第15章　補遺

15.1　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，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**とよばれる理由である．

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。

ここに記された解法は，第 6 章，例 6.6 の**解 2** と同じ趣旨であることがわかる． さらに，最後の「一般に…」以降は，

$$35u_1 \equiv 1 \pmod 3, \qquad 21u_2 \equiv 1 \pmod 5, \qquad 15u_3 \equiv 1 \pmod 7$$

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

$$x \equiv a_1 \pmod 3, \qquad x \equiv a_2 \pmod 5, \qquad x \equiv a_3 \pmod 7$$

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．

15.2　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） $2 \leq p_1,\ 3 \leq p_2,\ 4 \leq p_3, \ldots,\ r+1 \leq p_r$ 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． □

15.3　奇素数べきを法とする原始根

この節では，第 10 章で書き残した奇素数のべきを法とする原始根について述べる．

定理 15.1 任意の奇素数 p と自然数 n に対して，法 p^n に関する原始根が存在する．

定理の証明のために，補題を 2 つ用意する．

補題 15.2 p を素数，n を 2 以上の自然数，g を法 p^{n-1} に関する原始根とする．もし $g^{\varphi(p^{n-1})} \not\equiv 1 \pmod{p^n}$ ならば，g は法 p^n に関する原始根である．

証明　自然数 k が $g^k \equiv 1 \pmod{p^n}$ をみたすと仮定して，$\varphi(p^n) | k$ を示せばよい．このとき，$g^k \equiv 1 \pmod{p^{n-1}}$ であるが，g が法 p^{n-1} に関する原始根，すなわち法 p^{n-1} に関する g の位数が $\varphi(p^{n-1})$ であることから，ある $l \in \boldsymbol{N}$ がとれて $k = l\varphi(p^{n-1})$ と書ける．ここで，$t = g^{\varphi(p^{n-1})} - 1$ とおけば，$g^{\varphi(p^{n-1})} \equiv 1 \pmod{p^{n-1}}$ より $p^{n-1} | t$，とくに，$n \geq 2$ より $t^2 \equiv t^3 \equiv \cdots \equiv 0 \pmod{p^n}$ だから

$$g^k = (g^{\varphi(p^{n-1})})^l = (1+t)^l \equiv 1 + lt \pmod{p^n}.$$

一方，はじめに $g^k \equiv 1 \pmod{p^n}$ を仮定していたので，$p^n | lt$ であるが，補題の条件 $g^{\varphi(p^{n-1})} \not\equiv 1 \pmod{p^n}$ より $p^n \nmid t$ でもあったから $p | l$ が導かれる．そこで $l = mp$ ($m \in \boldsymbol{N}$) とおけば，$k = mp\varphi(p^{n-1}) = m\varphi(p^n)$，よって k は $\varphi(p^n)$ の倍数である． □

補題 15.3 p を奇素数，g を法 p^2 に関する原始根とする． このとき，2 以上の任意の自然数 n に対して，$g^{\varphi(p^{n-1})} \not\equiv 1 \pmod{p^n}$ が成り立つ．

証明 n に関する数学的帰納法を用いる． まず，g が法 p^2 に関する原始根であることよりその位数が $\varphi(p^2)$ であり，$\varphi(p)$ がそれより小さいことから $g^{\varphi(p)} \not\equiv 1 \pmod{p^2}$，すなわち $n = 2$ のときは成り立つ． 次に，$n \geq 2$ のとき正しいとすると，オイラーの定理を援用して

$$g^{\varphi(p^{n-1})} = 1 + kp^{n-1}, \quad k \not\equiv 0 \pmod{p}$$

と書けることがわかる． ここで $\varphi(p^n) = p\varphi(p^{n-1})$ だから，

$$g^{\varphi(p^n)} = (1 + kp^{n-1})^p = 1 + kp^n + \sum_{j=2}^{p-1} {}_pC_j (kp^{n-1})^j + (kp^{n-1})^p.$$

いま，$j = 2, \ldots, p-1$ については $p | {}_pC_j$ かつ $n \leq 2(n-1) \leq j(n-1)$ であり，さらに $n + 1 \leq p(n-1)$ がいえるから，

$$\sum_{j=2}^{p-1} {}_pC_j (kp^{n-1})^j \equiv (kp^{n-1})^p \equiv 0 \pmod{p^{n+1}}$$

が成り立つ． さらに $k \not\equiv 0 \pmod{p}$ に注意すれば

$$g^{\varphi(p^n)} \equiv 1 + kp^n \not\equiv 1 \pmod{p^{n+1}}$$

が得られ，$n + 1$ のときも正しいことが導かれた． □

定理 15.1 の証明 $n = 1$ の場合は定理 10.9 で示されているので，法 p に関する原始根 g がとれる． もし $g^{p-1} \equiv 1 \pmod{p^2}$ ならば，

$$(g + p)^{p-1} \equiv g^{p-1} + (p-1)pg^{p-2} \equiv 1 - pg^{p-2} \not\equiv 1 \pmod{p^2}$$

であり，かつ $g + p$ も法 p に関する原始根なので，はじめから g は，$g^{\varphi(p)} = g^{p-1} \not\equiv 1 \pmod{p^2}$ をみたすものとしてよい． このとき，補題 15.2 によれば，g は法 p^2 に関する原始根でもある． そこで今度は補題 15.3 によって，任意の $n \geq 2$ に対して $g^{\varphi(p^{n-1})} \not\equiv 1 \pmod{p^n}$ が得られる． とくに $n = 3$ の場合を考えれば，再び補題 15.2 を用いて，g が法 p^3 に関しても原始根であることがわかる． さらに補題 15.2 を繰り返し適用すれば，定理の主張が示されることになる． □

上の証明をまとめると，奇素数 p について次のことがわかる．

- g が法 p に関する原始根ならば，g または $g + p$ は法 p^2 に関する原始根である．
- 法 p^2 に関する原始根は，任意の $n > 2$ について法 p^n に関する原始根でもある．

15.4　補題 13.6 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，

$$R = \left\{ a_0 + a_1\zeta + a_2\zeta^2 + \cdots + a_{p-1}\zeta^{p-1} \,\middle|\, a_0, a_1, \ldots, a_{p-1} \in \boldsymbol{Z} \right\}.$$

(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，$\alpha \in R \cap \boldsymbol{Q}$ を任意にとる． このとき，$\alpha\zeta^i \in R$ だから

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

をみたす $a_{ij} \in \boldsymbol{Z}$ 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，

$$g(x) = x^p + c_{p-1}x^{p-1} + \cdots + c_1 x + c_0 \qquad (c_i \in \boldsymbol{Z})$$

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

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

で表せば，$g(\alpha) = 0$ より

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

$$\therefore \quad s^p + c_{p-1}s^{p-1}t + \cdots + c_1 s t^{p-1} + c_0 t^p = 0.$$

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，$\alpha = s \in \boldsymbol{Z}$． α は $R \cap \boldsymbol{Q}$ から任意にとった元なので，$R \cap \boldsymbol{Q} \subset \boldsymbol{Z}$ 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 13.6 が証明された． □