# Number Theory

Patrick Chen

Feb 26, 2025

## Divisor

A number $d$ is a divisor of a number $a$ if there is an integer $c$ such that $a = dc$. If $d$ is a divisor of $a$ it is denoted as as $d \mid a$.

- If $d \mid a$ and $d \mid b$ then $d \mid a + b$
- If $d \mid a$ and $a \mid b$ then $d \mid b$
- If $d \mid a$ then $d \mid an$ for all $n \in \mathbb{Z}$
- For all $m, n \in \mathbb{Z}$, if $d \mid a$ and $d \mid b$ then $d \mid ma + nb$

### Division

Let $a$ and $d$ be integers where $d > 0$. There exists unique integers $q$ and $r$ where $0 \leq r < d$ such that $a = q \cdot d + r$.

$$\begin{aligned}
a &= q \cdot d + r \\
\text{where } q &= a \text{ div } d \\
r &= a \bmod d \\
a \text{ div } d &= \left\lfloor \frac{a}{d} \right\rfloor \\
a \bmod d &= a - d\left\lfloor \frac{a}{d} \right\rfloor
\end{aligned}$$

### Modulo

For $a, b, m \in \mathbb{Z}$, we say $a$ is congruent to $b$ modulo $m$ if $m \mid a - b$. Congruence is denoted by $a \equiv b \pmod{m}$

### Example

Prove that $a \equiv b \pmod{m}$ if and only if $a \bmod m = b \bmod m$

$$\begin{aligned}
a &= q_1 m + r_1 \\
b &= q_2 m + r_2
\end{aligned}$$

$$
\begin{aligned}
& a \equiv b \pmod{m} \\
\Rightarrow\ & m \mid a - b \\
\Rightarrow\ & m \mid (q_1 - q_2)m + r_1 - r_2 \\
\Rightarrow\ & m \mid r_1 - r_2 \\
\Rightarrow\ & r_1 - r_2 = 0 && \text{since } r_1, r_2 < m \\
\Rightarrow\ & r_1 = r_2 \\
\Rightarrow\ & q_1 + r_1 \bmod m = q_2 + r_2 \bmod m \\
\Rightarrow\ & a \bmod m = b \bmod m
\end{aligned}
$$

$$
\begin{aligned}
& a \pmod{m} = b \pmod{m} \\
\Rightarrow\ & r_1 = r_2 \\
\Rightarrow\ & a - b = (q_1 - q_2)m + r_1 - r_2 \\
\Rightarrow\ & a - b = (q_1 - q_2)m \\
\Rightarrow\ & m \mid a - b \\
\Rightarrow\ & a \equiv m \pmod{m}
\end{aligned}
$$

### Modulo Ring

$\mathbb{Z}_m$ is the set of all natural numbers less than $m$

$$\mathbb{Z}_m = \{0, , 1, \dots, m-1\}$$

Addition and multiplication in the modulo $m$ ring $(\mathbb{Z}_m, +_m, \times_m)$ is defined as follows

$$
\begin{aligned}
a +_m b &= (a + b) \mod m \\
a \times_m b &= (ab) \mod m
\end{aligned}
$$

## Integer Representations

Let the base $b$ be an integer such that $b > 1$. All numbers $n$ can be represented uniquely with digits $a_0, \dots, a_k$ where all $0 \leq a_i < b$ for all $i \in (0, 1, \dots, k)$ in base $b$. A numbers $n$ represented in a base $b$ is written as $(n)_b$.

$$n = a_k b^k + a_{k-1} b^{k-1} + \dots + a_2 b^2 + a_1 b + a_0$$

For example, 25 in base 10 and base 2 are written as follows.

$$
\begin{aligned}
(25)_{10} &= 2 \cdot 10 + 5 = 25 \\
(11001)_2 &= 1 \cdot 2^4 + 1 \cdot 2^3 + 1 = 25
\end{aligned}
$$

## Converting between bases

Conversion between bases can be done with repeated division and remainder. The remainder will be the right-most digit. This process can be repeated until the quotient is zero.

$$
\begin{aligned}
n &= bq_0 + a_0 \\
q_0 &= bq_1 + a_1 \\
q_1 &= bq_2 + a_2 \\
&\vdots \\
q_n &= bq_{n+1} + a_n && \text{where } q_{n+1} = 0 \\
n &= b(b(\ldots(bq_{n+1} + a_n)\cdots + a_1) + a_0 \\
&= b(b(\ldots(a_n)\ldots) + a_1) + a_0 \\
&= b^n a_n + b^{n-1}a_{n-1} + \cdots + b^2 a_2 + ba_1 + a_0
\end{aligned}
$$

## Example

Write 43 in base 16

$$
\begin{aligned}
43 &= \underbrace{2}_{q_0} \cdot 16 + \underbrace{11}_{a_0} \\
2 &= \underbrace{0}_{q_1} \cdot 16 + \underbrace{2}_{a_1} \\
\therefore\ 42 &= 2 \cdot 16 + 11 = \texttt{0x2b}
\end{aligned}
$$

## Addition and Multiplication

The digit-wise addition and multiplication algorithms used in base 10 also work in other bases.

## Example

Calculate $12 + 8$ in base 3

$$
\begin{aligned}
12 &= (110)_3 \\
8 &= (22)_3
\end{aligned}
$$

$$
\begin{array}{r}
1\phantom{10} \\
110 \\
+\ \ 22 \\
\hline
202
\end{array}
$$

$$(202)_3 = 2 \cdot 9 + 0 \cdot 3 + 2 = 20$$

## Example 2

Calculate $12 \times 8$ in base 2

$$
\begin{aligned}
12 &= (1100)_2 \\
8 &= (1000)_2
\end{aligned}
$$

$$\begin{array}{r} 1\,1\,0\,0 \\ \times 1\,0\,0\,0 \\ \hline 0\,0\,0\,0 \\ 0\,0\,0\,0\phantom{0} \\ 0\;0\,0\,0\phantom{00} \\ +1\,1\;0\,0\phantom{000} \\ \hline 1\,1\;0\,0\,0\,0\,0 \end{array}$$

### Modular Exponentiation

A quick way to compute large exponents of numbers is to split the number into its base 2 components.

$$\begin{aligned} n &= n_k 2^k + \cdots + n_2 \cdot 2^2 + n_1 \cdot 2 + n_0 \\ x^n &= x^{(n_k 2^k + \cdots + n_2 \cdot 2^2 + n_1 \cdot 2 + n_0)} \\ &= x^{n_k 2^k} x^{n_{k-1} 2^{k-1}} \dots x^{n_2 \cdot 2^2} x^{n_1 \cdot 2} x^{n_0} \end{aligned}$$

This reduces the amount of multiplications

$$x^n = \underbrace{x \cdot x \cdot \cdots \cdot x}_{n} = \underbrace{x^{n_k 2^k} x^{n_{k-1} 2^{k-1}} \dots x^{n_2 \cdot 2^2} x^{n_1 \cdot 2} x^{n_0}}_{\lceil \log_2(n) \rceil}$$

## Prime Numbers

A number $p$ is prime if the only positive factors of $p$ are 1 and $p$. If a number is not prime, it is called composite. There are infinitely many prime numbers. Prime numbers in the form $2^p - 1$ where $p$ is a prime is called a Mersenne prime.

### Distribution of primes

Let $\pi(x)$ be the number of primes $p$ such that $p \leq x$.

$$\pi(x) \approx \frac{x}{\ln x} \text{ as } x \to \infty$$

### Fundamental Theorem of Arithmetic

Every integer greater than 2 is either prime or can be written uniquely as the product of two or more prime numbers.

### Prime Factorization

The prime factorization of a integer $n > 1$ is in the form of products of exponents of primes. Every prime factorization is unique.

$$n = p_1^{e_1} p_2^{e_2} \dots p_k^{e_k}$$
$$\text{where } p_i \text{ is prime for all } i$$

Any composite number $n$ must have at least one prime factors $p_i$ such that $p_i \leq \sqrt{n}$.

## Example

Prove there are infinitely many primes.
Suppose there are only a finite number of primes.

$$P = \{p_1, p_2, \dots, p_k\}$$

This means there is some largest prime $p_k$.

$$\text{let } q = p_1 p_2 p_3 \dots p_k + 1$$

Since all primes are greater than 2, no primes divide $q$.
Therefore $q$ is a prime.
Since $q$ is the product of primes plus one, $q$ is larger than $p_k$
This contradicts that a largest prime exists, therefore there is no largest prime.
Therefore there are infinitely many primes.

## GCD and LCM

The greatest common divisor (GCD) of two positive integers $a$ and $b$ is the largest integer $n$ such that $n \mid a$ and $n \mid b$.

$$\begin{aligned} a &= p_1^{a_1} p_2^{a_2} \dots p_n^{a_n} \\ b &= p_1^{b_1} p_2^{b_2} \dots p_n^{b_n} \\ \gcd(a,b) &= p_1^{\min(a_1,b_1)} p_2^{\min(a_2,b_2)} \dots p_n^{\min(a_n,b_n)} \end{aligned}$$

The least common multiple (LCM) of positive integers $a$ and $b$ is the smallest positive integer $n$ such that $a \mid n$ and $b \mid n$

$$\begin{aligned} a &= p_1^{a_1} p_2^{a_2} \dots p_n^{a_n} \\ b &= p_1^{b_1} p_2^{b_2} \dots p_n^{b_n} \\ \operatorname{lcm}(a,b) &= p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \dots p_n^{\max(a_n,b_n)} \end{aligned}$$

## Euclidean Algorithm

$$\gcd(a,b) = \gcd(a, b \mod a)$$

Assume that $b \geq a$.

$$\begin{aligned}
b &= qa + r \\
\text{let } d &= gcd(a,b) \\
&\Rightarrow d \mid a,\ d \mid b \\
&\Rightarrow d \mid b - qa \\
&\Rightarrow d \mid r \\
&\Rightarrow d \mid \text{ gcd}(a,r) = \text{gcd}(a, b \mod a) \\
\text{let } d_1 &= gcd(a,r) \\
&\Rightarrow d_1 \mid r = b - qa \\
&\Rightarrow d_1 \mid b \\
&\Rightarrow d_1 \mid gcd(a,b) \\
&\Rightarrow d_1 \mid d \\
d \mid d_1 \text{ and } d_1 \mid d &\Rightarrow gcd(a,b) = gcd(a, b \mod a)
\end{aligned}$$

This identity can be used to create a fast gcd algorithm.

```
function gcd(a,b)
    x = a
    y = b
    while y != 0
        r = x mod y
        x = y
        y = r
    return x
```

## Bezout's Theorem

If $a$ and $b$ are positive integers then there exists integers $r$ and $s$ such that $gcd(a,b) = ra + sb$. The values $r, s$ can be found by using the extended Euclidean algorithm.

```
def xgcd(a, b):
    s0, s1, t0, t1 = 1, 0, 0, 1
    while b != 0:
        q, r = divmod(a, b)
        a, b = b, r
        s0, s1 = s1, s0 - q * s1
        t0, t1 = t1, s0 - q * t1
    return a, s0, t_0
```

## Example

Prove that if $a$, $b$, and $c$ are positive integers such that $a|bc$ and $gcd(a,b) = 1$ then $a|c$

$$\begin{aligned}
ra + sb &= 1 \\
\Rightarrow rac + sbc &= c
\end{aligned}$$

Since $a|bc$, $a|sbc$

$$\Rightarrow a|rac + sbc$$
$$\Rightarrow a|c$$

## Congruence

Let $m \in \mathbb{Z}^+$ and $a, b, c \in \mathbb{Z}$. If $ac \equiv bc \pmod{m}$ and $\gcd(c, m) = 1$, then $a \equiv b \pmod{m}$

$$ac \equiv bc \pmod{m}$$
$$m \mid ac - bc = c(a - b)$$

since $gcd(c, m) = 1$, then $m \mid a - b$ and by definition $a = b \pmod{m}$

## Product of GCD and LCM

The product of the gcd and lcm is the product of the inputs.

$$ab = gcd(a, b)lcm(a, b)$$

$$\begin{aligned}
a &= p_1^{a_1} p_2^{a_2} \dots p_k^{a_k} \\
b &= p_1^{b_1} p_2^{b_2} \dots p_k^{b_k} \\
gcd(a, b) &= p_1^{min(a_1,b_1)} \dots p_k^{min(a_k,b_k)} \\
lcm(a, b) &= p_1^{max(a_1,b_1)} \dots p_k^{max(a_k,b_k)} \\
gcd(a, b)lcm(a, b) &= \left(p_1^{min(a_1,b_1)} \dots p_k^{min(a_k,b_k)}\right)\left(p_1^{max(a_1,b_1)} \dots p_k^{max(a_k,b_k)}\right) \\
&= p_1^{max(a_1,b_1)+max(a_1,b_1)} \dots p_k^{min(a_k,b_k)+max(a_k,b_k)} \\
&= p_1^{a_1+b_1} \dots p_k^{a_1+b_1} \\
&= \left(p_1^{a_1} \dots p_k^{a_k}\right)\left(p_1^{b_1} \dots p_k^{b_k}\right) \\
&= ab
\end{aligned}$$

## Modular Inverse

The inverse of a number $a$ mod m is a number $b$ such that $ab = 1 \pmod{m}$. If $a$ and $m$ is coprime, then the inverse exists and is unique.

$$\begin{aligned}
gcd(a, m) &= 1 \\
sa + tm &= 1 && \text{for some } s, t \\
sa + tm &= 1 \pmod{m} \\
sa &= 1 \pmod{m} && \text{since } tm \text{ is zero } \pmod{m} \\
s &= a^{-1} \pmod{m}
\end{aligned}$$

Proof of uniqueness

$$\begin{aligned}
\text{Suppose } s = a^{-1}, s' &= a^{-1} \\
sa = 1 &= s'a \pmod{m} \\
sa &= s'a \pmod{m} \\
s &= s' \pmod{m} && \text{because } a \text{ is coprime with } m
\end{aligned}$$