

第13章 補遺

13.1 孫子算経

【孫子算経】は、中国の南北朝時代(439–589)の成立と推定される著者不詳の算術書であり、その一題として、第6章の例6.6と同じ内容が書かれている。これが、定理6.5が中国の剰余定理と呼ばれる理由である。

該当部分の原文は次の通り（分かりやすいように句読点をほどこしてある）。

今有物、不知其数。三・三数之、剰二。五・五数之、剰三。七・七数之、剰二。

問物幾何？

答曰：二十三。

術曰：『三・三数之、剰二』、置一百四十。『五・五数之、剰三』、置六十三。『七・七数之、剰二』、置三十。并之、得二百三十三。以二百一十減之、即得。凡、三・三数之、剰一、則置七十。五・五数之、剰一、則置二十一。七・七数之、剰一、則置十五。一百六以上、以一百五減之、即得。

Wikipedia〈中国の剰余定理〉では、日本語によって次のように解説されている。

今物が有るが、その数はわからない。三つずつにして物を数えると、二余る。

五で割ると、三余る。七で割ると、二余る。物はいくつあるか？

答え：二十三。

解法：三で割ると、二余る数として、百四十と置く。五で割ると、三余る数として、六十三と置く。七で割ると、二余る数として、三十と置く。これらを足し合わせて、二百三十三を得る。これから二百十を引いて、答えを得る。一般に、三つずつにして物を数え、一余ると、その度に七十と置く。五で割った余りに二十一をかける。七で割った余りに十五をかける。百六以上ならば、百五を引くことで、答えを得る。

第6章の例6.6と比べると、解2と同じ趣旨の解答であることがわかる。さらに、最後の「一般に…」以降は、

$$35u_1 \equiv 1 \pmod{3}, \quad 21u_2 \equiv 1 \pmod{5}, \quad 15u_3 \equiv 1 \pmod{7}$$

の解 $(u_1, u_2, u_3) = (2, 1, 1)$ から得られる組 $(35u_1, 21u_2, 15u_3) = (70, 21, 15)$ を用いて

$$x \equiv a_1 \pmod{3}, \quad x \equiv a_2 \pmod{5}, \quad x \equiv a_3 \pmod{7}$$

の解 $x = 70a_1 + 21a_2 + 15a_3$ が一般的に得られることを説明している。

13.2 命題 8.5 の証明

m を素因数分解して $m = p_1^{e_1} \cdots p_r^{e_r}$ (p_i は相異なる素数, $e_i \geq 1$) と表せば, 定理 8.6 の公式より

$$\frac{\varphi(m)}{m} = \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \left(1 - \frac{1}{p_3}\right) \cdots \left(1 - \frac{1}{p_r}\right).$$

ここで $p_1 < p_2 < \cdots < p_r$ であるとしてよいが, このとき (ずいぶん荒っぽい評価だけれども) $2 \leq p_1, 3 \leq p_2, 4 \leq p_3, \dots, r+1 \leq p_r$ が成り立つ. よって,

$$\begin{aligned} \frac{\varphi(m)}{m} &\geq \left(1 - \frac{1}{2}\right) \left(1 - \frac{1}{3}\right) \left(1 - \frac{1}{4}\right) \cdots \left(1 - \frac{1}{r+1}\right) \\ &= \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{3}{4} \cdots \frac{r}{r+1} = \frac{1}{r+1}. \end{aligned}$$

一方, $m = p_1^{e_1} \cdots p_r^{e_r} \geq 2^{e_1 + \cdots + e_r} \geq 2^r$ (これも荒っぽいよね) より $\log_2 m \geq r$ だから,

$$\frac{\varphi(m)}{m} \geq \frac{1}{\log_2 m + 1}$$

すなわち, 左側の不等式が示された. 右側の不等式 $\varphi(m) \leq m - 1$ は φ の定義から明らかである. \square

13.3 補題 12.7 の証明

簡単のため, ζ_p を ζ と略記する. 整数係数多項式 $f(x)$ によって $f(\zeta)$ で表される複素数全体の集合が R であった. ところで, $\zeta^p = 1$ なので, $f(x)$ の次数は p 未満であるとしてよい. すなわち,

$$R = \{ a_0 + a_1\zeta + a_2\zeta^2 + \cdots + a_{p-1}\zeta^{p-1} \mid a_0, a_1, \dots, a_{p-1} \in \mathbf{Z} \}.$$

(実は, $p-1$ 次未満にできるが, 以下の議論には影響ないのでこのまま証明を続ける.) さて, $\alpha \in R \cap \mathbf{Q}$ を任意にとる. このとき, $\alpha\zeta^i \in R$ だから

$$\alpha\zeta^i = \sum_{j=0}^{p-1} a_{ij}\zeta^j \quad (i = 0, 1, \dots, p-1)$$

をみたく $a_{ij} \in \mathbf{Z}$ がとれる. p 次正方行列 $A = (a_{ij})$ を考えれば, 上式は

$$\alpha \begin{pmatrix} 1 \\ \zeta \\ \zeta^2 \\ \vdots \\ \zeta^{p-1} \end{pmatrix} = A \begin{pmatrix} 1 \\ \zeta \\ \zeta^2 \\ \vdots \\ \zeta^{p-1} \end{pmatrix}$$

と書き換えられ、これは α が A の固有値であることを示している。よって、 A の固有
多項式を $g(x)$ とすれば $g(\alpha) = 0$ である。 A の成分はすべて整数であるから、

$$g(x) = x^p + c_{p-1}x^{p-1} + \cdots + c_1x + c_0 \quad (c_i \in \mathbf{Z})$$

の形をしている。いま、 $\alpha \in \mathbf{Q}$ でもあったから、これを既約分数

$$\alpha = \frac{s}{t} \quad (s, t \in \mathbf{Z} : \text{互いに素, かつ } t \geq 1)$$

で表せば、 $g(\alpha) = 0$ より

$$\frac{s^p}{t^p} + c_{p-1} \frac{s^{p-1}}{t^{p-1}} + \cdots + c_1 \frac{s}{t} + c_0 = 0,$$

$$\therefore s^p + c_{p-1}s^{p-1}t + \cdots + c_1st^{p-1} + c_0t^p = 0.$$

よって、 $s^p \equiv 0 \pmod{t}$ となるから、もし $t \neq 1$ ならば、 s, t が互いに素であることに反
する。したがって $t = 1$ であり、 $\alpha = s \in \mathbf{Z}$ 。 α は $R \cap \mathbf{Q}$ から任意にとった元なので、
 $R \cap \mathbf{Q} \subset \mathbf{Z}$ が得られたことになる。逆の包含関係は明らかなので、補題 12.7 が証明さ
れた。 □