Randomized Algorithms

Abundance of Witnesses

Mohammad Heidari

Yazd University

May 8, 2016

Objectives

Definition

Abundance of witnesses is used in decision problems to decide whether an input x has a property $L(x \in L)$ or not. The object representing the property is called a *witness*.

Objectives

Definition

Abundance of witnesses is used in decision problems to decide whether an input x has a property $L(x \in L)$ or not. The object representing the property is called a *witness*.

Objectives

Definition

Abundance of witnesses is used in decision problems to decide whether an input x has a property $L(x \in L)$ or not. The object representing the property is called a *witness*.

Objective

Here we are trying to solve primality testing, which is the following decision problem. For a given positive integer n, decide whether n is a prime of a composite number. Our aim is to design an efficient, randomized algorithm for primality testing.

Prime Number

A positive integer n is a prime if and only if it does not have any factor (any nontrivial divisor), i.e if and only if it is not dividable by any number from $\{2, 3, ..., n-1\}$

Algorithm NAIV

input: A number $n \in \mathbb{N} - \{0, 1, 2\}$.

$I := 2$

$PRIME := TRUE$

While $I < n$ and $PRIME = TRUE$ do

begin

if n mod $I = 0$ then $PRIME := FALSE$;

$I := I + 1$

end

if $PRIME = TRUE$ then

output "n is a prime"

else

output "n is composite"

It is important to note that instead of testing from $\{2, 3, ..., n-1\}$ for divisibility of n, it suffices to consider the integers from $\{2, 3, ..., \lfloor\sqrt{n}\rfloor\}$

It is important to note that instead of testing from $\{2, 3, ..., n-1\}$ for divisibility of n, it suffices to consider the integers from $\{2, 3, ..., \lfloor\sqrt{n}\rfloor\}$

Time Complexity

After this improvement, the time complexity of the NAIV Algorithm is not $O(\sqrt{n})$, it is $2^{\frac{\log_2^n}{2}}$.

Requirements of a good witness

1. A witness of the fact "n is composite" has to offer a possibility of efficiently proving this fact.
2. Every candidate for a witness must be efficiently checkable, whether or not it is a witness.
3. The set of candidates must be specified in such a way that there is an abundance of witnesses in a set of candidates.

Requirements of a good witness

1. A witness of the fact "n is composite" has to offer a possibility of efficiently proving this fact.
2. Every candidate for a witness must be efficiently checkable, whether or not it is a witness.
3. The set of candidates must be specified in such a way that there is an abundance of witnesses in a set of candidates.

Requirements of a good witness

1. A witness of the fact "n is composite" has to offer a possibility of efficiently proving this fact.
2. Every candidate for a witness must be efficiently checkable, whether or not it is a witness.
3. The set of candidates must be specified in such a way that there is an abundance of witnesses in a set of candidates.

The Simplest Idea of Witness

Definition of a witness

let $PRIM$ denote the set of all primes. Number $a \in \{2, 3, ..., n-1\}$ is a witness of that fact $n \notin PRIM$ if and only if a divides n.

The Simplest Idea of Witness

Definition of a witness

let $PRIM$ denote the set of all primes. Number $a \in \{2, 3, ..., n-1\}$ is a witness of that fact $n \notin PRIM$ if and only if a divides n.

The Simplest Idea of Witness

Definition of a witness

let $PRIM$ denote the set of all primes. Number $a \in \{2, 3, ..., n-1\}$ is a witness of that fact $n \notin PRIM$ if and only if a divides n.

This definition fulfills the constraints (i) and (ii). For many integers n, the constraint (iii) is fulfilled, too. But for numbers $n = p.q$ where $p, q \in PRIM$, there are only two witness of the fact $n \notin PRIM$. Therefore the probability of choosing them is $\frac{2}{n-2}$.

Fermat's Little Theorem

Theorem

For every prime p and every $a \in \{1, 2, ..., p-1\}$, $a^{p-1} \bmod p = 1$

The Second Definition of a Witness

Definition

A number $a \in \{1, 2, ..., n-1\}$ is a witness of the fact $n \notin PRIM$ if and only if $a^{n-1} \bmod n \neq 1$

The Second Definition of a Witness

Definition

A number $a \in \{1, 2, ..., n-1\}$ is a witness of the fact $n \notin PRIM$ if and only if $a^{n-1} \bmod n \neq 1$

The Second Definition of a Witness

Definition

A number $a \in \{1, 2, ..., n-1\}$ is a witness of the fact $n \notin PRIM$ if and only if $a^{n-1} \bmod n \neq 1$

Using Squaring method we can efficiently compute the value $a^{n-1} \bmod n$, so it satisfies constraints (i), (ii). But there are composite numbers n that

$$a^{n-1} \ mod \ n = 1 \quad \forall a \in \{1, ..., n-1\}$$

For such numbers there is no witness of $n \notin PRIM$. These numbers are called Carmichael and there are infinitely many Carmichael numbers.

$$561 = 3.11.17, \ \ 1105 = 5.13.17, \ \ 1729 = 7.13.19$$

Theorem A.2.27

Theorem A.2.27

It is well known that

$$n \in PRIM \Leftrightarrow (\mathbb{Z}_n - \{0\}, \odot_{mod\ p})$$

is a group

Theorem 6.2.1

Theorem 6.2.1

Let $p > 2$ be an odd integer, Then

$$p \ is \ a \ prime \Leftrightarrow a^{\frac{p-1}{2}} \ mod \ p \in \{1, p-1\} \quad \forall a \in \mathbb{Z}_p - \{0\}$$

Theorem 6.2.1 - Proof (i)

$p > 2$ and it is odd, so

$$p = 2.p^{'} + 1$$

By Little Fermat's Theorem we have: $a^{p-1} \equiv 1(mod\ p)$
Since

$$a^{p-1} = a^{2.p^{'}} = (a^{p^{'}} - 1).(a^{p^{'}} + 1) + 1$$

Then

$$(a^{p^{'}} - 1).(a^{p^{'}} + 1) \equiv 0(mod\ p)$$

p is prime, so

$$a^{p^{'}} - 1 \equiv 0(mod\ p) \quad or \quad a^{p^{'}} + 1 \equiv 0(mod\ p) \qquad (6.4)$$

By inserting $p^{'} = \frac{(p-1)}{2}$ in the (6.4), we obtain

$$a^{\frac{(p-1)}{2}} \equiv 1(mod\ p) \quad or \quad a^{\frac{(p-1)}{2}} \equiv -1 \equiv p-1(mod\ p)$$

Theorem 6.2.1 - Proof (i)

$p > 2$ and it is odd, so

$$p = 2.p^{'} + 1$$

By Little Fermat's Theorem we have: $a^{p-1} \equiv 1(mod\ p)$

Since

$$a^{p-1} = a^{2.p^{'}} = (a^{p^{'}} - 1).(a^{p^{'}} + 1) + 1$$

Then

$$(a^{p^{'}} - 1).(a^{p^{'}} + 1) \equiv 0(mod\ p)$$

p is prime, so

$$a^{p^{'}} - 1 \equiv 0(mod\ p) \quad or \quad a^{p^{'}} + 1 \equiv 0(mod\ p) \qquad (6.4)$$

By inserting $p^{'} = \frac{(p-1)}{2}$ in the (6.4), we obtain

$$a^{\frac{(p-1)}{2}} \equiv 1(mod\ p) \quad or \quad a^{\frac{(p-1)}{2}} \equiv -1 \equiv p - 1(mod\ p)$$

Theorem 6.2.1 - Proof (i)

$p > 2$ and it is odd, so

$$p = 2.p^{'} + 1$$

By Little Fermat's Theorem we have: $a^{p-1} \equiv 1(mod\ p)$
Since

$$a^{p-1} = a^{2.p^{'}} = (a^{p^{'}} - 1).(a^{p^{'}} + 1) + 1$$

Then

$$(a^{p^{'}} - 1).(a^{p^{'}} + 1) \equiv 0(mod\ p)$$

p is prime, so

$$a^{p^{'}} - 1 \equiv 0(mod\ p) \quad or \quad a^{p^{'}} + 1 \equiv 0(mod\ p) \qquad (6.4)$$

By inserting $p^{'} = \frac{(p-1)}{2}$ in the (6.4), we obtain

$$a^{\frac{(p-1)}{2}} \equiv 1(mod\ p) \quad or \quad a^{\frac{(p-1)}{2}} \equiv -1 \equiv p-1(mod\ p)$$

Theorem 6.2.1 - Proof (i)

$p > 2$ and it is odd, so

$$p = 2.p^{'} + 1$$

By Little Fermat's Theorem we have: $a^{p-1} \equiv 1(mod\ p)$
Since

$$a^{p-1} = a^{2.p^{'}} = (a^{p^{'}} - 1).(a^{p^{'}} + 1) + 1$$

Then

$$(a^{p^{'}} - 1).(a^{p^{'}} + 1) \equiv 0(mod\ p)$$

p is prime, so

$$a^{p^{'}} - 1 \equiv 0(mod\ p) \quad or \quad a^{p^{'}} + 1 \equiv 0(mod\ p) \qquad (6.4)$$

By inserting $p^{'} = \frac{(p-1)}{2}$ in the (6.4), we obtain

$$a^{\frac{(p-1)}{2}} \equiv 1(mod\ p) \quad or \quad a^{\frac{(p-1)}{2}} \equiv -1 \equiv p-1(mod\ p)$$

Theorem 6.2.1 - Proof (i)

$p > 2$ and it is odd, so

$$p = 2.p^{'} + 1$$

By Little Fermat's Theorem we have: $a^{p-1} \equiv 1(mod\ p)$
Since

$$a^{p-1} = a^{2.p^{'}} = (a^{p^{'}} - 1).(a^{p^{'}} + 1) + 1$$

Then

$$(a^{p^{'}} - 1).(a^{p^{'}} + 1) \equiv 0(mod\ p)$$

p is prime, so

$$a^{p^{'}} - 1 \equiv 0(mod\ p) \quad or \quad a^{p^{'}} + 1 \equiv 0(mod\ p) \qquad (6.4)$$

By inserting $p^{'} = \frac{(p-1)}{2}$ in the (6.4), we obtain

$$a^{\frac{(p-1)}{2}} \equiv 1(mod\ p) \quad or \quad a^{\frac{(p-1)}{2}} \equiv -1 \equiv p - 1(mod\ p)$$

Theorem 6.2.1 - Proof (ii)

Let $p > 2$ be an odd integer such that

$$c^{\frac{(p-1)}{2}} \ mod \ p \in \{1, p-1\} \qquad \forall c \in \mathbb{Z}_p - \{0\}$$

Prove by contradiction, Let $p = a.b$ be a composite number, we have

$$a^{\frac{(p-1)}{2}} \ mod \ p \in \{1, -1\} \quad and \quad b^{\frac{(p-1)}{2}} \ mod \ p \in \{1, -1\}$$

Since $\odot_{mod \ p}$ is communicative, then

$$(a.b)^{\frac{(p-1)}{2}} \ mod \ p = a^{\frac{(p-1)}{2}}.b^{\frac{(p-1)}{2}} \ mod \ p \in \{1, -1\} \qquad (6.5)$$

since $a.b = p$, we have

$$0 = p \ mod \ p = p^{\frac{(p-1)}{2}} \ mod \ p = (a.b)^{\frac{(p-1)}{2}}$$

which contradicts (6.5) ■

Theorem 6.2.1 - Proof (ii)

Let $p > 2$ be an odd integer such that

$$c^{\frac{(p-1)}{2}} \ mod \ p \in \{1, p-1\} \qquad \forall c \in \mathbb{Z}_p - \{0\}$$

Prove by contradiction, Let $p = a.b$ be a composite number, we have

$$a^{\frac{(p-1)}{2}} \ mod \ p \in \{1, -1\} \quad and \quad b^{\frac{(p-1)}{2}} \ mod \ p \in \{1, -1\}$$

Since $\odot_{mod \ p}$ is communicative, then

$$(a.b)^{\frac{(p-1)}{2}} \ mod \ p = a^{\frac{(p-1)}{2}}.b^{\frac{(p-1)}{2}} \ mod \ p \in \{1, -1\} \qquad (6.5)$$

since $a.b = p$, we have

$$0 = p \ mod \ p = p^{\frac{(p-1)}{2}} \ mod \ p = (a.b)^{\frac{(p-1)}{2}}$$

which contradicts (6.5) ■

Theorem 6.2.1 - Proof (ii)

Let $p > 2$ be an odd integer such that

$$c^{\frac{(p-1)}{2}} \ mod \ p \in \{1, p-1\} \qquad \forall c \in \mathbb{Z}_p - \{0\}$$

Prove by contradiction, Let $p = a.b$ be a composite number, we have

$$a^{\frac{(p-1)}{2}} \ mod \ p \in \{1, -1\} \quad and \quad b^{\frac{(p-1)}{2}} \ mod \ p \in \{1, -1\}$$

Since $\odot_{mod \ p}$ is communicative, then

$$(a.b)^{\frac{(p-1)}{2}} \ mod \ p = a^{\frac{(p-1)}{2}}.b^{\frac{(p-1)}{2}} \ mod \ p \in \{1, -1\} \qquad (6.5)$$

since $a.b = p$, we have

$$0 = p \ mod \ p = p^{\frac{(p-1)}{2}} \ mod \ p = (a.b)^{\frac{(p-1)}{2}}$$

which contradicts (6.5)■

Theorem 6.2.1 - Proof (ii)

Let $p > 2$ be an odd integer such that

$$c^{\frac{(p-1)}{2}} \ mod \ p \in \{1, p-1\} \quad \forall c \in \mathbb{Z}_p - \{0\}$$

Prove by contradiction, Let $p = a.b$ be a composite number, we have

$$a^{\frac{(p-1)}{2}} \ mod \ p \in \{1, -1\} \quad and \quad b^{\frac{(p-1)}{2}} \ mod \ p \in \{1, -1\}$$

Since $\odot_{mod \ p}$ is communicative, then

$$(a.b)^{\frac{(p-1)}{2}} \ mod \ p = a^{\frac{(p-1)}{2}}.b^{\frac{(p-1)}{2}} \ mod \ p \in \{1, -1\} \quad (6.5)$$

since $a.b = p$, we have

$$0 = p \ mod \ p = p^{\frac{(p-1)}{2}} \ mod \ p = (a.b)^{\frac{(p-1)}{2}}$$

which contradicts (6.5)■

Third Definition of a Witness

Definition of a witness

Let n be an odd integer, $n \geq 3$. A number $a \in \{1, 2, ...n-1\}$ is a witness of the fact "$n \notin PRIM$", if and only if

$$a^{\frac{(n-1)}{2}} \ mod \ n \notin \{1, n-1\} \qquad (6.6)$$

Third Definition of a Witness

Definition of a witness

Let n be an odd integer, $n \geq 3$. A number $a \in \{1, 2, ...n-1\}$ is a witness of the fact "$n \notin PRIM$", if and only if

$$a^{\frac{(n-1)}{2}} \ mod \ n \notin \{1, n-1\} \qquad (6.6)$$

Third Definition of a Witness

Definition of a witness

Let n be an odd integer, $n \geq 3$. A number $a \in \{1, 2, ...n-1\}$ is a witness of the fact "$n \notin PRIM$", if and only if

$$a^{\frac{(n-1)}{2}} \ mod \ n \notin \{1, n-1\} \qquad (6.6)$$

This kind of witness satisfies conditions (i) and (ii). Theorem 6.2.2 shows that this definition assures the abundance of witnesses for at least every second odd integer greater than 2.

Theorem 6.2.2

Go Back

Theorem 6.2.2

For every positive integer n with an odd $\frac{(n-1)}{2}$ (i.e, for $n \equiv 3(mod\ 4)$),

(i) if n is a prime, then

$$a^{\frac{n-1}{2}}\ mod\ n \in \{1, n-1\} \qquad \forall a \in \{1, ..., n-1\}$$

(ii) if n is composite, then

$$a^{\frac{n-1}{2}}\ mod\ n \notin \{1, n-1\}$$

for at least half of the elements a from $\{1, 2, ..., n-1\}$

Theorem 6.2.2 - Proof (i)

The assertion (i) has already been proved in Theorem 6.2.1. Hence, it remains to show (ii).

Theorem 6.2.2 - Proof (ii) ...

Let

$$WITNESS = \{a \in \{1, 2, ..., n-1\} | a^{\frac{(n-1)}{2}} \ mod \ n \notin \{1, n-1\}\}$$

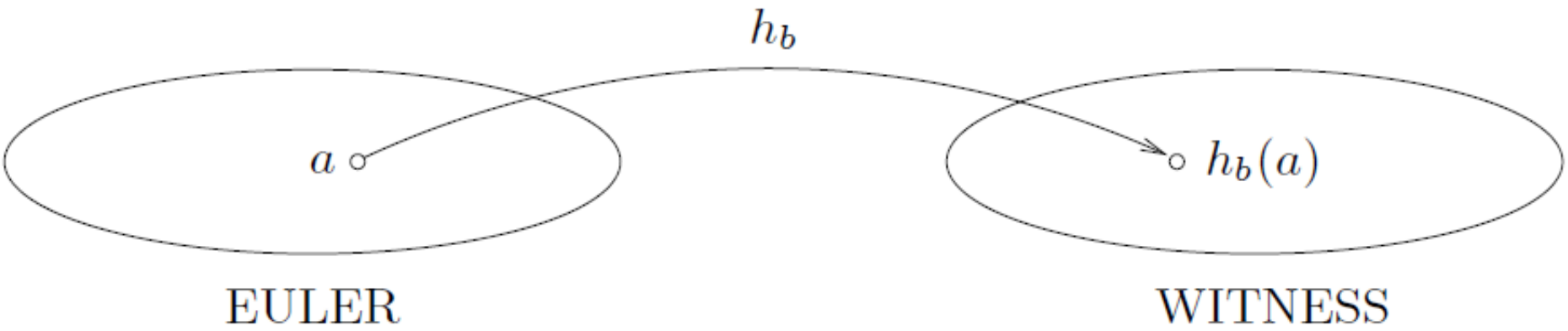
be the set of all witnesses of $n \notin PRIM$, and let

$$EULER = \{a \in \{1, 2, ..., n-1\} | a^{\frac{(n-1)}{2}} \ mod \ n \in \{1, n-1\}\}$$

be the complementary set of non-witnesses.

Theorem 6.2.2 - Proof (ii) ...

$$|\text{EULER}| \leq |\text{WITNESS}|.$$



Theorem 6.2.2 - Proof (ii) ...

Assume $b \in$ WITNESS for which there exists b^{-1} in the group $(\mathbb{Z}_n^*, \odot_{mod\ \ n})$.

Define

$$h_b(a) = a.b \ \ mod \ \ n$$

Next, we will show that h_b is an injective mapping from EULER to WITNESS.

Theorem 6.2.2 - Proof (ii) ...

Claim: $\forall a \in$ EULER, the $h_b(a) = a.b \notin$ EULER so is in WITNESS
Proof.

$$(a.b)^{\frac{(n-1)}{2}} \ mod \ n = \left(a^{\frac{(n-1)}{2}} \ mod \ n\right).\left(b^{\frac{(n-1)}{2}} \ mod \ n\right)$$

$$= \pm b^{\frac{(n-1)}{2}} \ mod \ n \notin \{1, n-1\}$$

(Since $a^{\frac{(n-1)}{2}} \ mod \ n \in \{1, n-1\}$ and $b \in$ WITNESS)

Thus, h_b is a mapping from EULER to WITNESS

Theorem 6.2.2 - Proof (ii) ...

Claim: h_b is injective:

$$\forall a_1, a_2 \in EULER, a_1 \neq a_2 \Rightarrow h_b(a_1) \neq h_b(a_2)$$

Proof. Assume $h_b(a_1) = h_b(a_2)$, then

$$a_1.b \equiv a_2.b \ (mod \ n) \qquad (6.7)$$

Multiplying the congruence (6.7) from the right by b^{-1}, we obtain

$$a_1 = a_1.b.b^{-1} \ mod \ n = a_2.b.b^{-1} \ mod \ n = a_2$$

Theorem 6.2.2 - Proof (ii) ...

Chinese Remainder Theorem

Let r, s be positive integers which are relatively prime and let a and b be any two integers. Then there is an integer N such that

$$N \equiv a(mod\ r)$$

and

$$N \equiv b(mod\ s)$$

Theorem 6.2.2 - Proof (ii) ...

To complete the proof we have still to show that there exists an element $b \in$ WITNESS $\cap \mathbb{Z}_n^*$.
Let $n = p.q$ for two nontrivial factors p and q with $GCD(p, q) = 1$. Since it is clearer to search for b in $\mathbb{Z}_p \times \mathbb{Z}_q$ instead of searching in $\mathbb{Z}_n$, we apply the Chinese Remainder Theorem.

$\forall a \in \mathbb{Z}_n$, the pair

$$(a \ mod \ p, a \ mod \ q)$$

is the representation of a in $\mathbb{Z}_p \times \mathbb{Z}_q$.

Theorem 6.2.2 - Proof (ii) ...

If $a \in$ EULER then

$$a^{\frac{(n-1)}{2}} \ mod \ p.q \in \{1, n-1\}$$

which implies for a $k \in \mathbb{N}$ either

$$a^{\frac{(n-1)}{2}} = k.p.q + 1$$

or

$$a^{\frac{(n-1)}{2}} = k.p.q + n - 1$$

Theorem 6.2.2 - Proof (ii) ...

A direct consequence of it is either

$$a^{\frac{(n-1)}{2}} \ mod \ p = a^{\frac{(n-1)}{2}} \ mod \ q = 1$$

or

$$a^{\frac{(n-1)}{2}} \ mod \ p = (n-1) \ mod \ p = (p.q-1) \ mod \ p = p-1 \ and$$

$$a^{\frac{(n-1)}{2}} \ mod \ q = (n-1) \ mod \ q = (p.q-1) \ mod \ q = q-1$$

Hence either $(1,1)$ or $(p-1, q-1) = (-1,-1)$ is the representation of $a^{\frac{(n-1)}{2}}$ mod n in $\mathbb{Z}_p \times \mathbb{Z}_q$ for every $a \in$ EULER.

Theorem 6.2.2 - Proof (ii) ...

Therefore we choose

$$(1, q-1) = (1, -1)$$

as the representation of b in $\mathbb{Z}_p \times \mathbb{Z}_q$.

We need to show that b has the required properties.
The representation of $b^{\frac{(n-1)}{2}} \bmod n$ in $\mathbb{Z}_p \times \mathbb{Z}_q$ is:

$$\left(b^{\frac{(n-1)}{2}} \ mod\ p, b^{\frac{(n-1)}{2}} \ mod\ q\right) = \left(1^{\frac{(n-1)}{2}} \ mod\ p, (-1)^{\frac{(n-1)}{2}} \ mod\ q\right) = (1, -1)$$

(because $\frac{n-1}{2}$ is odd).

Hence, b is not a Eulerian number, and so $b \in$ WITNESS

Theorem 6.2.2 - Proof (ii)

To complete the proof, we need to show $b^{-1} = b$. Since $(1, 1)$ is the natural element with respect to the multiplication in $\mathbb{Z}_p \times \mathbb{Z}_q$,

$$(1, q-1) \odot_{p,q} (1, q-1) = (1.1 \ mod \ p, (q-1).(q-1) \ mod \ q) = (1, 1)$$

implies that b is inverse to itself. ■

SSSA (Simplified Solovay-Strassen Algorithm)

input: An odd integer n with $n \equiv 3(mod\ 4)$

Step 1: Choose uniformly an $a \in \{1, 2, ...n-1\}$ at random.

Step 2: Compute $A := a^{\frac{(n-1)}{2}}\ mod\ n$.

Step 3:

if $A \in \{1, -1\}$ then

output "$n \in PRIM$" {reject}

else

output "$n \notin PRIM$" {accept}

Theorem 6.2.6

Theorem 6.2.6

SSSA is a polynomial-time 1MC algorithm for the recognition of composite numbers n with $n \bmod 4 = 3$.

Theorem 6.2.6 - Proof

The value of A can be efficiently computed by repeated squaring. The fact that SSSA is a 1MC algorithm is a direct consequence of Theorem 6.2.2. If p is a prime, then (i) of Theorem 6.2.2 assures that there is no witness of $p \notin PRIM$, and so the algorithm SSSA answers "$n \in PRIM$" with certainly.

If p is composite, then (ii) of Theorem 6.2.2 assures that

$$\text{Prob(SSSA outputs "}n \notin PRIM\text{")} \geq \frac{1}{2}\blacksquare$$

Objective

We have a kind of witness, that provides an efficient randomized algorithm for primality testing for all positive integers n with $n \equiv 3(\text{ mod } 4)$. This section aims to extend this kind of witness in a way that results in a randomized primality testing for all odd integers.

An Extension to Definition (6.6)

- An $a \in \{1, 2, ..., n-1\}$ with GCD$(a, n) \neq 1$ is also a witness of the fact $n \notin$ PRIM
- GCD(a, n) can be efficiently computed by the Euclidean algorithm

An Extension to Definition (6.6)

- An $a \in \{1, 2, ..., n-1\}$ with GCD$(a, n) \neq 1$ is also a witness of the fact $n \notin$ PRIM
- GCD(a, n) can be efficiently computed by the Euclidean algorithm

Extension of the definition (6.6) of witnesses

A number $a \in \{1, 2, ..., n-1\}$ is a witness of the fact $n \notin$ PRIM for an odd positive integer n if

(i) GCD$(a, n) > 1$, or (6.9)

(ii)GCD$(a, n) = 1$ and $a^{\frac{n-1}{2}} \bmod n \notin \{1, n-1\}$

An Extension to Definition (6.6)

- An $a \in \{1, 2, ..., n-1\}$ with GCD$(a, n) \neq 1$ is also a witness of the fact $n \notin$ PRIM
- GCD(a, n) can be efficiently computed by the Euclidean algorithm

Extension of the definition (6.6) of witnesses

A number $a \in \{1, 2, ..., n-1\}$ is a witness of the fact $n \notin$ PRIM for an odd positive integer n if

(i) GCD$(a, n) > 1$, or (6.9)

(ii)GCD$(a, n) = 1$ and $a^{\frac{n-1}{2}} \bmod n \notin \{1, n-1\}$

An Extension to Definition (6.6)

- An $a \in \{1, 2, ..., n-1\}$ with GCD$(a, n) \neq 1$ is also a witness of the fact $n \notin$ PRIM
- GCD(a, n) can be efficiently computed by the Euclidean algorithm

Extension of the definition (6.6) of witnesses

A number $a \in \{1, 2, ..., n-1\}$ is a witness of the fact $n \notin$ PRIM for an odd positive integer n if

(i) GCD$(a, n) > 1$, or (6.9)

(ii)GCD$(a, n) = 1$ and $a^{\frac{n-1}{2}} \bmod n \notin \{1, n-1\}$

Unfortunately, (6.9) does not guarantee the abundance of witnesses for Carmichael numbers, and so we cannot use this kind of witness for the design of a randomized algorithm for primality testing for all odd, positive integers.

Quadratic Residue Modulo

Definition

An integer q is called a quadratic residue modulo $n(qRn)$ if it is congruent to a perfect square modulo n; i.e., if there exists an integer x such that:

$$x^2 \equiv q(\text{mod } n)$$

Legendre Symbol

Definition 6.3.10: Legendre Symbol

For any prime $p > 2$ and any positive integer a with $\text{GCD}(a, p) = 1$ the Legendre symbol for a and p is:

$$\text{Leg}\left[\frac{a}{p}\right] = \begin{cases} 1 & \text{if } a \text{ is a quadratic residue modulo } p (aRp), \\ -1 & \text{if } a \text{ is a quadratic nonresidue modulo } p (aNp). \end{cases}$$

Lemma 6.3.11

The following assertion is a direct consequence of the Euclidean Criterion (Theorem 5.4.14).

Lemma

For every prime $p > 2$ and every positive integer a with $\text{GCD}(a, p) = 1$

$$\text{Leg}\left[\frac{a}{p}\right] = a^{\frac{p-1}{2}} \bmod p$$

Jacobi Symbol

Definition 6.3.12: Jacobi Symbol

Let

$$n = p_1^{k_1}.p_2^{k_2}.....p_l^{k_l}$$

be the factorization of an odd integer $n \geq 3$, where $p_1 < p_2 < ... < p_l$ are primes and $k_1, k_2, ..., k_l$ are positive integers for a positive integer l.
For all positive integers a with GCD$(a, n) = 1$, the Jacobi symbol of a and n is

$$\text{Jac}\left[\frac{a}{n}\right] = \prod_{i=1}^{l}\left(\text{Leg}\left[\frac{a}{p_i}\right]\right)^{k_i} = \prod_{i=1}^{l}\left(\text{a}^{\frac{p_i-1}{2}} \bmod p_i\right)^{k_i}.$$

Observation

Observation 6.3.13

For all positive integers a and n satisfying the assumptions of Definition 6.3.10

$$\text{Jac}\left[\frac{a}{n}\right] \in \{1, -1\}.$$

Lemma 6.3.14

Let n be an odd integer greater than 3, and let a, b be natural numbers with $\text{GCD}(a, n) = \text{GCD}(b, n) = 1$. Then

1. $\text{Jac}\left[\frac{a.b}{n}\right] = \text{Jac}\left[\frac{a}{n}\right].\text{Jac}\left[\frac{b}{n}\right]$
2. $\text{Jac}\left[\frac{a}{n}\right] = \text{Jac}\left[\frac{b}{n}\right] \forall a, b$ with $a \equiv b(\text{ mod } n)$
3. $\text{Jac}\left[\frac{a}{n}\right] = (-1)^{\frac{a-1}{2}\cdot\frac{n-1}{2}}.\text{Jac}\left[\frac{n}{a}\right]$, for all odd a
4. $\text{Jac}\left[\frac{1}{n}\right] = 1$ and $\text{Jac}\left[\frac{n-1}{n}\right] = (-1)^{\frac{n-1}{n}}$
5. $\text{Jac}\left[\frac{2}{n}\right] = -1$ for all n with $n \bmod 8 \in \{3, 5\}$, and
   $\text{Jac}\left[\frac{2}{n}\right] = 1$ for all n with $n \bmod 8 \in \{1, 7\}$

Lemma 6.3.14 - Proof (i)

Let $n = p_1^{k_1}.p_2^{k_2}.....p_l^{k_l}$:

$$\begin{aligned}
\text{Jac}\left[\frac{a.b}{n}\right] &= \prod_{i=1}^{l}\left((a.b)^{\frac{p_i-1}{2}} \bmod p_i\right)^{k_i} \\
&= \prod_{i=1}^{l}\left(\left(a^{\frac{p_i-1}{2}} \bmod p_i\right).\left(b^{\frac{p_i-1}{2}} \bmod p_i\right)\right)^{k_i} \\
&= \prod_{i=1}^{l}\left(a^{\frac{p_i-1}{2}} \bmod p_i\right)^{k_i}.\prod_{i=1}^{l}\left(b^{\frac{p_i-1}{2}} \bmod p_i\right)^{k_i} \\
&= \text{Jac}\left[\frac{a}{n}\right].\text{Jac}\left[\frac{b}{n}\right]
\end{aligned}$$

This completes the proof of (i).

Lemma 6.3.14 - Proof (ii)

Following the definition of Jacobi symbols, it is sufficient to show

$$\text{Leg}\left[\frac{a}{p}\right] = \text{Leg}\left[\frac{b}{p}\right]$$

$\forall$ prime p and all a, b with $\text{GCD}(a, p) = \text{GCD}(b, p) = 1$ and $a \equiv b(\bmod p)$.
For appropriate $r, s, z \in \mathbb{N}, z < p$ we have:

$$a = p.r + z \text{ and } b = p.s + z \qquad (6.10)$$

Then

$$\text{Jac}\left[\frac{a}{p}\right] = a^{\frac{p-1}{2}} \bmod p = (p.r + z)^{\frac{p-1}{2}} \bmod p$$

$$= \sum_{i=0}^{(p-1)/2} \binom{(p-1)/2}{i} .(p.r)^{\frac{p-1}{2}-i}.z^i \bmod p$$

$$= z^{(p-1)/2} \bmod p \quad \{\text{All other members of the sum are divisible by } pr\}$$

Analogously: $\text{Jac}\left[\frac{b}{p}\right] = z^{(p-1)/2} \bmod p \Rightarrow \text{Leg}\left[\frac{a}{p}\right] = \text{Leg}\left[\frac{b}{p}\right]$

Algorithm JACOBI

Input: An odd integer $n \geq 3$, and a positive integer a with GCD $(a, n) = 1$.
Procedure: JACOBI$[a, n]$

```
begin
    if a = 1 then
        JACOBI[a, n] := 1;
    if a = 2 and n mod 8 ∈ {3, 5} then
        JACOBI[a, n] := −1;
    if a = 2 and n mod 8 ∈ {1, 7} then
        JACOBI[a, n] := 1;
    if a is odd then
        JACOBI[a, n] := JACOBI[2, n] · JACOBI[a/2, n];
    if a > n then
        JACOBI[a, n] := JACOBI[a mod n, n]
    else
        JACOBI[a, n] := (−1)^((a−1)/2 · (n−1)/2) · JACOBI[n mod a, a]
end
```

New Definition of Witnesses of Compositeness

Definition

An a with

$$\text{Jac}\left[\frac{a}{n}\right] \neq a^{(n-1)/2} \bmod n$$

witnesses the fact "$n \notin PRIM$"

Jac-witness

Definition 6.3.16

Let n be an odd integer, $n \geq 3$. A number $a \in \{1, 2, ..., n-1\}$ is called **Jac-witness** of that fact "$n \notin PRIM$" if

- $\text{GCD}(a, n) \neq 1$, or
- $\text{Jac}\left[\frac{a}{n}\right] \neq a^{(n-1)/2} \bmod n$

Algebra

Algebra

Algebra is a pair (S, F), where

- S is a set of elements.
- F is a set of mappings that map arguments or tuples of arguments from S to S. More precisely, F is a set of operations on S, and an operation $f \in F$ is a mapping from S^m to S for nonnegative integer m.

Group

A group G is a finite or infinite set of elements together with a binary operation that together satisfy the four fundamental properties of closure, associativity, the identity property, and the inverse property.

Group

A group G is a finite or infinite set of elements together with a binary operation that together satisfy the four fundamental properties of closure, associativity, the identity property, and the inverse property.

1. Closure: If A and B are two elements in G, then the product AB is also in G.
2. Associativity: The defined multiplication is associative, i.e., for all $A, B, C \in G$, $(AB)C = A(BC)$.
3. Identity: There is an identity element I such that $IA = AI = A$ for every element $A \in G$.
4. Inverse: There must be an inverse (a.k.a. reciprocal) of each element. Therefore, for each element A of G, the set contains an element $B = A^{-1}$ such that $AA^{-1} = A^{-1}A = I$.

Group

A group G is a finite or infinite set of elements together with a binary operation that together satisfy the four fundamental properties of closure, associativity, the identity property, and the inverse property.

1. Closure: If A and B are two elements in G, then the product AB is also in G.
2. Associativity: The defined multiplication is associative, i.e., for all $A, B, C \in G$, $(AB)C = A(BC)$.
3. Identity: There is an identity element I such that $IA = AI = A$ for every element $A \in G$.
4. Inverse: There must be an inverse (a.k.a. reciprocal) of each element. Therefore, for each element A of G, the set contains an element $B = A^{-1}$ such that $AA^{-1} = A^{-1}A = I$.

Group

A group G is a finite or infinite set of elements together with a binary operation that together satisfy the four fundamental properties of closure, associativity, the identity property, and the inverse property.

1. Closure: If A and B are two elements in G, then the product AB is also in G.
2. Associativity: The defined multiplication is associative, i.e., for all $A, B, C \in G$, $(AB)C = A(BC)$.
3. Identity: There is an identity element I such that $IA = AI = A$ for every element $A \in G$.
4. Inverse: There must be an inverse (a.k.a. reciprocal) of each element. Therefore, for each element A of G, the set contains an element $B = A^{-1}$ such that $AA^{-1} = A^{-1}A = I$.

Group

A group G is a finite or infinite set of elements together with a binary operation that together satisfy the four fundamental properties of closure, associativity, the identity property, and the inverse property.

1. Closure: If A and B are two elements in G, then the product AB is also in G.
2. Associativity: The defined multiplication is associative, i.e., for all $A, B, C \in G$, $(AB)C = A(BC)$.
3. Identity: There is an identity element I such that $IA = AI = A$ for every element $A \in G$.
4. Inverse: There must be an inverse (a.k.a. reciprocal) of each element. Therefore, for each element A of G, the set contains an element $B = A^{-1}$ such that $AA^{-1} = A^{-1}A = I$.

Subgroup

Definition

Let $(A, *)$ be a group. An algebra $(H, *)$ is a **subgroup** of $(A, *)$ if

- $H \subseteq A$, and
- $(H, *)$ is a group. For instance, $(\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Q}, +)$.

Right and Left Coset

Definition

Let $(H, \circ)$ be a subgroup of $(A, \circ)$. For every $b \in A$, we define the sets

$$H \circ b = \{h \circ b | h \in H\} \text{ and } b \circ H = \{b \circ h | h \in H\}$$

as **right coset** and **left coset** of H in $(A, \circ)$ respectively.

Index of H in $(A, \circ)$

Definition

Let $(H, \circ)$ be a subgroup of a group $(A, \circ)$. We define **index of H in** $(A, \circ)$ by

$$\text{Index}_H(A) = |\{H \circ b | b \in A\}|$$

i.e, as the number of different right cosets of H in $(A, \circ)$.

Index of H in $(A, \circ)$

Definition

Let $(H, \circ)$ be a subgroup of a group $(A, \circ)$. We define **index of H in** $(A, \circ)$ by

$$\text{Index}_H(A) = |\{H \circ b | b \in A\}|$$

i.e, as the number of different right cosets of H in $(A, \circ)$.

Lagrange's Theorem

Theorem

For every subgroup $(H, \circ)$ of a finite group $(A, \circ)$,

$$|A| = \text{Index}_H(A).|H|$$

i.e, $|H|$ divides $|A|$.

Corollary A.2.49

Go Back

Corollary

Let $(H, \circ)$ be a proper algebra if a finite group $(A, \circ)$. Then,

$$|H| \leq |A|/2$$

Cyclic Group

Definition

Let $(S, *)$ be a group with the neutral element e. For every $a \in S$ and every $j \in \mathbb{Z}$, we define the j-th power of a as follows:

- $a^0 = e, a^1 = a, a^{-1} = i(a)$,
- $\forall j \geq 1, a^{j+1} = a * a^j$
- $\forall j \in \mathbb{Z}^+, a^{-j} = (i(a))^j$

An element g of S is called a generator of the group $(S, *)$ if

$$S = \{g^i | i \in \mathbb{Z}\}$$

Order of a

Definition

Let $(A, *)$ be a group with neutral element 1. For each $a \in A$, the **order of** a is defined by

$$\text{order}(a) = \min\{r \in \mathbb{N} - \{0\} \mid a^r = 1\}$$

if there exists at least one r with $a^r = 1$.

if $\forall i \in \mathbb{N} - \{0\}, a^i \neq 1,$ then we set $\text{order}(a) = \infty$

Theorem 6.3.17

Go Back

Theorem

For every odd integer n, $n \geq 3$, the following holds:

(a)If n is a prime, then

$$\text{Jac}\left[\frac{a}{n}\right] = \text{Leg}\left[\frac{a}{n}\right] = a^{\frac{n-1}{2}} \bmod n \quad \forall a \in \{1, 2, ..., n-1\}$$

(b)If n is composite, then

$$\text{Jac}\left[\frac{a}{n}\right] \neq a^{\frac{n-1}{2}} \bmod n$$

for at least half the elements $a \in \{1, 2, ..., n-1\}$ with the property $\text{GCD}(a, n) = 1$ (i.e, $a \in \mathbb{Z}_n^*$)

Remember: $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n - \{0\} | \text{GCD}(a, n) = 1\}$

Theorem 6.3.17 - Proof (a)

The claim (a) is a direct consequence of the definition of Jacobi symbols and the Eulerian Criterion.

Theorem 6.3.17 - Proof (b) ...

witness candidates $= \{1, 2, ..., n-1\} = \mathbb{Z}_n - \{0\}$

Jac-witness of $n \notin$PRIM according to definition 6.3.16(i) are all elements from $\{1, 2, ..., n-1\} - \mathbb{Z}_n^*$.

We denote the non-Jac-witness by:

$$\overline{Wit}_n = \{a \in \mathbb{Z}_n^* | \text{ Jac}\left[\frac{a}{n}\right] = a^{\frac{n-1}{2}} \bmod n\},$$

then

$$\mathbb{Z}_n^* - \overline{Wit}_n$$

is the set of Jac-witness of $n \notin$PRIM with respect to definition 6.3.16 (ii).

Theorem 6.3.17 - Proof (b) ...

Our aim is to show that

$$|\overline{Wit}_n| \leq |\mathbb{Z}_n^*|/2, \qquad (6.11)$$

so that

$$|\{1, 2, ..., n-1\} - \overline{Wit}_n| \geq |\overline{Wit}_n|$$

We need to show that

$$(\overline{Wit}_n, \odot_{\text{mod } n}) \text{ is a proper subgroup of } (\mathbb{Z}_n^*, \odot \text{ mod } n)$$

i.e, we need to look for an element $a \in \mathbb{Z}_n^* - \overline{Wit}_n$.

Theorem 6.3.17 - Proof (b) ...

Theorem A.2.40

Let $(A, \odot)$ be a finite group. Every algebra $(H, \odot)$ with $H \subseteq A$ is a subgroup of $(A, \odot)$

Theorem 6.3.17 - Proof (b) ...

First we show that $(\overline{Wit}_n, \odot \bmod n)$ is a group.

Following Corollary A.2.49 it is sufficient to show that $\overline{Wit}_n$ is closed according to $\odot \bmod n$:

Let $a, b \in \overline{Wit}_n$, From Lemma 6.3.14 (i),

$$\begin{aligned} \text{Jac}\left[\frac{a.b}{n}\right] &= \text{Jac}\left[\frac{a}{n}\right].\text{Jac}\left[\frac{b}{n}\right] \\ &= \left(a^{\frac{n-1}{2}} \bmod n\right).\left(b^{\frac{n-1}{2}} \bmod n\right) \qquad \{\text{Since } a, b \in \overline{Wit}_n\} \\ &= (a.b)^{\frac{n-1}{2}} \bmod n \end{aligned}$$

So $a.b \in \overline{Wit}_n$ therefore $\overline{Wit}_n$ is closed according to $\odot \bmod n$.

Theorem 6.3.17 - Proof (b) ...

Now we show that $\overline{Wit}_n$ is a proper subset of $\mathbb{Z}_n^*$, $(a \in \mathbb{Z}_n^* - \overline{Wit}_n)$. Let

$$n = p_1^{i_1}.p_2^{i_2}.\ldots.p_k^{i_k}$$

then we set

$$q = p_1^{i_1} \text{ and } m = p_2^{i_2}.\ldots.p_k^{i_k}$$

in order to search for an $a \in \mathbb{Z}_n^* - \overline{Wit}_n$ in $\mathbb{Z}_q \times \mathbb{Z}_m$ instead of searching directly in $\mathbb{Z}_n$.
Let g be the generator of the cyclic group $(\mathbb{Z}_q^*, \odot \bmod q)$. We make the choice of a by the following recurrences:

$$a \equiv g(\text{mod } q) \text{ and } a \equiv 1(\text{mod } m)$$

Hence we choose a as $(g, 1)$ in $\mathbb{Z}_q \times \mathbb{Z}_m$

Theorem 6.3.17 - Proof (b) ...

First, we show that $a \in \mathbb{Z}_n^*$, (i.e, GCD$(a, n) = 1$). So we have to show

$$\textit{none of the primes } p_1, p_2, ..., p_k \text{ divides the number } a. \qquad (6.13)$$

The proof is by contradiction. If $p_1 \mid a$, then the equality $g = a \bmod p_1^{i_1}$ contradicts the assumption that g is a generator of $\mathbb{Z}_q^*$, So $p_1 \nmid a$.

Hint: The equality $g = a \bmod p_1^{i_1}$ follows from $a \equiv g (\text{mod } q)$

Theorem 6.3.17 - Proof (b) ...

If, for an $r \in \{2, ..., k\}, p_r \mid a$, then $a = p_r.b, b \in \mathbb{N}$. From $a \equiv 1(\text{ mod } m)$ we have:

$$a = m.x + 1, x \in \mathbb{N}$$

Hence

$$a = p_r.b = m.x + 1 = p_r.(m/p_r).x + 1$$

which implies $p_r \mid 1$, Since $p_r > 1$ so it is a contradiction. Thus $a \in \mathbb{Z}_n^*$.

Hint: if $p \mid x, p \mid y$ and $x = y + z$ then $p \mid z$

Proof:

$$x = p.k, y = p.k^{'}, x = y + z$$

then

$$p.k = p.k^{'} + z \Rightarrow z = p(k - k^{'}) \Rightarrow p \mid z$$

Theorem 6.3.17 - Proof (b) ...

Finally, we have to prove that

$$a \notin \overline{Wit}_n$$

To do so, we distinguish two possibilities: $i_1 = 1$ and $i_1 \geq 2$.

Theorem 6.3.17 - Proof (b) ...

(1) let $i_1 = 1$

We have to prove $\text{Jac}\left[\frac{a}{n}\right] \neq a^{\frac{n-1}{2}} \bmod n$. Remember that

$n = p_1.m, m > 1$ and $\text{GCD}(p_1, m) = 1$(Since if $p \nmid a$ then $\forall b \in \mathbb{N}, p \nmid a^b$)

$$\text{Jac}\left[\frac{a}{n}\right] = \prod_{j=1}^{k} \left(\text{Jac}\left[\frac{a}{p_i}\right]\right)^{i_j}$$

$$= \text{Jac}\left[\frac{a}{p_1}\right] . \prod_{j=2}^{k} \left(\text{Jac}\left[\frac{a}{p_j}\right]\right)^{i_j}$$

$$= \text{Jac}\left[\frac{a}{p_1}\right] . \prod_{j=2}^{k} \left(\text{Jac}\left[\frac{1}{p_j}\right]\right)^{i_j} = \text{Jac}\left[\frac{a}{p_1}\right] = \text{Jac}\left[\frac{g}{p_1}\right] = \text{Leg}\left[\frac{g}{p_1}\right] = -1$$

Hence $\text{Jac}\left[\frac{a}{n}\right] = -1$

Theorem 6.3.17 - Proof (b) ...

Since $a \equiv 1(\bmod m)$, we obtain

$$\begin{aligned} a^{\frac{n-1}{2}} \bmod m &= (a \bmod m)^{\frac{n-1}{2}} \bmod m \\ &= 1^{\frac{n-1}{n}} \bmod m \\ &= 1 \qquad (6.14) \end{aligned}$$

Now, the equality $a^{\frac{n-1}{2}} \bmod n = -1$ for $n = q.m$ cannot hold because $a^{\frac{n-1}{2}} \bmod n = -1$ implies:

$$a^{\frac{n-1}{2}} \bmod m = -1 (= m - 1 \text{ in } \mathbb{Z}_m^*)$$

which contradicts (6.14). Hence:

$$-1 = \text{Jac}\left[\frac{a}{n}\right] \neq a^{\frac{n-1}{2}} \bmod n \Rightarrow a \in \mathbb{Z}_n^* - \overline{Wit}_n$$

Theorem 6.3.17 - Proof (b) ...

(2) Let $i_1 \geq 2$.
We prove $a \notin \overline{Wit}_n$ in an indirect way.

$$a \in \overline{Wit}_n \Rightarrow a^{\frac{n-1}{2}} \bmod n = \text{Jac}\left[\frac{a}{n}\right] \in \{1, -1\}$$

and so

$$a^{n-1} \bmod n = 1$$

Since $n = q.m$, we also have

$$a^{n-1} \bmod q = 1$$

Since $g = a \bmod q$ we obtain

$$1 = a^{n-1} \bmod q = (a \bmod q)^{n-1} \bmod q = g^{n-1} \bmod q. \quad (6.15)$$

Theorem 6.3.17 - Proof (b) ...

g is a generator of cyclic group $(\mathbb{Z}_q^*, \odot \bmod q)$, so the order of g is $|\mathbb{Z}_q^*|$. From (6.15) we have that:

$$|\mathbb{Z}_q^*| \text{ divides } n-1 \qquad (6.16)$$

since $q = p_1^{i_1}$ for an $i_1 \geq 2$, and

$$\mathbb{Z}_q^* = \{x \in \mathbb{Z}_q | \text{GCD}(x,1) = 1\} = \{x \in \mathbb{Z}_q | p1 \nmid x\}$$

and the number of elements of $\mathbb{Z}_q$ that are a multiple of p_1 is exactly $|\mathbb{Z}_q|/p_1$, one obtains

$$|\mathbb{Z}_q^*| = |\mathbb{Z}_q| - |\mathbb{Z}_q|/p_1 = p_1^{i_1} - p_1^{i_1-1} = p_1.(p_1^{i_1-1} - p_1^{i_1-2})$$

Hence

$$p_1 \text{ divides } |\mathbb{Z}_q^*| \qquad (6.17)$$

Theorem 6.3.17 - Proof (b)

From (6.16) and (6.17) together imply that

$$p_1 \text{ divides } n-1 \qquad (6.18)$$

Since $n = p_1^{i_1}$, we have obtained

$$p_1 \text{ divides } n \text{ and } p_1 \text{ divides } n-1$$

Since $\nexists$ prime p, such that $p \mid n$ and $p \mid n-1$, out assumption $a \in \overline{Wit}_n$ cannot hold, and we obtain

$$a \notin \overline{Wit}_n \blacksquare$$

Algorithm Solovay-Strassen

Algorithm Solovay-Strassen

Input: An odd integer n, $n \geq 3$.
Step 1: Choose uniformly an a from $\{1, 2, \ldots, n-1\}$ at random.
Step 2: Compute GCD (a, n).
Step 3:

```
if GCD (a, n) ≠ 1 then
    output ("n ∉ PRIM") {accept}
```

Step 4: Compute Jac $\left[\frac{a}{n}\right]$ and $a^{\frac{(n-1)}{2}} \bmod n$
Step 5:

```
if Jac [a/n] = a^((n-1)/2) mod n then
    output ("n ∈ PRIM") {reject}
else
    output ("n ∉ PRIM") {accept}.
```

Theorem 6.3.18

Theorem

The Solovay-Strassen algorithm is a polynomial-time one-sided-error Monte Carlo algorithm for the recognition of composite numbers.

Theorem 6.3.18 - Proof ...

Algorithm Solovay-Strassen

Input: An odd integer n, $n \geq 3$.
Step 1: Choose uniformly an a from $\{1, 2, \ldots, n-1\}$ at random.
Step 2: Compute GCD (a, n).
Step 3:

```
if GCD (a, n) ≠ 1 then
    output ("n ∉ PRIM") {accept}
```

$O((\log_2 n)^3)$

Step 4: Compute Jac $\left[\frac{a}{n}\right]$ and $a^{\frac{(n-1)}{2}} \bmod n$

$O((\log_2 n)^3)$

Step 5:

```
if Jac [a/n] = a^((n-1)/2) mod n then
    output ("n ∈ PRIM") {reject}
else
    output ("n ∉ PRIM") {accept}.
```

$O(\log_2 n)$ for comparison

Theorem 6.3.18 - Proof

If $n \in$ PRIM, then by Theorem 6.3.17 (a), the algorithm outputs the answer "$n \in$ PRIM" with certainly.

If n is composite, Theorem 6.3.17 (b) assures that at least half the elements of $\{1, 2, ..., n-1\}$ are Jac-witnesses of "$n \notin$ PRIM". Therefore, the Solovay-Strassen algorithm gives the right answer "$n \notin$ PRIM" with probability at least $1/2$.■

Objectives

Problem

For a given positive integer l, generate a random prime of the binary length l.

Objectives

Problem

For a given positive integer l, generate a random prime of the binary length l.

Objectives

Problem

For a given positive integer l, generate a random prime of the binary length l.

The number of primes of the length l of order hundreds, is larger that the number of protons in the known universe. Clearly, one cannot solve this task by generating all primes of length l and than choosing one of them at random.

Theorem A.2.9. Prime Number Theorem

Go Back

Prime Number Theorem

$$\lim_{n\to\infty} \frac{\text{PRIM}(n)}{n/\ln n} = 1$$

In other words, the Prime Number Theorem says that the density

$$(\text{PRIM}(n))/n$$

of the primes among the first n positive integers tends to

$$1/\ln n$$

as n increases.

The Strategy

Strategy

The strategy used simply generates a random integer of length l and then applies a randomized primality test in order to check whether or not the generated number is a prime.

The Strategy

Strategy

The strategy used simply generates a random integer of length l and then applies a randomized primality test in order to check whether or not the generated number is a prime.

The Strategy

Strategy

The strategy used simply generates a random integer of length l and then applies a randomized primality test in order to check whether or not the generated number is a prime.

This approach works due to the Primality Theorem (Theorem A.2.9), that assures an abundance of primes among natural numbers.

For a randomly chosen number n, the probability that n is a prime is approximately $1/\ln n$.

PRIMEGEN (l, k)

Input: Positive integers l and k, $l \geq 3$.

Step 1:

$X :=$ "still not found";

$I := 0$;

Step 2:

`while` $X :=$ "still not found" and $I < 2 \cdot l^2$ `do`

`begin`

generate a bit sequence $a_1, a_2, \ldots, a_{l-2}$ at random and compute

$$n := 2^{l-1} + \sum_{i=1}^{l-2} a_i \cdot 2^i + 1$$

{Hence, n is a random integer of length l}

Perform k independent runs of the Solovay-Strassen algorithm on n;

`if` at least one output is "$n \notin$ PRIM" `then`

$I := I + 1$

`else`

`begin`

$X :=$ already found;

`output` "n"

`end`;

`end`;

Step 3:

`if` $I = 2 \cdot l^2$ `then`

`output` "I was unable to find a prime."

Theorem 6.4.19

Theorem

The algorithm PRIMEGEN(l, l) is a bounded-error algorithm for generating primes that works in time polynomial in l.

PRIMEGEN (l, k)

For k= l, PRIMGEN(l, l)

Input: Positive integers l and k, $l \geq 3$.

Step 1:

$X :=$ "still not found";

$I := 0$;

Step 2:

O(l^2)

`while` $X :=$ "still not found" and $I < 2 \cdot l^2$ `do`

`begin`

generate a bit sequence $a_1, a_2, \ldots, a_{l-2}$ at random and compute

$$n := 2^{l-1} + \sum_{i=1}^{l-2} a_i \cdot 2^i + 1$$

O(l)

{Hence, n is a random integer of length l}

Perform k independent runs of the Solovay-Strassen algorithm on n;

O(l^3)

`if` at least one output is "$n \notin$ PRIM" `then`

$I := I + 1$

`else`

`begin`

$X :=$ already found;

`output` "n"

`end`;

`end`;

Step 3:

`if` $I = 2 \cdot l^2$ `then`

`output` "I was unable to find a prime."

Theorem 6.4.19 - Proof ...

Unwanted events include:

1. If none of the $2.l^2$ randomly generated numbers is a prime, and for every one of these generated numbers, the Solovay-Strassen primality test proves in l runs that the given number is composite.
2. PRIMEGEN(l, l) outputs a composite number n as a prime (the probability of a wrong output, error probability).

Theorem 6.4.19 - Proof ...

Unwanted events include:

1. If none of the $2.l^2$ randomly generated numbers is a prime, and for every one of these generated numbers, the Solovay-Strassen primality test proves in l runs that the given number is composite.
2. PRIMEGEN(l, l) outputs a composite number n as a prime (the probability of a wrong output, error probability).

Theorem 6.4.19 - Proof ...

Unwanted Event 1:
By Theorem A.2.9 since the probability, that a random number of length l is a prime, is at least

$$\frac{1}{\ln n} > \frac{1}{2.l}$$

the probability of generating no prime in one attempt is at most

$$1 - \frac{1}{2.l}. \qquad (6.19)$$

Let

$$w_l \geq 1 - \frac{1}{2^l}$$

be the probability, that l runs of the Solovay-Strassen primality test succeed in proving "$n \notin$ PRIM" for a given, composite n of length l.

Theorem 6.4.19 - Proof ...

Hence we obtain

$$\begin{aligned}\text{Prob}(\text{PRIMGEN}(l,l) = \text{"I was unable to find a prime"}) &< \left(\left(1-\frac{1}{2.l}\right).w_l\right)^{2.l^2} \\ &< \left(1-\frac{1}{2.l}\right)^{2.l^2} \\ &= \left[\left(1-\frac{1}{2.l}\right)^{2.l}\right]^l \\ &< \left(\frac{1}{e}\right)^l = e^{-l}\end{aligned}$$

e^{-l} tends to 0 with growing l. For $l \geq 2, e^{-l} < \frac{1}{4}$ and for $l \geq 100, e^{-l} < 10^{-40}$

Theorem 6.4.19 - Proof ...

Unwanted Event 2:
The algorithm PRIMEGEN(l, l) produces a composite number n only if

(i) all numbers generated before n were composite, and
(ii) n is composite, but PRIMEGEN(l, l) does not succeed in proving n's compositeness in l runs of the Solovay-Strassen algorithm.

Let p_i be the probability that the wrong answer n is the i-th generated number, for $i \in \{1, 2, ..., 2.l^2\}$.

The (6.19) implies

$$p_1 \leq \left(1 - \frac{1}{2.l}\right).\frac{1}{2^l}$$

Theorem 6.4.19 - Proof ...

For all $i = 2, 3, ..., 2.l^2$,

$$p_i \leq \left[\left(1 - \frac{1}{2.l}\right).w_l\right]^{i-1}.\left(1 - \frac{1}{2.l}\right).\frac{1}{2^l}$$

where $\left[\left(1 - \frac{1}{2.l}\right).w_l\right]^{i-1}$ is an upper bound on the probability that the first $i1$ generated numbers are composite and that this fact was successfully recognized.

Theorem 6.4.19 - Proof ...

Thus we obtain

$$\begin{aligned}
\text{Error}_{\text{PRIMEGEN}(l,l)}(l) &\leq p_1 + \sum_{j=2}^{2.l^2} p_j \\
&\leq \left(1 - \frac{1}{2.l}\right).\frac{1}{2^l} \\
&+ \sum_{i=1}^{2.l^2-1} \left[\left(1 - \frac{1}{2.l}\right).w_l\right]^i.\left(1 - \frac{1}{2.l}\right).\frac{1}{2^l} \\
&\leq \left(1 - \frac{1}{2.l}\right).\frac{1}{2^l}.\left(\sum_{i=1}^{2.l^2-1}\left(1 - \frac{1}{2.l}\right)^i + 1\right) \\
&\leq \left(1 - \frac{1}{2.l}\right).\frac{1}{2^l}.2.l^2 \\
&\leq \frac{l^2}{2^{l-1}}
\end{aligned}$$

Theorem 6.4.19 - Proof

Clearly the value $l^2.2^{-(l-1)}$ tends to 0 with growing l, and
$\text{Error}_{\text{PRIMEGEN}(5,5)}(5) \leq \frac{1}{5}$.
For $l \geq 100$,

$$\text{Error}_{\text{PRIMEGEN}(l,l)}(l) \leq l^2.2^{-(l-1)} \leq 1.58.10^{-26}\blacksquare$$

In order to increase the success probability of PRIMEGEN(l, k), we have probably chosen a too large k, that essentially increases the time complexity.