4 Number Theory 1

4.1 Divisors

Division
Let a and b be integers. We say that a divides b, or $a|b$ if:

$$\exists d \text{ s.t. } b = ad$$

If $b \neq 0$ then $|a| \leq |b|$.
Division Theorem: For any integer a and any positive integer n, there are unique integers q and r such that $0 \leq r < n$ and $a = qn + r$.
The value $r = a \bmod n$ is called the remainder or the residue of the division.
Theorem: If $d|a$ and $d|b$ then $d|(xa + yb)$ for any integers x, y.
Proof: $a = rd$ and $b = sd$ for some r, s. Therefore, $xa + yb = xrd + ysd = d(xr + ys)$, so $d|(xa + yb)$

Greatest Common Divisor
For integers a and b:
The greatest common divisor gcd(a,b) is defined as follows:

$$\gcd(a,b) = \max(d : d|a \text{ and } d|b)\ (a \neq 0 \text{ or } b \neq 0).$$

Note: This definition satisfies gcd(0,1) = 1.
The lowest common multiple lcm(a,b) is defined as follows:

$$\text{lcm}(a,b) = \min(m > 0 \text{ s.t. } a|m \text{ and } b|m)\ (\text{for } a \neq 0 \text{ and } b \neq 0).$$

a and b are coprimes (or relatively prime) iff gcd(a,b) = 1.

Prime Numbers
An integer $p \geq 2$ is called prime if it is divisible only by 1 and itself.
Fundamental Theorem of Arithmetic: every positive number can be represented as a product of primes in a unique way, up to a permutation of the order of primes.
There are infinitely many primes

- Euclid gave simple proof by contradiction (c. 300BC).

The number of primes $\leq n : \pi(n) \approx n/\ln n$

- Even though the number of primes is infinite, the density of primes gets increasingly sparse as $n \to \infty$.

4.2 Modular Arithmetic

Modular Arithmetic
Modular arithmetic is fundamental to modern public key cryptosystems.
Given integers $a, b, N \in \mathbb{Z}$ we say that a is congruent to b modulo N:

$$a \equiv b \pmod{N} \text{ iff } N \text{ divides } b - a$$

Often we are lazy and just write $a \equiv b$ if it is clear we are working modulo N.
The modulo operator is like the C-operator %.
Example: $16 \equiv 1 \pmod{5}$ since 16-1 = 3 $\times$ 5

Modular Arithmetic
For convenience we define the set:

$$\mathbb{Z}_N = \{0, \ldots, N-1\}$$

which is the set of remainders modulo N.
It is clear that given N, every integer $a \in \mathbb{Z}$ is congruent modulo N to an element in the set $\mathbb{Z}_N$, since we can write:

$$a = q \times N + r$$

with $0 \leq r < N$ and $a \equiv r \pmod{N}$

Modular Arithmetic
The set $\mathbb{Z}_N$ has two operations defined on it.

- Addition
  - $11 + 13 \mod 16 \equiv 24 \pmod{16} \equiv 8 \pmod{16}$.
- Multiplication
  - $11 \times 13 \pmod{16} \equiv 143 \pmod{16} \equiv 15 \pmod{16}$.

Given integers $a, b \in \mathbb{Z}$ we have:

- $a + b \pmod{N} \equiv (a \pmod{N} + b \pmod{N}) \pmod{N}$
- $a - b \pmod{N} \equiv (a \pmod{N} - b \pmod{N}) \pmod{N}$
- $a \times b \pmod{N} \equiv (a \pmod{N} \times b \pmod{N}) \pmod{N}$

Multiplicative Inverse
Division a/b in modular arithmetic is performed by multiplying a by the multiplicative inverse of b.
The multiplicative inverse of $b \in \mathbb{Z}_N$ is an element denoted $b^{-1} \in \mathbb{Z}_N$ with:

$$bb^{-1} \equiv b^{-1}b \equiv 1$$

Theorem: $b \in \mathbb{Z}_N$ has a unique inverse modulo N iff b and N are relatively prime i.e. gcd(b,N) = 1.
Theorem: If p is a prime then every non-zero element in $\mathbb{Z}_p$ has an inverse.

Multiplicative Inverse
Consider $\mathbb{Z}_{10}$:

- 3 has a multiplicative inverse, since gcd(3,10)=1.
  - $3 \times 7 \equiv 21 \equiv 1 \pmod{10}$.
- 5 has no multiplicative inverse, since gcd(5,10)=5.
  - We have the following table:

$$\begin{array}{ll}
0 \times 5 \equiv 0 \pmod{10} & 5 \times 5 \equiv 5 \pmod{10} \\
1 \times 5 \equiv 5 \pmod{10} & 6 \times 5 \equiv 0 \pmod{10} \\
2 \times 5 \equiv 0 \pmod{10} & 7 \times 5 \equiv 5 \pmod{10} \\
3 \times 5 \equiv 5 \pmod{10} & 8 \times 5 \equiv 0 \pmod{10} \\
5 \times 5 \equiv 0 \pmod{10} & 9 \times 5 \equiv 5 \pmod{10}
\end{array}$$

Modular Arithmetic

1. Addition is closed:
$$\forall a,b \in \mathbb{Z}_N : a+b \in \mathbb{Z}_N$$
2. Addition is associative:
$$\forall a,b,c \in \mathbb{Z}_N : (a+b)+c \equiv a+(b+c)$$
3. 0 is an additive identity:
$$\forall a \in \mathbb{Z}_N : a+0 \equiv 0+a \equiv a$$
4. The additive inverse always exists:
$$\forall a \in \mathbb{Z}_N : a+(N-a) \equiv (N-a)+a \equiv 0$$
5. Addition is commutative:
$$\forall a,b \in \mathbb{Z}_N : a+b \equiv b+a$$

Modular Arithmetic

6. Multiplication is closed:
$$\forall a,b \in \mathbb{Z}_N : a \times b \in \mathbb{Z}_N$$
7. Multiplication is associative:
$$\forall a,b,c \in \mathbb{Z}_N : (a \times b) \times c \equiv a \times (b \times c)$$

8. 1 is a multiplicative identity:

$$\forall a \in \mathbb{Z}_N : a \times 1 \equiv 1 \times a \equiv a$$

9. Multiplication is commutative:

$$\forall a, b \in \mathbb{Z}_N : a \times b \equiv b \times a$$

10. Multiplication distributes over addition:

$$\forall a, b, c \in \mathbb{Z}_N : (a + b) \times c \equiv a \times c + b \times c$$

4.3 Groups, Rings and Fields

Groups
A group $(S, \oplus)$ consists of a set S and an operation $\oplus$, satisfying:

- Closure: $\forall a, b \in S : a \oplus b \in S$
- Associativity: $\forall a, b, c \in S : a \oplus (b \oplus c) = (a \oplus b) \oplus c$
- Identity element e: $\exists e \in S : \forall a \in S : a \oplus e = e \oplus a = a$
- Every element has an inverse element:

$$\forall a \in S : \exists a^{-1} \in S : a \oplus a^{-1} = a^{-1} \oplus a = e$$

- The group S is called commutative or Abelian if:

$$\forall a, b \in S : a \oplus b = b \oplus a$$

- The order of a group S, denoted by $|S|$, is the number of elements in S. If a group S satisfies $|S| < \infty$ then it is called a finite group.

Groups
Integers, real numbers and complex numbers are groups under addition.

- the identity is 0, the inverse of x is $-x$

Non-zero real numbers and non-zero rational numbers are groups under multiplication.

- the identity is 1, the inverse of x is x^{-1}

These are all examples of infinite Abelian groups.
Questions:

- Why are the integers not a group under multiplication?
- Why do we say non-zero real numbers above?

Modular Arithmetic
Going back to our 10 properties of modular arithmetic we see:

- Properties 1-4 say that $\mathbb{Z}_N$ is a group with respect to addition.
- Property 5 says that the group $\mathbb{Z}_N$ is abelian.
- Properties 1-10 say that $\mathbb{Z}_N$ is a ring.
- Other rings you have seen before are the integers, real numbers and complex numbers.
  - These are all infinite rings, whereas $\mathbb{Z}_N$ is a finite ring.

Fields
A field $(S, \oplus, \otimes)$ is a set with two operations $\oplus$ and $\otimes$ and two special elements 0, 1 such that:

- $(S, \oplus)$ is an abelian group with identity 0.
- $(S \setminus \{0\}, \otimes)$ is an abelian group with identity 1.
- $(S, \oplus, \otimes)$ satisfies the distributive law:

$$\forall a, b, c \in S : a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$$

Example fields: rational numbers, real numbers, complex numbers.

Finite Fields
A finite field is a field that contains a finite number of elements.
There is exactly one finite field of size (order) p^n where p is a prime (called the characteristic of the field) and n is a positive integer.
If p is a prime $\mathbb{Z}_p$ is the finite field GF(p) (note here that $n = 1$ and so is omitted).
Finite fields are of central importance in coding theory and cryptography.
GF(2^8) is of particular importance as an element can represented in a single byte.

Euler Groups
We define the set of invertible elements of $\mathbb{Z}_N$ as:

$$\mathbb{Z}_N^* = \{a \in \mathbb{Z}_N : \gcd(a, N) = 1\}$$

The set $\mathbb{Z}_N^*$ is always a group with respect to multiplication and is called an Euler group.
When N is a prime p we have:

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

Examples:

$$\begin{array}{ll}
\mathbb{Z}_1 = \{0\} & \mathbb{Z}_1^* = \{0\} \\
\mathbb{Z}_2 = \{0,1\} & \mathbb{Z}_2^* = \{1\} \\
\mathbb{Z}_3 = \{0,1,2\} & \mathbb{Z}_3^* = \{1,2\} \\
\mathbb{Z}_4 = \{0,1,2,3\} & \mathbb{Z}_4^* = \{1,3\} \\
\mathbb{Z}_5 = \{0,1,2,3,4\} & \mathbb{Z}_5^* = \{1,2,3,4\}
\end{array}$$

Euler Totient Function $\phi(N)$
Euler's totient function $\phi(N)$ represents the number of elements in $\mathbb{Z}_N^*$:

$$\phi(N) = |\mathbb{Z}_N^*| = |\{a \in \mathbb{Z}_N : \gcd(a,N) = 1\}|$$

$\phi(N)$ is therefore the number of integers in $\mathbb{Z}_N$ which are relatively prime to N.
We know that an element $a \in \mathbb{Z}_N$ has a multiplicative inverse modulo N iff gcd(a,N) = 1.
Therefore, there are precisely $\phi(N)$ invertible elements in $\mathbb{Z}_N$.

Euler Totient Function $\phi(N)$
Given the prime factorization of N:

$$N = \prod_{i=1}^{n} p_i^{e_i}$$

we can compute $\phi(N)$ using the following formula:

$$\phi(N) = \prod_{i=1}^{n} p_i^{e_i-1}(p_i - 1)$$

The most important cases for cryptography are:

- If p is prime then:
$$\phi(p) = p - 1$$
- If p and q are both prime and $p \neq q$ then:
$$\phi(pq) = (p-1)(q-1)$$

Lagranges Theorem
The order of an element a of a group $(S, \otimes)$ is the smallest positive integer t such that $a^t = 1$.
Lagrange's Theorem:

$$\text{If } S \text{ is a group of size } |S| = n \text{ then } \forall a \in S : a^n = 1$$

Corollary: the order t of an element $a \in S$ divides $n = |S|$, so if $a \in \mathbb{Z}_N^*$ then the order of a always divides $\phi(N)$
Thus if $a \in \mathbb{Z}_N^*$ then $a^{\phi(N)} \equiv 1 \pmod{N}$, since $|\mathbb{Z}_N^*| = \phi(N)$ (Euler's Theorem).

Fermat's Little Theorem
Not to be confused with Fermat's Last Theorem . . .
Fermat's Little Theorem:

$$\text{if } p \text{ is a prime then } a^p \equiv a \pmod{p}$$

Fermat's Little Theorem is a special case of Lagrange's Theorem.

4.4 Calculating Multiplicative Inverses

Greatest Common Divisor (GCD)
We need a method to determine when $a \in \mathbb{Z}_N$ has a multiplicative inverse and compute it when it does.
We know this happens iff $\gcd(a,N) = 1$.
Therefore we need to compute the GCD of two integers $a, b \in \mathbb{Z}$.

- This is easy if we know the prime factorization of a and b, since:

$$a = \prod p_i^{\alpha_i} \text{ and } b = \prod p_i^{\beta_i} \Rightarrow d = \gcd(a,b) = \prod p_i^{min(\alpha_i,\beta_i)}$$

- However, factoring is a very expensive operation, so we cannot use the above formula.
- A much faster algorithm to compute GCDs is Euclids algorithm.

GCD - Euclidean Algorithm
To compute the GCD of $r_0 = a$ and $r_1 = b$ we compute:

$$\begin{array}{rcl} r_0 & = & q_1 r_1 + r_2 \\ r_1 & = & q_2 r_2 + r_3 \\ & \vdots & \\ r_{m-2} & = & q_{m-1} r_{m-1} + r_m \\ r_{m-1} & = & q_m r_m \end{array}$$

If d divides a and b then d divides r_2, r_3, r_4 and so on.
Therefore: $\gcd(a, b) = \gcd(r_0, r_1) = \gcd(r_1, r_2) = \cdots = \gcd(r_{m-1}, r_m) = r_m$

GCD - Euclidean Algorithm
As an example of this algorithm we want to show that:

$$3 = \gcd(21,12)$$

Using the Euclidean algorithm we compute gcd(21,12) as:

$$\begin{array}{rcl} \gcd(21,12) & = & \gcd(21 \pmod{12},12) \\ & = & \gcd(9,12) \\ & = & \gcd(12 \pmod 9,9) \\ & = & \gcd(3, 9) \\ & = & \gcd(9 \pmod 3,3) \\ & = & \gcd(0,3) = 3 \end{array}$$

XGCD - Extended Euclidean Algorithm
Using the Euclidean algorithm, we can determine when a has an inverse modulo N i.e. iff $\gcd(a,N) = 1$.

- But we do not know yet how to compute the inverse.

Solution: use an extended version of the Euclidean algorithm.
Recall that during the Euclidean algorithm we had:

$$r_{i-2} = q_{i-1} r_{i-1} + r_i$$

and finally $r_m = \gcd(r_0, r_1)$.
Now we unwind the above and write each $r_i, i \geq 2$ in terms of a and b.

XGCD - Extended Euclidean Algorithm
Unwinding the various steps in the Euclidean algorithm gives:

$$\begin{array}{lcl}
r_2 & = & r_0 - q_1 r_1 = a - q_1 b \\
r_3 & = & r_1 - q_2 r_2 = b - q_2(a - q_1 b) = -q_2 a + (1 + q_1 q_2) b \\
. & \vdots & \\
r_{i-2} & = & s_{i-2} a + t_{i-2} b \\
r_{i-1} & = & s_{i-1} a + t_{i-1} b \\
r_i & = & r_{i-2} - q_{i-1} r_{i-1} \\
 & = & a(s_{i-2} - q_{i-1} s_{i-1}) + b(t_{i-2} - q_{i-1} t_{i-1}) \\
 & \vdots & \\
r_m & = & s_m a + t_m b
\end{array}$$

The XGCD takes as input a and b and outputs s_m, t_m, r_m such that:

$$r_m = \gcd(a,b) = s_m a + t_m b$$

XGCD - Multiplicative Inverse
Given $a, N \in \mathbb{Z}$ we can compute d, x, y using XGCD such that:

$$d = \gcd(a,N) = xa + yN$$

Considering the above equation modulo N we get:

$$d \equiv xa + yN \pmod{N} \equiv xa \pmod{N}$$

Thus if $d = 1$ then a has a multiplicative inverse given by:

$$a^{-1} \equiv x \pmod{N}$$

Remark: the more general equation $ax \equiv b \pmod{N}$ has precisely $d = \gcd(a,N)$ solutions iff d divides b.

4.5 Calculating Modular Exponents

Modular Exponentiation

Given a prime p and $a \in \mathbb{Z}_p^*$ we want to calculate $a^x \pmod{p}$.
It does not make sense to compute $y = a^x$ and then $y \pmod{p}$.
Consider $123^5 \pmod{511} = 28153056843 \pmod{511} = 359$
There is a large intermediate result so this method takes a very long time and a great deal of space for large a, x and p.
$123^5 \pmod{511}$ could also be calculated as follows:

$$\begin{array}{rcl} a & = & 123 \\ a^2 & = & a \times a \pmod{511} = 310 \\ a^3 & = & a \times a^2 \pmod{511} = 316 \\ a^4 & = & a \times a^3 \pmod{511} = 32 \\ a^5 & = & a \times a^4 \pmod{511} = 359 \end{array}$$

This requires four modular multiplications; it is still far too slow.

Modular Exponentiation

It is much better to compute this example using the steps below:

$$\begin{array}{rcl} a & = & 123 \\ a^2 & = & a \times a \pmod{511} = 310 \\ a^4 & = & a^2 \times a^2 = 310 \times 310 \pmod{511} = 32 \\ a^5 & = & a \times a^4 = 123 \times 32 \pmod{511} = 359 \end{array}$$

This requires only 3 multiplications.
This shows that if we consider the binary representation of the exponent $x = x_{n-1}x_{n-2}\ldots x_1x_0$, then the value represented by each bit of the exponent x_i can be obtained by squaring the value represented by the previous bit x_{i-1}.
Multiplication is required for every bit which is set after the first one.
Thus for an exponent with n bits of which t bits are set, $n-1$ squarings and $t-1$ multplications.

Modular Exponentiation

This suggests an algorithm which works through the exponent one bit at a time squaring and multiplying.
This is commonly known as the square and multiply algorithm.
Right to left variant for calculating $y = a^x \pmod{p}$:

```
y = 1
for i = 0 to n-1 do
   if x_i = 1 then y = (y*a) mod p
   a = (a*a) mod p
end
```

Left to right variant for calculating $y = a^x \pmod{p}$:

```
y = 1
for i = n-1 downto 0 do
    y = (y*y) mod p
    if x_i = 1 then y = (y*a) mod p
end
```

Chinese Remainder Theorem (CRT)
Consider $N = 15 = 3 \times 5$.
We can represent every element a of $\mathbb{Z}_N$ by its coordinates $(a \pmod 3, a \pmod 5)$.
This leads to the following table:

	0	1	2	3	4
0	0	6	12	3	9
1	10	1	7	13	4
2	5	11	2	8	14

Note that all elements in $\mathbb{Z}_N$ have different coordinates, i.e. given (a_1, a_2) with $0 \leq a_1 < 3$ and $0 \leq a_2 < 5$ we can reconstruct a.

Chinese Remainder Theorem (CRT)
Consider $N = 24 = 4 \times 6$.
We can represent every element a of $\mathbb{Z}_N$ by its coordinates $(a \pmod 4, a \pmod 6)$.
This leads to the following table:

	0	1	2	3	4	5
0	0/12		8/20		4/16	
1		1/13		9/21		5/17
2	6/18		2/14		10/22	
3		7/19		3/15		11/23

Note that a and $a + 12 \pmod{24}$ map to the same coordinates.
Therefore, given (a_1, a_2) with $0 \leq a_1 < 4$ and $0 \leq a_2 < 6$ we cannot uniquely reconstruct a.

Chinese Remainder Theorem (CRT)
The previous examples indicate that if $N = n_1 \times n_2$ with $\gcd(n_1, n_2) = 1$, we can replace computing modulo N by computing modulo n_1 and modulo n_2:

$$\mathbb{Z}_N \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \text{ iff } \gcd(n_1, n_2) = 1$$

If $N = n_1 \times n_2$ then it is very easy to compute the coordinates of $a \in \mathbb{Z}_N$, since these are simply $(a \pmod{n_1}), a \pmod{n_2})$.
However, given the coordinates (a_1, a_2) with $0 \leq a_1 < n_1$ and $0 \leq a_2 < n_2$ how do we compute the corresponding a?

Chinese Remainder Theorem (CRT)
We can reformulate our reconstruction problem as:
Given: $N = n_1 \times n_2$ with $\gcd(n_1, n_2) = 1$
Compute: $x \in \mathbb{Z}_N$ with $x \equiv a_1 \pmod{n_1}$ and $x \equiv a_2 \pmod{n_2}$
Example: If $x \equiv 4 \pmod 7$ and $x \equiv 3 \pmod 5$ then we have:

$$x \equiv 18 \pmod{35}$$

How did we work this out?

CRT - Example
We want to find $x \in \mathbb{Z}_N$ with $N = 35$ such that:

$$x \equiv 4 \pmod 7 \text{ and } x \equiv 3 \pmod 5$$

Therefore, for some $n \in \mathbb{Z}$ we have:

$$x = 4 + 7n \text{ and } x \equiv 3 \pmod 5$$

Substituting the equality in the second equation gives:

$$4 + 7n \equiv 3 \pmod 5$$

Therefore, n is given by the solution of:

$$2n \equiv 7n \equiv 3 - 4 \equiv 4 \pmod 5$$

Hence we can compute n as $n \equiv 4/2 \pmod 5 \equiv 2 \pmod 5$, so:

$$x \equiv 4 + 7n \equiv 4 + 7 \times 2 \equiv 18 \pmod{35}$$

CRT - General Case
Let $n_1, \ldots, n_k$ be pairwise relatively prime and let $a_1, \ldots, a_k$ be integers.
We want to find x modulo $N = n_1 n_2 \cdots n_k$ such that:

$$x \equiv a_i \pmod{n_i} \text{ for all } i$$

The CRT guarantees a unique solution given by:

$$x = \sum_{i=1}^{k} a_i \times N_i \times y_i \pmod N$$

$$N_i = N/n_i \text{ and } y_i = N_i^{-1} \pmod{n_i}$$

Note that $N_i \equiv 0 \pmod{n_j}$ for $j \neq i$ and that $N_i \times y_i \equiv 1 \pmod{n_i}$

CRT - General Case Example
We want to find the unique x modulo $N = 1001 = 7 \times 11 \times 13$ such that:

$$x \equiv 5 \pmod{7} \text{ and } x \equiv 3 \pmod{11} \text{ and } x \equiv 10 \pmod{13}$$

We compute:

$$N_1 = 143, y_1 = 5 \text{ and } N_2 = 91, y_2 = 4 \text{ and } N_3 = 77, y_3 = 12.$$

Then we reconstruct x as:

$$\begin{aligned} x &\equiv \sum_{i=1}^{k} a_i \times N_i \times y_i \pmod{N} \\ &\equiv 5 \times 143 \times 5 + 3 \times 91 \times 4 + 10 \times 77 \times 12 \pmod{1001} \\ &\equiv 894 \pmod{1001} \end{aligned}$$

CRT - Modular Exponentiation
Let $N = 55 = 5 \times 11$ and suppose we want to compute $27^{37} \pmod{N}$.
This can be done in a number of ways:

- Really stupid: using 36 multiplications modulo 55:

$$(((27 \times 27) \pmod{N}) \times 27 \pmod{N}) \cdots 27 \pmod{N}$$

- Less stupid: using 5 squarings and 2 multiplications modulo 55:

$$((27^{2^5} \pmod{N}) \times 27^{2^2} \pmod{N}) \times 27 \pmod{N}$$

- Rather intelligent: using 5 squarings and 2 multiplications modulo 5 and modulo 11 and CRT to combine both results.

- Really intelligent: using Lagrange's theorem, a few multiplications modulo 5 and 11 and CRT to combine both results.

4.6 Primitive Roots

Generators
For $a \in \mathbb{Z}_n^*$ the set $\{a^0, a^1, a^2, a^3, \ldots\}$ is called the group generated by a, denoted $\langle a \rangle$.
The order of $a \in \mathbb{Z}_n^*$ is the size of $\langle a \rangle$, denoted $|\langle a \rangle|$.
Examples for $\mathbb{Z}_7^*$:
$\langle 3 \rangle = \{1,3,2,6,4,5\}$, so the order of 3 is 6
$\langle 2 \rangle = \{1,2,4\}$, so the order of 2 is 3
$\langle 1 \rangle = \{1\}$, so the order of 1 is 1

Primitive Roots
$a \in \mathbb{Z}_n^*$ is called a primitive root of $\mathbb{Z}_n^*$ if the order of a is $\phi(n)$.
Not all groups possess primitive roots e.g. $\mathbb{Z}_n^*$ where $n = pq$ and p, q are odd primes.
If $\mathbb{Z}_n^*$ possesses a primitive root a, then $\mathbb{Z}_n^*$ is called cyclic.
If a is a primitive root of $\mathbb{Z}_n^*$ and $b \in \mathbb{Z}_n^*$ then $\exists x$ s.t. $a^x \equiv b \pmod{n}$. This x is called the discrete logarithm or index of b modulo n to the base a.
Examples for $\mathbb{Z}_7^*$:
3 is a primitive root: $\{3^0, 3^1, 3^2, 3^3, 3^4, 3^5\} = \{1, 3, 2, 6, 4, 5\} = \mathbb{Z}_7^*$
2 is not a primitive root: $\{2^0, 2^1, 2^2, 2^3, 2^4, 2^5\} = \{1, 2, 4\} \neq \mathbb{Z}_7^*$

Primitive Roots
A primitive root exists in $\mathbb{Z}_n^*$ iff n has a value 2, 4, p^k or $2p^k$ for some odd prime p and integer k.
To determine whether a is a primitive root of $\mathbb{Z}_n^*$, we need to show for all prime factors $p_1, \ldots, p_k$ of $\phi(n)$ that:

$$\forall i \in \{1 \ldots k\} : a^{\phi(n)/p_i} \neq 1$$

This can be determined using modular exponentiation.
For a prime p the number of primitive roots mod p is $\phi(p-1)$

4.7 Quadratic Residues

Quadratic Residues
An integer q is called a quadratic residue modulo n if there exists an integer x such that:

$$x^2 \equiv q \pmod{n}$$

Integer x is called the square root of $q \pmod{n}$.
If no such integer x exists, q is called a quadratic nonresidue modulo n.

Example (n = 11):

x	0	1	2	3	4	5	6	7	8	9	10
$x^2 \pmod{11}$	0	1	4	9	5	3	3	5	9	4	1

There are six quadratic residues modulo 11: 0, 1, 3, 4, 5, and 9.
There are five quadratic non-residues modulo 11: 2, 6, 7, 8, 10.

Quadratic Residues
If p is a prime exactly half of the numbers in $\mathbb{Z}_p^*$ are quadratic residues.
Euler's Criterion: Given odd prime p and $q \in \mathbb{Z}_p^*$:

- q is a quadratic residue iff $q^{(p-1)/2} \equiv 1 \pmod{p}$.
- q is quadratic nonresidue, iff $q^{(p-1)/2} \equiv -1 \pmod{p}$.

A quadratic residue $q \in \mathbb{Z}_p^*$ cannot be a primitive root, since $q^{(p-1)/2} \equiv 1 \pmod{p}$ and the order of a primitive root is $p-1$.

Quadratic Residues Modulo $n = pq$
Let $n = pq$ where p and q are large primes.
If $a \in \mathbb{Z}_n^*$ is a quadratic residue modulo n, then a has exactly four square roots modulo n in $\mathbb{Z}_n^*$.
Therefore exactly a quarter of the numbers in $\mathbb{Z}_n^*$ are quadratic residues modulo n.

4.8 Calculating Modular Square Roots

Legendre's Symbol
If p is a prime and a is an integer.

Legendre's symbol $\left(\dfrac{a}{p}\right) = \begin{cases} 0, & \text{if } a|p \\ +1, & \text{if } a \text{ is a quadratic residue modulo } p \\ -1, & \text{if } a \text{ is a quadratic non-residue modulo } p \end{cases}$

By Euler's criterion: $\left(\frac{a}{p}\right) = a^{(p-1)/2} \pmod{p}$.

Legendre's Symbol
Properties of Legendre's symbol:

1. $a \equiv b \pmod{p} \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
3. $\left(\frac{1}{p}\right) = 1$
4. $\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod{4} \\ -1, & \text{if } p \equiv 3 \pmod{4} \end{cases}$
5. $\left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}$
6. If p and q are odd primes: $\left(\frac{p}{q}\right) = (-1)^{((p-1)/2)((q-1)/2)}\left(\frac{q}{p}\right)$

Jacobi's Symbol
Jacobi's symbol is a generalization of Legendre's symbol to composite numbers.
If n is odd with prime factorization $n = p_1 \times p_2 \times \ldots \times p_k$ and a is relatively prime to n:
Jacobi's symbol $\left(\frac{a}{n}\right) = \left(\frac{a}{p_1}\right) \times \left(\frac{a}{p_2}\right) \times \ldots \times \left(\frac{a}{p_k}\right)$
$\left(\frac{a}{n}\right) = -1 \Rightarrow a$ is a quadratic non-residue
$\left(\frac{a}{n}\right) = 1 \not\Rightarrow a$ is a quadratic residue

Jacobi's Symbol
Properties of Jacobi's symbol:

1. $a \equiv b \pmod{n} \Rightarrow \left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$
2. $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$
3. $\left(\frac{a}{mn}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{n}\right)$
4. $\left(\frac{1}{n}\right) = 1$
5. $\left(\frac{-1}{n}\right) = (-1)^{(n-1)/2}$
6. $\left(\frac{2}{n}\right) = (-1)^{(n^2-1)/8}$
7. If m and n are odd co-primes: $\left(\frac{m}{n}\right) = (-1)^{((m-1)/2)((n-1)/2)}\left(\frac{n}{m}\right)$

Computing Square Roots Modulo a Prime
If the Legendre symbol is -1, then there is no solution.
If p is a prime and a is a quadratic residue modulo p then:

$$a^{(p-1)/2} \equiv 1 \pmod{p} \text{ (by Euler's criterion).}$$

Multiplying both sides by a:

$$a^{(p+1)/2} \equiv a \pmod{p}$$

Taking the square roots of both sides:

$$\pm a^{(p+1)/4} \equiv \sqrt{a} \pmod{p}$$

If $p \equiv 3 \pmod{4}$, then $(p+1)/4$ is an integer, and this can be used to calculate the square root.

Computing Square Roots Modulo a Prime
If p is a prime s.t. $p \equiv 5 \pmod{8}$ and a is a quadratic residue modulo p then:

$$a^{(p-1)/2} \equiv 1 \pmod{p} \text{ (by Euler's criterion).}$$

so $a^{(p-1)/4} \equiv \pm 1 \pmod{p}$
If $a^{(p-1)/4} \equiv 1 \pmod{p}$ then:

$$\sqrt{a} = a^{(p+3)/8} \pmod{p}$$

If $a^{(p-1)/4} \equiv -1 \pmod{p}$ then:

$$\sqrt{a} = 2a(4a)^{(p-5)/8} \pmod{p}$$

If p is a prime s.t. $p \equiv 1 \pmod{8}$ and a is a quadratic residue modulo p the probabilistic Shanks' algorithm can be used to calculate $\sqrt{a}$.

Computing Square Roots Modulo $n = pq$
If the Jacobi symbol is -1, then there is no solution.
If a is a quadratic residue and $\sqrt{a} \pmod{p} = \pm x$ and $\sqrt{a} \pmod{q} = \pm y$, then we can use the Chinese Remainder Theorem to calculate $\sqrt{a}$.
Example: Compute the square root of 3 modulo 11×13
$\sqrt{3} \pmod{11} = \pm 5$
$\sqrt{3} \pmod{13} = \pm 4$
Using the Chinese Remainder Theorem, we can calculate the four square roots as 82, 126, 17 and 61.