WEEKLY TIPS

知识小料

「电计 2203 班」周常规知识整理共享

ISSUE.
11

日期：2023-11-25
学科：离散数学

本文档给出《离散数学》被跳过的必备数论相关知识，对理解等价关系、划分、群论相关概念有帮助。请读者重点阅读举例部分，以便理解相关概念。

1 整除与约数相关

p185 **整除** a 整除 b，表示整数 b 除以 a 得到的结果是整数，记为 $a|b$；不整除记为 $a\nmid b$。

举例：$3|12$，$4|-16$，$-3|0$，$5\nmid 21$，$2\nmid -3$。

p185 **因数与倍数** 若 $a|b$，则称 a 是 b 的因数（也称 约数），b 是 a 的倍数。

举例：12 的正因数有 1,2,3,4,6,12，共六个。

p188 **最大公因数** 表示两个正整数的公因数中最大的一个，用 gcd 或 GCD 表示，记为 $\gcd\{a,b\}$，在不引起混淆的情况下也记为 (a,b)。多个数的最大公因数记法类似。其英文为 greatest common divisor。

举例：$\gcd\{4,6\}=2$，$\gcd\{8,12\}=4$，$\gcd\{1,3\}=1$。

思考：对于半群 $\langle \mathbf{N}^*,\odot\rangle$，其中 $a\odot b=\gcd\{a,b\}$，其零元为 1。

p190 **最小公倍数** 表示两个正整数的公倍数中最小的一个，用 lcm 或 LCM 表示，记为 $\mathrm{lcm}\{a,b\}$，在不引起混淆的情况下也记为 $[a,b]$。多个数的最小公倍数记法类似。其英文为 lowest common multiple。

举例：$\mathrm{lcm}\{4,6\}=12$，$\mathrm{lcm}\{8,12\}=24$，$\mathrm{lcm}\{1,3\}=3$。

思考：对于独异点 $\langle \mathbf{N}^*,\otimes\rangle$，其中 $a\otimes b=\mathrm{lcm}\{a,b\}$，其幺元为 1。

2 质数相关

p186 **质数与合数** 大于 1 且只能被 1 和它本身整除的数，称为质数（也称 素数）；否则称为合数。由此定义可知，正整数分为质数、合数和 1。

举例：2,3,5,7,11,13,17,19,23,29 等是质数，4,6,8,9 等是合数。

p188 **互质** 如果两个正整数的最大公因数为 1，则它们互质（也称 互素）。

举例：$\gcd\{25,36\}=1$，因此 25 和 36 互质，但其实它们都是合数。

p196 **欧拉函数 $\varphi(m)$** 小于或等于 m 且与 m 互质的正整数个数，记为 $\varphi(m)$，称为欧拉函数。

举例：$\varphi(6)=2$，因为在 $\{1,2,3,4,5,6\}$ 中，只有 1,5 与 6 互质。

思考：课本 p266 的定理 13.5.6：若 $\langle G, \odot\rangle$ 是 n 阶循环群，则其含有 $\varphi(n)$ 个生成元。例如，6 阶循环群 $\langle\{e,a,a^2,a^3,a^4,a^5\},\odot\rangle$ 中，a,a^5 可成为生成元（因为只有由 a 或 a^5 才可生成集合中的所有元素），共 2 个，即 $\varphi(6)$ 个。

3　余数与同余相关

p186 **带余数除法**　若 a,b 为两个整数，$b \neq 0$，则唯一地存在两个整数 q,r，使得 $a = bq+r$（余数 $0 \leqslant r < |b|$）。

举例：$7 \div 3 = 2 \cdots 1$，$7 = 3 \times 2 + 1$。

p192 **余数**　整数 a 除以正整数 m 得到的余数，记为 $a(\bmod m)$ 或 $a \bmod m$。

举例：$7(\bmod 3) = 1$，$14(\bmod 5) = 4$；$-14(\bmod 5) = 1$ 因为 $-14 = 5 \times (-3) + 1$。

p192 **同余**　给定正整数 m，若整数 a 和 b 除以 m 得到的余数相同，则称 a,b 同余，记为 $a \equiv b \pmod m$ 或者 $a \equiv_m b$。

举例：$1 \equiv 4 \pmod 3$，$0 \equiv -5 \pmod 5$，$-1 \not\equiv -2 \pmod 3$。

思考：(1) $\equiv_m$ 其实也是以符号表示的等价关系，定义 $\equiv_m := \{\langle x,y\rangle | x \equiv y \pmod m\}$。

(2) 同余运算满足下面的式子：

$$(a \pm b) \pmod m = (a(\bmod m) \pm b(\bmod m)) \pmod m$$
$$(a \times b) \pmod m = (a(\bmod m) \times b(\bmod m)) \pmod m$$

即对于加、减、乘运算，运算后的模数等于模数的运算。

(3) 若 $x_1 \equiv y_1(\bmod m)$，$x_2 \equiv y_2(\bmod m)$，则 $x_1 + x_2 \equiv y_1 + y_2(\bmod m)$。此所谓满足加法的代换性质（p244），因此群 $\langle \mathbf{Z}, +\rangle$ 的等价关系 $\equiv_m$ 事实上还是同余关系。这也正是「同余关系」一词的由来。

p195 **模 m 剩余类**　由模 m 余数相同的那些整数构成的集合，称为模 m 剩余类，用 $[r]$ 表示。

形式定义：$[r] := \{i | i \in \mathbf{Z} \land i \equiv r(\bmod m)\}$，其中 $0 \leqslant r \leqslant m-1$。

举例：$m=3$，比如模 3 余数都为 0 的那些整数有 $-3,0,3,6,\ldots$，我们说 $[0] = \{-3,0,3,6,\ldots\}$，再比如 $[1] = \{-2,1,4,7,\ldots\}$，$[2] = \{-1,2,5,8,\ldots\}$。事实上模 3 剩余类共有 3 个：$[0],[1],[2]$。一般地，模 m 剩余类共有 m 个，它们分别是 $[0],[1],\ldots,[m-1]$。

思考：(1) 对于等价关系 R，由元素 x 产生的等价类一般写成 $[x]_R$。对于“$\equiv_m$”这个用符号表示的等价关系，每一个模 m 剩余系 $[r]$ 就是一个等价类，即 $[r]_{\equiv_m}$。俗话说「物以类聚」——将两个整数聚在同一个模 m 剩余系的条件，就是它们对 m 的模数相同。

(2) 有了等价类，还可以对集合进行划分，产生商集，表示所有等价类构成的集合，记为 A/R（A 是集合，R 是等价关系）。在这里，我们可以用关系“$\equiv_m$”对 $\mathbf{Z}$ 进行划分，产生商集 $\mathbf{Z}/\equiv_m = \{[0],[1],\ldots,[m-1]\}$。这就相当于把 $\mathbf{Z}$ 分成 m 个「小团体」，每一个「小团体」内的整数对 m 的模数均相同。

你了解这些「基数」、「阶数」、「次数」吗？

- 集合 S 的基数（也称「势」），表示 S 含有的元素个数，记为 $|S|$。
- 运算 f 的阶（也称元数），表示 f 所接受的自变量个数。习惯上，用 $\odot$、$\otimes$ 等符号表示的运算是二元运算。
- 群 $\langle G, \odot\rangle$ 的阶数，表示集合 G 的元素个数（即 $|G|$）。一般来说有限群才有「阶数」这一说法。
- 群中元素 a 的阶（也称周期），表示满足 $a^k = e$ 的最小正整数 k。如不存在这样的 k，则称 a 的阶是无穷的。
- 循环群的生成元 g 的阶，表示满足 $g^k = e$ 的最小正整数 k。如不存在这样的 k，则称 g 的阶是无穷的。
- 置换 $p: X \to X$ 的阶表示 X 含有的元素个数（即 $|X|$）。
- 轮换 $p: X \to X$ 的阶表示其「发生变动」的元素个数。

  举例：$X = \{1,2,3,4,5\}$，$p = \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{bmatrix} = (1\ 2\ 4)$ 是 5 阶置换、3 阶轮换。这是因为 $|X| = 5$，且「发生变动」的元素有 3 个（即 1,2,4）。
- 对称群 $\langle S_n, \diamond\rangle$ 的次数表示其所依赖的置换集合 X 的基数（即 $|X|$），它的阶数就是 $|S_n|$，即这个群就是 n 次 $n!$ 阶对称群。

  举例：对称群 $\langle S_3, \diamond\rangle$，其集合 S_3 有 6 个置换 $\{p_1, p_2, p_3, p_4, p_5, p_6\}$（详见课本 p262 例 13.5.1），其复合运算 $\diamond$ 的运算表如课本 p263 页首所示。这些置换 p_i 所依赖的集合是 $X = \{1,2,3\}$，$|X| = 3$，因此对称群次数为 3；又因为 $|S_3| = 6$，因此对称群阶数为 6。