基礎數論

陳信睿

2023 年 7 月 21 日

定義 1 (同餘)**.** 給定兩整數 $a, b \in \mathbb{Z}$，n 爲正整數，若 $a-b$ 被 n 整除，則我們說 a 同餘 b，並寫爲

$$a \equiv b \pmod{n}。$$

在解決很多不定方程的問題時，我們常常對等號兩邊取同於某個質數 (如 2、3、5 等等) 或是一些小的合數 (如 4、6 等等)，因此同餘爲一個很好用的工具。

性質 1. *若* $a \equiv b \pmod{n}$ *且* $c \equiv d \pmod{n}$，*則*

1. $ac \equiv bd \pmod{n}$。
2. $a+c \equiv b+d \pmod{n}$。
3. $a-c \equiv b-d \pmod{n}$。

然而以上關係在除法不一定是對的，因爲除法的結果不一定還是整數。不過在 $n=p$ 爲一質數的狀況下，我們可以定義一個類似除法的運算，讓他在同餘的語言下是對的。若 p 爲一質數，我們把 $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z} := \{0, 1, \ldots, p-1\}$ 稱爲 p 的完全剩餘系。以下我們將證明，若 $k \in \mathbb{Z}_p$ 不爲 0，則存在 $h \in \mathbb{Z}_p$ 使得 $hk \equiv 1 \pmod{p}$。這樣我們就可以把 k^{-1} 定義爲 h。

定理 2 (貝祖定理/Bézout's identity)**.** *假設* a, b *爲非零整數，令* $d = \gcd(a, b)$ *爲* a, b *的最大公因數，則存在整數* x, y *使得*

$$ax + by = d。$$

證明. 考慮集合 $S := \{ax + by > 0 : x \in \mathbb{Z}, y \in \mathbb{Z}\}$。由於 $|a| \in S$，故 S 不爲空集合。假設 S 當中的最小元素爲 c，根據 S 的定義，存在整數 s, t 使得 $as + bt = c$。我們現在證明 c 就是 $\gcd(a, b)$。我們先證明 c 是 a, b 的公因數。

首先根據除法原理，我們寫下 $a = qc + r$，其中 $q \in \mathbb{N} \cup \{0\}$ 且 $0 \le r < c$，因此

$$r = a - qc = (1-qs)a + (-qt)b，$$

這強迫 $r = 0$，否則 $0 < r < c$ 且 $r \in S$，與 c 是最小元素的假設矛盾。因此，我們知道 c 是 a 的因數，同理，c 也是 b 因數。

現在，我們證明 c 是 a,b 的最大公因數。假設 k 爲 a,b 的公因數，我們即要證明 $k \leq c$。由於 k 爲 a,b 的公因數，存在整數 $u,v \in \mathbb{Z}$ 使得 $a = ku$，$b = kv$。現在我們有

$$c = as + bt = k(us + vt)。$$

我們推論 k 爲 c 的因數，故得證。 □

推論. 在 $\mathbb{Z}_p$ 中，每個非零元素 k 的反元素 k^{-1} 存在。

證明. 根據貝祖定理 (定理2)，我們知道，存在整數 $s,t \in \mathbb{Z}$ 使得

$$ks + pt = \gcd(k,p) = 1。$$

左右兩式取同餘 p，即可得到 $ks \equiv 1 \pmod p$。 □

另一個推論則是下面的定理：

定理 3 (威爾森定理/Wilson's theorem). *假設 p 爲一奇質數，則 $(p-1)! \equiv -1 \pmod p$。*

證明. 首先，我們可以將 $\{2,3,\ldots,p-2\}$ 中的元素兩兩配對，使得兩兩互爲 $\mathbb{Z}_p$ 下的反元素，故我們可以推論：

$$(p-1)! \equiv 1 \cdot (-1) \equiv -1 \pmod p。$$

□