目录

初等数论

Fulcrum4Math

1 整除理论

1.1 整除

定义 1.1.1 整除 (Divides)
设 $a, b : \mathbb{Z}$, $a \neq 0$, 定义 a **整除** b 当且仅当: $\exists n : \mathbb{Z}, b = an$, 记作 $a \mid b$.
定义 a **不整除** b 当且仅当: $\neg(a \mid b)$, 记作 $a \nmid b$.

性质 1.1.1.1 整除的偏序性 (Partial Order of Divisibility)
整除关系是偏序关系.

性质 1.1.1.2 整除的线性性 (Linearity of Divisibility)
整除关系是线性关系.

性质 1.1.1.3 整除的绝对值性质
设, 则: .

定理 1.1.2 余数唯一性
设 $a, b : \mathbb{Z}$, $a > 0$, 则: $\exists! r : \mathbb{Z}/a\mathbb{Z}, \exists! n : \mathbb{Z}, b = an + r$.

定义 1.1.3 不完全商
设 $a, b : \mathbb{Z}$, $a \neq 0$, 定义 b **除以** a **的不完全商**为: , 记作 b/a.

定义 1.1.4 余数 (Remainder)
设 $a, b : \mathbb{Z}$, $a > 0$, 定义 b **除以** a **的余数**为: $b - a \cdot (b/a)$, 记作 $b\%a$.

1.2 最大公因数

定义 1.2.1 最大公因数 (Greatest Common Divisor)
设 $a, b : \mathbb{Z}$, $a \neq 0$, $b \neq 0$, 定义 a **和** b **的最大公因数**为: $\max\{d | d \mid a \wedge d \mid b\}$, 记作 $\gcd(a, b)$.
设 S 是 $\mathbb{Z}$ 上的集合, $S \neq \{0\}$, 定义 S **的最大公因数**为: $\max\{d | \forall n \in S, d \mid n\}$, 记作 $\gcd S$.

性质 1.2.1.1 最大公因数非负

性质 1.2.1.2
设 $a, b, c, q : \mathbb{Z}$, $q \neq 0$, $a = bq + c$, 则: $\gcd(a, b) = \gcd(b, c)$.

性质 1.2.1.3
设 $a, b, n : \mathbb{Z}$, 则: $\gcd(an, bn) = n \gcd(a, b)$.

定理 1.2.2 Euclid 辗转相除法

定理 1.2.3 Bezout 定理 (Bezout's Theorem)

定义 1.2.4 互素 (Coprime)
设 $a, b : \mathbb{Z}$, $a \neq 0 \vee b \neq 0$, 定义 a 与 b 互素当且仅当: $\gcd(a, b) = 1$.
设 S 是 $\mathbb{Z}$ 上的集合, $S \neq \{0\}$, 定义 S 互素当且仅当: $\gcd S = 1$.

定义 1.2.5 最小公倍数 (Least Common Multiple)

定理 1.2.6 两数之积等于其最大公因数与最小公倍数之积

1.3 素数

定义 1.3.1 素数与合数 (Prime Number & Composite Number)
设 $p : \mathbb{Z}$, $p > 1$, 定义 p 是素数当且仅当: $\forall a, b \in \mathbb{Z}, p = ab \Rightarrow a = 1 \vee a = p$.
设 $n : \mathbb{Z}$, $n > 1$, 定义 n 是合数当且仅当: $\exists a, b \in \mathbb{Z}, n = ab \wedge a \neq 1 \wedge a \neq n$.

性质 1.3.1.1

性质 1.3.1.2
设, 则: .

性质 1.3.1.3 Eratosthenes 筛法

定理 1.3.2 素数无穷性 (Infinitude of Primes)
.

定理 1.3.3 算术基本定理 (Fundamental Theorem of Arithmetic)

1.4 整数部分

定义 1.4.1 整数部分 / Gauss 函数 (Gauss Function)
设 $x:\mathbb{R}$, 定义 x 的**整数部分 / Gauss 函数**为: $\max\{n|n\in\mathbb{Z}\wedge n\le x\}$, 记作 $\lfloor x\rfloor$.

2 不定方程

2.1 二元一次不定方程

定理 2.1.1 二元一次不定方程整数解系
设 $a,b,c,x_0,y_0:\mathbb{Z}$, $a\neq 0$, $b\neq 0$, $ax_0+by_0=c$, 则:

$$\forall x,y:\mathbb{Z},ax+by=c\implies\exists k:\mathbb{Z},\begin{cases}x=x_0+\dfrac{b}{\gcd(a,b)}k\\ y=y_0-\dfrac{a}{\gcd(a,b)}k\end{cases}$$

定理 2.1.2 二元一次不定方程有解的充要条件
设 $a,b,c:\mathbb{Z}$, $a\neq 0$, $b\neq 0$, 则:

$$\exists x,y:\mathbb{Z},ax+by=c\iff\gcd(a,b)\mid c$$

定理 2.1.3 二元一次不定方程解的形状

2.2 多元一次不定方程

定理 2.2.1

3 同余方程

4 原根与指标