数论基础

本文对于数论的开头部分做一个简介。

整除

定义

设 $a,b\in\mathbf{Z}$，$a\neq 0$。如果 $\exists q\in\mathbf{Z}$，使得 $b=aq$，那么就说 b 可被 a **整除**，记作 $a\mid b$；b 不被 a 整除记作 $a\nmid b$。

整除的性质：

- $a\mid b\iff -a\mid b\iff a\mid -b\iff |a|\mid |b|$
- $a\mid b\wedge b\mid c\implies a\mid c$
- $a\mid b\wedge a\mid c\iff \forall x,y\in\mathbf{Z},a\mid (xb+yc)$
- $a\mid b\wedge b\mid a\implies b=\pm a$
- 设 $m\neq 0$，那么 $a\mid b\iff ma\mid mb$。
- 设 $b\neq 0$，那么 $a\mid b\implies |a|\leq |b|$。
- 设 $a\neq 0,b=qa+c$，那么 $a\mid b\iff a\mid c$。

约数

定义

若 $a\mid b$，则称 b 是 a 的 **倍数**，a 是 b 的 **约数**。

0 是所有非 0 整数的倍数。对于整数 $b\neq 0$，b 的约数只有有限个。

平凡约数（平凡因数）：对于整数 $b\neq 0$，± 1、$\pm b$ 是 b 的平凡约数。当 $b=\pm 1$ 时，b 只有两个平凡约数。

对于整数 $b\neq 0$，b 的其他约数称为真约数（真因数、非平凡约数、非平凡因数）。

约数的性质：

- 设整数 $b\neq 0$。当 d 遍历 b 的全体约数的时候，$\frac{b}{d}$ 也遍历 b 的全体约数。

- 设整数 $b>0$，则当 d 遍历 b 的全体正约数的时候，$\frac{b}{d}$ 也遍历 b 的全体正约数。

在具体问题中，**如果没有特别说明，约数总是指正约数。**

带余数除法

余数

设 a,b 为两个给定的整数，$a\neq 0$。设 d 是一个给定的整数。那么，一定存在唯一的一对整数 q 和 r，满足 $b=qa+r, d\leq r<|a|+d$。

无论整数 d 取何值，r 统称为余数。$a\mid b$ 等价于 $a\mid r$。

一般情况下，d 取 0，此时等式 $b=qa+r, 0\leq r<|a|$ 称为带余数除法（带余除法）。这里的余数 r 称为最小非负余数。

余数往往还有两种常见取法：

- 绝对最小余数：d 取 a 的绝对值的一半的相反数。即 $b=qa+r, -\frac{|a|}{2}\leq r<|a|-\frac{|a|}{2}$。
- 最小正余数：d 取 1。即 $b=qa+r, 1\leq r<|a|+1$。

带余数除法的余数只有最小非负余数。**如果没有特别说明，余数总是指最小非负余数。**

余数的性质：

- 任一整数被正整数 a 除后，余数一定是且仅是 0 到 $(a-1)$ 这 a 个数中的一个。
- 相邻的 a 个整数被正整数 a 除后，恰好取到上述 a 个余数。特别地，一定有且仅有一个数被 a 整除。

最大公约数与最小公倍数

关于公约数、公倍数、最大公约数与最小公倍数，四个名词的定义，见 最大公约数。

Warning

一些作者认为 0 和 0 的最大公约数无定义，其余作者一般将其视为 0。C++ STL 的实现中采用后者，即认为 0 和 0 的最大公约数为 0[5]。

最大公约数有如下性质：

- $(a_1,\dots,a_n)=(|a_1|,\dots,|a_n|)$；

- $(a,b)=(b,a)$；
- 若 $a\neq 0$，则 $(a,0)=(a,a)=|a|$；
- $(bq+r,b)=(r,b)$；
- $(a_1,\dots,a_n)=((a_1,a_2),a_3,\dots,a_n)$。进而 $\forall 1<k<n-1,\ (a_1,\dots,a_n)=((a_1,\dots,a_k),(a_{k+1},\dots,a_n))$；
- 对不全为 0 的整数 $a_1,\dots,a_n$ 和非零整数 m，$(ma_1,\dots,ma_n)=|m|(a_1,\dots,a_n)$；
- 对不全为 0 的整数 $a_1,\dots,a_n$，若 $(a_1,\dots,a_n)=d$，则 $(a_1/d,\dots,a_n/d)=1$；
- $(a^n,b^n)=(a,b)^n$。

最大公约数还有如下与互素相关的性质：

- 若 $b|ac$ 且 $(a,b)=1$，则 $b\mid c$；
- 若 $b|c$、$a|c$ 且 $(a,b)=1$，则 $ab\mid c$；
- 若 $(a,b)=1$，则 $(a,bc)=(a,c)$；
- 若 $(a_i,b_j)=1,\ \forall 1\leq i\leq n,1\leq j\leq m$，则 $\left(\prod_i a_i,\prod_j b_j\right)=1$。特别地，若 $(a,b)=1$，则 $(a^n,b^m)=1$；
- 对整数 $a_1,\dots,a_n$，若 $\exists v\in\mathbf{Z},\ \prod_i a_i=v^m$，且 $(a_i,a_j)=1,\ \forall i\neq j$，则 $\forall 1\leq i\leq n,\ \sqrt[m]{a_i}\in\mathbf{Z}$。

最小公倍数有如下性质：

- $[a_1,\dots,a_n]=[|a_1|,\dots,|a_n|]$；
- $[a,b]=[b,a]$；
- 若 $a\neq 0$，则 $[a,1]=[a,a]=|a|$；
- 若 $a\mid b$，则 $[a,b]=|b|$；
- $[a_1,\dots,a_n]=[[a_1,a_2],a_3,\dots,a_n]$。进而 $\forall 1<k<n-1,\ [a_1,\dots,a_n]=[[a_1,\dots,a_k],[a_{k+1},\dots,a_n]]$；
- 若 $a_i\mid m,\ \forall 1\leq i\leq n$，则 $[a_1,\dots,a_n]\mid m$；
- $[ma_1,\dots,ma_n]=|m|[a_1,\dots,a_n]$；
- $[a,b,c][ab,bc,ca]=[a,b][b,c][c,a]$；
- $[a^n,b^n]=[a,b]^n$。

最大公约数和最小公倍数可以组合出很多奇妙的等式，如：

- $(a,b)[a,b]=|ab|$；
- $(ab,bc,ca)[a,b,c]=|abc|$；
- $\dfrac{(a,b,c)^2}{(a,b)(b,c)(a,c)}=\dfrac{[a,b,c]^2}{[a,b][b,c][a,c]}$。

这些性质均可通过定义或 唯一分解定理 证明，其中使用唯一分解定理的证明更容易理解。

互素

定义

若 $(a_1, a_2) = 1$，则称 a_1 和 a_2 **互素（既约）**。

若 $(a_1, \ldots, a_k) = 1$，则称 $a_1, \ldots, a_k$ **互素（既约）**。

多个整数互素，不一定两两互素。例如 6、10 和 15 互素，但是任意两个都不互素。

互素的性质与最大公约数理论：裴蜀定理（Bézout's identity）。见 裴蜀定理。

辗转相除法

辗转相除法是一种算法，也称 Euclid 算法。见 最大公约数。

素数与合数

关于素数的算法见 素数。

定义

设整数 $p \neq 0, \pm 1$。如果 p 除了平凡约数外没有其他约数，那么称 p 为 **素数（不可约数）**。

若整数 $a \neq 0, \pm 1$ 且 a 不是素数，则称 a 为 **合数**。

p 和 $-p$ 总是同为素数或者同为合数。**如果没有特别说明，素数总是指正的素数。**

整数的因数是素数，则该素数称为该整数的素因数（素约数）。

素数与合数的简单性质：

- 大于 1 的整数 a 是合数，等价于 a 可以表示为整数 d 和 e（$1 < d, e < a$）的乘积。
- 如果素数 p 有大于 1 的约数 d，那么 $d = p$。
- 大于 1 的整数 a 一定可以表示为素数的乘积。
- 对于合数 a，一定存在素数 $p \leq \sqrt{a}$ 使得 $p \mid a$。
- 素数有无穷多个。
- 所有大于 3 的素数都可以表示为 $6n \pm 1$ 的形式[1]。

算术基本定理

算术基本引理

设 p 是素数，$p \mid a_1a_2$，那么 $p \mid a_1$ 和 $p \mid a_2$ 至少有一个成立。

算术基本引理的逆命题稍加修改也可以得到素数的另一种定义。

素数的另一种定义

对整数 $p \neq 0, \pm 1$，若对任意满足 $p \mid a_1a_2$ 的整数 a_1, a_2 均有 $p \mid a_1$ 或 $p \mid a_2$ 成立，则称 p 是素数。

Tip

这个定义的动机可以从 素理想 中找到。

算术基本定理（唯一分解定理）

设正整数 a，那么必有表示：

$$a = p_1p_2 \cdots p_s$$

其中 $p_j (1 \leq j \leq s)$ 是素数。并且在不计次序的意义下，该表示唯一。

标准素因数分解式

将上述表示中，相同的素数合并，可得：

$$a = {p_1}^{\alpha_1}{p_2}^{\alpha_2} \cdots {p_s}^{\alpha_s}, p_1 < p_2 < \cdots < p_s$$

称为正整数 a 的标准素因数分解式。

算术基本定理和算术基本引理，两个定理是等价的。

同余

定义

设整数 $m \neq 0$。若 $m \mid (a-b)$，称 m 为 **模数（模）**，a 同余于 b 模 m，b 是 a 对模 m 的 **剩余**。记作 $a \equiv b \pmod{m}$。

否则，a 不同余于 b 模 m，b 不是 a 对模 m 的剩余。记作 $a \not\equiv b \pmod{m}$。

这样的等式，称为模 m 的同余式，简称 **同余式**。

根据整除的性质，上述同余式也等价于 $a \equiv b \pmod{(-m)}$。

如果没有特别说明，模数总是正整数。

式中的 b 是 a 对模 m 的剩余，这个概念与余数完全一致。通过限定 b 的范围，相应的有 a 对模 m 的最小非负剩余、绝对最小剩余、最小正剩余。

同余的性质：

- 同余是 等价关系，即同余具有
  - 自反性：$a \equiv a \pmod{m}$。
  - 对称性：若 $a \equiv b \pmod{m}$，则 $b \equiv a \pmod{m}$。
  - 传递性：若 $a \equiv b \pmod{m}, b \equiv c \pmod{m}$，则 $a \equiv c \pmod{m}$。
- 线性运算：若 $a, b, c, d \in \mathbf{Z}, m \in \mathbf{N}^*, a \equiv b \pmod{m}, c \equiv d \pmod{m}$ 则有：
  - $a \pm c \equiv b \pm d \pmod{m}$。
  - $a \times c \equiv b \times d \pmod{m}$。
- 设 $f(x) = \sum_{i=0}^{n} a_i x^i$ 和 $g(x) = \sum_{i=0}^{n} b_i x^i$ 是两个整系数多项式，$m \in \mathbf{N}^*$，且 $a_i \equiv b_i \pmod{m}$, $0 \leq i \leq n$，则对任意整数 x 均有 $f(x) \equiv g(x) \pmod{m}$。进而若 $s \equiv t \pmod{m}$，则 $f(s) \equiv g(t) \pmod{m}$。
- 若 $a, b \in \mathbf{Z}, k, m \in \mathbf{N}^*, a \equiv b \pmod{m}$, 则 $ak \equiv bk \pmod{mk}$。
- 若 $a, b \in \mathbf{Z}, d, m \in \mathbf{N}^*, d \mid a, d \mid b, d \mid m$，则当 $a \equiv b \pmod{m}$ 成立时，有 $\frac{a}{d} \equiv \frac{b}{d} \left(\bmod \frac{m}{d} \right)$。
- 若 $a, b \in \mathbf{Z}, d, m \in \mathbf{N}^*, d \mid m$，则当 $a \equiv b \pmod{m}$ 成立时，有 $a \equiv b \pmod{d}$。
- 若 $a, b \in \mathbf{Z}, d, m \in \mathbf{N}^*$，则当 $a \equiv b \pmod{m}$ 成立时，有 $(a, m) = (b, m)$。若 d 能整除 m 及 a, b 中的一个，则 d 必定能整除 a, b 中的另一个。

还有性质是乘法逆元。见 乘法逆元。

C/C++ 的整数除法和取模运算

在 C/C++ 中，整数除法和取模运算，与数学上习惯的取模和除法不一致。

对于所有标准版本的 C/C++，规定在整数除法中：

1. 当除数为 0 时，行为未定义；
2. 否则 `(a / b) * b + a % b` 的运算结果与 `a` 相等。

也就是说，取模运算的符号取决于除法如何取整；而除法如何取整，这是实现定义的（由编译器决定）。

从 C99[3]和 C++11[4]标准版本起，规定 **商向零取整**（舍弃小数部分）；取模的符号即与被除数相同。从此以下运算结果保证为真：

```
5 % 3 == 2;
5 % -3 == 2;
-5 % 3 == -2;
-5 % -3 == -2;
```

快速乘

在素性测试与质因数分解中，经常会遇到模数在 `long long` 范围内的乘法取模运算。为了避免运算中的整型溢出问题，本节介绍一种可以处理模数在 `long long` 范围内，不需要使用 `__int128` 且复杂度为 $O(1)$ 的「快速乘」。

我们发现：

$$a \times b \bmod m = a \times b - \left\lfloor \frac{ab}{m} \right\rfloor \times m$$

我们巧妙运用 `unsigned long long` 的自然溢出：

$$a \times b \bmod m = a \times b - \left\lfloor \frac{ab}{m} \right\rfloor \times m = \left(a \times b - \left\lfloor \frac{ab}{m} \right\rfloor \times m \right) \bmod 2^{64}$$

于是在算出 $\left\lfloor \frac{ab}{m} \right\rfloor$ 后，两边的乘法和中间的减法部分都可以使用 `unsigned long long` 直接计算，现在我们只需要解决如何计算 $\left\lfloor \frac{ab}{m} \right\rfloor$。

我们考虑先使用 `long double` 算出 $\frac{a}{m}$ 再乘上 b。

既然使用了 `long double`，就无疑会有精度误差。极端情况就是第一个有效数字（二进制下）在小数点后一位。在 64 位系统中，`long double` 通常表示为 80 位扩展精度浮点数（即符号为 1 位，指数为 15 位，尾数为 64 位），所以 `long double` 最多能精确表示的有效位数为 64^2。所以 $\frac{a}{m}$ 最差从第 65 位开始出错，误差范围为 $\left(-2^{-64}, 2^{-64}\right)$。乘上 b 这个 64 位整数，误差范围为 $(-0.5, 0.5)$，再加上 0.5 误差范围为 $(0, 1)$，取整后误差范围位 $\{0, 1\}$。于是乘上 $-m$ 后，误差范围变成 $\{0, -m\}$，我们需要判断这两种情况。

因为 m 在 `long long` 范围内，所以如果计算结果 r 在 $[0, m)$ 时，直接返回 r，否则返回 $r + m$，当然你也可以直接返回 $(r + m) \bmod m$。

代码实现如下：

```
long long binmul(long long a, long long b, long long m) {
  unsigned long long c =
      (unsigned long long)a * b -
      (unsigned long long)((long double)a / m * b + 0.5L) * m;
  if (c < m) return c;
  return c + m;
}
```

如今，绝大多数测评系统所配备的 C/C++ 编译器已支持 `__int128` 类型，因此也可以利用 Barrett Reduction 进行快速乘。之所以不直接将乘数类型提升至 `__int128` 后取模计算是因为此方法仍然可以节省一次时间可观的 `__int128` 类型取模。

同余类与剩余系

为方便讨论，对集合 A, B 和元素 r，我们引入如下记号：

- $r + A := \{r + a : a \in A\}$；
- $rA := \{ra : a \in A\}$；
- $A + B := \{a + b : a \in A, b \in B\}$；
- $AB := \{ab : a \in A, b \in B\}$。

同余类

对非零整数 m，把全体整数分成 $|m|$ 个两两不交的集合，且同一个集合中的任意两个数模 m 均同余，我们把这 $|m|$ 个集合均称为模 m 的 **同余类** 或 **剩余类**。用 $r \bmod m$ 表示含有整数 r 的模 m 的同余类。

不难证明对任意非零整数 m，上述划分方案一定存在且唯一。

由同余类的定义可知：

- $r \bmod m = \{r + km : k \in \mathbf{Z}\}$；
- $r \bmod m = s \bmod m \iff r \equiv s \pmod m$；
- 对任意 $r, s \in \mathbf{Z}$，要么 $r \bmod m = s \bmod m$，要么 $(r \bmod m) \cap (s \bmod m) = \varnothing$；
- 若 $m_1 \mid m$，则对任意整数 r 均有 $r + m\mathbf{Z} \subseteq r + m_1\mathbf{Z}$。

注意到同余是等价关系，所以同余类即为同余关系的等价类。

我们把模 m 的同余类全体构成的集合记为 $\mathbf{Z}_m$，即

$$\mathbf{Z}_m := \{r \bmod m : 0 \le r < m\}$$

不难发现：

- 对任意整数 a，$a+\mathbf{Z}_m=\mathbf{Z}_m$；
- 对任意与 m 互质的整数 b，$b\mathbf{Z}_m=\mathbf{Z}_m$。

由 商群 的定义可知 $\mathbf{Z}_m=\mathbf{Z}/m\mathbf{Z}$，所以有时我们也会用 $\mathbf{Z}/m\mathbf{Z}$ 表示 $\mathbf{Z}_m$。

由 抽屉原理 可知：

- 任取 $m+1$ 个整数，必有两个整数模 m 同余。
- 存在 m 个两两模 m 不同余的整数。

由此我们给出完全剩余系的定义：

（完全）剩余系

对 m 个整数 $a_1,a_2,\dots,a_m$，若对任意的数 x，有且仅有一个数 a_i 使得 x 与 a_i 模 m 同余，则称这 m 个整数 $a_1,a_2,\dots,a_m$ 为模 m 的 **完全剩余系**，简称 **剩余系**。

我们还可以定义模 m 的：

- 最小非负（完全）剩余系：$0,\dots,m-1$；
- 最小正（完全）剩余系：$1,\dots,m$；
- 绝对最小（完全）剩余系：$-\lfloor m/2\rfloor,\dots,-\lfloor -m/2\rfloor-1$；
- 最大非正（完全）剩余系：$-m+1,\dots,0$；
- 最大负（完全）剩余系：$-m,\dots,-1$。

若无特殊说明，一般我们只用最小非负剩余系。

我们注意到如下命题成立：

- 在模 m 的任意一个同余类中，任取两个整数 a_1,a_2 均有 $(a_1,m)=(a_2,m)$。

考虑同余类 $r \bmod m$，若 $(r,m)=1$，则该同余类的所有元素均与 m 互质，这说明我们也许可以通过类似方式得知所有与 m 互质的整数构成的集合的结构。

既约同余类

对同余类 $r \bmod m$，若 $(r,m)=1$，则称该同余类为 **既约同余类** 或 **既约剩余类**。

我们把模 m 既约剩余类的个数记作 $\varphi(m)$，称其为 Euler 函数。

我们把模 m 的既约同余类全体构成的集合记为 $\mathbf{Z}_m^*$，即

$$\mathbf{Z}_m^* := \{r \bmod m : 0 \le r < m, (r, m) = 1\}$$

> **Warning**
>
> 对于任意的整数 a 和与 m 互质的整数 b，$b\mathbf{Z}_m^* = \mathbf{Z}_m^*$，但是 $a + \mathbf{Z}_m^*$ 不一定为 $\mathbf{Z}_m^*$。这一点与 $\mathbf{Z}_m$ 不同。

由 抽屉原理 可知：

- 任取 $\varphi(m) + 1$ 个与 m 互质的整数，必有两个整数模 m 同余。
- 存在 $\varphi(m)$ 个与 m 互质且两两模 m 不同余的整数。

由此我们给出既约剩余系的定义：

> **既约剩余系**
>
> 对 $t = \varphi(m)$ 个整数 $a_1, a_2, \ldots, a_t$，若 $(a_i, m) = 1,\ \forall 1 \le i \le t$，且对任意满足 $(x, m) = 1$ 的数 x，有且仅有一个数 a_i 使得 x 与 a_i 模 m 同余，则称这 t 个整数 $a_1, a_2, \ldots, a_t$ 为模 m 的 **既约剩余系**、**缩剩余系** 或 **简化剩余系**。

类似地，我们也可以定义最小非负既约剩余系等概念。

若无特殊说明，一般我们只用最小非负既约剩余系。

剩余系的复合

对正整数 m，我们有如下定理：

- 若 $m = m_1 m_2,\ 1 \le m_1, m_2$，令 Z_{m_1}, Z_{m_2} 分别为模 m_1, m_2 的 **完全** 剩余系，则对任意与 m_1 互质的 a 均有：

  $$Z_m = aZ_{m_1} + m_1 Z_{m_2}.$$

  为模 m 的 **完全** 剩余系。进而，若 $m = \prod_{i=1}^{k} m_i,\ 1 \le m_1, m_2, \ldots, m_k$，令 $Z_{m_1}, \ldots, Z_{m_k}$ 分别为模 $m_1, \ldots, m_k$ 的 **完全** 剩余系，则：

  $$Z_m = \sum_{i=1}^{k} \left(\prod_{j=1}^{i-1} m_j \right) Z_{m_i}.$$

  为模 m 的 **完全** 剩余系。

证明

只需证明对任意满足 $ax + m_1y \equiv ax' + m_1y' \pmod{m_1m_2}$ 的 $x, x' \in Z_{m_1}$，$y, y' \in Z_{m_2}$，都有：

$$ax + m_1y = ax' + m_1y'.$$

实际上，由 $m_1 \mid m_1m_2$，我们有 $ax + m_1y \equiv ax' + m_1y' \pmod{m_1}$，进而 $ax \equiv ax' \pmod{m_1}$，由 $(a, m_1) = 1$ 可知 $x \equiv x' \pmod{m_1}$，进而有 $x = x'$。

进一步，$m_1y \equiv m_1y' \pmod{m_1m_2}$，则 $y \equiv y' \pmod{m_2}$，即 $y = y'$。

因此，

$$ax + m_1y = ax' + m_1y'.$$

- 若 $m = m_1m_2,\ 1 \leq m_1, m_2, (m_1, m_2) = 1$，令 $Z^*_{m_1}, Z^*_{m_2}$ 分别为模 m_1, m_2 的 **既约** 剩余系，则：

  $$Z^*_m = m_2Z^*_{m_1} + m_1Z^*_{m_2}.$$

  为模 m 的 **既约** 剩余系。

Tip

该定理等价于证明 Euler 函数为 积性函数。

证明

令 Z_{m_1}, Z_{m_2} 分别为模 m_1, m_2 的完全剩余系，我们已经证明了

$$Z_m = m_2 Z_{m_1} + m_1 Z_{m_2}$$

为模 m 的完全剩余系。令 $M = \{a \in Z_m : (a, m) = 1\} \subseteq Z_m$，显然 M 为模 m 的既约剩余系，所以我们只需证明 $M = Z_m^*$ 即可。

显然 $Z_m^* \subseteq Z_m$。

任取 $m_2 x + m_1 y \in M$，其中 $x \in Z_{m_1}$ 且 $y \in Z_{m_2}$，有 $(m_2 x + m_1 y, m_1 m_2) = 1$，由 $(m_1, m_2) = 1$ 可得

$$1 = (m_2 x + m_1 y, m_1) = (m_2 x, m_1) = (x, m_1),$$
$$1 = (m_2 x + m_1 y, m_2) = (m_1 y, m_2) = (y, m_2).$$

因此可得 $x \in Z_{m_1}^*$ 且 $y \in Z_{m_2}^*$，即 $M \subseteq Z_m^*$。

任取 $m_2 x + m_1 y \in Z_m^*$，其中 $x \in Z_{m_1}^*$ 且 $y \in Z_{m_2}^*$，有 $(x, m_1) = 1$ 且 $(y, m_2) = 1$，由 $(m_1, m_2) = 1$ 可得

$$(m_2 x + m_1 y, m_1) = (m_2 x, m_1) = (x, m_1) = 1,$$
$$(m_2 x + m_1 y, m_2) = (m_1 y, m_2) = (x, m_2) = 1,$$

因此可得 $(m_2 x + m_1 y, m_1 m_2) = 1$，即 $Z_m^* \subseteq M$。

综上所述，

$$Z_m^* = m_2 Z_{m_1}^* + m_1 Z_{m_2}^*.$$

为模 m 的 **既约** 剩余系。

数论函数

数论函数（也称算数函数）指定义域为正整数的函数。数论函数也可以视作一个数列。

积性函数

定义

在数论中，若函数 $f(n)$ 满足 $f(1) = 1$，且 $f(xy) = f(x)f(y)$ 对任意互质的 $x, y \in \mathbf{N}^*$ 都成立，则 $f(n)$ 为 **积性函数**。

在数论中，若函数 $f(n)$ 满足 $f(1) = 1$ 且 $f(xy) = f(x)f(y)$ 对任意的 $x, y \in \mathbf{N}^*$ 都成立，则 $f(n)$ 为 **完全积性函数**。

性质

若 $f(x)$ 和 $g(x)$ 均为积性函数，则以下函数也为积性函数：

$$
\begin{aligned}
h(x) &= f(x^p) \\
h(x) &= f^p(x) \\
h(x) &= f(x)g(x) \\
h(x) &= \sum_{d|x} f(d)g\left(\frac{x}{d}\right)
\end{aligned}
$$

对正整数 x，设其唯一质因数分解为 $x = \prod p_i^{k_i}$，其中 p_i 为质数。

若 $F(x)$ 为积性函数，则有 $F(x) = \prod F(p_i^{k_i})$。

若 $F(x)$ 为完全积性函数，则有 $F(x) = \prod F(p_i^{k_i}) = \prod F(p_i)^{k_i}$。

例子

- 单位函数：$\varepsilon(n) = [n = 1]$。（完全积性）
- 恒等函数：$\mathrm{id}_k(n) = n^k$，$\mathrm{id}_1(n)$ 通常简记作 $\mathrm{id}(n)$。（完全积性）
- 常数函数：$1(n) = 1$。（完全积性）
- 除数函数：$\sigma_k(n) = \sum_{d|n} d^k$。$\sigma_0(n)$ 通常简记作 $d(n)$ 或 $\tau(n)$，$\sigma_1(n)$ 通常简记作 $\sigma(n)$。
- 欧拉函数：$\varphi(n) = \sum_{i=1}^{n} [(i, n) = 1]$。
- 莫比乌斯函数：$\mu(n) = \begin{cases} 1 & n = 1 \\ 0 & \exists d > 1, d^2 \mid n \\ (-1)^{\omega(n)} & \text{otherwise} \end{cases}$，其中 $\omega(n)$ 表示 n 的本质不同质因子个数。

加性函数

定义

在数论中，若函数 $f(n)$ 满足 $f(1) = 0$ 且 $f(xy) = f(x) + f(y)$ 对任意互质的 $x, y \in \mathbf{N}^*$ 都成立，则 $f(n)$ 为 **加性函数**。

在数论中，若函数 $f(n)$ 满足 $f(1) = 0$ 且 $f(xy) = f(x) + f(y)$ 对任意的 $x, y \in \mathbf{N}^*$ 都成立，则 $f(n)$ 为 **完全加性函数**。

加性函数

本节中的加性函数指数论上的加性函数 (Additive function)，应与代数中的 Additive map 做区分。

性质

对正整数 x，设其唯一质因数分解为 $x=\prod p_i^{k_i}$，其中 p_i 为质数。

若 $F(x)$ 为加性函数，则有 $F(x)=\sum F(p_i^{k_i})$。

若 $F(x)$ 为完全加性函数，则有 $F(x)=\sum F(p_i^{k_i})=\sum F(p_i)\cdot k_i$。

例子

为方便叙述，令所有质数组成的集合为 P.

- 所有质因子数目：$\Omega(n)=\sum_{p|n}[p\in P]\sum_{k=1}^{\lceil\log_p n\rceil}[p^k\mid n\wedge p^{k+1}\nmid n]\cdot k$。（完全加性）
- 相异质因子数目：$\omega(n)=\sum_{p|n}[p\in P]$。
- 所有质因子之和：$a_0(n)=\sum_{p|n}[p\in P]\sum_{k=1}^{\lceil\log_p n\rceil}[p^k\mid n\wedge p^{k+1}\nmid n]\cdot kp$。（完全加性）
- 相异质因子之和：$a_1(n)=\sum_{p|n}[p\in P]\cdot p$。

参考资料与注释

1. 潘承洞，潘承彪。初等数论。北京大学出版社。

---

1. Are all primes (past 2 and 3) of the forms 6n+1 and 6n-1? ↩
2. 参见 C 语言小数表示法 - 维基百科 ↩
3. Arithmetic operators (C) - cppreference.com ↩
4. Arithmetic operators (C++) - cppreference.com ↩
5. std::gcd - cppreference.com ↩
