Elementary Number Theory for Public Key Cryptography

Rana Barua

IAI, TCG CREST, Kolkata

1 Modular Arithmetic, Elementary Properties

Let $\mathbb{Z}$ denote the set of all integers and $\mathbb{N}$ the set of natural numbers. For $a, b \in \mathbb{Z}$ we write $a|b$ if a divides b.
We now state a result that is fundamental and useful and is known as the *Division Algorithm*.

Lemma 1. *Let a be an integer and b a positive integer. Then there exist unique integers q, r such that $0 \leq r < b$ and*

$$a = qb + r.$$

Proof. First assume that $a \geq 0$. If $a = 0$, then set $q = 0$ and $r = 0$. So assume that $a > 0$. If $a < b$ then set $q = 0$ and $r = a$. So assume $a > b$. Now the set of positive integers i such that $ib \leq a$ is non-empty and finite. Let q be the largest such integer. Set $r = a - qb$. By our choice of q, $0 \leq r < q$. The case when $a < 0$ is left as an exercise. The uniqueness is not hard to see. □

Remark 1. q is called the **quotient** and r the **remainder**. We denote r by $a \bmod b$.

Definition 1. *Let n be a fixed positive integer. For two integers $a, b \in \mathbb{Z}$, we say that a is congruent to b modulo n, and we write*

$$a \equiv b \bmod n$$

if $n|(a - b)$.

Exercise 1. Show that $\equiv$ is an equivalence relation on $\mathbb{Z}$.
Consequently, The equivalence classes $[0], [1], [2], \ldots, [n-1]$ form a partition of $\mathbb{Z}$.

Exercise 2. Suppose $a \equiv b \bmod n$ and $c \equiv d \bmod n$. Then show that $(a + c) \equiv (b + d) \bmod n$, $(a - c) \equiv (b - d) \bmod n$ and $ac \equiv bd \bmod n$.

Exercise 3. Let $p(x) \in \mathbb{Z}[x]$ be a polynomial with integer coefficients. Show that if $a \equiv b \bmod n$, then $p(a) \equiv p(b) \bmod n$.
Hence show that an m digit number is divisible by 3 iff the sum of the digits is divisible by 3.
Obtain a similar result for 11.

We know that when an integer $a \in \mathbb{Z}$ is divided by n it leaves a remainder r where $0 \leq r \leq n-1$. Let $\mathbb{Z}_n$ denote the set of these remainders i.e. $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$. Clearly, for any integer $a \in \mathbb{Z}$, there exists a unique integer $r \in \mathbb{Z}_n$ such that $a \equiv r \bmod n$ and $a \equiv b \bmod n$ iff their remainders are the same on dividing by n.

On $\mathbb{Z}_n$ we shall define two binary operations $+$ and $\times$ or . as follows.
For $a, b \in \mathbb{Z}_n$ let $c \in \mathbb{Z}_n$ be the unique integer such that $a + b \equiv c \bmod n$. Then we define

$$a + b = c$$

in $\mathbb{Z}_n$.
Similarly, let $d \in \mathbb{Z}_n$ be the unique integer such that $ab \equiv d \bmod n$. Then in $\mathbb{Z}_n$ we define

$$a.b = d.$$

Clearly, in $\mathbb{Z}_n$, $a + b = c$ iff $a + b \equiv c \bmod n$ and $a.b = d$ iff $ab \equiv d \bmod n$.

Exercise 4. Write down the addition and multiplication tables for $\mathbb{Z}_7$ and $\mathbb{Z}_8$.

Exercise 5. Show that $\mathbb{Z}_n$ with the binary operations $+$ and $\times$ defined above forms a commutative *ring* with *identity* 1.

1.1 Euclidean Algorithm

We now define

Definition 2. *Let $a, b \in \mathbb{Z}$. The greatest common divisor of a and b, denoted by $GCD(a, b)$, is the largest of all common divisors of a and b. In other words, $GCD(a, b) = d$ if $d|a$ and $d|b$, and if $c|a$ and $c|b$, then $c|d$. We define $GCD(0, 0) = 0$.*

We now present one of the most celebrated algorithms in Number Theory called the *Euclidean Algorithm*. It computes the GCD of two integers a, b.

Since $GCD(a, b) = GCD(|a|, |b|)$, we assume without loss of generality that a and b are non-negative. If one of them, say a is 0, then $GCD(a, b) = b$. So assume both a and b are positive. Without loss of generality assume that $a > b$. Let $GCD(a, b) = d$ and set $r_0 = a$ and $r_1 = b$. By the **division algorithm** we have for some integers q_1 (*quotient*), r_2 (*remainder*) ,

$$r_0 = q_1 r_1 + r_2 \text{ with } 0 \leq \mathrm{r}_2 < \mathrm{r}_1.$$

Repeating this process until the remainder becomes 0, we have

$$r_1 = q_2 r_2 + r_3 \text{ with } 0 \leq \mathrm{r}_3 < \mathrm{r}_2;$$

$$r_2 = q_3 r_3 + r_4 \text{ with } 0 \leq \mathrm{r}_4 < \mathrm{r}_3;$$

$$\vdots$$

$$r_{n-1} = q_n r_n.$$

Claim: For all $i, 0 \leq i < n$,

$$d = GCD(r_i, r_{i+1}).$$

First note that $d = GCD(a, b) = GCD(r_0, r_1)$. Let $d' = GCD(r_1, r_2)$. Since $d'|r_1$ and $d'|r_2$, from the first equation it follows that $d'|r_0$. Hence, $d'|GCD(r_0, r_1)$ i.e. $d'|d$. On the other hand, from the first equation, it follows that $d|r_2$. Since $d|r_1$ also we have $d|GCD(r_1, r_2)$ i.e. $d|d'$. Thus $d = d'$.

Proceeding as above, one can show(*exercise*) by induction on $i, 0 \leq i < n$ that $d = GCD(r_i, r_{i+1})$. Thus we have $d = GCD(r_{n-1}, r_n) = r_n$.
This yields the following algorithm of Euclid. The inputs a and b are arbitrary non-negative integers.

EUCLID(a, b)

1. **If** $b := 0$
2. **then return** a
3. **else return** EUCLID$(b, a \bmod b)$

Correctness and Complexity
The correctness follows from the arguments above. For the complexity, one can prove by induction on k the following.
• Suppose $a > b \geq 1$ and EUCLID(a, b) preforms k recursive calls. Then $a \geq F_{k+2}$ and $b \geq F_{k+1}$, where F_k is the kth Fibonacci number.

Recall thta the kth Fibonacci number $F_k = \frac{1}{\sqrt{5}}\left((\frac{1+\sqrt{5}}{2})^k - (\frac{1-\sqrt{5}}{2})^k\right)$.

We may improve the complexity by observing the following.

Lemma 2. *Suppose $a > b \geq 1$. Then there exist integers q, r such that $0 \leq |r| \leq b/2$ satisfying $a = bq + r$.*

Proof. By the division algorithm we have for some integers q, r

$$a = qb + r.$$

If $r \leq b/2$ then we are done. So asume that $r > b/2$. Then $b - r < b/2$ and
$a = bq + r = b(q + 1) - (b - r)$. Let $r' = -(b - r)$ and $q' = q + 1$. Then $a = bq' + r'$, where $|r'| = (q - r) < b/2$. □

Next we observe that

Theorem 1. *Let $a, b \in \mathbb{Z}$. Suppose $GCD(a, b) = d$. Then there exist integers $\lambda, \mu \in \mathbb{Z}$ such that*

$$a\lambda + b\mu = d. \tag{1}$$

Proof. Without loss of generality, assume that a, b are non-negative integers. Arguing as above we have for some integers $r_i, 0 \leq r_i < r_{i+1}$,

$$r_0 = q_1 r_1 + r_2 \ \text{ with } \ 0 \leq \mathrm{r}_2 < \mathrm{r}_1.$$

$$r_1 = q_2 r_2 + r_3 \ \text{ with } \ 0 \leq \mathrm{r}_3 < \mathrm{r}_2;$$

$$r_2 = q_3 r_3 + r_4 \ \text{ with } \ 0 \leq \mathrm{r}_4 < \mathrm{r}_3;$$

$$\vdots$$

$$r_{n-1} = q_n r_n,$$

where $r_0 = a, r_1 = b$ and $r_n = GCD(a, b)$.
Now we have the following

Claim: For every $i, 0 \leq i \leq n, r_i$ is a linear combination of a and b. In other words, for each i there exist integers $\lambda_i, \mu_i \in \mathbb{Z}$ such that

$$r_i = a\lambda_i + b\mu_i.$$

Clearly true for $i = 0, 1$. So assume that the claim holds for integers $\leq i$. We shall show that it holds for $i + 1$. . Now from the ith equation we have

$$r_{i-1} = r_i q_i + r_{i+1}.$$

Hence we have
r_{i+1}
$= -q_i r_i + r_{i-1}$
$= -q_i(a\lambda_i + b\mu_i) + (a\lambda_{i-1} + b\mu_{i-1})$, by induction hypothesis
$= a(\lambda_{i-1} - \lambda_i q_i) + b(\mu_{i-1} - \mu_i q_i)$.
Set $\lambda_{i+1} = \lambda_{i-1} - \lambda_i q_i$ and $\mu_{i+1} = \mu_{i-1} - \mu_i q_i$ and we are done. Thus we have $d = r_n = a\lambda_n + b\mu_n$. This completes the proof. □

Remark 2. The above proof shows that $\{\lambda_i\}$ and $\{\mu_i\}$ can be defined recursively.
Set $\lambda_0 = 1, \mu_0 = 0$ and $\lambda_1 = 0, \mu_1 = 1$. Define

$$\lambda_{i+1} = \lambda_{i-1} - \lambda_i q_i,$$

$$\mu_{i+1} = \mu_{i-1} - \mu_i q_i$$

We now obtain the **Extended Euclidean Algorithm** that expresses the GCD of a, b as a linear combination.

EXTENDED-EUCLID(a, b)

Input: A pair of non-negative integers.
Output: A triplet of the form (d, λ, μ) such that $d = GCD(a, b) = a\lambda + b\mu$.

```
If b := 0
then return (a, 1, 0)
else  (d', λ', μ') = EXTENDED-EUCLID(b, a mod b)
      (d, λ, μ) = (d', μ', λ' − ⌊a/b⌋μ')
      return (d, λ, μ)
```

Correctness and Complexity
If $b = 0$ then we have $GCD(a, b) = a = 1.a + 0.b$ and the algorithm correctly returns $(a, 1, 0)$. So assume $b \neq 0$. The algorithm returns (d', λ', μ') such that, by induction hypothesis,
$d' = GCD(b, a \bmod b)$ and

$$d' = b\lambda' + (a \bmod b)\mu' \tag{2}$$

Since $GCD(a, b) = GCD(b, a \bmod b)$ we have $d = d'$. Hence, by (2), we have
$d = d' = b\lambda' + (a \bmod b)\mu'$
$= b\lambda' + (a - \lfloor a/b \rfloor b)\mu'$
$= a\mu' + (\lambda' - \lfloor a/b \rfloor \mu')b = a\lambda + b\mu$.
Since the number of recursive calls in EXTENDED-EUCLID is the same as in EUCLID, the procedure makes $O(\log n)$ recursive calls.

As an immediate corollary to Theorem 1 we have

Corollary 1. *Let $a, n \in \mathbb{Z}$ such that $GCD(a, n) = 1$. Then there exists an integer $b \in \mathbb{Z}$ such that*

$$ab \equiv 1 \bmod n. \tag{3}$$

In other words, for every integer a co-prime to n, there is an integer b such that $ab \equiv 1 \bmod n$.

Proof. By Theorem 1 we have integers λ and μ such that

$$a\lambda + n\mu = 1.$$

This clearly implies that $a\lambda \equiv 1 \bmod n$. Set $b = \lambda$ and we are done.

Remark 3. The integer b is called a *multiplicative inverse of a modulo n.*

The following important result is an immediate consequence

Theorem 2. *Let p be a prime number. Then $\mathbb{Z}_p$ with $+$ and $\times$ defined above is a field.*
In fact, $\mathbb{Z}_n$ is a field iff n is prime.

Proof. It is enough to show that $\mathbb{Z}_p^* = \mathbb{Z}_p - \{0\}$ is a commutative group with respect to $\times$ i.e. multiplication modulo n. The only non-trivial axiom is to show that every element of of $\mathbb{Z}_p^*$ has an inverse. So fix $a \in \mathbb{Z}_p^*$. Since $GCD(a, p) = 1$ by Corollary 1, there is an integer $b \in \mathbb{Z}$ such that $ab \equiv 1 \bmod p$. Clearly $b \not\equiv 0 \bmod p$. Let $b' \in \mathbb{Z}_p^*$ be the unique integer such that $b \equiv b' \bmod p$. Then $ab' \equiv ab \equiv 1 \bmod p$. By definition, $b' \in \mathbb{Z}_p^*$ is the inverse of a in $(\mathbb{Z}_p^*, \times)$. $\square$.
As a nice application we have **Wilson's Theorem.**

Theorem 3. *Let n be a positive integer. Then n is prime iff n divides $(n-1)!+1$.*

Proof. . Suppose n is prime. Then $\mathbb{Z}_n^* = \{1, 2, \ldots, n-1\}$ is a multiplicative group. The product of all the elements in $\mathbb{Z}_n^*$ is $(n-1)!$. We now show that, *in* $\mathbb{Z}_n^*$, the product of all the elements is -1 i.e. the element $(n-1) \in \mathbb{Z}_n^*$.

First note that the equation $X^2 = 1$ has two solutions in $\mathbb{Z}_n^*$ *viz* $+1$ and -1 (Why?) Thus in the multiplicative group $\mathbb{Z}_n^*$, the only elements which are inverse of itself are $+1$ and -1. Hence in the product $(n-1)!$, each element $a \neq \pm 1$ cancels out with its inverse. This means that the product

$$2.3.4.\ldots.(n-2) \equiv 1 \bmod n.$$

Consequently

$$1.2.3.4.\ldots.(n-2).(n-1) \equiv 1.1.(-1) \equiv -1 \bmod n.$$

Hence n divides $(n-1)!+1$. The converse is easy and is left as an exercise. □

1.2 The Chinese Remainder Theorem

We now state a result that is useful not only in Number Theory but also in Cryptography. It is known as the **Chinese Remainder Theorem (CRT)**.

Theorem 4. *Let $n_1, n_2, \ldots, n_k$ be positive integers that are pairwise relatively co-prime. Set $N = n_1 \ldots n_k$. Then the following system of congruence relations*

$$X \equiv a_1 \bmod n_1,$$

$$X \equiv a_2 \bmod n_2.$$

$$\vdots$$

$$X \equiv a_k \bmod n_k$$

has a unique solution modulo N for the unknown X.

.

Proof. Uniqueness. Let Y be another solution. Then $X \equiv Y \bmod n_i$, for $i = 1, \ldots, k$. Hence $n_i | (X-Y)$ for $i = 1, \ldots, k$. Since n_i's are pairwise co-prime, this implies that $N|(X-Y)$ and so $X \equiv Y \bmod N$.
Existence. We shall prove it for $k = 2$. The general solution is left as an exercise. Since $GCD(n_1, n_2) = 1$ by Corollary 1, there exists an integer $\bar{n}_1 \in \mathbb{Z}$ such that $n_1\bar{n}_1 \equiv 1 \bmod n_2$. Similarly, there exists an integer $\bar{n}_2 \in \mathbb{Z}$ such that $n_2\bar{n}_2 \equiv 1 \bmod n_1$. Now consider the integer $X = a_1n_2\bar{n}_2 + a_2n_1\bar{n}_1$. Then $X \equiv a_1n_2\bar{n}_2 \equiv a_1.1 \equiv a_1 \bmod n_1$. Also $X \equiv a_2n_1\bar{n}_1 \equiv a_2 \bmod n_2$. Thus X is a solution. □

Exercise 6. Prove the Chinese Remainder Theorem in its most general form.
(Hints: Set $m_i = \frac{N}{n_i}$ and find integers $\bar{m}_i$ such that $m_i\bar{m}_i \equiv 1 \bmod n_i$.)

Exercise 7. Find all solutions of the following

$$x \equiv 4 \bmod 5,$$

$$x \equiv 5 \bmod 11.$$

We now introduce a very important function known as Euler's **phi-function** or **totient-function**.

Definition 3. *Let n be a positive integer. Define*
$\phi(n) = \begin{cases} 1 & if \;\; n = 1 \\ |\{r : 0 < r < n \wedge GCD(r,n) = 1\}| & if \;\; n > 1 \end{cases}.$

Thus for $n > 1$, $\phi(n)$ denotes the number of positive integers less that n that are co-prime to n. Before we enumerate some properties of the phi-function in the following theorem we introduce the following set that will play an important role later.

Definition 4. *Let n be a positive integer. Define*

$$\mathbb{Z}_n^* \stackrel{\text{def}}{=} \{a \in \mathbb{Z}_n : GCD(a,n) = 1\}.$$

Clearly, by definition of ϕ, the cardinality $|\mathbb{Z}_n^*| = \phi(n)$. Also for a prime p, $\mathbb{Z}_p^* = \mathbb{Z}_p - \{0\}$.

Theorem 5. *1. For any prime p and a positive integer α,*

$$\phi(p^\alpha) = p^\alpha(1 - \frac{1}{p}).$$

2. Let m, n be two positive integers such that $GCD(m,n) = 1$. Then

$$\phi(mn) = \phi(m)\phi(n).$$

In other words, ϕ is multiplicative for relatively prime integers.

3. Let $n = p_1^{e_1} \dots p_k^{e_k}$ be a prime factorisation of n, where $p_1, \dots, p_k$ are distinct prime divisors of n. Then

$$\phi(n) = n(1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_k}).$$

Proof. 1. First observe that an integer $a \in [1, p^\alpha]$ is **not** co-prime to p^α iff a is a multiple of p. Thus the number of integers $a \in [1, p^\alpha]$ that are nor co-prime to p^α is $p^{\alpha-1}$. Consequently, $\phi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha(1 - \frac{1}{p})$
2. Set $N = mn$. First observe that $|\mathbb{Z}_N^*| = \phi(N)$ and $|\mathbb{Z}_m^* \times \mathbb{Z}_n^*| = \phi(m)\phi(n)$. We shall now define a bijection between these two sets and that will prove (2). Define $F : \mathbb{Z}_N^* \longrightarrow \mathbb{Z}_m^* \times \mathbb{Z}_n^*$ as follows. For $x \in \mathbb{Z}_N^*$ define

$$F(x) = (x \bmod m, x \bmod n),$$

where $x \bmod m$ denotes the remainder when x is divided by m. First note that F is well-defined and moreover, by the Chinese remainder Theorem it is onto and one-one. Thus F is a bijection and we are done.
3. By repeatedly applying (2) we have

$$\phi(n) = \phi(p_1^{e_1}) \dots \phi(p_k^{e_k})$$

$$= p_1^{e_1}(1 - \frac{1}{p_1}) \dots p^{e_k}(1 - \frac{1}{p_k})$$

$$= n(1 - \frac{1}{p_1}) \dots (1 - \frac{1}{p_k}).$$

□

We now obtain a useful result of Algebra.

Theorem 6. *Let n be a positive integer. Consider the binary operation $\times$ defined on $\mathbb{Z}_n$ restricted to $\mathbb{Z}_n^*$. Then $(\mathbb{Z}_n^*, \times)$ is a commutative group of order $\phi(n)$.*

Proof. Clearly $|\mathbb{Z}_n^*| = \phi(n)$. We now show closure property. So fix $a, b \in \mathbb{Z}_n^*$. Let $c \in \mathbb{Z}_n$ be such that $ab \equiv c \bmod n$. Suppose p is a prime divisor of both c and n. Then since $n|(ab-c)$ it follows that $p|(ab-c)$ and hence $p|ab$, This implies that $p|a$ or $p|b$. In either case we obtain a contradiction. This shows that $GCD(c, n) = 1$. So $ab = c \in \mathbb{Z}_n^*$. Associativity is immediate and 1 is the multiplicative identity of $\mathbb{Z}_n^*$. It remains to show that each element of $\mathbb{Z}_n^*$ has a multiplicative inverse. So fix $a \in \mathbb{Z}_n^*$, By Corollary 1, there is an integer $b \in \mathbb{Z}$ such that $ab \equiv 1 \bmod n$. Let c be the unique integer in $\mathbb{Z}_n$ such that $b \equiv c \bmod n$. Clearly, $ab = 1 + kn$ for some $k \in \mathbb{Z}$. If p is a prime divisor of both b and n the $p|(ab - kn)$ i.e. p divides 1. This contradiction shows that $GCD(b, n) = 1$.. Since $b \equiv c \bmod n$, it is not hard to see that c is co-prime to n. Thus $ac \equiv ab \equiv 1 \bmod n$. This shows that $c \in \mathbb{Z}_n^*$ is the multiplicative inverse of $a \in \mathbb{Z}_n^*$. This completes the proof. □

Remark 4. Suppose $n = p^k$ is a prime power. Then one can show that $\mathbb{Z}_n^*$ is a cyclic group.

We now state(without proof) a result in Algebra that is a consequence of *Lagrange's Theorem.*

Theorem 7. *Let $(G, .)$ be a finite group of order n with identity e. Then for $a \in G$*

$$a^n = e.$$

The following is known as **Euler's Theorem**

Theorem 8. *Let a be an integer that is co-prime to n. Then*

$$a^{\phi(n)} \equiv 1 \bmod n.$$

Proof. Since $GCD(a, n) = 1$, there is an $x \in \mathbb{Z}_n^*$ such that $a \equiv x \bmod n$. By Theorem 7, $x^{\phi(n)} = 1$ in $\mathbb{Z}_n^*$ and hence $x^{\phi(n)} \equiv 1 \bmod n$. Thus we have

$$a^{\phi(n)} \equiv x^{\phi(n)} \equiv 1 \bmod n.$$

This completes the proof. □

As an immediate consequence we have **Fermat's Theorem**.

Theorem 9. *Let p be a prime. For any integer $a \not\equiv 0 \bmod p$*

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

Proof. In Theorem 8, take $n = p$ so that $\phi(n) = \phi(p) = p - 1$. Thus we have

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

2 Quadratic Residues, Legendre and Jacobi Symbols

We now introduce a concept that has played an important role in Public Key Cryptography.

Definition 5. *Let p be an odd prime. An integer $a \not\equiv 0 \bmod p$ is said to be a quadratic residue modulo p if the exist an integer $x \in \mathbb{Z}$ such that*

$$x^2 \equiv a \bmod p.$$

Otherwise, a is said to be a quadratic non-residue modulo p.

Remark 5. For any positive integer m and a co-prime to m one can define quadratic residuocity of a modulo m.

Since a and $a+p$ are both quadratic residue or non-residue modulo p, we usually confine ourselves to $\mathbb{Z}_p^*$. Thus $a \in \mathbb{Z}_p^*$ is a quadratic residue modulo p iff it has a square root in $\mathbb{Z}_p$ iff it is a square modulo p. We denote the set of quadratic residues modulo p in $\mathbb{Z}_p^*$ by $\mathbf{QR}_p$. The set of quadratic non-residues is denoted by $\mathbf{QNR}_p$. Thus in $\mathbb{Z}_7$ we have

$$1^2 = 1; 2^2 = 4; 3^2 = 2; 4^2 = 2; 5^2 = 4; 6^2 = 1.$$

Hence $1, 2, 4$ are the 3 quadratic residues modulo 7. The number of quadratic residues is given by the following

Proposition 1. *Let p be an odd prime. Then the number of quadratic residues modulo p is $\frac{(p-1)}{2}$.*

Proof. Consider the function $f : \mathbb{Z}_p^* \longrightarrow \mathbb{Z}_p^*$ defined as follows. For $x \in \mathbb{Z}_p^*$,

$$f(x) \equiv x^2 \bmod p.$$

Clear the function $x \longmapsto x^2$ is well-defined whose range is the set of quadratic residues $\mathbf{QR}_p$. Also if $f(x) = a$ i.e. $x^2 \equiv a \bmod p$, then $(p-x)^2 \equiv (-x)^2 \equiv a \bmod p$ and hence $f(p-x) = a$ Thus the function f is a $2-1$ function and so $|Range(f)| = |\mathbf{QR}_p| = \frac{(p-1)}{2}$. □

Testing whether a given integer is a quadratic residue or non-residue modulo p is given by the following **Euler's Criterion**

Theorem 10. *Let p be an odd prime. An integer a is a quadratic residue modulo p iff*

$$a^{\frac{p-1}{2}} \equiv 1 \bmod p. \tag{4}$$

Proof. Suppose a is a quadratic residue modulo p. Then for integer x, we have $x^2 \equiv a \bmod p$. First note that $x \not\equiv 0 \bmod p$. Thus $a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \bmod p$ by Fermat's Theorem. (Theorem 9)

Conversely, suppose a satisfies equation (4). It is well-know $\mathbb{Z}_p^*$ is a cyclic group with respect to multiplication modulo p. Hence there exits $\alpha \in \mathbb{Z}_p^*$ that generates $\mathbb{Z}_p^*$. Thus we have

$$\mathbb{Z}_p^* = \{1, \alpha, \alpha^2, \ldots, \alpha^{p-2}\}.$$

Suppose $a \equiv \alpha^i \bmod p$ for some $i, 0 \leq i \leq (p-2)$. Then

$$a^{\frac{p-1}{2}} \equiv \alpha^{i\,\frac{(p-1)}{2}} \bmod p.$$

Thus $\alpha^{\frac{i}{2}(p-1)} \equiv 1 \bmod p$. Since the order of α is $p-1$, it follows that $\frac{i}{2}(p-1)$ is a multiple of $(p-1)$ and hence $2|i$. Set $i = 2j$. Hence

$$\left(\alpha^j\right)^2 \equiv a \bmod p.$$

This shows that a is a quadratic residue modulo p. □

As a corollary we have

Corollary 2. *An integer a is a quadratic non-residue iff*

$$a^{\frac{p-1}{2}} \equiv -1 \bmod p.$$

Proof. By Fermat's Theorem we have

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

This implies

$$a^{p-1} - 1 \equiv 0 \bmod p$$

$$or, \quad \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0 \bmod p.$$

The result now follows from Theorem 10. □

Exercise 8. (a) Write a program for testing whether an integer a is a quadratic residue modulo p or not. Check whether 3 is a quadratic residue modulo 7/ modulo 13.

(b) Show that if a, b are quadratic residues (or, non-residues) modulo p, then ab is also a quadratic residue.
Thus $\mathbf{QR}_p$ is a subgroup of $\mathbb{Z}_p^*$.

(c) Let $N = pq$, where p, q are odd primes. Show that the following equation has 4 solutions.

$$x^2 \equiv 1 \bmod N.$$

(Hint: Use CRT)
Two of the solutions are $+1$ and -1. These are called the *trivial square roots* of 1 and the remaining two are the **non-trivial square roots** of 1 modulo N.

Definition 6. *For an odd prime p we now define **Legendre symbol** $\left(\frac{a}{p}\right)$ as follows.*

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{if } a \equiv 0 \bmod p \\ +1 & \text{if } a \text{ is a quadratic residue mod } p \\ -1 & \text{if } a \text{ is a quadratic non-residue mod } p \end{cases}.$$

From Theorem 10 and Corollary 2 we have

Theorem 11. *Let p be an odd prime. Then*

$$a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \bmod p. \tag{5}$$

The following lists some properties of the Legendre symbol. They follow easily from Theorem 11.

Theorem 12. *Let p be an odd prime. Then*

1. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$,
2. $a \equiv b \bmod p$ *implies that* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$,
3. $\left(\frac{1}{p}\right) = 1$; $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

We now compute the value of $\left(\frac{2}{p}\right)$

Theorem 13. *Let p be an odd prime. Then*

$$\left(\frac{2}{p}\right) \equiv \begin{cases} (-1)^{\frac{p-1}{4}} \bmod p & \text{if } p \equiv 1 \bmod 4 \\ (-1)^{\frac{p+1}{4}} \bmod p & \text{if } p \equiv 3 \bmod 4 \end{cases}. \tag{6}$$

Proof. Let $p = 4n + 1$. We shall compute $((p-1)!) \bmod p$ as follows

$$\begin{aligned} & 1.2.3.4.5.\ldots.(4n) \\ & \equiv (1.3.5.\ldots.(4n-1)).(2.4.\ldots.4n) \bmod p \\ & \equiv (1.3.5.\ldots.(4n-1)).((2n)!).2^{2n} \bmod p \\ & \equiv (1.3.\ldots.(2n-1)).((2n+1).\ldots.(4n-1)).((2n)!).2^{2n} \bmod p \\ & \equiv ((-1)(-3)\ldots(-2n+1))(-1)^n.((2n+1)\ldots(4n-1)).((2n)!)2^{2n} \bmod p \\ & \equiv ((4n)(4n-2)\ldots(2n+2)).(-1)^n.((2n+1)\ldots(4n-1))((2n)!)2^{2n} \bmod p \\ & \equiv ((2n+1)(2n+2)\ldots(4n)).(-1)^n.((2n)!).2^{2n} \bmod p \end{aligned}$$

$$\equiv (1.2.3.\ldots.(4n)).(-1)^n.2^{2n} \bmod p.$$

Here we have used the fact that $-1 \equiv 4n; -3 \equiv 4n-2$ etc. On cancellation we have,

$$1 \equiv (-1)^n 2^{2n} \equiv (-1)^{\frac{p-1}{4}} 2^{\frac{p-1}{2}} \bmod p.$$

$$i.e.\ \ 2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{4}} \bmod p.$$

Thus

$$\left(\frac{2}{p}\right) \equiv (-1)^{\frac{p-1}{4}} \bmod p.$$

By a similar argument(exercise) one can show that

$$\left(\frac{2}{p}\right) \equiv (-1)^{\frac{p+1}{4}} \bmod p,$$

when $p \equiv 3 \bmod 4$.

Exercise 9. 1. Show that $\left(\frac{2}{p}\right) = 1$ iff $p \equiv \pm 1 \bmod 8$.

2. Show that

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}. \tag{7}$$

We now state(without proof) the celebrated **Law of Quadratic Reciprocity** due to Gauss.

Theorem 14. *If p and q are distinct odd primes, then*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}. \tag{8}$$

Exercise 10. 1. Show that

$$\left(\frac{p}{q}\right) = \begin{cases} -\left(\frac{q}{p}\right) & \text{if } \ p, q \equiv 3 \bmod 4 \\ +\left(\frac{q}{p}\right) & \text{otherwise} \end{cases}. \tag{9}$$

2. Compute $\left(\frac{37}{59}\right), \left(\frac{-42}{61}\right)$.

2.1 Jacobi Symbol

The Legendre symbol can be extended to any odd positive integer a follows.

Definition 7. *Let Q be an odd positive integer. Suppose $Q = \Pi_{i=1}^{k} q_i$, be a prime factorisation, where the primes q_i are odd and not necessarily distinct. Then the **Jacobi Symbol** $\left(\frac{P}{Q}\right)$ is defined by*

$$\left(\frac{P}{Q}\right) = \prod_{i=1}^{k} \left(\frac{P}{q_i}\right),$$

where each $\left(\frac{P}{q_i}\right)$ is the Legendre symbol.

Remark 6. Clearly, if $GCD(P, Q) > 1$, then $\left(\frac{P}{Q}\right) = 0$ while if $GCD(P, Q) = 1$ then $\left(\frac{P}{Q}\right) = \pm 1$.

The following follows from definition.

Theorem 15. *Suppose P, Q are odd positive integers. Then*

1. $\left(\frac{P}{Q}\right)\left(\frac{P}{Q'}\right) = \left(\frac{P}{QQ'}\right)$.
2. $\left(\frac{P}{Q}\right)\left(\frac{P'}{Q}\right) = \left(\frac{PP'}{Q}\right)$.
3. $P \equiv P' \bmod Q$ *implies that* $\left(\frac{P}{Q}\right) = \left(\frac{P'}{Q}\right)$.

Exercise 11. Let Q be an odd positive integer. Then show that

1.
$$\left(\frac{-1}{Q}\right) = (-1)^{\frac{Q-1}{2}}, \tag{10}$$

2.
$$\left(\frac{2}{Q}\right) = (-1)^{\frac{Q^2-1}{8}}. \tag{11}$$

Hints: For (1) use the fact that $\frac{a-1}{2} + \frac{b-1}{2} \equiv \frac{ab-1}{2} \bmod 2$ and for (2) note that $\frac{a^2-1}{8} + \frac{b^2-1}{8} \equiv \frac{a^2b^2-1}{8} \bmod 2$.

The Gaussian Reciprocity Law gives us the following

Theorem 16. *Let P, Q be odd positive integers. Then*

$$\left(\frac{P}{Q}\right)\left(\frac{Q}{P}\right) = (-1)^{\frac{P-1}{2}\frac{Q-1}{2}}. \tag{12}$$

Proof. Let $P = \prod_{i=1}^{r} p_i$ and $Q = \prod_{j=1}^{s} q_j$. Then

$$\left(\frac{P}{Q}\right) = \prod_{j=1}^{s}\left(\frac{P}{q_j}\right)$$

$$= \prod_{j-1}^{s}\prod_{i=1}^{r}\left(\frac{p_i}{q_j}\right) = \prod_{j=1}^{s}\prod_{i=1}^{r}\left(\frac{q_j}{p_i}\right)(-1)^{\frac{p_i-1}{2}\frac{q_j-1}{2}}$$

$$= \left(\frac{Q}{P}\right)(-1)^{\sum_{j=1}^{s}\sum_{i=1}^{r}\frac{p_i-1}{2}\frac{q_j-1}{2}}.$$

Note that

$$\sum_{j=1}^{s}\sum_{i=1}^{r}\frac{p_i-1}{2}\frac{q_j-1}{2} = \sum_{i=1}^{r}\frac{p_i-1}{2}\sum_{j=1}^{s}\frac{q_j-1}{2}$$

$$\equiv \frac{P-1}{2}\frac{Q-1}{2} \bmod 2.$$

Therefore we have

$$\left(\frac{P}{Q}\right) = \left(\frac{Q}{P}\right)(-1)^{\frac{P-1}{2}\frac{Q-1}{2}}.$$

This completes the proof ∎

Exercise 12. 1. Evaluate $\left(\frac{-35}{97}\right)$; $\left(\frac{7411}{9283}\right)$; $\left(\frac{12345}{111111}\right)$.
2. Write an algorithm for computing the Jacobi symbol without factorisation.

2.2 Primality Tests

1. **Miller-Rabin Primality Test**
   We have already seen that if n is a prime, then by Fermat's little theorem, $a^{n-1} \equiv 1 \bmod n$, for any $a \in [1, n-1]$. The Miller-Rabin test tries to find a "witness" to the compositeness of n by choosing a random $a, 1 \le a \le n-1$ such that $a^{n-1} \not\equiv 1 \bmod n$. The pseudo-code for Miller-Rabin is given below.

   Miller-Rabin(n, s)

   Write $n-1 = 2^k m$, where m is odd.
   Choose a random integer $a, 1 \le a \le n-1$
   $b \leftarrow a^m \bmod n$
   If $b \equiv 1 \bmod n$
   then return ("n is prime")
   for $i \leftarrow 0$ **to** $k-1$
   do { **If** $b \equiv -1 \bmod n$ **then return** ("*n is prime*") } **else** $b \leftarrow b^2 \bmod n$
   return ("n is composite")
   Repeat s times.

   We now show

   Theorem 17. *The Miller-Rabin algorithm for* **composites** *is a Yes-baised Monte Carlo algorithm.*

   Proof. Assume that Miller-Rabin returns "n is composite". Then we claim that n must be composite. Assume that n is prime. Observe that in the **for** loop we are testing for the values $a^m, a^{2m}, \ldots, a^{2^{k-1}m}$. Since the algorithm returns "n is composite", we have for all $i, 0 \le i \le k-1$

   $$a^{2^i m} \not\equiv -1 \bmod n.$$

   Also, by Fermat's theorem, $a^{n-1} \equiv 1 \bmod n$ i.e.

   $$a^{2^k m} \equiv 1 \bmod n.$$

   Thus $a^{2^{k-1}m}$ is a square root of 1 modulo n. Since, by our assumption, n is prime, 1 has exactly two square roots modulo $n viz$ $+1$ and -1. But $a^{2^{k-1}m} \not\equiv -1 \bmod n$. So

   $$a^{2^{k-1}m} \equiv 1 \bmod n.$$

   Repeating this argument we ultimately obtain

   $$a^m \equiv 1 \bmod n.$$

   But this is a contradiction since, otherwise, Miller-Rabin would have retuned "n is prime". Thus n must be composite. □
   We have just shown that if n is prime, then Miller-Rabin algorithm would always return "n is prime". However, if Miller-Rabin returns "n is prime" then it is likely to make an error. We now compute the error probability.

   Theorem 18. *If n is an odd composite number, then the number of witnesses to the compositeness of n is at least $(n-1)/2$.*

Proof. * It suffices to show that the number of non-witnesses is at most $(n-1)/2$. We first show that all non-witnesses are in $\mathbb{Z}_n^*$. Fix a non-witness a. Then we msut have $a^{n-1} \equiv 1 \bmod n$ and hence $a^{n-1} = 1 + tn$, for some integer t. Now $GCD(a, n)|a^{n-1}$ and $GCD(a, n)|tn$ and so $GCD(a, n)|(a^{n-1} - tn)$ i.e. $GCD(a, n)|1$. Thus $GCD(a, n) = 1$ and so $a \in \mathbb{Z}_n^*$. We now show that all non-witnesses are in a proper sub-group of $\mathbb{Z}_n^*$. We shall consider two cases.
Case 1: There exists $x \in \mathbb{Z}_n^*$ such that $x^{n-1} \not\equiv 1 \bmod n$.
Let $B = \{b \in \mathbb{Z}_n^* : b^{n-1} \equiv 1 \bmod n\}$. Clearly, B is non-empty. Also B is closed under multiplication modulo n. Hence, B is a subgroup of $\mathbb{Z}_n^*$. Also all non-witnesses are in B and, by our assumption, $x \in \mathbb{Z}_n^* - B$. So B is a proper subgroup of $\mathbb{Z}_n^*$. Hence

$$\text{number of non-witnesses} \leq |B| \leq |\mathbb{Z}_n^*|/2 \leq (n-1)/2.$$

Case 2: For all $x \in \mathbb{Z}_n^*, x^{n-1} \equiv 1 \bmod n$.
In other words, n is a **Carmicheal Number**.
We first show that n is not a prime power. Suppose $n = p^e$, where p is an odd prime and $e > 1$. Then $\mathbb{Z}_n^*$ is a cyclic group. Suppose g is a generator of $\mathbb{Z}_n^*$. By our assumption $g^{n-1} \equiv 1 \bmod n$. Hence, the order of g divides $n-1$. But, the order of $g = |\mathbb{Z}_n^*| = \phi(n) = p^{e-1}(p-1)$. So $p^{e-1}(p-1)|(p^e - 1)$, a contradiction, since $p^e - 1$ is not divisible by p. Hence $n = n_1.n_2$, where n_1, n_2 are odd primes greater than 1 and $GCD(n_1, n_2) = 1$.
Note that $n - 1 = 2^k m$ and that on input $a \in \mathbb{Z}_n^*$ Miller-Rabin computes the sequence

$$X = (a^m, a^{2m}, a^{2^2 m}, \ldots, a^{2^k m}).$$

Now fix a pair (c, j) where $c \in \mathbb{Z}_n^*, 0 \leq j \leq k$ and

$$c^{2^j m} \equiv -1 \bmod n. \tag{13}$$

Such a pair exists, since for $j = 0$, we have $(n-1)^m \equiv (-1)^m \equiv -1 \bmod n$. Choose j as large as possible. Let

$$B = \{x \in \mathbb{Z}_n^* : x^{2^j m} \equiv \pm 1 \bmod n\}.$$

Clearly, B is closed under multiplication modulo n. Hence, B is a sub-group of $\mathbb{Z}_n^*$. Also every non-witness must be in B, since for a non-witness a, the sequence X computed by the algorithm must all be 1 or for some $j' \leq j, a^{2^{j'} m} \equiv -1 \bmod n$, by maximality of j.
We claim that B is a proper sub-group of $\mathbb{Z}_n^*$. To see this, by CRT, fix an integer w such that

$$w \equiv c \bmod n_1$$

$$w \equiv 1 \bmod n_2.$$

Observe that, if $w \equiv +1 \bmod n$, then $w \equiv +1 \bmod n_1$. This would imply that $w^{2^j m} \equiv c^{2^j m} \bmod n_1$. But by (13), $c^{2^j m} \equiv -1 \bmod n_1$. So $w^{2^j m} \equiv -1 \bmod n_1$, a contradiction. This contradiction shows that $w \not\equiv +1 \bmod n$. Similarly, if $w \equiv -1 \bmod n$ then $w \equiv -1 \bmod n_2$, which is a contradiction again. Hence $w \notin B$. To complete the proof, we show that $w \in \mathbb{Z}_n^*$. Since $w \equiv c \bmod n_1$ and $GCD(c, n_1) = 1$ it follows that $GCD(w, n_1) = 1$. Further $w \equiv 1 \bmod n_2$ and so $GCD(w, n_2) = 1$. Consequently $GCD(w, n_1 n_2) = GCD(w, n) = 1$. Hence $w \in \mathbb{Z}_n^* - B$ and so B is a proper sub-group of $\mathbb{Z}_n^*$. In this case also

$$\text{number of non-witnesses} \leq |B| \leq |\mathbb{Z}_n^*|/2 \leq (n-1)/2.$$

This completes the proof. □
We now compute the probability of error.

Theorem 19. *For any odd integer $n > 2$ and any positive integer s, the probabilty that Miller-Rabin(n, s) errs is at most $1/2^s$.*

Proof. If n is composite, in each execution, Miller-Rabin is likely to err if it chooses a non-witness. Hence, Miller-Rabin will err with probability at most $1/2$. Thus the probability of erring s times is at most $1/2^s$. □

2 Solovay-Strassen Primality Test

Recall that for an odd integer n, $\left(\frac{a}{n}\right)$ denote the Jacobi symbol of a w.r.t. n.

SOLOVAY-STRASSEN(n)

> choose an random integer a such that $1 \leq a \leq n-1$
> $x \leftarrow \left(\frac{a}{n}\right)$
> **if** $x = 0$
>   **then return** ("n is composite")
> $y \leftarrow a^{\frac{n-1}{2}} \bmod n$
> **if** $x \equiv y \bmod n$
>   **then return** ("n is prime")
>   **else return** ("n is composite) □

We shall now show that the Solovay-Strassen algorithm is a yes-biased Monte Carlo algorithm for composite. To see this, note that if n is prime, then by Theorem 11, the condition "$x \equiv y \bmod n$" will always hold and hence the algorithm will return "n is prime". This means that if the algorithm returns "n is composite", then n must be composite with probability 1. Furthermore, observe that if n is composite and the algorithm returns "n is prime", then it must be the case that for some integer a with $1 \leq a \leq n-1$ we have

$$\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \bmod n. \tag{14}$$

In this case n is called an **Euler pseudo-prime** to the base a. For example one can check that

$$\left(\frac{10}{91}\right) \equiv 10^{45} \bmod 91.$$

Thus, 91 is an Euler pseudo-prime to the base 10.
For an odd composite n, if n is an Euler pseudo-prime to the base a, then one may view a as a witness to the fact that n is an Euler pseudo-prime. If the number of witnesses is not too large, then the probability of error will not be large. In fact, the next theorem shows that the error probability is at most $1/2$.

Theorem 20. *Let n be an odd composite integer. Recall that $\mathbb{Z}_n^*$ is a multiplicative group of order $\phi(n)$. Define*

$$G(n) = \left\{ a \in \mathbb{Z}_n^* : \left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \bmod n \right\}.$$

*Then $G(n)$ is a **proper** subgroup of $\mathbb{Z}_n^*$. Consequently, $|G(n)| \leq \frac{n-1}{2}$.*

Proof. [1] It is not hard to see that if $a, b \in G(n)$ then $a.b \in G(n)$. Since $G(n)$ is finite, this shows that $G(n)$ is a subgroup of $\mathbb{Z}_n^*$. We now show that it is a proper subgroup.
We have two cases.
Case 1. n is not a product of distinct primes. In this case, for some prime p we have $n = p^k q$,

[1] May be omitted

where $k \geq 2$ and q is odd. Let $a = 1 + p^{k-1}q$. Now using Theorem 15, we see that

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right)^k \left(\frac{a}{q}\right) = \left(\frac{1}{p}\right)^k \left(\frac{1}{q}\right) = 1,$$

since $a \equiv 1 \bmod p$ and $a \equiv 1 \bmod q$.
On the other hand,

$$a^{\frac{n-1}{2}} = (1 + p^{k-1}q)^{\frac{n-1}{2}} = 1 + \frac{n-1}{2}(p^{k-1}q) + \text{terms which are multiples of n}.$$

Thus we have

$$a^{\frac{n-1}{2}} \equiv 1 + \frac{n-1}{2} p^{k-1} q \bmod n. \tag{15}$$

Now if $a^{\frac{n-1}{2}} \equiv 1 \bmod n$, then from (15), we would have

$$\frac{n-1}{2} p^{k-1} q \equiv 0 \bmod n.$$

This would imply that $p | \frac{n-1}{2}$. This is easily seen to be false. Hence, we have

$$a^{\frac{n-1}{2}} \not\equiv 1 \bmod n,$$

and so

$$\left(\frac{a}{n}\right) \not\equiv a^{\frac{n-1}{2}} \bmod n.$$

Thus $a \in \mathbb{Z}_n^* - G(n)$ and so $G(n)$ is a proper subgroup of $\mathbb{Z}_n^*$.

Case 2. n is a product of distinct primes. Suppose

$$n = p_1 p_2 \ldots p_k,$$

where the p_i's are distinct odd primes. Let u be a fixed quadratic non-residue modulo p_1. By the Chinese remainder theorem, find an integer a such that

$$a \equiv u \bmod p_1$$

and

$$a \equiv 1 \bmod p_2 \ldots . p_k.$$

Observe that

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \left(\frac{a}{p_2 \ldots p_k}\right) = \left(\frac{u}{p_1}\right) \left(\frac{1}{p_2 \ldots . p_k}\right) = (-1).1 = -1.$$

Also,trivially, we have

$$a^{\frac{n-1}{2}} \equiv 1 \bmod p_2 \ldots p_k. \tag{16}$$

This implies that

$$a^{\frac{n-1}{2}} \not\equiv -1 \bmod n.$$

For, if this equation does not hold, then we would have

$$a^{\frac{n-1}{2}} \equiv -1 \bmod p_2 \ldots p_k,$$

contradicting equation (16). Consequently, we have

$$a^{\frac{n-1}{2}} \not\equiv \left(\frac{a}{n}\right) \bmod n.$$

Therefore, $a \in \mathbb{Z}_n^* - G(n)$. So $G(n)$ is a proper subgroup of $\mathbb{Z}_n^*$.
Hence, by Lagrange's theorem, $|G(n)|$ is a proper divisor of $|\mathbb{Z}_n^*| = \phi(n)$. Therefore, $|G(n)| \leq \frac{\phi(n)}{2} \leq \frac{n-1}{2}$.
This completes the proof □

The above theorem tells us that, given that n is composite, the probability that the algorithm will return "n is prime" is at most 1/2. If the algorithm returns "n is prime" m times in succession, how sure can we be that n is indeed prime? To compute the required probability, consider the following two events.
A: "a random odd integer n of specified size is composite"
B: "the algorithm returns 'n is prime' m times in succession"

Clearly, $\mathbf{Pr[B \mid A]} \leq \frac{1}{2^m}$. By Bayes's theorem,

$$\mathbf{Pr[A \mid B]} = \frac{\mathbf{Pr[B \mid A]Pr[A]}}{\mathbf{Pr[B]}} = \frac{\mathbf{Pr[B \mid A]Pr[A]}}{\mathbf{Pr[B \mid A]Pr[A]+Pr[B} \,|\bar{A}]\mathbf{Pr}[\bar{A}]} \tag{17}$$

Now suppose $N \leq n \leq 2N$. Then by the Prime number theorem, the number of primes in the interval $[N, 2N]$ is approximately

$$\frac{2N}{\log 2N} - \frac{N}{\log n} \approx \frac{N}{\log n} \approx \frac{n}{\log n},$$

where $\log x$ denotes $\log_e x$. Since there are $N/2 \approx n/2$ odd integers in the interval $[N, 2N]$, we have the following estimate.

$$\mathbf{Pr[A]} \approx 1 - \frac{2}{\log n}.$$

Thus from (17) we have

$$\begin{aligned}
\mathbf{Pr[A \mid B]} &\approx \frac{\mathbf{Pr[B \mid A]}(1 - \frac{2}{\log n})}{\mathbf{Pr[B \mid A]}(1 - \frac{2}{\log n}) + \mathbf{Pr[B} \,|\bar{A}]\frac{2}{\log n}} \\
&\approx \frac{\mathbf{Pr[B \mid A]}(1 - \frac{2}{\log n})}{\mathbf{Pr[B \mid A]}(1 - \frac{2}{\log n}) + \frac{2}{\log n}} \\
&\approx \frac{\mathbf{Pr[B \mid A]}(\log n - 2)}{\mathbf{Pr[B \mid A]}(\log n - 2) + 2} \\
&\leq \frac{\frac{1}{2^m}(\log n - 2)}{\frac{1}{2^m}(\log n - 2) + 2} \leq \frac{\log n - 2}{(\log n - 2) + 2^{m+1}} \\
&\leq \frac{\log n}{\log n + 2^{m+1}},
\end{aligned}$$

which is very small for sufficiently large m. Thus if the algorithm returns "n is prime" m times in succession, then for sufficiently large m, n is prime with high probability.

Complexity: One can evaluate $a^{\frac{n-1}{2}} \bmod n$ in time $O((\log n)^3)$. Also, it is not hard to show that the Jacobi symbol $\left(\frac{a}{n}\right)$ can be computed in polynomial time. In fact, using the properties listed in Theorem 15 and Theorem 16, one can show that the Jacobi symbol can be computed in $O((\log n)^3)$ time. Thus the time complexity of the Solovay-Strassen algorithm is $O((\log n)^3)$.□

References

1. J.Stillwell, *Elements of Number Theory*, Springer.
2. I. Niven, H.S. Zukerman and H.L. Montgomary, *An Introduction to the Theory of Numbers*, Wiley.