The complexity class coNP

Piotr Wojciechowski[1]

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

Outline

1. Description of coNP and examples of problems
   - What is coNP
   - Examples of problems in coNP
2. The NP $\cap$ coNP complexity class
   - Properties of NP $\cap$ coNP
   - Problems in NP $\cap$ coNP
3. NP, coNP, and P
   - The P, NP, coNP Hierarchy

Outline

Outline

Outline

coNP as related to NP

Definition (coNP)

coNP is the complexity class which contains the complements of problems found in NP.

Another way of looking at coNP

Just as NP can be considered to be the set of problems with succinct ”yes” certificates, coNP can be considered to be the set of problems with succinct ”no” certificates. This means that a ”no” instance of a problem in coNP has a short proof of it being a ”no” instance.

coNP as related to NP

Definition (coNP)

coNP is the complexity class which contains the complements of problems found in NP.

Another way of looking at coNP

Just as NP can be considered to be the set of problems with succinct ”yes” certificates, coNP can be considered to be the set of problems with succinct ”no” certificates. This means that a ”no” instance of a problem in coNP has a short proof of it being a ”no” instance.

Outline

Examples

1. coSAT $= \{\langle b \rangle : b$ is a boolean expression with no satisfying assignments$\}$
2. PRIMES $= \{\langle p \rangle : p$ is a prime number$\}$

Examples

1. coSAT $= \{\langle b \rangle : b$ is a boolean expression with no satisfying assignments$\}$
2. PRIMES $= \{\langle p \rangle : p$ is a prime number$\}$

Outline

Properties

Problems have both succinct ”yes” and succinct ”no” certificates.

Outline

Examples

1. PRIMES
2. All problems in **P**

Examples

1. PRIMES
2. All problems in **P**

PRIMES is in NP ∩ coNP

Goal

We first want to develop a different way of determining primality.
Want to show that a number $p > 1$ is prime if and only if there is a number $1 < r < p$ such that $r^{p-1} = 1 \mod p$ and $r^{\frac{p-1}{q}} \neq 1 \mod p$ for all prime divisors q of $p-1$.

Definition (Relative Primality)

Two numbers a and b are relatively prime iff their greatest common divisor, (a, b), is 1.

Examples

5 and 234 are relatively prime,
57 and 95 are not, 19 is a common factor.

PRIMES is in NP ∩ coNP

Goal

We first want to develop a different way of determining primality.
Want to show that a number $p > 1$ is prime if and only if there is a number $1 < r < p$ such that $r^{p-1} = 1 \mod p$ and $r^{\frac{p-1}{q}} \neq 1 \mod p$ for all prime divisors q of $p - 1$.

Definition (Relative Primality)

Two numbers a and b are relatively prime iff their greatest common divisor, (a, b), is 1.

Examples

5 and 234 are relatively prime,
57 and 95 are not, 19 is a common factor.

PRIMES is in NP ∩ coNP

Goal

We first want to develop a different way of determining primality.
Want to show that a number $p > 1$ is prime if and only if there is a number $1 < r < p$ such that $r^{p-1} = 1 \mod p$ and $r^{\frac{p-1}{q}} \neq 1 \mod p$ for all prime divisors q of $p - 1$.

Definition (Relative Primality)

Two numbers a and b are relatively prime iff their greatest common divisor, (a, b), is 1.

Examples

5 and 234 are relatively prime,
57 and 95 are not, 19 is a common factor.

PRIMES is in NP ∩ coNP

Goal

We first want to develop a different way of determining primality.
Want to show that a number $p > 1$ is prime if and only if there is a number $1 < r < p$ such that $r^{p-1} = 1 \mod p$ and $r^{\frac{p-1}{q}} \neq 1 \mod p$ for all prime divisors q of $p - 1$.

Definition (Relative Primality)

Two numbers a and b are relatively prime iff their greatest common divisor, (a, b), is 1.

Examples

5 and 234 are relatively prime,
57 and 95 are not, 19 is a common factor.

An alternate look at primality

Definition ($\Phi(n)$)

$\Phi(n) = \{m : 1 \leq m < n, (m, n) = 1\}$.

Definition (Euler ϕ function)

$\phi(n) = |\Phi(n)|$ and $\phi(1) = 1$.
In other words, $\phi(n)$ is the number of numbers between 1 and $n - 1$ which are relatively prime to n

Lemma (1)

$\phi(n) = n \prod_{p|n}(1 - \frac{1}{p})$ where p is a prime.

Proof.

Assume that $p_1, p_2 \ldots, p_k$ are the prime divisors of n. Observe that each p_i knocks off one in every p_i candidates for $\phi(n)$, leaving $n \cdot (1 - \frac{1}{p_i})$ candidates for $\phi(n)$. It therefore follows that $\phi(n) = n \prod_{p|n}(1 - \frac{1}{p})$ where p is a prime. □

An alternate look at primality

Definition ($\Phi(n)$)

$\Phi(n) = \{m : 1 \leq m < n, (m, n) = 1\}$.

Definition (Euler ϕ function)

$\phi(n) = |\Phi(n)|$ and $\phi(1) = 1$.
In other words, $\phi(n)$ is the number of numbers between 1 and $n - 1$ which are relatively prime to n

Lemma (1)

$\phi(n) = n \prod_{p|n}(1 - \frac{1}{p})$ *where p is a prime.*

Proof.

Assume that $p_1, p_2 \ldots, p_k$ are the prime divisors of n. Observe that each p_i knocks off one in every p_i candidates for $\phi(n)$, leaving $n \cdot (1 - \frac{1}{p_i})$ candidates for $\phi(n)$. It therefore follows that $\phi(n) = n \prod_{p|n}(1 - \frac{1}{p})$ where p is a prime. □

An alternate look at primality

Definition ($\Phi(n)$)

$\Phi(n) = \{m : 1 \leq m < n, (m, n) = 1\}$.

Definition (Euler ϕ function)

$\phi(n) = |\Phi(n)|$ and $\phi(1) = 1$.
In other words, $\phi(n)$ is the number of numbers between 1 and $n - 1$ which are relatively prime to n

Lemma (1)

$\phi(n) = n \prod_{p|n}(1 - \frac{1}{p})$ *where p is a prime.*

Proof.

Assume that $p_1, p_2 \ldots, p_k$ are the prime divisors of n. Observe that each p_i knocks off one in every p_i candidates for $\phi(n)$, leaving $n \cdot (1 - \frac{1}{p_i})$ candidates for $\phi(n)$. It therefore follows that $\phi(n) = n \prod_{p|n}(1 - \frac{1}{p})$ where p is a prime. □

An alternate look at primality

Definition ($\Phi(n)$)

$\Phi(n) = \{m : 1 \leq m < n, (m, n) = 1\}$.

Definition (Euler ϕ function)

$\phi(n) = |\Phi(n)|$ and $\phi(1) = 1$.
In other words, $\phi(n)$ is the number of numbers between 1 and $n - 1$ which are relatively prime to n

Lemma (1)

$\phi(n) = n \prod_{p|n}(1 - \frac{1}{p})$ *where* p *is a prime.*

Proof.

Assume that $p_1, p_2 \ldots, p_k$ are the prime divisors of n. Observe that each p_i knocks off one in every p_i candidates for $\phi(n)$, leaving $n \cdot (1 - \frac{1}{p_i})$ candidates for $\phi(n)$. It therefore follows that $\phi(n) = n \prod_{p|n}(1 - \frac{1}{p})$ where p is a prime. $\square$

An alternate look at primality

Definition ($\Phi(n)$)

$\Phi(n) = \{m : 1 \leq m < n, (m, n) = 1\}$.

Definition (Euler ϕ function)

$\phi(n) = |\Phi(n)|$ and $\phi(1) = 1$.
In other words, $\phi(n)$ is the number of numbers between 1 and $n - 1$ which are relatively prime to n

Lemma (1)

$\phi(n) = n \prod_{p|n}(1 - \frac{1}{p})$ *where p is a prime.*

Proof.

Assume that $p_1, p_2 \ldots, p_k$ are the prime divisors of n. Observe that each p_i knocks off one in every p_i candidates for $\phi(n)$, leaving $n \cdot (1 - \frac{1}{p_i})$ candidates for $\phi(n)$. It therefore follows that $\phi(n) = n \prod_{p|n}(1 - \frac{1}{p})$ where p is a prime. $\square$

An alternate look at primality

Examples

$\Phi(8) = \{1, 3, 5, 7\}$
$\phi(8) = 8 \cdot (1 - \frac{1}{2}) = 4$

Theorem

If $(m, n) = 1$, then $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$.

Proof.

Follows from the previous lemma as m and n share no common prime factors. Thus the terms in the product $m \cdot n \prod_{p|m \cdot n}(1 - \frac{1}{p})$ are distributed without overlap to $n \prod_{p|n}(1 - \frac{1}{p})$ and $m \prod_{p|m}(1 - \frac{1}{p})$. □

Example

$\phi(95) = 95 \cdot (1 - \frac{1}{5}) \cdot (1 - \frac{1}{19}) = 72 = 4 \cdot 18 = \phi(5) \cdot \phi(19)$

An alternate look at primality

Examples

$\Phi(8) = \{1, 3, 5, 7\}$
$\phi(8) = 8 \cdot (1 - \frac{1}{2}) = 4$

Theorem

If $(m, n) = 1$*, then* $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$*.*

Proof.

Follows from the previous lemma as m and n share no common prime factors. Thus the terms in the product $m \cdot n \prod_{p|m \cdot n}(1 - \frac{1}{p})$ are distributed without overlap to $n \prod_{p|n}(1 - \frac{1}{p})$ and $m \prod_{p|m}(1 - \frac{1}{p})$. □

Example

$\phi(95) = 95 \cdot (1 - \frac{1}{5}) \cdot (1 - \frac{1}{19}) = 72 = 4 \cdot 18 = \phi(5) \cdot \phi(19)$

An alternate look at primality

Examples

$\Phi(8) = \{1, 3, 5, 7\}$
$\phi(8) = 8 \cdot (1 - \frac{1}{2}) = 4$

Theorem

If $(m, n) = 1$, then $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$.

Proof.

Follows from the previous lemma as m and n share no common prime factors. Thus the terms in the product $m \cdot n \prod_{p|m \cdot n}(1 - \frac{1}{p})$ are distributed without overlap to $n \prod_{p|n}(1 - \frac{1}{p})$ and $m \prod_{p|m}(1 - \frac{1}{p})$. □

Example

$\phi(95) = 95 \cdot (1 - \frac{1}{5}) \cdot (1 - \frac{1}{19}) = 72 = 4 \cdot 18 = \phi(5) \cdot \phi(19)$

An alternate look at primality

Examples

$\Phi(8) = \{1, 3, 5, 7\}$
$\phi(8) = 8 \cdot (1 - \frac{1}{2}) = 4$

Theorem

If $(m, n) = 1$, then $\phi(m \cdot n) = \phi(m) \cdot \phi(n)$.

Proof.

Follows from the previous lemma as m and n share no common prime factors. Thus the terms in the product $m \cdot n \prod_{p|m \cdot n}(1 - \frac{1}{p})$ are distributed without overlap to $n \prod_{p|n}(1 - \frac{1}{p})$ and $m \prod_{p|m}(1 - \frac{1}{p})$. □

Example

$\phi(95) = 95 \cdot (1 - \frac{1}{5}) \cdot (1 - \frac{1}{19}) = 72 = 4 \cdot 18 = \phi(5) \cdot \phi(19)$

An alternate look at primality

Theorem

$\sum_{m|n} \phi(m) = n$

Proof.

Let $\prod_{i=1}^{l} p_i^{k_i}$ be the prime factorization of n. Consider the following product $\prod_{i=1}^{l}(\phi(1) + \phi(p_i) + \phi(p_i^2) + \cdots + \phi(p_i^{k_i}))$

Its easy to see that the ith term in this product is simply $p_i^{k_i}$. Thus the product is simply equal to n. If the product is expanded out one term for each divisor of n is produced.

The term corresponding to $m = \prod_{i=1}^{l} p_i^{k_i'}$ where $1 \leq k_i' < k_i$, is $\prod_{i=1}^{l} \phi(p_i^{k_i'})$. However, by the previous theorem, this term is simply $\phi(m)$. □

Example

$\sum_{m|27} \phi(m) = \phi(1) + \phi(3) + \phi(9) + \phi(27) = 1 + 2 + 6 + 18 = 27$

An alternate look at primality

Theorem

$\sum_{m|n} \phi(m) = n$

Proof.

Let $\prod_{i=1}^{l} p_i^{k_i}$ be the prime factorization of n. Consider the following product
$\prod_{i=1}^{l}(\phi(1) + \phi(p_i) + \phi(p_i^2) + \cdots + \phi(p_i^{k_i}))$
Its easy to see that the ith term in this product is simply $p_i^{k_i}$. Thus the product is simply equal to n. If the product is expanded out one term for each divisor of n is produced.
The term corresponding to $m = \prod_{i=1}^{l} p_i^{k_i'}$ where $1 \leq k_i' < k_i$, is $\prod_{i=1}^{l} \phi(p_i^{k_i'})$. However, by the previous theorem, this term is simply $\phi(m)$. □

Example

$\sum_{m|27} \phi(m) = \phi(1) + \phi(3) + \phi(9) + \phi(27) = 1 + 2 + 6 + 18 = 27$

An alternate look at primality

Theorem

$\sum_{m|n} \phi(m) = n$

Proof.

Let $\prod_{i=1}^{l} p_i^{k_i}$ be the prime factorization of n. Consider the following product

$\prod_{i=1}^{l}(\phi(1) + \phi(p_i) + \phi(p_i^2) + \cdots + \phi(p_i^{k_i}))$

Its easy to see that the ith term in this product is simply $p_i^{k_i}$. Thus the product is simply equal to n. If the product is expanded out one term for each divisor of n is produced.

The term corresponding to $m = \prod_{i=1}^{l} p_i^{k_i'}$ where $1 \leq k_i' < k_i$, is $\prod_{i=1}^{l} \phi(p_i^{k_i'})$. However, by the previous theorem, this term is simply $\phi(m)$. □

Example

$\sum_{m|27} \phi(m) = \phi(1) + \phi(3) + \phi(9) + \phi(27) = 1 + 2 + 6 + 18 = 27$

An alternate look at primality

Theorem

$\sum_{m|n} \phi(m) = n$

Proof.

Let $\prod_{i=1}^{l} p_i^{k_i}$ be the prime factorization of n. Consider the following product $\prod_{i=1}^{l} (\phi(1) + \phi(p_i) + \phi(p_i^2) + \cdots + \phi(p_i^{k_i}))$
Its easy to see that the ith term in this product is simply $p_i^{k_i}$. Thus the product is simply equal to n. If the product is expanded out one term for each divisor of n is produced. The term corresponding to $m = \prod_{i=1}^{l} p_i^{k_i'}$ where $1 \leq k_i' < k_i$, is $\prod_{i=1}^{l} \phi(p_i^{k_i'})$. However, by the previous theorem, this term is simply $\phi(m)$. □

Example

$\sum_{m|27} \phi(m) = \phi(1) + \phi(3) + \phi(9) + \phi(27) = 1 + 2 + 6 + 18 = 27$

An alternate look at primality

Theorem

$\sum_{m|n} \phi(m) = n$

Proof.

Let $\prod_{i=1}^{l} p_i^{k_i}$ be the prime factorization of n. Consider the following product $\prod_{i=1}^{l}(\phi(1) + \phi(p_i) + \phi(p_i^2) + \cdots + \phi(p_i^{k_i}))$
Its easy to see that the ith term in this product is simply $p_i^{k_i}$. Thus the product is simply equal to n. If the product is expanded out one term for each divisor of n is produced.
The term corresponding to $m = \prod_{i=1}^{l} p_i^{k_i'}$ where $1 \leq k_i' < k_i$, is $\prod_{i=1}^{l} \phi(p_i^{k_i'})$. However, by the previous theorem, this term is simply $\phi(m)$. □

Example

$\sum_{m|27} \phi(m) = \phi(1) + \phi(3) + \phi(9) + \phi(27) = 1 + 2 + 6 + 18 = 27$

An alternate look at primality

Theorem

$\sum_{m|n} \phi(m) = n$

Proof.

Let $\prod_{i=1}^{l} p_i^{k_i}$ be the prime factorization of n. Consider the following product
$\prod_{i=1}^{l}(\phi(1) + \phi(p_i) + \phi(p_i^2) + \cdots + \phi(p_i^{k_i}))$
Its easy to see that the ith term in this product is simply $p_i^{k_i}$. Thus the product is simply equal to n. If the product is expanded out one term for each divisor of n is produced.
The term corresponding to $m = \prod_{i=1}^{l} p_i^{k_i'}$ where $1 \leq k_i' < k_i$, is $\prod_{i=1}^{l} \phi(p_i^{k_i'})$. However, by the previous theorem, this term is simply $\phi(m)$. □

Example

$\sum_{m|27} \phi(m) = \phi(1) + \phi(3) + \phi(9) + \phi(27) = 1 + 2 + 6 + 18 = 27$

An alternate look at primality

Theorem

$\sum_{m|n} \phi(m) = n$

Proof.

Let $\prod_{i=1}^{l} p_i^{k_i}$ be the prime factorization of n. Consider the following product
$\prod_{i=1}^{l}(\phi(1) + \phi(p_i) + \phi(p_i^2) + \cdots + \phi(p_i^{k_i}))$
Its easy to see that the ith term in this product is simply $p_i^{k_i}$. Thus the product is simply equal to n. If the product is expanded out one term for each divisor of n is produced.
The term corresponding to $m = \prod_{i=1}^{l} p_i^{k_i'}$ where $1 \leq k_i' < k_i$, is $\prod_{i=1}^{l} \phi(p_i^{k_i'})$. However, by the previous theorem, this term is simply $\phi(m)$. □

Example

$\sum_{m|27} \phi(m) = \phi(1) + \phi(3) + \phi(9) + \phi(27) = 1 + 2 + 6 + 18 = 27$

An alternate look at primality

Theorem (Fermat's Little Theorem)

For all $0 < a < p$, $a^{p-1} \equiv 1 \mod p$, *where p is a prime.*

Proof.

Lets consider the set $a \cdot \Phi(p) = \{a \cdot i \mod p : 0 < i < p\}$. We have that this set is equal to the set $\Phi(p) = \{i, 0 < i < p\}$. Suppose otherwise, thus there exist elements $m \neq m'$ in $\Phi(p)$ such that $a \cdot m \equiv a \cdot m' \mod p$. Thus $a \cdot (m - m') \equiv 0 \mod p$ leading to a contradiction. Now take the products of all the elements in each set, thus we have that $a^{p-1} \cdot (p-1)! \equiv (p-1)! \mod p$. Thus $(a^{p-1} - 1) \cdot (p-1)! \equiv 0 \mod p$. Since $(p-1)! \not\equiv 0 \mod p$ we have the desired result. □

Corollary

For all $a \in \Phi(n)$, $a^{\phi(n)} \equiv 1 \mod n$

An alternate look at primality

Theorem (Fermat's Little Theorem)

For all $0 < a < p$, $a^{p-1} \equiv 1 \mod p$, *where p is a prime.*

Proof.

Lets consider the set $a \cdot \Phi(p) = \{a \cdot i \mod p : 0 < i < p\}$. We have that this set is equal to the set $\Phi(p) = \{i, 0 < i < p\}$. Suppose otherwise, thus there exist elements $m \neq m'$ in $\Phi(p)$ such that $a \cdot m \equiv a \cdot m' \mod p$. Thus $a \cdot (m - m') \equiv 0 \mod p$ leading to a contradiction. Now take the products of all the elements in each set, thus we have that $a^{p-1} \cdot (p-1)! \equiv (p-1)! \mod p$. Thus $(a^{p-1} - 1) \cdot (p-1)! \equiv 0 \mod p$. Since $(p-1)! \not\equiv 0 \mod p$ we have the desired result. □

Corollary

For all $a \in \Phi(n)$, $a^{\phi(n)} \equiv 1 \mod n$

An alternate look at primality

Theorem (Fermat's Little Theorem)

For all $0 < a < p$, $a^{p-1} \equiv 1 \mod p$, *where p is a prime.*

Proof.

Lets consider the set $a \cdot \Phi(p) = \{a \cdot i \mod p : 0 < i < p\}$. We have that this set is equal to the set $\Phi(p) = \{i, 0 < i < p\}$. Suppose otherwise, thus there exist elements $m \neq m'$ in $\Phi(p)$ such that $a \cdot m \equiv a \cdot m' \mod p$. Thus $a \cdot (m - m') \equiv 0 \mod p$ leading to a contradiction. Now take the products of all the elements in each set, thus we have that $a^{p-1} \cdot (p-1)! \equiv (p-1)! \mod p$. Thus $(a^{p-1} - 1) \cdot (p-1)! \equiv 0 \mod p$. Since $(p-1)! \not\equiv 0 \mod p$ we have the desired result. $\square$

Corollary

For all $a \in \Phi(n)$, $a^{\phi(n)} \equiv 1 \mod n$

An alternate look at primality

Theorem (Fermat's Little Theorem)

For all $0 < a < p$, $a^{p-1} \equiv 1 \mod p$, *where p is a prime.*

Proof.

Lets consider the set $a \cdot \Phi(p) = \{a \cdot i \mod p : 0 < i < p\}$. We have that this set is equal to the set $\Phi(p) = \{i, 0 < i < p\}$. Suppose otherwise, thus there exist elements $m \neq m'$ in $\Phi(p)$ such that $a \cdot m \equiv a \cdot m' \mod p$. Thus $a \cdot (m - m') \equiv 0 \mod p$ leading to a contradiction. Now take the products of all the elements in each set, thus we have that $a^{p-1} \cdot (p-1)! \equiv (p-1)! \mod p$. Thus $(a^{p-1} - 1) \cdot (p-1)! \equiv 0 \mod p$. Since $(p-1)! \not\equiv 0 \mod p$ we have the desired result. □

Corollary

For all $a \in \Phi(n)$, $a^{\phi(n)} \equiv 1 \mod n$

An alternate look at primality

Theorem (Fermat's Little Theorem)

For all $0 < a < p$, $a^{p-1} \equiv 1 \mod p$, *where p is a prime.*

Proof.

Lets consider the set $a \cdot \Phi(p) = \{a \cdot i \mod p : 0 < i < p\}$. We have that this set is equal to the set $\Phi(p) = \{i, 0 < i < p\}$. Suppose otherwise, thus there exist elements $m \neq m'$ in $\Phi(p)$ such that $a \cdot m \equiv a \cdot m' \mod p$. Thus $a \cdot (m - m') \equiv 0 \mod p$ leading to a contradiction. Now take the products of all the elements in each set, thus we have that $a^{p-1} \cdot (p-1)! \equiv (p-1)! \mod p$. Thus $(a^{p-1} - 1) \cdot (p-1)! \equiv 0 \mod p$. Since $(p-1)! \neq 0 \mod p$ we have the desired result. □

Corollary

For all $a \in \Phi(n)$, $a^{\phi(n)} \equiv 1 \mod n$

An alternate look at primality

Theorem (Fermat's Little Theorem)

For all $0 < a < p$, $a^{p-1} \equiv 1 \mod p$, *where* p *is a prime.*

Proof.

Lets consider the set $a \cdot \Phi(p) = \{a \cdot i \mod p : 0 < i < p\}$. We have that this set is equal to the set $\Phi(p) = \{i, 0 < i < p\}$. Suppose otherwise, thus there exist elements $m \neq m'$ in $\Phi(p)$ such that $a \cdot m \equiv a \cdot m' \mod p$. Thus $a \cdot (m - m') \equiv 0 \mod p$ leading to a contradiction. Now take the products of all the elements in each set, thus we have that $a^{p-1} \cdot (p-1)! \equiv (p-1)! \mod p$. Thus $(a^{p-1} - 1) \cdot (p-1)! \equiv 0 \mod p$. Since $(p-1)! \not\equiv 0 \mod p$ we have the desired result. □

Corollary

For all $a \in \Phi(n)$, $a^{\phi(n)} \equiv 1 \mod n$

An alternate look at primality

Theorem (Fermat's Little Theorem)

For all $0 < a < p$, $a^{p-1} \equiv 1 \mod p$, *where* p *is a prime.*

Proof.

Lets consider the set $a \cdot \Phi(p) = \{a \cdot i \mod p : 0 < i < p\}$. We have that this set is equal to the set $\Phi(p) = \{i, 0 < i < p\}$. Suppose otherwise, thus there exist elements $m \neq m'$ in $\Phi(p)$ such that $a \cdot m \equiv a \cdot m' \mod p$. Thus $a \cdot (m - m') \equiv 0 \mod p$ leading to a contradiction. Now take the products of all the elements in each set, thus we have that $a^{p-1} \cdot (p-1)! \equiv (p-1)! \mod p$. Thus $(a^{p-1} - 1) \cdot (p-1)! \equiv 0 \mod p$. Since $(p-1)! \not\equiv 0 \mod p$ we have the desired result. □

Corollary

For all $a \in \Phi(n)$, $a^{\phi(n)} \equiv 1 \mod n$

An alternative look at primality

Definition (Exponent of a number $\mod n$)

The exponent of a number $m \in \Phi(n)$ is the smallest integer $k > 0$ for which $m^k \equiv 1 \mod n$. It is worth noting that if $m^l \equiv 1 \mod n$ then $k|l$. As otherwise $l \mod k$ would be the exponent of m.

Example

The exponent of $10 \mod 11$ is 2 as $10^2 \equiv 1 \mod 11$ but $10 \not\equiv 1 \mod 11$.

Definition

Let $R(k)$, for a given prime p, denote the number of residues in $\Phi(p)$ which have exponent k.

Example

Let $p = 5$ thus $R(3) = 0$ and $R(2) = 1$.

An alternative look at primality

Definition (Exponent of a number $\mod n$)

The exponent of a number $m \in \Phi(n)$ is the smallest integer $k > 0$ for which $m^k \equiv 1 \mod n$. It is worth noting that if $m^l \equiv 1 \mod n$ then $k|l$. As otherwise $l \mod k$ would be the exponent of m.

Example

The exponent of $10 \mod 11$ is 2 as $10^2 \equiv 1 \mod 11$ but $10 \not\equiv 1 \mod 11$.

Definition

Let $R(k)$, for a given prime p, denote the number of residues in $\Phi(p)$ which have exponent k.

Example

Let $p = 5$ thus $R(3) = 0$ and $R(2) = 1$.

An alternative look at primality

Definition (Exponent of a number $\mod n$)

The exponent of a number $m \in \Phi(n)$ is the smallest integer $k > 0$ for which $m^k \equiv 1 \mod n$. It is worth noting that if $m^l \equiv 1 \mod n$ then $k|l$. As otherwise $l \mod k$ would be the exponent of m.

Example

The exponent of $10 \mod 11$ is 2 as $10^2 \equiv 1 \mod 11$ but $10 \neq 1 \mod 11$.

Definition

Let $R(k)$, for a given prime p, denote the number of residues in $\Phi(p)$ which have exponent k.

Example

Let $p = 5$ thus $R(3) = 0$ and $R(2) = 1$.

An alternative look at primality

Definition (Exponent of a number $\mod n$)

The exponent of a number $m \in \Phi(n)$ is the smallest integer $k > 0$ for which $m^k \equiv 1 \mod n$. It is worth noting that if $m^l \equiv 1 \mod n$ then $k|l$. As otherwise $l \mod k$ would be the exponent of m.

Example

The exponent of $10 \mod 11$ is 2 as $10^2 \equiv 1 \mod 11$ but $10 \neq 1 \mod 11$.

Definition

Let $R(k)$, for a given prime p, denote the number of residues in $\Phi(p)$ which have exponent k.

Example

Let $p = 5$ thus $R(3) = 0$ and $R(2) = 1$.

An alternative look at primality

Definition (Exponent of a number $\mod n$)

The exponent of a number $m \in \Phi(n)$ is the smallest integer $k > 0$ for which $m^k \equiv 1 \mod n$. It is worth noting that if $m^l \equiv 1 \mod n$ then $k|l$. As otherwise $l \mod k$ would be the exponent of m.

Example

The exponent of $10 \mod 11$ is 2 as $10^2 \equiv 1 \mod 11$ but $10 \neq 1 \mod 11$.

Definition

Let $R(k)$, for a given prime p, denote the number of residues in $\Phi(p)$ which have exponent k.

Example

Let $p = 5$ thus $R(3) = 0$ and $R(2) = 1$.

An alternate look at primality

Theorem

Any polynomial of degree k that is not identically zero has at most k distinct roots mod *p.*

Proof.

This will be shown by induction on k. If $k = 0$ this is obvious as the polynomial is constant. Assume that the theorem holds for al polynomials of degree at most $k-1$. Let $\pi(x) = a_k x^k + \ldots + a_1 x + a_0$ be a polynomial of degree k with $k+1$ distinct roots, say $x_1, x_2, \ldots, x_{k+1}$. Now let $\pi'(x) = \pi(x) - a_k \cdot \prod_{i=1}^{k}(x - x_i)$. Thus $\pi'(x)$ is a polynomial of degree at most $k-1$, *which is not identically* 0. Therefore, $\pi'(x)$ must have $k-1$ distinct roots as per the inductive hypothesis, but $x_1, \ldots, x_k$ are all distinct roots of $\pi'(x)$ contradicting the hypothesis! □

Application to $R(k)$

Since $x^k - 1$ for $k \notin \phi(p)$ is a non-zero polynomial it has at most k roots mod p and thus $R(k) \leq k$.

An alternate look at primality

Theorem

Any polynomial of degree k that is not identically zero has at most k distinct roots mod p*.*

Proof.

This will be shown by induction on k. If $k = 0$ this is obvious as the polynomial is constant. Assume that the theorem holds for al polynomials of degree at most $k - 1$. Let $\pi(x) = a_k x^k + \ldots + a_1 x + a_0$ be a polynomial of degree k with $k + 1$ distinct roots, say $x_1, x_2, \ldots, x_{k+1}$. Now let $\pi'(x) = \pi(x) - a_k \cdot \prod_{i=1}^{k}(x - x_i)$. Thus $\pi'(x)$ is a polynomial of degree at most $k - 1$, *which is not identically* 0. Therefore, $\pi'(x)$ must have $k - 1$ distinct roots as per the inductive hypothesis, but $x_1, \ldots, x_k$ are all distinct roots of $\pi'(x)$ contradicting the hypothesis! $\square$

Application to $R(k)$

Since $x^k - 1$ for $k \notin \phi(p)$ is a non-zero polynomial it has at most k roots mod p and thus $R(k) \leq k$.

An alternate look at primality

Theorem

Any polynomial of degree k that is not identically zero has at most k distinct roots mod *p.*

Proof.

This will be shown by induction on k. If $k = 0$ this is obvious as the polynomial is constant. Assume that the theorem holds for al polynomials of degree at most $k - 1$. Let $\pi(x) = a_k x^k + \ldots + a_1 x + a_0$ be a polynomial of degree k with $k + 1$ distinct roots, say $x_1, x_2, \ldots, x_{k+1}$. Now let $\pi'(x) = \pi(x) - a_k \cdot \prod_{i=1}^{k}(x - x_i)$. Thus $\pi'(x)$ is a polynomial of degree at most $k - 1$, *which is not identically* 0. Therefore, $\pi'(x)$ must have $k - 1$ distinct roots as per the inductive hypothesis, but $x_1, \ldots, x_k$ are all distinct roots of $\pi'(x)$ contradicting the hypothesis! □

Application to $R(k)$

Since $x^k - 1$ for $k \notin \phi(p)$ is a non-zero polynomial it has at most k roots mod p and thus $R(k) \leq k$.

An alternate look at primality

Theorem

Any polynomial of degree k that is not identically zero has at most k distinct roots mod p*.*

Proof.

This will be shown by induction on k. If $k = 0$ this is obvious as the polynomial is constant. Assume that the theorem holds for al polynomials of degree at most $k - 1$. Let $\pi(x) = a_k x^k + \ldots + a_1 x + a_0$ be a polynomial of degree k with $k + 1$ distinct roots, say $x_1, x_2, \ldots, x_{k+1}$. Now let $\pi'(x) = \pi(x) - a_k \cdot \prod_{i=1}^{k}(x - x_i)$. Thus $\pi'(x)$ is a polynomial of degree at most $k - 1$, *which is not identically* 0. Therefore, $\pi'(x)$ must have $k - 1$ distinct roots as per the inductive hypothesis, but $x_1, \ldots, x_k$ are all distinct roots of $\pi'(x)$ contradicting the hypothesis! □

Application to $R(k)$

Since $x^k - 1$ for $k \notin \phi(p)$ is a non-zero polynomial it has at most k roots mod p and thus $R(k) \leq k$.

An alternate look at primality

Theorem

Any polynomial of degree k *that is not identically zero has at most* k *distinct roots* mod p*.*

Proof.

This will be shown by induction on k. If $k = 0$ this is obvious as the polynomial is constant. Assume that the theorem holds for al polynomials of degree at most $k - 1$. Let $\pi(x) = a_k x^k + \ldots + a_1 x + a_0$ be a polynomial of degree k with $k + 1$ distinct roots, say $x_1, x_2, \ldots, x_{k+1}$. Now let $\pi'(x) = \pi(x) - a_k \cdot \prod_{i=1}^{k}(x - x_i)$. Thus $\pi'(x)$ is a polynomial of degree at most $k - 1$, *which is not identically* 0. Therefore, $\pi'(x)$ must have $k - 1$ distinct roots as per the inductive hypothesis, but $x_1, \ldots, x_k$ are all distinct roots of $\pi'(x)$ contradicting the hypothesis! □

Application to $R(k)$

Since $x^k - 1$ for $k \notin \phi(p)$ is a non-zero polynomial it has at most k roots $\mod p$ and thus $R(k) \leq k$.

An alternate look at primality

Theorem

For a given prime p, for all $k \in \Phi(p)$ *we have that* $R(k) \leq \phi(k)$.

Proof.

If $R(k) = 0$ then were done. So we assume that there is an element s with exponent k. Then $(1, s, s^2, \ldots, s^{k-1})$ are all distinct. And for all $0 \leq i < k$, $(s^i)^k = s^{ik} \equiv 1^i = 1 \mod p$. Thus these s^i constitute all k possible roots of $x^k - 1 \mod p$. Let s^l have exponent k. If $l \notin \Phi(k)$ then $d = (l, k) > 1$ and $(s^l)^{k/d} = s^{\frac{lk}{d}} = (s^k)^{l/d} \equiv 1 \mod p$ leading to a contradiction. Thus if s^l has exponent $k \mod p$ then $l \in \Phi(k)$, which means that $R(k) \leq \phi(k)$. □

An alternate look at primality

Theorem

For a given prime p, for all $k \in \Phi(p)$ we have that $R(k) \leq \phi(k)$.

Proof.

If $R(k) = 0$ then were done. So we assume that there is an element s with exponent k. Then $(1, s, s^2, \ldots, s^{k-1})$ are all distinct. And for all $0 \leq i < k$, $(s^i)^k = s^{ik} \equiv 1^i = 1 \mod p$. Thus these s^i constitute all k possible roots of $x^k - 1 \mod p$. Let s^l have exponent k. If $l \notin \Phi(k)$ then $d = (l, k) > 1$ and $(s^l)^{k/d} = s^{\frac{lk}{d}} = (s^k)^{l/d} \equiv 1 \mod p$ leading to a contradiction. Thus if s^l has exponent $k \mod p$ then $l \in \Phi(k)$, which means that $R(k) \leq \phi(k)$. □

An alternate look at primality

Theorem

For a given prime p, for all $k \in \Phi(p)$ we have that $R(k) \leq \phi(k)$.

Proof.

If $R(k) = 0$ then were done. So we assume that there is an element s with exponent k. Then $(1, s, s^2, \ldots, s^{k-1})$ are all distinct. And for all $0 \leq i < k$, $(s^i)^k = s^{ik} \equiv 1^i = 1 \mod p$. Thus these s^i constitute all k possible roots of $x^k - 1 \mod p$. Let s^l have exponent k. If $l \notin \Phi(k)$ then $d = (l, k) > 1$ and $(s^l)^{k/d} = s^{\frac{lk}{d}} = (s^k)^{l/d} \equiv 1 \mod p$ leading to a contradiction. Thus if s^l has exponent $k \mod p$ then $l \in \Phi(k)$, which means that $R(k) \leq \phi(k)$. □

An alternate look at primality

Theorem

For a given prime p, for all $k \in \Phi(p)$ we have that $R(k) \leq \phi(k)$.

Proof.

If $R(k) = 0$ then were done. So we assume that there is an element s with exponent k. Then $(1, s, s^2, \ldots, s^{k-1})$ are all distinct. And for all $0 \leq i < k$, $(s^i)^k = s^{ik} \equiv 1^i = 1 \mod p$. Thus these s^i constitute all k possible roots of $x^k - 1 \mod p$. Let s^l have exponent k. If $l \notin \Phi(k)$ then $d = (l, k) > 1$ and $(s^l)^{k/d} = s^{\frac{lk}{d}} = (s^k)^{l/d} \equiv 1 \mod p$ leading to a contradiction. Thus if s^l has exponent $k \mod p$ then $l \in \Phi(k)$, which means that $R(k) \leq \phi(k)$. □

An alternate look at primality

Theorem

For a given prime p, for all $k \in \Phi(p)$ we have that $R(k) \leq \phi(k)$.

Proof.

If $R(k) = 0$ then were done. So we assume that there is an element s with exponent k. Then $(1, s, s^2, \ldots, s^{k-1})$ are all distinct. And for all $0 \leq i < k$, $(s^i)^k = s^{ik} \equiv 1^i = 1 \mod p$. Thus these s^i constitute all k possible roots of $x^k - 1 \mod p$. Let s^l have exponent k. If $l \notin \Phi(k)$ then $d = (l, k) > 1$ and $(s^l)^{k/d} = s^{\frac{lk}{d}} = (s^k)^{l/d} \equiv 1 \mod p$ leading to a contradiction. Thus if s^l has exponent $k \mod p$ then $l \in \Phi(k)$, which means that $R(k) \leq \phi(k)$. □

An alternate look at primality

Theorem

For a given prime p, for all $k \in \Phi(p)$ *we have that* $R(k) \leq \phi(k)$.

Proof.

If $R(k) = 0$ then were done. So we assume that there is an element s with exponent k. Then $(1, s, s^2, \ldots, s^{k-1})$ are all distinct. And for all $0 \leq i < k$, $(s^i)^k = s^{ik} \equiv 1^i = 1 \mod p$. Thus these s^i constitute all k possible roots of $x^k - 1 \mod p$. Let s^l have exponent k. If $l \notin \Phi(k)$ then $d = (l, k) > 1$ and $(s^l)^{k/d} = s^{\frac{lk}{d}} = (s^k)^{l/d} \equiv 1 \mod p$ leading to a contradiction. Thus if s^l has exponent $k \mod p$ then $l \in \Phi(k)$, which means that $R(k) \leq \phi(k)$. □

An alternate look at primality

Theorem

A number $p > 1$ is prime if and only if there is a number $1 < r < p$ such that $r^{p-1} = 1 \mod p$ and $r^{\frac{p-1}{q}} \neq 1 \mod p$ for all prime divisors q of $p - 1$.

Proof.

p is a prime: As each $0 < i < p$ has an exponent, that divides $p-1$, $p-1 = \sum_{l|p-1} R(l) \leq \sum_{l|p-1} \phi(l) = p-1$. Thus $R(l) = \phi(l)$ for all $l|p-1$. Namely $R(p-1) = \phi(p-1) > 0$ and so there is at least one r that has exponent $p-1$.
p is not a prime: let $r \in \Phi(p)$ be a number such that $r^{p-1} \equiv 1 \mod p$, we also have that $r^{\phi(p)} \equiv 1 \mod p$. Let k be the exponent of $r \mod p$. Thus $k|p-1$ and $k|\phi(p)$. Since p is not a prime $k \leq \phi(p) < p-1$. Let q be a prime factor of $\frac{p-1}{k}$. Thus $k|\frac{p-1}{q}$ and so $r^{\frac{p-1}{q}} \equiv 1 \mod p$ $\square$

An alternate look at primality

Theorem

A number $p > 1$ is prime if and only if there is a number $1 < r < p$ such that $r^{p-1} = 1 \mod p$ and $r^{\frac{p-1}{q}} \neq 1 \mod p$ for all prime divisors q of $p - 1$.

Proof.

p is a prime: As each $0 < i < p$ has an exponent, that divides $p - 1$, $p - 1 = \sum_{l|p-1} R(l) \leq \sum_{l|p-1} \phi(l) = p - 1$. Thus $R(l) = \phi(l)$ for all $l|p-1$. Namely $R(p-1) = \phi(p-1) > 0$ and so there is at least one r that has exponent $p - 1$.
p is not a prime: let $r \in \Phi(p)$ be a number such that $r^{p-1} \equiv 1 \mod p$, we also have that $r^{\phi(p)} \equiv 1 \mod p$. Let k be the exponent of $r \mod p$. Thus $k|p-1$ and $k|\phi(p)$. Since p is not a prime $k \leq \phi(p) < p - 1$. Let q be a prime factor of $\frac{p-1}{k}$. Thus $k|\frac{p-1}{q}$ and so $r^{\frac{p-1}{q}} \equiv 1 \mod p$ □

An alternate look at primality

Theorem

A number $p > 1$ is prime if and only if there is a number $1 < r < p$ such that $r^{p-1} = 1 \mod p$ and $r^{\frac{p-1}{q}} \neq 1 \mod p$ for all prime divisors q of $p - 1$.

Proof.

p is a prime: As each $0 < i < p$ has an exponent, that divides $p - 1$, $p - 1 = \sum_{l|p-1} R(l) \leq \sum_{l|p-1} \phi(l) = p - 1$. Thus $R(l) = \phi(l)$ for all $l|p - 1$. Namely $R(p - 1) = \phi(p - 1) > 0$ and so there is at least one r that has exponent $p - 1$.

p is not a prime: let $r \in \Phi(p)$ be a number such that $r^{p-1} \equiv 1 \mod p$, we also have that $r^{\phi(p)} \equiv 1 \mod p$. Let k be the exponent of $r \mod p$. Thus $k|p - 1$ and $k|\phi(p)$. Since p is not a prime $k \leq \phi(p) < p - 1$. Let q be a prime factor of $\frac{p-1}{k}$. Thus $k|\frac{p-1}{q}$ and so $r^{\frac{p-1}{q}} \equiv 1 \mod p$ □

An alternate look at primality

Theorem

A number $p > 1$ is prime if and only if there is a number $1 < r < p$ such that $r^{p-1} = 1 \mod p$ and $r^{\frac{p-1}{q}} \neq 1 \mod p$ for all prime divisors q of $p-1$.

Proof.

p is a prime: As each $0 < i < p$ has an exponent, that divides $p-1$, $p - 1 = \sum_{l|p-1} R(l) \leq \sum_{l|p-1} \phi(l) = p - 1$. Thus $R(l) = \phi(l)$ for all $l|p-1$. Namely $R(p-1) = \phi(p-1) > 0$ and so there is at least one r that has exponent $p-1$.
p is not a prime: let $r \in \Phi(p)$ be a number such that $r^{p-1} \equiv 1 \mod p$, we also have that $r^{\phi(p)} \equiv 1 \mod p$. Let k be the exponent of $r \mod p$. Thus $k|p-1$ and $k|\phi(p)$. Since p is not a prime $k \leq \phi(p) < p - 1$. Let q be a prime factor of $\frac{p-1}{k}$. Thus $k|\frac{p-1}{q}$ and so $r^{\frac{p-1}{q}} \equiv 1 \mod p$ □

An alternate look at primality

Theorem

A number $p > 1$ is prime if and only if there is a number $1 < r < p$ such that $r^{p-1} = 1 \mod p$ and $r^{\frac{p-1}{q}} \neq 1 \mod p$ for all prime divisors q of $p - 1$.

Proof.

p is a prime: As each $0 < i < p$ has an exponent, that divides $p - 1$, $p - 1 = \sum_{l|p-1} R(l) \leq \sum_{l|p-1} \phi(l) = p - 1$. Thus $R(l) = \phi(l)$ for all $l|p - 1$. Namely $R(p - 1) = \phi(p - 1) > 0$ and so there is at least one r that has exponent $p - 1$.
p is not a prime: let $r \in \Phi(p)$ be a number such that $r^{p-1} \equiv 1 \mod p$, we also have that $r^{\phi(p)} \equiv 1 \mod p$. Let k be the exponent of $r \mod p$. Thus $k|p - 1$ and $k|\phi(p)$. Since p is not a prime $k \leq \phi(p) < p - 1$. Let q be a prime factor of $\frac{p-1}{k}$. Thus $k|\frac{p-1}{q}$ and so $r^{\frac{p-1}{q}} \equiv 1 \mod p$ □

An alternate look at primality

Theorem

A number $p > 1$ is prime if and only if there is a number $1 < r < p$ such that $r^{p-1} = 1 \mod p$ and $r^{\frac{p-1}{q}} \neq 1 \mod p$ for all prime divisors q of $p - 1$.

Proof.

p is a prime: As each $0 < i < p$ has an exponent, that divides $p - 1$, $p - 1 = \sum_{l|p-1} R(l) \leq \sum_{l|p-1} \phi(l) = p - 1$. Thus $R(l) = \phi(l)$ for all $l|p - 1$. Namely $R(p - 1) = \phi(p - 1) > 0$ and so there is at least one r that has exponent $p - 1$.
p is not a prime: let $r \in \Phi(p)$ be a number such that $r^{p-1} \equiv 1 \mod p$, we also have that $r^{\phi(p)} \equiv 1 \mod p$. Let k be the exponent of $r \mod p$. Thus $k|p - 1$ and $k|\phi(p)$. Since p is not a prime $k \leq \phi(p) < p - 1$. Let q be a prime factor of $\frac{p-1}{k}$. Thus $k|\frac{p-1}{q}$ and so $r^{\frac{p-1}{q}} \equiv 1 \mod p$ □

Showing that PRIMES is in NP ∩ coNP

Theorem (Pratt's Theorem)

PRIMES is in NP ∩ coNP

Proof.

Part 1: PRIMES is in coNP. Trivially true, since the succinct disqualification for $x \notin PRIMES$ is simply the factorization of x.
eg. $12 = 3 \cdot 4$ and $117 = 9 \cdot 13$. □

Showing that PRIMES is in NP ∩ coNP

Theorem (Pratt's Theorem)

PRIMES is in NP ∩ coNP

Proof.

Part 1: PRIMES is in coNP. Trivially true, since the succinct disqualification for $x \notin PRIMES$ is simply the factorization of x.
eg. $12 = 3 \cdot 4$ and $117 = 9 \cdot 13$. □

Showing that PRIMES is in NP ∩ coNP

Theorem (Pratt's Theorem)

PRIMES is in NP ∩ coNP

Proof.

Part 1: PRIMES is in coNP. Trivially true, since the succinct disqualification for $x \notin PRIMES$ is simply the factorization of x.
eg. $12 = 3 \cdot 4$ and $117 = 9 \cdot 13$. □

Showing that PRIMES is in NP ∩ coNP

Theorem (Pratt's Theorem)

PRIMES is in NP ∩ coNP

Proof.

Part 1: PRIMES is in coNP. Trivially true, since the succinct disqualification for $x \notin PRIMES$ is simply the factorization of x.
eg. $12 = 3 \cdot 4$ and $117 = 9 \cdot 13$. □

Proof.

Part 2: PRIMES is in NP. First we will try to construct a certificate for any $x \in PRIMES$. Once a reasonable certificate is found we will show that it is succinct. □

Possible Certificates, $C(p)$, for $p \in PRIMES$

1. $C(p) = r$ such that $r^{p-1} = 1 \mod p$.
   Insufficient as 20 is a "valid" certificate for $21 \notin PRIMES$.
2. $C(p) = (r, p_1, p_2, \ldots, p_k)$ where $r^{p-1} = 1 \mod p$ and $r^{\frac{p-1}{p_i}} \neq 1 \mod p$ for $1 \leq i \leq k$ and $p_1 \cdot \cdots \cdot p_k = p - 1$.
   Insufficient as $(10, 2, 45)$ is a "valid" certificate for $91 \notin PRIMES$.
   Need some way to ensure that $p_1, \ldots, p_k$ are primes without having to check.
3. $C(p) = (r; p_1, C(p_1), p_2, C(p_2), \ldots, p_k, C(p_k))$ where C(1)=(1), $r^{p-1} = 1 \mod p$, and $r^{\frac{p-1}{p_i}} \neq 1 \mod p$ for $1 \leq i \leq k$ and $p_1 \cdot \cdots \cdot p_k = p - 1$.
   eg. $C(67) = (2; 2, (1), 3, (2; 2, (1)), 11, (8; 2, (1), 5, (3; 2, (1))))$.

Proof.

Part 2: PRIMES is in NP. First we will try to construct a certificate for any $x \in PRIMES$. Once a reasonable certificate is found we will show that it is succinct.

Possible Certificates, $C(p)$, for $p \in PRIMES$

1. $C(p) = r$ such that $r^{p-1} = 1 \mod p$.
   Insufficient as 20 is a "valid" certificate for $21 \notin PRIMES$.
2. $C(p) = (r, p_1, p_2, \dots, p_k)$ where $r^{p-1} = 1 \mod p$ and $r^{\frac{p-1}{p_i}} \neq 1 \mod p$ for $1 \leq i \leq k$ and $p_1 \cdot \dots \cdot p_k = p - 1$.
   Insufficient as $(10, 2, 45)$ is a "valid" certificate for $91 \notin PRIMES$.
   Need some way to ensure that $p_1, \dots, p_k$ are primes without having to check.
3. $C(p) = (r; p_1, C(p_1), p_2, C(p_2), \dots, p_k, C(p_k))$ where C(1)=(1), $r^{p-1} = 1 \mod p$, and $r^{\frac{p-1}{p_i}} \neq 1 \mod p$ for $1 \leq i \leq k$ and $p_1 \cdot \dots \cdot p_k = p - 1$.
   eg. $C(67) = (2; 2, (1), 3, (2; 2, (1)), 11, (8; 2, (1), 5, (3; 2, (1))))$.

Proof.

Part 2: PRIMES is in NP. First we will try to construct a certificate for any $x \in PRIMES$. Once a reasonable certificate is found we will show that it is succinct. □

Possible Certificates, $C(p)$, for $p \in PRIMES$

1. $C(p) = r$ such that $r^{p-1} = 1 \mod p$.
   Insufficient as 20 is a "valid" certificate for $21 \notin PRIMES$.
2. $C(p) = (r, p_1, p_2, \ldots, p_k)$ where $r^{p-1} = 1 \mod p$ and $r^{\frac{p-1}{p_i}} \neq 1 \mod p$ for $1 \leq i \leq k$ and $p_1 \cdot \cdots \cdot p_k = p - 1$.
   Insufficient as $(10, 2, 45)$ is a "valid" certificate for $91 \notin PRIMES$.
   Need some way to ensure that $p_1, \ldots, p_k$ are primes without having to check.
3. $C(p) = (r; p_1, C(p_1), p_2, C(p_2), \ldots, p_k, C(p_k))$ where C(1)=(1), $r^{p-1} = 1 \mod p$, and $r^{\frac{p-1}{p_i}} \neq 1 \mod p$ for $1 \leq i \leq k$ and $p_1 \cdot \cdots \cdot p_k = p - 1$.
   eg. $C(67) = (2; 2, (1), 3, (2; 2, (1)), 11, (8; 2, (1), 5, (3; 2, (1))))$.

Proof.

Part 2: PRIMES is in NP. First we will try to construct a certificate for any $x \in PRIMES$. Once a reasonable certificate is found we will show that it is succinct. □

Possible Certificates, $C(p)$, for $p \in PRIMES$

1. $C(p) = r$ such that $r^{p-1} = 1 \mod p$.
   Insufficient as 20 is a "valid" certificate for $21 \notin PRIMES$.
2. $C(p) = (r, p_1, p_2, \ldots, p_k)$ where $r^{p-1} = 1 \mod p$ and $r^{\frac{p-1}{p_i}} \neq 1 \mod p$ for $1 \leq i \leq k$ and $p_1 \cdot \cdots \cdot p_k = p - 1$.
   Insufficient as $(10, 2, 45)$ is a "valid" certificate for $91 \notin PRIMES$.
   Need some way to ensure that $p_1, \ldots, p_k$ are primes without having to check.
3. $C(p) = (r; p_1, C(p_1), p_2, C(p_2), \ldots, p_k, C(p_k))$ where C(1)=(1), $r^{p-1} = 1 \mod p$, and $r^{\frac{p-1}{p_i}} \neq 1 \mod p$ for $1 \leq i \leq k$ and $p_1 \cdot \cdots \cdot p_k = p - 1$.
   eg. $C(67) = (2; 2, (1), 3, (2; 2, (1)), 11, (8; 2, (1), 5, (3; 2, (1))))$.

Proof.

Part 2: PRIMES is in NP. First we will try to construct a certificate for any $x \in PRIMES$. Once a reasonable certificate is found we will show that it is succinct. □

Possible Certificates, $C(p)$, for $p \in PRIMES$

1. $C(p) = r$ such that $r^{p-1} = 1 \mod p$.
   Insufficient as 20 is a "valid" certificate for $21 \notin PRIMES$.
2. $C(p) = (r, p_1, p_2, \ldots, p_k)$ where $r^{p-1} = 1 \mod p$ and $r^{\frac{p-1}{p_i}} \neq 1 \mod p$ for $1 \leq i \leq k$ and $p_1 \cdot \cdots \cdot p_k = p - 1$.
   Insufficient as $(10, 2, 45)$ is a "valid" certificate for $91 \notin PRIMES$.
   Need some way to ensure that $p_1, \ldots, p_k$ are primes without having to check.
3. $C(p) = (r; p_1, C(p_1), p_2, C(p_2), \ldots, p_k, C(p_k))$ where C(1)=(1), $r^{p-1} = 1 \mod p$, and $r^{\frac{p-1}{p_i}} \neq 1 \mod p$ for $1 \leq i \leq k$ and $p_1 \cdot \cdots \cdot p_k = p - 1$.
   eg. $C(67) = (2; 2, (1), 3, (2; 2, (1)), 11, (8; 2, (1), 5, (3; 2, (1))))$.

Proof.

Part 2: PRIMES is in NP. First we will try to construct a certificate for any $x \in PRIMES$. Once a reasonable certificate is found we will show that it is succinct. □

Possible Certificates, $C(p)$, for $p \in PRIMES$

1. $C(p) = r$ such that $r^{p-1} = 1 \mod p$.
   Insufficient as 20 is a "valid" certificate for $21 \notin PRIMES$.
2. $C(p) = (r, p_1, p_2, \ldots, p_k)$ where $r^{p-1} = 1 \mod p$ and $r^{\frac{p-1}{p_i}} \neq 1 \mod p$ for $1 \leq i \leq k$ and $p_1 \cdot \cdots \cdot p_k = p - 1$.
   Insufficient as $(10, 2, 45)$ is a "valid" certificate for $91 \notin PRIMES$.
   Need some way to ensure that $p_1, \ldots, p_k$ are primes without having to check.
3. $C(p) = (r; p_1, C(p_1), p_2, C(p_2), \ldots, p_k, C(p_k))$ where C(1)=(1), $r^{p-1} = 1 \mod p$, and $r^{\frac{p-1}{p_i}} \neq 1 \mod p$ for $1 \leq i \leq k$ and $p_1 \cdot \cdots \cdot p_k = p - 1$.
   eg. $C(67) = (2; 2, (1), 3, (2; 2, (1)), 11, (8; 2, (1), 5, (3; 2, (1))))$.

Proof.

Part 2: PRIMES is in NP. First we will try to construct a certificate for any $x \in PRIMES$. Once a reasonable certificate is found we will show that it is succinct. □

Possible Certificates, $C(p)$, for $p \in PRIMES$

1. $C(p) = r$ such that $r^{p-1} = 1 \mod p$.
   Insufficient as 20 is a "valid" certificate for $21 \notin PRIMES$.
2. $C(p) = (r, p_1, p_2, \ldots, p_k)$ where $r^{p-1} = 1 \mod p$ and $r^{\frac{p-1}{p_i}} \neq 1 \mod p$ for $1 \leq i \leq k$ and $p_1 \cdot \cdots \cdot p_k = p - 1$.
   Insufficient as $(10, 2, 45)$ is a "valid" certificate for $91 \notin PRIMES$.
   Need some way to ensure that $p_1, \ldots, p_k$ are primes without having to check.
3. $C(p) = (r; p_1, C(p_1), p_2, C(p_2), \ldots, p_k, C(p_k))$ where C(1)=(1), $r^{p-1} = 1 \mod p$, and $r^{\frac{p-1}{p_i}} \neq 1 \mod p$ for $1 \leq i \leq k$ and $p_1 \cdot \cdots \cdot p_k = p - 1$.
   eg. $C(67) = (2; 2, (1), 3, (2; 2, (1)), 11, (8; 2, (1), 5, (3; 2, (1))))$.

Proof.

Part 2: PRIMES is in NP. First we will try to construct a certificate for any $x \in \mathit{PRIMES}$. Once a reasonable certificate is found we will show that it is succinct. □

Possible Certificates, $C(p)$, for $p \in \mathit{PRIMES}$

1. $C(p) = r$ such that $r^{p-1} = 1 \mod p$.
   Insufficient as 20 is a "valid" certificate for $21 \notin \mathit{PRIMES}$.
2. $C(p) = (r, p_1, p_2, \ldots, p_k)$ where $r^{p-1} = 1 \mod p$ and $r^{\frac{p-1}{p_i}} \neq 1 \mod p$ for $1 \leq i \leq k$ and $p_1 \cdot \cdots \cdot p_k = p - 1$.
   Insufficient as $(10, 2, 45)$ is a "valid" certificate for $91 \notin \mathit{PRIMES}$.
   Need some way to ensure that $p_1, \ldots, p_k$ are primes without having to check.
3. $C(p) = (r; p_1, C(p_1), p_2, C(p_2), \ldots, p_k, C(p_k))$ where C(1)=(1), $r^{p-1} = 1 \mod p$, and $r^{\frac{p-1}{p_i}} \neq 1 \mod p$ for $1 \leq i \leq k$ and $p_1 \cdot \cdots \cdot p_k = p - 1$.
   eg. $C(67) = (2; 2, (1), 3, (2; 2, (1)), 11, (8; 2, (1), 5, (3; 2, (1))))$.

Proof.

Part 2: PRIMES is in NP. First we will try to construct a certificate for any $x \in PRIMES$. Once a reasonable certificate is found we will show that it is succinct. $\square$

Possible Certificates, $C(p)$, for $p \in PRIMES$

1. $C(p) = r$ such that $r^{p-1} = 1 \mod p$.
   Insufficient as 20 is a ”valid” certificate for $21 \notin PRIMES$.
2. $C(p) = (r, p_1, p_2, \ldots, p_k)$ where $r^{p-1} = 1 \mod p$ and $r^{\frac{p-1}{p_i}} \neq 1 \mod p$ for $1 \leq i \leq k$ and $p_1 \cdot \cdots \cdot p_k = p - 1$.
   Insufficient as $(10, 2, 45)$ is a ”valid” certificate for $91 \notin PRIMES$.
   Need some way to ensure that $p_1, \ldots, p_k$ are primes without having to check.
3. $C(p) = (r; p_1, C(p_1), p_2, C(p_2), \ldots, p_k, C(p_k))$ where C(1)=(1), $r^{p-1} = 1 \mod p$, and $r^{\frac{p-1}{p_i}} \neq 1 \mod p$ for $1 \leq i \leq k$ and $p_1 \cdot \cdots \cdot p_k = p - 1$.
   eg. $C(67) = (2; 2, (1), 3, (2; 2, (1)), 11, (8; 2, (1), 5, (3; 2, (1))))$.

Proof.

First we will show that the certificate is succinct. We will show that for all primes p the certificate has length at most $4 \cdot \log^2(p)$. If $p = 2$ or $p = 3$ this is trivial. For any $p > 3$, $p - 1$ will have $k < \log(p)$ prime divisors $q_1 = 2, q_2, \ldots, q_k$. Thus $C(p)$ will contain $2k$ separators, the number r, 2 and its certificate (1), the q_is (at most $2 \log p$ bits), and the $C(q_i)$s.

By the inductive hypothesis, we have that $|C(q_i)| \leq 4 \log^2 q_i$. Thus

$|C(p)| \leq 4 \log p + 5 + 4 \sum_{i=2}^{k} \log^2 q_i$

The logarithms of the q_1s add up to $\log \frac{p-1}{2} < \log p - 1$, so the sum of their squares is at most $(\log p - 1)^2$. Thus

$|C(p)| \leq 4 \log^2 p + 9 - 4 \log p$, which is less than $4 \log^2 p$ when $p \geq 5$. □

Proof.

First we will show that the certificate is succinct. We will show that for all primes p the certificate has length at most $4 \cdot \log^2(p)$. If $p = 2$ or $p = 3$ this is trivial. For any $p > 3$, $p - 1$ will have $k < \log(p)$ prime divisors $q_1 = 2, q_2, \ldots, q_k$. Thus $C(p)$ will contain $2k$ separators, the number r, 2 and its certificate (1), the q_is (at most $2 \log p$ bits), and the $C(q_i)$s.

By the inductive hypothesis, we have that $|C(q_i)| \leq 4 \log^2 q_i$. Thus
$|C(p)| \leq 4 \log p + 5 + 4 \sum_{i=2}^{k} \log^2 q_i$

The logarithms of the q_1s add up to $\log \frac{p-1}{2} < \log p - 1$, so the sum of their squares is at most $(\log p - 1)^2$. Thus
$|C(p)| \leq 4 \log^2 p + 9 - 4 \log p$, which is less than $4 \log^2 p$ when $p \geq 5$. □

Proof.

First we will show that the certificate is succinct. We will show that for all primes p the certificate has length at most $4 \cdot \log^2(p)$. If $p = 2$ or $p = 3$ this is trivial. For any $p > 3$, $p - 1$ will have $k < \log(p)$ prime divisors $q_1 = 2, q_2, \ldots, q_k$. Thus $C(p)$ will contain $2k$ separators, the number r, 2 and its certificate (1), the q_is (at most $2 \log p$ bits), and the $C(q_i)$s.

By the inductive hypothesis, we have that $|C(q_i)| \leq 4 \log^2 q_i$. Thus $|C(p)| \leq 4 \log p + 5 + 4 \sum_{i=2}^{k} \log^2 q_i$

The logarithms of the q_1s add up to $\log \frac{p-1}{2} < \log p - 1$, so the sum of their squares is at most $(\log p - 1)^2$. Thus $|C(p)| \leq 4 \log^2 p + 9 - 4 \log p$, which is less than $4 \log^2 p$ when $p \geq 5$. □

Proof.

First we will show that the certificate is succinct. We will show that for all primes p the certificate has length at most $4 \cdot \log^2(p)$. If $p = 2$ or $p = 3$ this is trivial. For any $p > 3$, $p - 1$ will have $k < \log(p)$ prime divisors $q_1 = 2, q_2, \ldots, q_k$. Thus $C(p)$ will contain $2k$ separators, the number r, 2 and its certificate (1), the q_is (at most $2 \log p$ bits), and the $C(q_i)$s.

By the inductive hypothesis, we have that $|C(q_i)| \leq 4 \log^2 q_i$. Thus
$|C(p)| \leq 4 \log p + 5 + 4 \sum_{i=2}^{k} \log^2 q_i$

The logarithms of the q_1s add up to $\log \frac{p-1}{2} < \log p - 1$, so the sum of their squares is at most $(\log p - 1)^2$. Thus
$|C(p)| \leq 4 \log^2 p + 9 - 4 \log p$, which is less than $4 \log^2 p$ when $p \geq 5$. □

Proof.

First we will show that the certificate is succinct. We will show that for all primes p the certificate has length at most $4 \cdot \log^2(p)$. If $p = 2$ or $p = 3$ this is trivial. For any $p > 3$, $p - 1$ will have $k < \log(p)$ prime divisors $q_1 = 2, q_2, \ldots, q_k$. Thus $C(p)$ will contain $2k$ separators, the number r, 2 and its certificate (1), the q_is (at most $2 \log p$ bits), and the $C(q_i)$s.

By the inductive hypothesis, we have that $|C(q_i)| \leq 4 \log^2 q_i$. Thus
$|C(p)| \leq 4 \log p + 5 + 4 \sum_{i=2}^{k} \log^2 q_i$

The logarithms of the q_1s add up to $\log \frac{p-1}{2} < \log p - 1$, so the sum of their squares is at most $(\log p - 1)^2$. Thus
$|C(p)| \leq 4 \log^2 p + 9 - 4 \log p$, which is less than $4 \log^2 p$ when $p \geq 5$. □

Proof.

First we will show that the certificate is succinct. We will show that for all primes p the certificate has length at most $4 \cdot \log^2(p)$. If $p = 2$ or $p = 3$ this is trivial. For any $p > 3$, $p - 1$ will have $k < \log(p)$ prime divisors $q_1 = 2, q_2, \ldots, q_k$. Thus $C(p)$ will contain $2k$ separators, the number r, 2 and its certificate (1), the q_is (at most $2 \log p$ bits), and the $C(q_i)$s.

By the inductive hypothesis, we have that $|C(q_i)| \leq 4 \log^2 q_i$. Thus $|C(p)| \leq 4 \log p + 5 + 4 \sum_{i=2}^{k} \log^2 q_i$

The logarithms of the q_1s add up to $\log \frac{p-1}{2} < \log p - 1$, so the sum of their squares is at most $(\log p - 1)^2$. Thus $|C(p)| \leq 4 \log^2 p + 9 - 4 \log p$, which is less than $4 \log^2 p$ when $p \geq 5$. □

Proof.

First we will show that the certificate is succinct. We will show that for all primes p the certificate has length at most $4 \cdot \log^2(p)$. If $p = 2$ or $p = 3$ this is trivial. For any $p > 3$, $p - 1$ will have $k < \log(p)$ prime divisors $q_1 = 2, q_2, \ldots, q_k$. Thus $C(p)$ will contain $2k$ separators, the number r, 2 and its certificate (1), the q_is (at most $2 \log p$ bits), and the $C(q_i)$s.

By the inductive hypothesis, we have that $|C(q_i)| \leq 4 \log^2 q_i$. Thus

$|C(p)| \leq 4 \log p + 5 + 4 \sum_{i=2}^{k} \log^2 q_i$

The logarithms of the q_1s add up to $\log \frac{p-1}{2} < \log p - 1$, so the sum of their squares is at most $(\log p - 1)^2$. Thus

$|C(p)| \leq 4 \log^2 p + 9 - 4 \log p$, which is less than $4 \log^2 p$ when $p \geq 5$. □

Proof.

First we will show that the certificate is succinct. We will show that for all primes p the certificate has length at most $4 \cdot \log^2(p)$. If $p = 2$ or $p = 3$ this is trivial. For any $p > 3$, $p - 1$ will have $k < \log(p)$ prime divisors $q_1 = 2, q_2, \ldots, q_k$. Thus $C(p)$ will contain $2k$ separators, the number r, 2 and its certificate (1), the q_is (at most $2 \log p$ bits), and the $C(q_i)$s.

By the inductive hypothesis, we have that $|C(q_i)| \leq 4 \log^2 q_i$. Thus

$|C(p)| \leq 4 \log p + 5 + 4 \sum_{i=2}^{k} \log^2 q_i$

The logarithms of the q_1s add up to $\log \frac{p-1}{2} < \log p - 1$, so the sum of their squares is at most $(\log p - 1)^2$. Thus

$|C(p)| \leq 4 \log^2 p + 9 - 4 \log p$, which is less than $4 \log^2 p$ when $p \geq 5$. □

Proof.

First we will show that the certificate is succinct. We will show that for all primes p the certificate has length at most $4 \cdot \log^2(p)$. If $p = 2$ or $p = 3$ this is trivial. For any $p > 3$, $p - 1$ will have $k < \log(p)$ prime divisors $q_1 = 2, q_2, \ldots, q_k$. Thus $C(p)$ will contain $2k$ separators, the number r, 2 and its certificate (1), the q_is (at most $2 \log p$ bits), and the $C(q_i)$s.

By the inductive hypothesis, we have that $|C(q_i)| \leq 4 \log^2 q_i$. Thus
$|C(p)| \leq 4 \log p + 5 + 4 \sum_{i=2}^{k} \log^2 q_i$

The logarithms of the q_1s add up to $\log \frac{p-1}{2} < \log p - 1$, so the sum of their squares is at most $(\log p - 1)^2$. Thus
$|C(p)| \leq 4 \log^2 p + 9 - 4 \log p$, which is less than $4 \log^2 p$ when $p \geq 5$. □

Proof.

First we will show that the certificate is succinct. We will show that for all primes p the certificate has length at most $4 \cdot \log^2(p)$. If $p = 2$ or $p = 3$ this is trivial. For any $p > 3$, $p - 1$ will have $k < \log(p)$ prime divisors $q_1 = 2, q_2, \ldots, q_k$. Thus $C(p)$ will contain $2k$ separators, the number r, 2 and its certificate (1), the q_is (at most $2 \log p$ bits), and the $C(q_i)$s.

By the inductive hypothesis, we have that $|C(q_i)| \leq 4 \log^2 q_i$. Thus
$|C(p)| \leq 4 \log p + 5 + 4 \sum_{i=2}^{k} \log^2 q_i$
The logarithms of the q_1s add up to $\log \frac{p-1}{2} < \log p - 1$, so the sum of their squares is at most $(\log p - 1)^2$. Thus
$|C(p)| \leq 4 \log^2 p + 9 - 4 \log p$, which is less than $4 \log^2 p$ when $p \geq 5$. □

Proof.

Now it needs to be shown that $C(p)$ is verifiable in polynomial time. This hinges of the computation of $r^{p-1} \mod p$. If repeated multiplication by r is done then this process clearly takes exponential time. However, repeated squaring can be used. Let $l = \lceil \log(p) \rceil$. First $r, r^2, r^4, \ldots, r^{2^l} \mod p$ are computed. Each of these steps takes $O(l^2)$ time. Then multiply the appropriate exponents of r to obtain $r^{p-1} \mod p$. As there are $O(l)$ multiplications this entire process takes $O(l^3)$ time. □

Example

$p = 7, \; r = 5$
thus $p - 1 = 6$ and $l = 3$.
so $r^2 = 25 \equiv 4, r^4 = 16 \equiv 2, r^8 = 4 \mod 7$ thus $r^{p-1} = r^4 \cdot r^2 = 8 \equiv 1 \mod 7$.

Proof.

Now it needs to be shown that $C(p)$ is verifiable in polynomial time. This hinges of the computation of $r^{p-1} \mod p$. If repeated multiplication by r is done then this process clearly takes exponential time. However, repeated squaring can be used.

Let $l = \lceil \log(p) \rceil$. First $r, r^2, r^4, \ldots, r^{2^l} \mod p$ are computed. Each of these steps takes $O(l^2)$ time. Then multiply the appropriate exponents of r to obtain $r^{p-1} \mod p$. As there are $O(l)$ multiplications this entire process takes $O(l^3)$ time. □

Example

$p = 7,\ r = 5$
thus $p - 1 = 6$ and $l = 3$.
so $r^2 = 25 \equiv 4, r^4 = 16 \equiv 2, r^8 = 4 \mod 7$ thus $r^{p-1} = r^4 \cdot r^2 = 8 \equiv 1 \mod 7$.

Proof.

Now it needs to be shown that $C(p)$ is verifiable in polynomial time. This hinges of the computation of $r^{p-1} \mod p$. If repeated multiplication by r is done then this process clearly takes exponential time. However, repeated squaring can be used. Let $l = \lceil \log(p) \rceil$. First $r, r^2, r^4, \ldots, r^{2^l} \mod p$ are computed. Each of these steps takes $O(l^2)$ time. Then multiply the appropriate exponents of r to obtain $r^{p-1} \mod p$. As there are $O(l)$ multiplications this entire process takes $O(l^3)$ time. □

Example

$p = 7, \ r = 5$
thus $p - 1 = 6$ and $l = 3$.
so $r^2 = 25 \equiv 4, r^4 = 16 \equiv 2, r^8 = 4 \mod 7$ thus $r^{p-1} = r^4 \cdot r^2 = 8 \equiv 1 \mod 7$.

Proof.

Now it needs to be shown that $C(p)$ is verifiable in polynomial time. This hinges of the computation of $r^{p-1} \mod p$. If repeated multiplication by r is done then this process clearly takes exponential time. However, repeated squaring can be used.

Let $l = \lceil \log(p) \rceil$. First $r, r^2, r^4, \ldots, r^{2^l} \mod p$ are computed. Each of these steps takes $O(l^2)$ time. Then multiply the appropriate exponents of r to obtain $r^{p-1} \mod p$. As there are $O(l)$ multiplications this entire process takes $O(l^3)$ time. □

Example

$p = 7, \; r = 5$
thus $p - 1 = 6$ and $l = 3$.
so $r^2 = 25 \equiv 4, r^4 = 16 \equiv 2, r^8 = 4 \mod 7$ thus $r^{p-1} = r^4 \cdot r^2 = 8 \equiv 1 \mod 7$.

Proof.

Now it needs to be shown that $C(p)$ is verifiable in polynomial time. This hinges of the computation of $r^{p-1} \mod p$. If repeated multiplication by r is done then this process clearly takes exponential time. However, repeated squaring can be used.

Let $l = \lceil \log(p) \rceil$. First $r, r^2, r^4, \ldots, r^{2^l} \mod p$ are computed. Each of these steps takes $O(l^2)$ time. Then multiply the appropriate exponents of r to obtain $r^{p-1} \mod p$. As there are $O(l)$ multiplications this entire process takes $O(l^3)$ time. □

Example

$p = 7,\ r = 5$
thus $p - 1 = 6$ and $l = 3$.
so $r^2 = 25 \equiv 4, r^4 = 16 \equiv 2, r^8 = 4 \mod 7$ thus $r^{p-1} = r^4 \cdot r^2 = 8 \equiv 1 \mod 7$.

Proof.

Now it needs to be shown that $C(p)$ is verifiable in polynomial time. This hinges of the computation of $r^{p-1} \mod p$. If repeated multiplication by r is done then this process clearly takes exponential time. However, repeated squaring can be used.

Let $l = \lceil \log(p) \rceil$. First $r, r^2, r^4, \ldots, r^{2^l} \mod p$ are computed. Each of these steps takes $O(l^2)$ time. Then multiply the appropriate exponents of r to obtain $r^{p-1} \mod p$. As there are $O(l)$ multiplications this entire process takes $O(l^3)$ time. □

Example

$p = 7, \ r = 5$
thus $p - 1 = 6$ and $l = 3$.
so $r^2 = 25 \equiv 4, r^4 = 16 \equiv 2, r^8 = 4 \mod 7$ thus $r^{p-1} = r^4 \cdot r^2 = 8 \equiv 1 \mod 7$.

Proof.

Now it needs to be shown that $C(p)$ is verifiable in polynomial time. This hinges of the computation of $r^{p-1} \mod p$. If repeated multiplication by r is done then this process clearly takes exponential time. However, repeated squaring can be used.

Let $l = \lceil \log(p) \rceil$. First $r, r^2, r^4, \ldots, r^{2^l} \mod p$ are computed. Each of these steps takes $O(l^2)$ time. Then multiply the appropriate exponents of r to obtain $r^{p-1} \mod p$. As there are $O(l)$ multiplications this entire process takes $O(l^3)$ time. □

Example

$p = 7,\ r = 5$
thus $p - 1 = 6$ and $l = 3$.
so $r^2 = 25 \equiv 4, r^4 = 16 \equiv 2, r^8 = 4 \mod 7$ thus $r^{p-1} = r^4 \cdot r^2 = 8 \equiv 1 \mod 7$.

Proof.

Now it needs to be shown that $C(p)$ is verifiable in polynomial time. This hinges of the computation of $r^{p-1} \mod p$. If repeated multiplication by r is done then this process clearly takes exponential time. However, repeated squaring can be used.

Let $l = \lceil \log(p) \rceil$. First $r, r^2, r^4, \ldots, r^{2^l} \mod p$ are computed. Each of these steps takes $O(l^2)$ time. Then multiply the appropriate exponents of r to obtain $r^{p-1} \mod p$. As there are $O(l)$ multiplications this entire process takes $O(l^3)$ time. $\square$

Example

$p = 7,\ r = 5$

thus $p - 1 = 6$ and $l = 3$.

so $r^2 = 25 \equiv 4, r^4 = 16 \equiv 2, r^8 = 4 \mod 7$ thus $r^{p-1} = r^4 \cdot r^2 = 8 \equiv 1 \mod 7$.

Proof.

Now it needs to be shown that $C(p)$ is verifiable in polynomial time. This hinges of the computation of $r^{p-1} \mod p$. If repeated multiplication by r is done then this process clearly takes exponential time. However, repeated squaring can be used.

Let $l = \lceil \log(p) \rceil$. First $r, r^2, r^4, \ldots, r^{2^l} \mod p$ are computed. Each of these steps takes $O(l^2)$ time. Then multiply the appropriate exponents of r to obtain $r^{p-1} \mod p$. As there are $O(l)$ multiplications this entire process takes $O(l^3)$ time. □

Example

$p = 7,\ r = 5$
thus $p - 1 = 6$ and $l = 3$.
so $r^2 = 25 \equiv 4, r^4 = 16 \equiv 2, r^8 = 4 \mod 7$ thus $r^{p-1} = r^4 \cdot r^2 = 8 \equiv 1 \mod 7$.

Proof.

Now it needs to be shown that $C(p)$ is verifiable in polynomial time. This hinges of the computation of $r^{p-1} \mod p$. If repeated multiplication by r is done then this process clearly takes exponential time. However, repeated squaring can be used.

Let $l = \lceil \log(p) \rceil$. First $r, r^2, r^4, \ldots, r^{2^l} \mod p$ are computed. Each of these steps takes $O(l^2)$ time. Then multiply the appropriate exponents of r to obtain $r^{p-1} \mod p$. As there are $O(l)$ multiplications this entire process takes $O(l^3)$ time. □

Example

$p = 7,\ r = 5$
thus $p - 1 = 6$ and $l = 3$.
so $r^2 = 25 \equiv 4, r^4 = 16 \equiv 2, r^8 = 4 \mod 7$ thus $r^{p-1} = r^4 \cdot r^2 = 8 \equiv 1 \mod 7$.

Proof.

However, it is not enough that $r^{p-1} \mod p$ takes $O(l^3)$ time. We need to show that the entire verification process of $C(p)$ runs in polynomial time. To do this we need to compute $r^{p-1} \mod p$, $r^{\frac{p-1}{q_i}} \mod p$ for each of the $O(l)$ q_is, $q_1, q_2, \ldots, q_k$, and each of the $C(q_i)$s. This entire process takes $O(l^4)$ time. □

Proof.

However, it is not enough that $r^{p-1} \mod p$ takes $O(l^3)$ time. We need to show that the entire verification process of $C(p)$ runs in polynomial time. To do this we need to compute $r^{p-1} \mod p$, $r^{\frac{p-1}{q_i}} \mod p$ for each of the $O(l)$ q_is, $q_1, q_2, \ldots, q_k$, and each of the $C(q_i)$s. This entire process takes $O(l^4)$ time. □

Proof.

However, it is not enough that $r^{p-1} \mod p$ takes $O(l^3)$ time. We need to show that the entire verification process of $C(p)$ runs in polynomial time. To do this we need to compute $r^{p-1} \mod p$, $r^{\frac{p-1}{q_i}} \mod p$ for each of the $O(l)$ q_is, $q_1, q_2, \ldots, q_k$, and each of the $C(q_i)$s. This entire process takes $O(l^4)$ time. $\square$

Proof.

However, it is not enough that $r^{p-1} \mod p$ takes $O(l^3)$ time. We need to show that the entire verification process of $C(p)$ runs in polynomial time. To do this we need to compute $r^{p-1} \mod p$, $r^{\frac{p-1}{q_i}} \mod p$ for each of the $O(l)$ q_is, $q_1, q_2, \ldots, q_k$, and each of the $C(q_i)$s. This entire process takes $O(l^4)$ time. $\square$

Outline

1. Description of coNP and examples of problems
   - What is coNP
   - Examples of problems in coNP
2. The NP ∩ coNP complexity class
   - Properties of NP ∩ coNP
   - Problems in NP ∩ coNP
3. NP, coNP, and P
   - The P, NP, coNP Hierarchy

Inclusion Relationships

Relation to P

Just as $P \subseteq NP$, we have that $P = coP \subseteq coNP$. Thus $P \subseteq NP \cap coNP$.
It is also unknown if $P = NP \cap coNP$.

Inclusion Relationships

Relation to P

Just as $P \subseteq NP$, we have that $P = coP \subseteq coNP$. Thus $P \subseteq NP \cap coNP$.
It is also unknown if $P = NP \cap coNP$.

Inclusion Relationships

Relation to P

Just as $P \subseteq NP$, we have that $P = coP \subseteq coNP$. Thus $P \subseteq NP \cap coNP$.
It is also unknown if $P = NP \cap coNP$.

The Complexity Picture