Part I

Basic Number Theory

1. Basic Number Theory

Modular Arithmetic

Let n a positive integer. Then $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$.

Addition and multiplication are defined as the usual addition and multiplication. If the result is equal to or larger than n, we reduce modulo n (divide by n and take the reminder).

Example

In $\mathbb{Z}_6$, we have:

$$4 + 5 = 9 \bmod 6 = 3$$
$$4 \times 5 = 20 \bmod 6 = 2$$

Greatest Common Divisor (gcd)

Definition (Greatest Common Divisor (gcd))

Given the integers x, y, we define $d = \gcd(x, y)$ as the largest number that divides both x and y.

Definition (Relatively Prime)

If $\gcd(x, y) = 1$, we say that x and y are *relatively prime*.

Modular Inversion

Consider an element x in $\mathbb{Z}_n$. We call inverse of x an element y such that $xy \bmod n = 1$.
If the inverse exists, we will indicate it as x^{-1}.

Example

In $\mathbb{Z}_7$ the inverse of 2 is $2^{-1} = 4$. In fact, $2 \times 4 = 8 \bmod 7 = 1$.

- The integer x has an inverse mod n if and only if $\gcd(x, n) = 1$.
- The set $\mathbb{Z}_n^*$ contains all the elements in $\mathbb{Z}_n$ that have an inverse mod n.

How to Solve Modular Equations

Consider the equation in which all the coefficients and unknowns are defined in $\mathbb{Z}_n$:

$$ax + b = 0 \pmod{n}$$

Let $d = \gcd(a, n)$, there are three cases:

- If $d = 1$, then $x = -ba^{-1} \bmod n$
- If $d > 1$ and $b \bmod d = 0$, then there are d solutions
  1. Solve the new equation
     $$(a/d)x_0 + (b/d) = 0 \pmod{n/d}$$
  2. The d solutions to the original equation are
     $$x_0, x_0 + (n/d), x_0 + 2(n/d), \ldots, x_0 + (d-1)(n/d)$$
- If $d > 1$ and $b \bmod d > 0$, then there is no solution.

1. Basic Number Theory

Fermat's Little Theorem

Let p be a prime number. Then $\mathbb{Z}_p^* = \{1, \ldots, p-1\}$.
For any integer in $\mathbb{Z}_p^*$, we have $x^{p-1} \bmod p = 1$.

Example

Multiplying both sides by x, we have $x^p \bmod p = x$.
Dividing by both sides by x, we have $x^{p-2} \bmod p = x^{-1}$.

Fermat Primality Test

- Let n be an integer. It is unknown if n is prime. Let a be a random integer smaller than n.
- Calculate $a^{n-1} \bmod n$.
    - If n is prime, then $a^{n-1} = 1$.
    - If n is composite, then a^{n-1} may or may not be equal to 1.
- Thus
    - If $a^{n-1} \neq 1$, then n is composite.
    - If $a^{n-1} = 1$, n may be prime or not.

There is a non-negligible probability that $a^{n-1} = 1$ for some a even if n is composite. The probability that this happens for multiple values of a drops quickly.

Fermat Primality Test

Fermat Primality Test

Input: integer n, candidate prime
Choose a from $\mathbb{Z}_n$
if $a^n \bmod n = 1$ **then**
    return n may be prime
else
    return n is composite
end if

The test is repeated several times to reduce the probability of error.
This test has a fairly large probability of error. In practice, there are other tests with lower probability of error.

Generating Random Primes

Problem: generate a random prime number with l bits. No fast deterministic algorithm. Standard practice is

1. Generate a random odd integer n with l bits
2. Apply non-deterministic test of primality.

How long does it take to find a prime? It depends on the density of prime numbers.

Let $\pi(x)$ be the number of primes smaller than x. Gauss approximation says that $\pi(x) \sim x/\log x$.

The density of primes is $\pi(x)/x = 1/\log x$.

Thus, the average number of attempts to find a prime smaller than x is $\log x$. For $x = 2^l$, the average number of attempts is $l \log 2$.