關於同餘式的一個定理

楊武之

定理. 若 $f(x)$ 代表 $\frac{x^p-x}{2p}$; 又若 s, x, p, n 俱爲整數且 $s \geqq 0$, $x \geqq 0$, p 爲奇素數, $n > 0$; 則有一整數 $m = m(s, x, n, p)$ 存在適合於

$$0 \leqq m < p^n \quad \text{及} \quad s \equiv f(x+pm) \pmod{p^n}.$$

證明. 先設 $0 < m < p^n$. 則

$$f(x+pm) = \frac{1}{2p}\left[(x+pm)^p - (x+pm)\right] = f(x) + \frac{m}{2}\cdot r,$$

$$r = px^{p-1} + \binom{p}{2}x^{p-2}(pm) + \cdots\cdots + (pm)^{p-1} - 1.$$

因 $r \equiv -1 \pmod{p}$, 故 $\frac{m}{2}\cdot r \not\equiv 0 \pmod{p^n}$, 故

$$f(x+pm) \not\equiv f(x) \pmod{p^n}. \tag{1}$$

次設 k 爲整數且 $0 < k$, $0 < m-k < p^n$. 則由 (1)

$$f(x+pm) - f(x+pk) = f\left[(x+pk)+p(m-k)\right] - f(x+pk) \not\equiv 0 \pmod{p^n} \tag{2}$$

綜 (1) 與 (2) 得知

$$f(x),\ f(x+p.1),\ f(x+p.2),\cdots\cdots,\ f\left[x+p(p^n-1)\right] \tag{3}$$

之 p^n 個數彼此各無同餘 $(\bmod p^n)$. 故任給之整數 s 必與 (3) 中之唯一的一個有同餘 $(\bmod p^n)$.

附論1. 當 $p=3$ 時, $f(x)=\frac{x^3-x}{6}$ 代表所謂塔數(pyramidal numbers).應用本定理可證"凡整數皆可以九個或少於九個之塔數之和代表之."

附論2. (3)啓示一全付剩餘(mod p^n).