i) = (M|N)$
3. $(M|N)(N|M) = \prod_{i=1}^{n}\prod_{j=1}^{m}(p_j|q_i)(q_i|p_j) = (-1)^{\sum_{i=1}^{n}\sum_{j=1}^{m}\frac{p_j-1}{2}\frac{q_i-1}{2}} = (-1)^{\sum_{i=1}^{n}\frac{q_i-1}{2}\sum_{j=1}^{m}\frac{p_j-1}{2}} = (-1)^{\frac{M-1}{2}\frac{N-1}{2}}$

The final step for the third part holds because if a and b are odd then $\frac{a-1}{2} + \frac{b-1}{2} = \frac{ab-1}{2} \mod 2$

□

Theorem

1. $(M_1M_2|N) = (M_1|N)(M_2|N)$
2. $(M+N|N) = (M|N)$
3. $(M|N)(N|M) = (-1)^{\frac{M-1}{2}\frac{N-1}{2}}$

Proof.

Let $N = q_1 \dots q_n$ be the prime factorization of N and $M = p_1 \dots p_m$ be the prime factorization of M.

1. $(M_1M_2|N) = \prod_{i=1}^{n}(M_1M_2|q_i) = \prod_{i=1}^{n}(M_1|q_i)(M_2|q_i) = (M_1|N)(M_2|N)$
2. $(M+N|N) = \prod_{i=1}^{n}(M+N|q_i) = \prod_{i=1}^{n}(M|q_i) = (M|N)$
3. $(M|N)(N|M) = \prod_{i=1}^{n}\prod_{j=1}^{m}(p_j|q_i)(q_i|p_j) = (-1)^{\sum_{i=1}^{n}\sum_{j=1}^{m}\frac{p_j-1}{2}\frac{q_i-1}{2}} = (-1)^{\sum_{i=1}^{n}\frac{q_i-1}{2}\sum_{j=1}^{m}\frac{p_j-1}{2}} = (-1)^{\frac{M-1}{2}\frac{N-1}{2}}$

The final step for the third part holds because if a and b are odd then $\frac{a-1}{2} + \frac{b-1}{2} = \frac{ab-1}{2} \mod 2$

□

Theorem

1. $(M_1M_2|N) = (M_1|N)(M_2|N)$
2. $(M+N|N) = (M|N)$
3. $(M|N)(N|M) = (-1)^{\frac{M-1}{2}\frac{N-1}{2}}$

Proof.

Let $N = q_1 \dots q_n$ be the prime factorization of N and $M = p_1 \dots p_m$ be the prime factorization of M.

1. $(M_1M_2|N) = \prod_{i=1}^{n}(M_1M_2|q_i) = \prod_{i=1}^{n}(M_1|q_i)(M_2|q_i) = (M_1|N)(M_2|N)$
2. $(M+N|N) = \prod_{i=1}^{n}(M+N|q_i) = \prod_{i=1}^{n}(M|q_i) = (M|N)$
3. $(M|N)(N|M) = \prod_{i=1}^{n}\prod_{j=1}^{m}(p_j|q_i)(q_i|p_j) = (-1)^{\sum_{i=1}^{n}\sum_{j=1}^{m}\frac{p_j-1}{2}\frac{q_i-1}{2}} =$
$(-1)^{\sum_{i=1}^{n}\frac{q_i-1}{2}\sum_{j=1}^{m}\frac{p_j-1}{2}} = (-1)^{\frac{M-1}{2}\frac{N-1}{2}}$

The final step for the third part holds because if a and b are odd then $\frac{a-1}{2} + \frac{b-1}{2} = \frac{ab-1}{2} \mod 2$ □

Theorem

1. $(M_1M_2|N) = (M_1|N)(M_2|N)$
2. $(M+N|N) = (M|N)$
3. $(M|N)(N|M) = (-1)^{\frac{M-1}{2}\frac{N-1}{2}}$

Proof.

Let $N = q_1 \dots q_n$ be the prime factorization of N and $M = p_1 \dots p_m$ be the prime factorization of M.

1. $(M_1M_2|N) = \prod_{i=1}^{n}(M_1M_2|q_i) = \prod_{i=1}^{n}(M_1|q_i)(M_2|q_i) = (M_1|N)(M_2|N)$
2. $(M+N|N) = \prod_{i=1}^{n}(M+N|q_i) = \prod_{i=1}^{n}(M|q_i) = (M|N)$
3. $(M|N)(N|M) = \prod_{i=1}^{n}\prod_{j=1}^{m}(p_j|q_i)(q_i|p_j) = (-1)^{\sum_{i=1}^{n}\sum_{j=1}^{m}\frac{p_j-1}{2}\frac{q_i-1}{2}} = (-1)^{\sum_{i=1}^{n}\frac{q_i-1}{2}\sum_{j=1}^{m}\frac{p_j-1}{2}} = (-1)^{\frac{M-1}{2}\frac{N-1}{2}}$

The final step for the third part holds because if a and b are odd then $\frac{a-1}{2} + \frac{b-1}{2} = \frac{ab-1}{2} \mod 2$ □

Theorem

1. $(M_1M_2|N) = (M_1|N)(M_2|N)$
2. $(M+N|N) = (M|N)$
3. $(M|N)(N|M) = (-1)^{\frac{M-1}{2}\frac{N-1}{2}}$

Proof.

Let $N = q_1 \dots q_n$ be the prime factorization of N and $M = p_1 \dots p_m$ be the prime factorization of M.

1. $(M_1M_2|N) = \prod_{i=1}^{n}(M_1M_2|q_i) = \prod_{i=1}^{n}(M_1|q_i)(M_2|q_i) = (M_1|N)(M_2|N)$
2. $(M+N|N) = \prod_{i=1}^{n}(M+N|q_i) = \prod_{i=1}^{n}(M|q_i) = (M|N)$
3. $(M|N)(N|M) = \prod_{i=1}^{n}\prod_{j=1}^{m}(p_j|q_i)(q_i|p_j) = (-1)^{\sum_{i=1}^{n}\sum_{j=1}^{m}\frac{p_j-1}{2}\frac{q_i-1}{2}} = (-1)^{\sum_{i=1}^{n}\frac{q_i-1}{2}\sum_{j=1}^{m}\frac{p_j-1}{2}} = (-1)^{\frac{M-1}{2}\frac{N-1}{2}}$

The final step for the third part holds because if a and b are odd then $\frac{a-1}{2} + \frac{b-1}{2} \equiv \frac{ab-1}{2} \mod 2$ □

Outline

Goal

We now want to show that $(M|N)$ can be computed without knowing the factorization of M or N

Computing $(M|N)$

1. If $M = 2$ compute $(M|N) = (2|N) = (-1)^{\frac{N^2-1}{8}}$
2. If $M = 2K$ is even compute $(M|N) = (2|N)(K|N)$
3. If $M < N$ compute $(M|N) = (-1)^{\frac{M-1}{2}\frac{N-1}{2}} \cdot (N|M)$
4. If $M > N$ compute $(M|N) = (M \mod N|N)$

Example

$(21|55) = (-1)^{10*27} * (55|21) = (13|21) = (-1)^{6*10}(21|13) = (8|13) = (2|13)^3 = (-1)^{3*21} = -1$

Goal

We now want to show that $(M|N)$ can be computed without knowing the factorization of M or N

Computing $(M|N)$

1. If $M = 2$ compute $(M|N) = (2|N) = (-1)^{\frac{N^2-1}{8}}$
2. If $M = 2K$ is even compute $(M|N) = (2|N)(K|N)$
3. If $M < N$ compute $(M|N) = (-1)^{\frac{M-1}{2}\frac{N-1}{2}} \cdot (N|M)$
4. If $M > N$ compute $(M|N) = (M \mod N|N)$

Example

$(21|55) = (-1)^{10*27} * (55|21) = (13|21) = (-1)^{6*10}(21|13) = (8|13) = (2|13)^3 = (-1)^{3*21} = -1$

Goal

We now want to show that $(M|N)$ can be computed without knowing the factorization of M or N

Computing $(M|N)$

1. If $M = 2$ compute $(M|N) = (2|N) = (-1)^{\frac{N^2-1}{8}}$
2. If $M = 2K$ is even compute $(M|N) = (2|N)(K|N)$
3. If $M < N$ compute $(M|N) = (-1)^{\frac{M-1}{2}\frac{N-1}{2}} \cdot (N|M)$
4. If $M > N$ compute $(M|N) = (M \mod N|N)$

Example

$(21|55) = (-1)^{10*27} * (55|21) = (13|21) = (-1)^{6*10}(21|13) = (8|13) = (2|13)^3 = (-1)^{3*21} = -1$

Goal

We now want to show that $(M|N)$ can be computed without knowing the factorization of M or N

Computing $(M|N)$

1. If $M = 2$ compute $(M|N) = (2|N) = (-1)^{\frac{N^2-1}{8}}$
2. If $M = 2K$ is even compute $(M|N) = (2|N)(K|N)$
3. If $M < N$ compute $(M|N) = (-1)^{\frac{M-1}{2}\frac{N-1}{2}} \cdot (N|M)$
4. If $M > N$ compute $(M|N) = (M \mod N|N)$

Example

$(21|55) = (-1)^{10*27} * (55|21) = (13|21) = (-1)^{6*10}(21|13) = (8|13) = (2|13)^3 = (-1)^{3*21} = -1$

Goal

We now want to show that $(M|N)$ can be computed without knowing the factorization of M or N

Computing $(M|N)$

1. If $M = 2$ compute $(M|N) = (2|N) = (-1)^{\frac{N^2-1}{8}}$
2. If $M = 2K$ is even compute $(M|N) = (2|N)(K|N)$
3. If $M < N$ compute $(M|N) = (-1)^{\frac{M-1}{2}\frac{N-1}{2}} \cdot (N|M)$
4. If $M > N$ compute $(M|N) = (M \mod N|N)$

Example

$(21|55) = (-1)^{10*27} * (55|21) = (13|21) = (-1)^{6*10}(21|13) = (8|13) = (2|13)^3 = (-1)^{3*21} = -1$

Goal

We now want to show that $(M|N)$ can be computed without knowing the factorization of M or N

Computing $(M|N)$

1. If $M = 2$ compute $(M|N) = (2|N) = (-1)^{\frac{N^2-1}{8}}$
2. If $M = 2K$ is even compute $(M|N) = (2|N)(K|N)$
3. If $M < N$ compute $(M|N) = (-1)^{\frac{M-1}{2}\frac{N-1}{2}} \cdot (N|M)$
4. If $M > N$ compute $(M|N) = (M \mod N|N)$

Example

$(21|55) = (-1)^{10*27} * (55|21) = (13|21) = (-1)^{6*10}(21|13) = (8|13) = (2|13)^3 = (-1)^{3*21} = -1$

Theorem

$(M|N)$ *and* $\gcd(M,N)$ *can be computed in* $O(\log(I = MN)^3)$ *time.*

Proof.

The computation of powers of -1 is trivial if given the binary expansion of the exponent. The computation of the exponents is also doable within this time frame as such computations involve only multiplications additions and divisions each reduction of $(M|N)$ takes $O(I^2)$ time. As the algorithm takes $O(I)$ reductions the entire algorithm runs in the desired time. A similar argument shows that Euclid's algorithm for finding the GCD runs in similar time as the algorithms are similar. □

Theorem

$(M|N)$ *and* $\gcd(M,N)$ *can be computed in* $O(\log(I = MN)^3)$ *time.*

Proof.

The computation of powers of -1 is trivial if given the binary expansion of the exponent. The computation of the exponents is also doable within this time frame as such computations involve only multiplications additions and divisions each reduction of $(M|N)$ takes $O(I^2)$ time. As the algorithm takes $O(I)$ reductions the entire algorithm runs in the desired time. A similar argument shows that Euclid's algorithm for finding the GCD runs in similar time as the algorithms are similar. □

Theorem

$(M|N)$ *and* $\gcd(M,N)$ *can be computed in* $O(\log(I = MN)^3)$ *time.*

Proof.

The computation of powers of -1 is trivial if given the binary expansion of the exponent. The computation of the exponents is also doable within this time frame as such computations involve only multiplications additions and divisions each reduction of $(M|N)$ takes $O(I^2)$ time. As the algorithm takes $O(I)$ reductions the entire algorithm runs in the desired time. A similar argument shows that Euclid's algorithm for finding the GCD runs in similar time as the algorithms are similar. □

Theorem

$(M|N)$ *and* $\gcd(M,N)$ *can be computed in* $O(\log(I = MN)^3)$ *time.*

Proof.

The computation of powers of -1 is trivial if given the binary expansion of the exponent. The computation of the exponents is also doable within this time frame as such computations involve only multiplications additions and divisions each reduction of $(M|N)$ takes $O(I^2)$ time. As the algorithm takes $O(I)$ reductions the entire algorithm runs in the desired time. A similar argument shows that Euclid's algorithm for finding the GCD runs in similar time as the algorithms are similar. □

Theorem

$(M|N)$ and $\gcd(M,N)$ can be computed in $O(\log(I = MN)^3)$ time.

Proof.

The computation of powers of -1 is trivial if given the binary expansion of the exponent. The computation of the exponents is also doable within this time frame as such computations involve only multiplications additions and divisions each reduction of $(M|N)$ takes $O(I^2)$ time. As the algorithm takes $O(I)$ reductions the entire algorithm runs in the desired time. A similar argument shows that Euclid's algorithm for finding the GCD runs in similar time as the algorithms are similar. □

Outline

Theorem

If $(M|N) = M^{\frac{N-1}{2}} \mod N$ *for all* $M \in \Phi(N)$, *then* N *is a prime.*

Proof.

Assume that there is a contradiction. Let N be a composite number for which $(M|N) = M^{\frac{N-1}{2}} \mod N$ for all $M \in \Phi(N)$. First lets suppose that $N = p_1 \dots p_n$ for distinct odd primes $p_1, \dots, p_n$ and let $r \in \Phi(p_1)$ have $(r|p_1) = -1$. Choose M such that $M \equiv r \mod p_1$ and $M \equiv 1 \mod p_i$ for $1 < i \leq n$. So we have that $M^{\frac{N-1}{2}} \equiv (M|N) \equiv -1 \mod N$. However $M^{\frac{N-1}{2}} \equiv 1 \mod p_2$ leading to a contradiction. Thus there must be a prime p such that $N = p^2 * m$. Let r be a primitive root of p^2. As $(r|N)$ is ± 1 we have that $r^{N-1} \equiv (r|N)^2 \equiv 1 \mod N$. Thus $r^{N-1} \equiv 1 \mod p^2$ and so $p \mid \phi(p^2) \mid N - 1$ leading to a contradiction. □

Theorem

If $(M|N) = M^{\frac{N-1}{2}} \mod N$ *for all* $M \in \Phi(N)$, *then* N *is a prime.*

Proof.

Assume that there is a contradiction. Let N be a composite number for which $(M|N) = M^{\frac{N-1}{2}} \mod N$ for all $M \in \Phi(N)$. First lets suppose that $N = p_1 \dots p_n$ for distinct odd primes $p_1, \dots, p_n$ and let $r \in \Phi(p_1)$ have $(r|p_1) = -1$. Choose M such that $M \equiv r \mod p_1$ and $M \equiv 1 \mod p_i$ for $1 < i \leq n$. So we have that $M^{\frac{N-1}{2}} \equiv (M|N) \equiv -1 \mod N$. However $M^{\frac{N-1}{2}} \equiv 1 \mod p_2$ leading to a contradiction. Thus there must be a prime p such that $N = p^2 * m$. Let r be a primitive root of p^2. As $(r|N)$ is ± 1 we have that $r^{N-1} \equiv (r|N)^2 \equiv 1 \mod N$. Thus $r^{N-1} \equiv 1 \mod p^2$ and so $p \mid \phi(p^2) \mid N - 1$ leading to a contradiction. □

Theorem

If $(M|N) = M^{\frac{N-1}{2}} \mod N$ *for all* $M \in \Phi(N)$, *then* N *is a prime.*

Proof.

Assume that there is a contradiction. Let N be a composite number for which $(M|N) = M^{\frac{N-1}{2}} \mod N$ for all $M \in \Phi(N)$. First lets suppose that $N = p_1 \dots p_n$ for distinct odd primes $p_1, \dots, p_n$ and let $r \in \Phi(p_1)$ have $(r|p_1) = -1$. Choose M such that $M \equiv r \mod p_1$ and $M \equiv 1 \mod p_i$ for $1 < i \leq n$. So we have that $M^{\frac{N-1}{2}} \equiv (M|N) \equiv -1 \mod N$. However $M^{\frac{N-1}{2}} \equiv 1 \mod p_2$ leading to a contradiction. Thus there must be a prime p such that $N = p^2 * m$. Let r be a primitive root of p^2. As $(r|N)$ is ± 1 we have that $r^{N-1} \equiv (r|N)^2 \equiv 1 \mod N$. Thus $r^{N-1} \equiv 1 \mod p^2$ and so $p \mid \phi(p^2) \mid N - 1$ leading to a contradiction. □

Theorem

If $(M|N) = M^{\frac{N-1}{2}} \mod N$ *for all* $M \in \Phi(N)$, *then* N *is a prime.*

Proof.

Assume that there is a contradiction. Let N be a composite number for which $(M|N) = M^{\frac{N-1}{2}} \mod N$ for all $M \in \Phi(N)$. First lets suppose that $N = p_1 \dots p_n$ for distinct odd primes $p_1, \dots, p_n$ and let $r \in \Phi(p_1)$ have $(r|p_1) = -1$. Choose M such that $M \equiv r \mod p_1$ and $M \equiv 1 \mod p_i$ for $1 < i \leq n$. So we have that $M^{\frac{N-1}{2}} \equiv (M|N) \equiv -1 \mod N$. However $M^{\frac{N-1}{2}} \equiv 1 \mod p_2$ leading to a contradiction. Thus there must be a prime p such that $N = p^2 * m$. Let r be a primitive root of p^2. As $(r|N)$ is ± 1 we have that $r^{N-1} \equiv (r|N)^2 \equiv 1 \mod N$. Thus $r^{N-1} \equiv 1 \mod p^2$ and so $p \mid \phi(p^2) \mid N - 1$ leading to a contradiction. □

Theorem

If $(M|N) = M^{\frac{N-1}{2}} \mod N$ *for all* $M \in \Phi(N)$, *then* N *is a prime.*

Proof.

Assume that there is a contradiction. Let N be a composite number for which $(M|N) = M^{\frac{N-1}{2}} \mod N$ for all $M \in \Phi(N)$. First lets suppose that $N = p_1 \dots p_n$ for distinct odd primes $p_1, \dots, p_n$ and let $r \in \Phi(p_1)$ have $(r|p_1) = -1$. Choose M such that $M \equiv r \mod p_1$ and $M \equiv 1 \mod p_i$ for $1 < i \leq n$. So we have that $M^{\frac{N-1}{2}} \equiv (M|N) \equiv -1 \mod N$. However $M^{\frac{N-1}{2}} \equiv 1 \mod p_2$ leading to a contradiction. Thus there must be a prime p such that $N = p^2 * m$. Let r be a primitive root of p^2. As $(r|N)$ is ± 1 we have that $r^{N-1} \equiv (r|N)^2 \equiv 1 \mod N$. Thus $r^{N-1} \equiv 1 \mod p^2$ and so $p \mid \phi(p^2) \mid N - 1$ leading to a contradiction. □

Theorem

If $(M|N) = M^{\frac{N-1}{2}} \mod N$ *for all* $M \in \Phi(N)$, *then* N *is a prime.*

Proof.

Assume that there is a contradiction. Let N be a composite number for which $(M|N) = M^{\frac{N-1}{2}} \mod N$ for all $M \in \Phi(N)$. First lets suppose that $N = p_1 \dots p_n$ for distinct odd primes $p_1, \dots, p_n$ and let $r \in \Phi(p_1)$ have $(r|p_1) = -1$. Choose M such that $M \equiv r \mod p_1$ and $M \equiv 1 \mod p_i$ for $1 < i \leq n$. So we have that $M^{\frac{N-1}{2}} \equiv (M|N) \equiv -1 \mod N$. However $M^{\frac{N-1}{2}} \equiv 1 \mod p_2$ leading to a contradiction. Thus there must be a prime p such that $N = p^2 * m$. Let r be a primitive root of p^2. As $(r|N)$ is ± 1 we have that $r^{N-1} \equiv (r|N)^2 \equiv 1 \mod N$. Thus $r^{N-1} \equiv 1 \mod p^2$ and so $p \mid \phi(p^2) \mid N - 1$ leading to a contradiction. □

Theorem

If N is an odd composite, then for at least half the $M \in \Phi(N)$, $(M|N) \not\equiv M^{\frac{N-1}{2}} \mod N$.

Proof.

From the previous theorem there is at least one $a \in \Phi(N)$ for which $(a|N) \not\equiv a^{\frac{N-1}{2}} \mod N$. Let $B = \{b_1, b_2, ..., b_n\}$ be the set of all distinct residues such that $(b_i|N) \equiv b_i^{\frac{N-1}{2}} \mod N$ and let $a \cdot B = \{ab_1 \mod N, ab_2 \mod N, ..., ab_n \mod N\}$. We have that the elements of $a \cdot B$ are distinct because $a \in \Phi(N)$ and the residues in B are distinct. Let ab be an arbitrary element of $a \cdot B$. Thus $(ab)^{\frac{N-1}{2}} = a^{\frac{N-1}{2}} b^{\frac{N-1}{2}} \not\equiv (a|N)(b|N) \equiv (ab|N) \mod N$. Thus there are at least $|B|$ elements, M of $\Phi(n)$ for which $(M|N) \not\equiv M^{\frac{N-1}{2}} \mod N$. □

Theorem

If N is an odd composite, then for at least half the $M \in \Phi(N)$, $(M|N) \not\equiv M^{\frac{N-1}{2}} \mod N$.

Proof.

From the previous theorem there is at least one $a \in \Phi(N)$ for which $(a|N) \not\equiv a^{\frac{N-1}{2}} \mod N$. Let $B = \{b_1, b_2, ..., b_n\}$ be the set of all distinct residues such that $(b_i|N) \equiv b_i^{\frac{N-1}{2}} \mod N$ and let $a \cdot B = \{ab_1 \mod N, ab_2 \mod N, ..., ab_n \mod N\}$. We have that the elements of $a \cdot B$ are distinct because $a \in \Phi(N)$ and the residues in B are distinct. Let ab be an arbitrary element of $a \cdot B$. Thus $(ab)^{\frac{N-1}{2}} = a^{\frac{N-1}{2}} b^{\frac{N-1}{2}} \not\equiv (a|N)(b|N) \equiv (ab|N) \mod N$. Thus there are at least $|B|$ elements, M of $\Phi(n)$ for which $(M|N) \not\equiv M^{\frac{N-1}{2}} \mod N$. □

Theorem

If N is an odd composite, then for at least half the $M \in \Phi(N)$, $(M|N) \not\equiv M^{\frac{N-1}{2}} \mod N$.

Proof.

From the previous theorem there is at least one $a \in \Phi(N)$ for which $(a|N) \not\equiv a^{\frac{N-1}{2}} \mod N$. Let $B = \{b_1, b_2, ..., b_n\}$ be the set of all distinct residues such that $(b_i|N) \equiv b_i^{\frac{N-1}{2}} \mod N$ and let $a \cdot B = \{ab_1 \mod N, ab_2 \mod N, ..., ab_n \mod N\}$. We have that the elements of $a \cdot B$ are distinct because $a \in \Phi(N)$ and the residues in B are distinct. Let ab be an arbitrary element of $a \cdot B$. Thus $(ab)^{\frac{N-1}{2}} = a^{\frac{N-1}{2}} b^{\frac{N-1}{2}} \not\equiv (a|N)(b|N) \equiv (ab|N) \mod N$. Thus there are at least $|B|$ elements, M of $\Phi(n)$ for which $(M|N) \not\equiv M^{\frac{N-1}{2}} \mod N$. □

Theorem

If N is an odd composite, then for at least half the $M \in \Phi(N)$, $(M|N) \not\equiv M^{\frac{N-1}{2}} \mod N$.

Proof.

From the previous theorem there is at least one $a \in \Phi(N)$ for which $(a|N) \not\equiv a^{\frac{N-1}{2}} \mod N$. Let $B = \{b_1, b_2, ..., b_n\}$ be the set of all distinct residues such that $(b_i|N) \equiv b_i^{\frac{N-1}{2}} \mod N$ and let $a \cdot B = \{ab_1 \mod N, ab_2 \mod N, ..., ab_n \mod N\}$. We have that the elements of $a \cdot B$ are distinct because $a \in \Phi(N)$ and the residues in B are distinct. Let ab be an arbitrary element of $a \cdot B$. Thus $(ab)^{\frac{N-1}{2}} = a^{\frac{N-1}{2}} b^{\frac{N-1}{2}} \not\equiv (a|N)(b|N) \equiv (ab|N) \mod N$. Thus there are at least $|B|$ elements, M of $\Phi(n)$ for which $(M|N) \not\equiv M^{\frac{N-1}{2}} \mod N$. □

Theorem

If N is an odd composite, then for at least half the $M \in \Phi(N)$, $(M|N) \not\equiv M^{\frac{N-1}{2}} \mod N$.

Proof.

From the previous theorem there is at least one $a \in \Phi(N)$ for which $(a|N) \not\equiv a^{\frac{N-1}{2}} \mod N$. Let $B = \{b_1, b_2, ..., b_n\}$ be the set of all distinct residues such that $(b_i|N) \equiv b_i^{\frac{N-1}{2}} \mod N$ and let $a \cdot B = \{ab_1 \mod N, ab_2 \mod N, ..., ab_n \mod N\}$. We have that the elements of $a \cdot B$ are distinct because $a \in \Phi(N)$ and the residues in B are distinct. Let ab be an arbitrary element of $a \cdot B$. Thus $(ab)^{\frac{N-1}{2}} = a^{\frac{N-1}{2}} b^{\frac{N-1}{2}} \not\equiv (a|N)(b|N) \equiv (ab|N) \mod N$. Thus there are at least $|B|$ elements, M of $\Phi(n)$ for which $(M|N) \not\equiv M^{\frac{N-1}{2}} \mod N$. □

Theorem

If N is an odd composite, then for at least half the $M \in \Phi(N)$, $(M|N) \not\equiv M^{\frac{N-1}{2}} \mod N$.

Proof.

From the previous theorem there is at least one $a \in \Phi(N)$ for which $(a|N) \not\equiv a^{\frac{N-1}{2}} \mod N$. Let $B = \{b_1, b_2, ..., b_n\}$ be the set of all distinct residues such that $(b_i|N) \equiv b_i^{\frac{N-1}{2}} \mod N$ and let $a \cdot B = \{ab_1 \mod N, ab_2 \mod N, ..., ab_n \mod N\}$. We have that the elements of $a \cdot B$ are distinct because $a \in \Phi(N)$ and the residues in B are distinct. Let ab be an arbitrary element of $a \cdot B$. Thus $(ab)^{\frac{N-1}{2}} = a^{\frac{N-1}{2}} b^{\frac{N-1}{2}} \not\equiv (a|N)(b|N) \equiv (ab|N) \mod N$. Thus there are at least $|B|$ elements, M of $\Phi(n)$ for which $(M|N) \not\equiv M^{\frac{N-1}{2}} \mod N$. □

Outline

Conclusion

From the previous theorem we can form a randomized algorithm for checking Primality

Algorithm

1. Generate a random integer, M, from 2 to $N-1$.
2. If $\gcd(M,N) \neq 1$ conclude that N is composite.
3. If $(M|N) \not\equiv M^{\frac{N-1}{2}} \mod N$ conclude that N is composite.
4. Otherwise conclude that N is probably a prime.

Conclusion

From the previous theorem we can form a randomized algorithm for checking Primality

Algorithm

1. Generate a random integer, M, from 2 to $N-1$.
2. If $\gcd(M,N) \neq 1$ conclude that N is composite.
3. If $(M|N) \not\equiv M^{\frac{N-1}{2}} \mod N$ conclude that N is composite.
4. Otherwise conclude that N is probably a prime.

Conclusion

From the previous theorem we can form a randomized algorithm for checking Primality

Algorithm

1. Generate a random integer, M, from 2 to $N-1$.
2. If $\gcd(M,N) \neq 1$ conclude that N is composite.
3. If $(M|N) \not\equiv M^{\frac{N-1}{2}} \mod N$ conclude that N is composite.
4. Otherwise conclude that N is probably a prime.

Conclusion

From the previous theorem we can form a randomized algorithm for checking Primality

Algorithm

1. Generate a random integer, M, from 2 to $N-1$.
2. If $\gcd(M,N) \neq 1$ conclude that N is composite.
3. If $(M|N) \not\equiv M^{\frac{N-1}{2}} \mod N$ conclude that N is composite.
4. Otherwise conclude that N is probably a prime.

Conclusion

From the previous theorem we can form a randomized algorithm for checking Primality

Algorithm

1. Generate a random integer, M, from 2 to $N - 1$.
2. If $\gcd(M, N) \neq 1$ conclude that N is composite.
3. If $(M|N) \not\equiv M^{\frac{N-1}{2}} \mod N$ conclude that N is composite.
4. Otherwise conclude that N is probably a prime.