# 数論からの問題二つ

三浦午次郎

## I. 既約剰余系の元の位数について

いくつかの既約剰余系に共通な元の位数の間の関係について調べてみよう。

〔補助定理〕 $(a, p) = 1$ で

(1) $a^n \equiv 1 \pmod{p} \rightarrow \mathrm{ord}_p a \mid n$

(2) $a \equiv 1 \pmod{p} \rightarrow \sum_{i=0}^{p-1} a^i \equiv 0 \pmod{p}$

(3) $\left.\begin{array}{l} a \equiv 1 \pmod{p} \\ \sum_{i=0}^{n-1} a^i \equiv 0 \pmod{p} \end{array}\right\} \rightarrow p \mid n$

(証明)

$\mathrm{ord}_p a = \lambda$ で $n$ をわった商を $q$, 余りを $r$, とすると

$$n = \lambda q + r \quad 0 \leqq r < \lambda$$

$$a^n = (a^\lambda)^q \cdot a^r \equiv 1 \pmod{p}$$

$a^\lambda \equiv 1 \pmod{p}$ より

$$a^r \equiv 1 \pmod{p}$$

$r \neq 0$ とすると $\lambda$ の最小性に矛盾するから

$r = 0$, $n = \lambda q$ 即ち

$$\mathrm{ord}_p a \mid n \cdots\cdots (1)$$

又 $a \equiv 1 \pmod{p}$ より $a^i \equiv 1 \pmod{p}$

$\therefore$ $\sum_{i=0}^{p-1} a^i \equiv p \pmod{p}$

$$\sum_{i=0}^{p-1} a^i \equiv 0 \pmod{p} \cdots\cdots (2)$$

同様にして

$\sum_{i=0}^{n-1} a^i \equiv n \equiv 0 \pmod{p}$ より

$$p \mid n \cdots\cdots (3)$$

〔定理〕 1

$(a, pq) = 1 \rightarrow \mathrm{ord}_{\{p, q\}} a = \{\mathrm{ord}_p a, \mathrm{ord}_q a\}$

(証明)

$\mathrm{ord}_p a = \lambda$, $\mathrm{ord}_p a = \mu$, $\mathrm{ord}_{\{p, q\}} a = \nu$,

$\{\lambda, \mu\} = \sigma = \lambda\lambda' = \mu\mu'$ とおくと

$$a^\nu \equiv 1 \ (\{\mathrm{mod}\ p, q\})$$

$\therefore$ $a^\nu \equiv 1 \pmod{p}, \pmod{q}$

〔補定〕(1) から $\lambda \mid \nu,\ \mu \mid \nu$

$\therefore \quad \{\lambda,\ \mu\} = \sigma \mid \nu$ ……(1)

又 $a^{\sigma} = (a^{\lambda})^{\lambda'} \equiv 1 \pmod{p}$

$a^{\sigma} = (a^{\mu})^{\mu'} \equiv 1 \pmod{q}$

$\therefore \quad a^{\sigma} \equiv 1 \pmod{\{p,\ q\}}$

〔補定〕(1) から $\nu \mid \sigma$ ……(2)

(1), (2) から $\nu = \sigma$

即ち $\mathrm{ord}_{\{p,\ q\}}\, a = \{\mathrm{ord}_p a,\ \mathrm{ord}_q a\}$

〔定理〕2.

$(a,\ pq) = 1,\ (p,\ q) = 1 \rightarrow \mathrm{ord}_{pq} a = \{\mathrm{ord}_p a,\ \mathrm{ord}_q a\}$

(証明)

$(p,\ q) = 1$ より $\{p,\ q\} = pq$, よって前定理から明らかである。

〔定理〕3.

$(a,\ pq) = 1,\ (p,\ q) = d$

$\mathrm{ord}_p a = \lambda,\ \mathrm{ord}_q a = \mu,\ \mathrm{ord}_{pq} a = \nu,\ \{\lambda,\ \mu\} = \sigma$

$d \left| \dfrac{a^{\sigma} - 1}{\{p,\ q\}} \right. \rightarrow \nu = \sigma$

(証明)

〔定理〕1 から $\{p,\ q\} \mid (a^{\sigma} - 1)$

よって $d \left| \dfrac{a^{\sigma} - 1}{\{p,\ q\}} \right.$ から $d.\ \{p,\ q\} \mid (a^{\sigma} - 1)$

然るに $(p,\ q)\ \{p,\ q\} = pq$, よって $pq \mid (a^{\sigma} - 1)$

$\therefore$〔補定〕(1) から $\nu \mid \sigma$ ……(1)

逆に $a^{\nu} \equiv 1 \pmod{pq}$ より

$a^{\nu} \equiv 1 \pmod{\{p,\ q\}}$

$\therefore$〔補定〕(1) から $\sigma \mid \nu$ ……(2)

(1), (2) から $\nu = \sigma$

即ち $\mathrm{ord}_{pq} a = \{\mathrm{ord}_p a,\ \mathrm{ord}_q a\}$

〔定理〕4.

$(a,\ pq) = 1.\ (p,\ q) = d$

$\mathrm{ord}_p a = \lambda,\ \mathrm{ord}_q a = \mu,\ \mathrm{ord}_{pq} a = \nu,\ \{\lambda,\ \mu\} = \sigma$

$\left(d, \dfrac{a^{\sigma} - 1}{\{p,\ q\}}\right) = g < d \rightarrow \nu = \dfrac{d}{g}.\ \sigma$

(証明)

仮定から $a^{\nu} \equiv 1 \pmod{pq}$

$\therefore \quad a^{\nu} \equiv 1 \pmod{\{p,\ q\}}$

〔定理〕1 から $\sigma \mid \nu,\ \nu = n\sigma$ ……(1)

逆に $a^{n\sigma} \equiv 1 \pmod{pq}$

とすると

$a^{n\sigma} - 1 = (a^{\sigma})^{n} - 1 = (a^{\sigma} - 1) \sum_{i=0}^{n-1} (a^{\sigma})^{i} \equiv 0 \pmod{pq}$ ……(2)

$(p,\ q) = d$ より

$p = p'd,\ q = q'd,\ (p',\ q') = 1,\ \{p,\ q\} = p'q'd$

$\dfrac{a^\sigma-1}{\{p,\ q\}}=A$ とおくと $(d,\ A)=g$ より

$$d=d'g,\quad A=A'g,\ (d'A')=1$$

$a^\sigma-1=\{p,\ q\}\ A=p'q'dgA'$, $\sum_{i=0}^{n-1}(a^\sigma)^i=B$ を (2) に代入して

$$p'q'dgA'B\equiv 0\ (\mathrm{mod}\ p'q'd^2)$$

$$\therefore\quad gA'B\equiv 0\ (\mathrm{mod}\ d'g)$$

$$A'B\equiv 0\ (\mathrm{mod}\ d')$$

$(A',\ d')=1$ より

$$B\equiv 0\ (\mathrm{mod}\ d')$$

又 $a^\sigma\equiv 1\ (\mathrm{mod}\ p)$ より $\quad a^\sigma\equiv 1\ (\mathrm{mod}\ d')$

∴〔補定〕(3) から

$$B=\sum_{i=0}^{n-1}(a^\sigma)^i\equiv n\ (\mathrm{mod}\ d')$$

$$\therefore\quad d'\mid n \qquad \cdots\cdots(3)$$

(1), (3) から $\quad \nu=md'\sigma \qquad \cdots\cdots(4)$

次に (4) において $\quad m=1$ とすると

$$a^{d'\sigma}-1=(a^\sigma-1)\sum_{i=0}^{d'-1}(a^\sigma)^i,\quad \sum_{i=0}^{d'-1}(a^\sigma)^i\equiv 0\ (\mathrm{mod}\ d')$$

$$\therefore\quad a^{d'\sigma}-1=p'q'dgA'B'd'$$

$d'g=d$ を代入して

$$=p'q'd^2A'B'=pqA'B'$$

即ち $\quad pq\mid(a^{d'\sigma}-1)$

$$\therefore\quad \nu=d'\sigma=\frac{d}{g}\cdot\sigma$$

次に $p=q$ であるときは如何なる関係になるかを調べよう。

〔定理〕5.

$(a,\ p)=1,\qquad \mathrm{ord}_p a=\lambda,\ \mathrm{ord}_{p^2}a=\nu,$

$$p\ \Big|\ \frac{a^\lambda-1}{p}\rightarrow\nu=\lambda$$

(証明)

$p\ \Big|\ \dfrac{a^\lambda-1}{p}$ より $\quad a^\lambda\equiv 1\ (\mathrm{mod}\ p^2)$

∴〔補定〕(1) から $\quad \nu\mid\lambda \qquad \cdots\cdots(1)$

又 $\quad a^\nu\equiv 1\ (\mathrm{mod}\ p^2)$ より

$$a^\nu\equiv 1\ (\mathrm{mod}\ p)$$

∴〔補定〕(1) から $\quad \lambda\mid\nu \qquad \cdots\cdots(2)$

(1), (2) より $\quad \nu=\lambda$

〔定理〕6.

$$p\nmid\frac{a^\lambda-1}{p},\ \mathrm{ord}_p a=\lambda,\quad ord_{p^2}a=\nu\rightarrow\nu=\frac{p}{p,\dfrac{a^\lambda-1}{p}}\cdot\lambda$$

(証明)

仮定から　　$a^{\nu} \equiv 1 \pmod{p^2}$

$\therefore$　　$a^{\nu} \equiv 1 \pmod{p}$

〔補定〕(1) から　　$\lambda \mid \nu,\ \nu = n\lambda$ ……(1)

次に　　$a^{n\lambda} \equiv 1 \pmod{p^2}$ とすると

$$a^{n\lambda} - 1 = (a^{\lambda} - 1) \sum_{i=0}^{n-1} (a^{\lambda})^i \equiv 0 \pmod{p^2} \quad \cdots\cdots(2)$$

$\left(p, \dfrac{a^{\lambda} - 1}{p}\right) = d$ とおくと

$$p = p'd,\ \frac{a^{\lambda} - 1}{p} = Ad,\ (p',\ A) = 1$$

$$a^{\lambda} \equiv 1 \pmod{p'}$$

〔補定〕(3) から

$$\sum_{i=0}^{n-1} (a^{\lambda})^i \equiv n \pmod{p'}$$

$\therefore$

$$\sum_{i=0}^{n-1} (a^{\lambda})^i = n + tp'$$

$\therefore$ (2) は　　$pdA\ (n + tp') \equiv 0 \pmod{pp'd}$

$\therefore$　　$A\ (n + tp') \equiv 0 \pmod{p'}$

$(A,\ p') = 1$より　　$n + tp' \equiv 0 \pmod{p'}$

$$n \equiv 0 \pmod{p'}$$

よって

$$n = mp' \quad \cdots\cdots(3)$$

(1), (3) から

$$\nu = mp'\lambda \quad \cdots\cdots(4)$$

然るに

$$a^{p'\lambda} - 1 = (a^{\lambda} - 1) \sum_{i=0}^{p'-1} (a^{\lambda})^i$$

仮定から　　$a^{\lambda} - 1 = pdA$

〔補定〕(2) から

$$\sum_{i=0}^{p'-1} (a^{\lambda})^i \equiv 0 \pmod{p'}$$

$$\sum_{i=0}^{p'-1} (a^{\lambda}) = mp'$$

$\therefore$　　$a^{p'\lambda} - 1 = pdA \cdot mp' = p^2 mA$

$\therefore$

$$a^{p'\lambda} \equiv 1 \pmod{p^2}$$

$$\nu = p'\lambda = \frac{p}{d} \cdot \lambda = \frac{p}{\left(p.\ \dfrac{a^{\sigma} - 1}{p}\right.} \cdot \lambda$$

次に前定理のいくつかを一般化してみる。

〔定理〕7.　$n$ 個の数 $p_1, p_2, \cdots\cdots p_n$ が，どの二つも互に素で，且つすべて $a$ と互に素であるとすると

$$\operatorname{ord}_{\{p_1, p_2, \cdots p_n\}} a = \{\operatorname{ord} p,\ a,\ \operatorname{ord} p_2 a, \cdots\cdots \operatorname{ord} p_n\}$$

(証明)

〔定理〕1. から帰納法で簡単に証明できる。

〔定理〕6. の一般化のために次の補助定理をおく。

〔補助定理〕(4)　$p$ は素数で，$(a,\ p) = 1$,

$a \equiv 1 \pmod{p^n}$ ならば

$$a^{p^s} \equiv 1 \pmod{p^{n+s}}$$

（証明）$s$ についての帰納法で証明しよう。

$a^p - 1 = (a-1)\sum_{i=0}^{p-1} a^i$ において

仮定から　　$p^n \mid (a-1)$

〔補・定〕(2) から　$p \mid \sum_{i=0}^{p-1} a^i$

$\therefore$　　$p^{n+1} \mid (a^p - 1)$

即ち　　$a^p \equiv 1 \pmod{p^{n+1}}$ ……(1)

よって $s=1$ のとき定理は成立つ。

次に $s=k$ で成立つと仮定する。即ち

$$a^{p^k} \equiv 1 \pmod{p^{n+k}}$$

が成立つとする。

(1) から　　$(a^{p^k})^p \equiv 1 \pmod{p^{(n+k)+1}}$

$\therefore$　　$a^{p^{k+1}} \equiv 1 \pmod{p^{n+(k+1)}}$

即ち $s=k$ で成立つと仮定すると，$s=k+1$ でも成立つ。よって，すべての自然数 $s$ について定理は成立つ。

〔補助定理〕(5) $p$ は素数で，$(a, p)=1$,

$a^{p^s} \equiv 1 \pmod{p^{n+s}}$ ならば

$$a \equiv 1 \pmod{p^n}$$

（証明）$n$, $s$ についての二重帰納法で証明しよう。

(A) $s=1$ のとき $a^p \equiv 1 \pmod{p^{n+1}}$ ならば

$a \equiv 1 \pmod{p^n}$ の証明

(1) $n=1$ のとき成立つ。

$\therefore$　仮定から　$a^{p-1} \cdot a \equiv 1 \pmod{p^2}$

$p$ は素数だから，Fermat の定理によって，

$$a^{p-1} \equiv 1 \pmod{p}$$

$\therefore$　　$a \equiv 1 \pmod{p}$

(2) $n=k$ で成立っと仮定する。即ち

$a^p \equiv 1 \pmod{p^{k+1}} \rightarrow a \equiv 1 \pmod{p^k}$ ……〔i〕

が成立つとする。

従って　　$a^p \equiv 1 \pmod{p^{(k+1)+1}}$ ……〔ii〕

とすると　　$a^p \equiv 1 \pmod{p^{k+1}}$ が成立ち，

〔i〕から　　$a \equiv 1 \pmod{p^k}$

$\therefore$　　$a-1 = tp^k$, $\sum_{i=0}^{p-1} a^i \equiv p \pmod{p^k}$

よって　　$\sum_{i=0}^{p-1} a^i = p + mp^k$

これらを〔ii〕に代入すると

$$a^p - 1 = (a-1)\sum_{i=0}^{p-1} a^i = tp^k (p + mp^k) \equiv 0 \pmod{p^{k+2}}$$

$$t(1 + mp^{k-1}) \equiv 0 \pmod{p}$$

$1+mp^{k-1}\equiv 1 \pmod{p}$ であるから

$$t\equiv 0 \pmod{p}$$

即ち $t=mp$

$\therefore$ $a-1=tp^k=mp^{k+1}$, $a\equiv 1 \pmod{p^{k+1}}$

よって，すべての自然数 $n$ について（A）は成立つ。

（B） $s=k$ のとき，定理が成立つと仮定する。

$$a^{p^k}\equiv 1 \pmod{p^{n+k}} \rightarrow a\equiv 1 \pmod{p^n}$$

が成立つとする。

$$a^{p^{k+1}}=(a^p)^{p^k}\equiv 1 \pmod{p^{n+(k+1)}}$$

とすると

$$(a^p)^{p^k}\equiv 1 \pmod{p^{(n+1)+k}}$$

仮定から $a^p\equiv 1 \pmod{p^{n+1}}$

（A）から $a\equiv 1 \pmod{p^n}$

よって $s=k+1$ でも成立つ。

従って，すべての自然数，$n$，$s$ について，

$$a^{p^s}\equiv 1 \pmod{p^{n+s}} \rightarrow a\equiv 1 \pmod{p^n}$$

これらの補助定理を用いて，〔定理〕6 の一般化を考えよう。但し $p$ は素数とする。

〔定理〕8.

$\mathrm{ord}_p a=\lambda$, $\mathrm{ord}p^n=\nu$, $(a,\ p)=1$, $s<n$,

$p^s \mid (a^\lambda-1)$, $p^{s+1}\nmid(a^\lambda-1)\rightarrow$

$$\nu=p^{n-s}\lambda$$

（証明）

仮定から $a^\lambda\equiv 1 \pmod{p^s}$

〔補定〕(4) から $a^{\lambda p^{n-s}}\equiv 1 \pmod{p^n}$

〔補定〕(1) から $\nu \mid \lambda p^{n-s}$ ……（1）

$\lambda p^{n-s}$ の本来の約数の任意の一つを $d$,

$$d=\lambda_1 p^r,\ \lambda_1 \mid \lambda,\ r\leqq n-s \quad \cdots\cdots(2)$$

とするとき

$$a^d=a^{\lambda_1 p^r}\equiv 1 \pmod{p^n}$$

が成立ったとすると，

〔補定〕(5) から

$$a^{\lambda_1}\equiv 1 \pmod{p^{n-r}}$$

$\therefore$ $a^{\lambda_1}\equiv 1 \pmod{p}$

〔補定〕(1) から $\lambda \mid \lambda_1$

又 (2) から $\lambda_1 \mid \lambda$

$\therefore$ $\lambda_1=\lambda$.

従って (2) から $d=\lambda p^r$ $r<n-s$ ……$(2)'$

$p^s \mid (a^\lambda-1)$, $p^{s+1}\nmid(a^\lambda-1)$ から

$$n-r\leqq s \quad \cdots\cdots(3)$$

$(2)'$ と (3) とは矛盾，

故に $a^d\not\equiv 1 \pmod{p^n}$

故に $\nu=\lambda p^{n-s}$

$p^s \mid (a^\lambda - 1)$, $p^{s+1} \nmid (a^\lambda - 1)$ を $p^s \| (a^\lambda - 1)$ で表わすことにすると，〔定理〕8. は次のようになる。

$p$ は素数，$(a, p) = 1$, $\mathrm{ord}_p a = \lambda$, $s < n$

$p^s \| (a^\lambda - 1) \rightarrow \mathrm{ord}_{p^n} a = p^{n-s} \mathrm{ord}_p a$

$s \geqq n$ のときは ？

$p^s \mid (a^\lambda - 1)$ より $a^\lambda \equiv 1 \pmod{p^n}$

∴〔補定〕(1) から $\nu \mid \lambda$ ……(1)

又 $a^\nu \equiv 1 \pmod{p^n}$ より

$a^\nu \equiv 1 \pmod{p}$

∴ $\lambda \mid \nu$ ……(2)

(1), (2) から $\nu = \lambda$

これは〔定理〕5 の一般化にほかならない。

次に $p$ が素数でない場合に〔定理〕8 を拡張することを考えてみよう。即ち，$p_1$, $p_2$ を異なる素数で，$a$ と互に素であるとし，

$\mathrm{ord}_{p_1 p_2} a = \lambda$, $\mathrm{ord}_{(p_1 p_2)^n} a = \nu$ とするとき，$\nu$ と $\lambda$ との間に〔定理〕8 におけると同様の関係が成立っであろうか，をしらべよう。

〔定理〕8 から

$\mathrm{ord}_{p_1} a = \lambda_1$ $p_1^{s_1} \| (a^{\lambda_1} - 1) \rightarrow \mathrm{ord}_{p_1^n} a = p_1^{n-s_1} \lambda_1$

$\mathrm{ord}_{p_2} a = \lambda_2$ $p_2^{s_2} \| (a^{\lambda_2} - 1) \rightarrow \mathrm{ord}_{p_2^n} a = p_2^{n-s_2} \lambda_2$

従って〔定理〕2 から

$$\mathrm{ord}_{p_1 p_2} a = \{\lambda_1, \lambda_2\} = \lambda$$

$$\mathrm{ord}_{(p_1 p_2)^n} a = \{p_1^{n-s_1}\lambda_1, p_2^{n-s_2}\lambda_2\} = \nu$$

又 Fermat の定理から

$$\lambda_1 \mid (p_1 - 1), \quad \lambda_2 \mid (p_2 - 1)$$

いま $p_1 < p_2$ とすると，明らかに

$$p_2 \nmid \lambda_1 \quad \cdots\cdots(1)$$

$(\lambda_1, \lambda_2) = d$, $\lambda_1 = \lambda_1' d$, $\lambda_2 = \lambda_2' d$ とすると

$$(\lambda_1', \lambda_2') = 1, \quad \{\lambda_1, \lambda_2\} = \lambda_1' \lambda_2' d \quad \cdots\cdots(2)$$

$$\{p_1^{n-s_1}\lambda_1, p_2^{n-s_2}\lambda_2\} = \{p_1^{n-s_1}\lambda_1', p_2^{n-s_2}\lambda_2'\} d$$

ここで $p_1 \nmid \lambda_2$ ……(3)

と仮定すると，(1), (2), (3) から

$$\begin{aligned}\{p_1^{n-s_1}\lambda_1', p_2^{n-s_2}\lambda_2'\} d &= p_1^{n-s_1} p_2^{n-s_2} \lambda_1' \lambda_2' d \\ &= p_1^{n-s_1} p_2^{n-s_2} \{\lambda_1, \lambda_2\} \\ &= p_1^{n-s_1} p_2^{n-s_2} \lambda\end{aligned}$$

即ち $\mathrm{ord}_{(p_1 p_2)^u} a = p_1^{n-s_1} p_2^{n-s_2} \mathrm{ord}_{p_1 p_2} a$

更に $p_1 \nmid \lambda_2$ となるのは $p_1, p_2$ の間に如何なる条件があるときかをしらべよう。

いま $p_1 \mid \lambda_2$

とすると $\lambda_2 \mid (p_2 - 1)$

より

$$p_1 \mid (p_2 - 1), \quad p_2 \equiv 1 \pmod{p_1}$$

逆も亦明らかに成立つから，次の定理が得られる。

〔定理〕9.

$p_1$, $p_2$ は$a$ と互に素なる素数で

$\mathrm{ord}_{p_1} a = \lambda_1$, $\mathrm{ord}_{p_2} a = \lambda_2$, $p_1^{s_1} \parallel (a^{\lambda_1} - 1)$, $p_2^{s_2} \parallel (a^{\lambda_2} - 1)$,

$p_1 < p_2$, $p_2 \not\equiv 1 \pmod{p_1}$ ならば

$$\mathrm{ord}_{(p_1 p_2)^n} a = p_1^{n-s_1} p_2^{n-s_2} \mathrm{ord}_{p_1 p_2} a$$

である。

更に三つの異なる素数について〔定理〕9 はどうなるか。

〔定理〕10.

$p_1 < p_2 < p_3$ なる三個の素数が $a$ と互に素で，$\mathrm{ord}_{p_1} a = \lambda_1$，$\mathrm{ord}_{p_2} a = \lambda_2$，$\mathrm{ord}_{p_3} a = \lambda_3$ とするとき，

$$p_1^{s_1} \parallel (a^{\lambda_1} - 1),\quad p_2^{s_2} \parallel (a^{\lambda_2} - 1),\quad p_3^{s_3} \parallel (a^{\lambda_3} - 1)$$

$$p_2 \not\equiv 1 \pmod{p_1},\quad p_3 \not\equiv 1 \pmod{p_1},\ \pmod{p_2}$$

更に $(\lambda_1, \lambda_2, \lambda_3) = d$，$\lambda_1 = \lambda_1' d$，$\lambda_2 = \lambda_2' d$，$\lambda_3 = \lambda_3' d$ とするとき，$\lambda_1'$, $\lambda_2'$, $\lambda_3'$ のどの二つも，互に素であれば

$$\mathrm{ord}_{(p_1 p_2 p_3)^n} = p_1^{n-s_1} p_2^{n-s_2} p_3^{n-s_3} \mathrm{ord}_{p_1 p_2 p_3} a$$

である。

（証明）

前定理におけると殆んど同様にして

$$\mathrm{ord}_{(p_1 p_2 p_3)^n} a = \{p_1^{n s_1} \lambda_1',\ p_2^{n-s_2} \lambda_2',\ p_3^{n-s_3} \lambda_2'\}\ d$$

仮定の $p_1 < p_2 < p_3$，$p_2 \not\equiv 1 \pmod{p_1}$，$p_3 \not\equiv 1 \pmod{p_1}$，$\pmod{p_2}$

$$(\lambda_1', \lambda_2') = (\lambda_1', \lambda_3') = (\lambda_2, \lambda_3) = 1$$

から $p_1^{n-s_1} \lambda_1'$，$p_2^{n-s_2} \lambda_2'$，$p_3^{n-s_3} \lambda_3'$ はどの二つも亦互に素となるから

$$\begin{aligned} \{p_1^{n-s_1} \lambda_1',\ p_2^{n-s_2} \lambda_2',\ p_3^{n-s_3} \lambda_3'\}\ d &= p_1^{n-s_1} p_2^{n-s_2} p_3^{n-s_3} \lambda_1' \lambda_2' \lambda_3' d \\ &= p_1^{n-s_1} p_2^{n-s_2} p_3^{n-s_3} \{\lambda_1, \lambda_2, \lambda_3\} \\ &= p_1^{n-s_1} p_2^{n-s_2} p_3^{n-s_3} \mathrm{ord}_{p_1 p_2 p_3} a \end{aligned}$$

同様に，$n$ 個の異なる素数について定理は成立つ。

$(b, 10) = 1$ なる既約真分数 $\frac{a}{b}$ を小数で表わすと，純循環小数となり，その循環節の桁数，即ち「週期」$\lambda$ は $b$ のみの函数で

$$\mathrm{ord}_b 10 = \lambda$$

である。従って前の諸定理において，$a = 10$ とすれば，いくつかの循環小数の「週期」の間の関係が得られる。いま，分母のみに着目して，$(b, 10) = 1$ の分数 $\frac{1}{b}$ を表わす循環小数の週期を $\Pi(\frac{1}{b})$ と表わすと，次のような法則が得られる。

〔1〕 $(p, q) = 1 \rightarrow \Pi(\frac{1}{pq}) = \{\Pi(\frac{1}{p}),\ \Pi(\frac{1}{q})\}$

これは〔定理〕2 から得られる。

例

$$\Pi(\frac{1}{7}) = 6,\ \Pi(\frac{1}{11}) = 2 \therefore\ \Pi(\frac{1}{7 \times 11}) = \{6, 2\} = 6$$

$$\Pi(\frac{1}{13}) = 6,\ \Pi(\frac{1}{41}) = 5 \therefore\ \Pi(\frac{1}{13 \times 41}) = \{6, 5\} = 30$$

$$\Pi(\frac{1}{11 \times 41}) = \{2, 5\} = 10$$

実際に計算してみると，

$$\left.\begin{aligned}\frac{1}{7}&=0.\dot{1}42857\dot{}\\ \frac{1}{11}&=0.\dot{0}\dot{9}\end{aligned}\right\}\quad \frac{1}{77}=0.\dot{0}12989\dot{}$$

$$\left.\begin{aligned}\frac{1}{13}&=0.\dot{0}76923\dot{}\\ \frac{1}{41}&=0.\dot{0}2439\dot{}\end{aligned}\right\}\quad \frac{1}{11\times41}=0.\dot{0}022172949\dot{}$$

〔2〕 $\Pi(\frac{1}{p})=\lambda,\ p^s \parallel (10^\lambda-1)\rightarrow$

$$\Pi(\frac{1}{p^n})=p^{n-s}\ \Pi\ (\frac{1}{p})=p^{n-s}\lambda$$

これは〔定理〕8 から得られる。

例

$$\Pi(\frac{1}{3})=1,\ 3^2 \parallel (10^1-1)\ \therefore$$

$$\therefore\qquad \Pi\ (\frac{1}{3^2})=3^{2-2}\cdot 1=1$$

$$\Pi\ (\frac{1}{3^3})=3^{3-2}\cdot 1=3$$

$$\Pi\ (\frac{1}{3^4})=3^{4-2}\cdot 1=9$$

実際に計算してみると

$$\frac{1}{3}=0.\dot{3},\ \frac{1}{3^2}=0.\dot{1}\dot{},\ \frac{1}{3^3}=0.\dot{0}3\dot{7}$$

$$\frac{1}{3^4}=0.\dot{0}12345679\dot{}$$

〔3〕 $\Pi(\frac{1}{p})=\lambda,\ \Pi\ (\frac{1}{q})=\mu,\ \{\lambda,\ \mu\}=\sigma$

$$(p,\ q)=d,\ \{p,\ q\}=l,\ \Pi\ (\frac{1}{pq})=\nu$$

$$(d,\ \frac{a^\sigma-1}{l})=g\rightarrow\nu=\frac{d}{g}\cdot\sigma$$

これは〔定理〕4 から得られる。

例

$$\Pi(\frac{1}{21})=6,\ \Pi(\frac{1}{33})=2,\ \{6,\ 2\}=6=\sigma$$

$$(21,\ 33)=3=d,\ \{21,\ 33\}=3\cdot7\cdot11=l.$$

$$\frac{10^\sigma-1}{l}=\frac{10^6-1}{3\cdot7\cdot11}=4329\qquad g=(3,\ 4329)=3$$

$$\therefore\qquad \nu=\frac{d}{g}\cdot\sigma=\frac{3}{3}\cdot6=6$$

$$\therefore\qquad \Pi\ (\frac{1}{21\times33})=6$$

実際に計算してみると

$$\frac{1}{21}=0.\dot{0}47619\dot{}\quad \frac{1}{33}=0.\dot{0}\dot{9}$$

$$\frac{1}{21\times33}=0.\dot{0}01443\dot{}$$

ここで循環小数で表わす方法の一つについて述べる。

$$\frac{1}{p} = 0.\dot{A}_1A_2\cdots\cdots\dot{A}_\lambda$$

とすると，　$10^\lambda - 1 = p \times \overline{A_1A_2\cdots\cdots A_\lambda}$

循環節 $\overline{A_1A_2\cdots\cdots A_\lambda}$ を簡単に $\overline{A}$ で表わすと

$$10^\lambda - 1 = p \cdot \overline{A}$$

$$10^{2\lambda} - 1 = p \cdot \overline{A}\,\overline{A}$$

$$10^{3\lambda} - 1 = p \cdot \overline{A}\,\overline{A}\,\overline{A}$$

一般に　$10^{n\lambda} - 1 = p\ \underbrace{\overline{A}\,\overline{A}\cdots\cdots\overline{A}}_{n\text{ 個}}$ ……(1)

いま　$\frac{1}{pq} = 0.\ \dot{B}_1B_2\cdots\cdots\dot{B}_\mu$

とすると　$10^\mu \equiv 1 \pmod{pq}$

∴　$10^\mu \equiv 1 \pmod{p}$

∴　$\lambda \mid \mu,\quad \mu = n\lambda$

∴　$10^{n\lambda} - 1 = pq\ \overline{B_1B_2\cdots\cdots B_\mu} = pq\ \overline{B}$ ……(2)

∴ (1), (2) から

$$pq\overline{B} = p \cdot \underbrace{\overline{A}\,\overline{A}\cdots\cdots\overline{A}}_{n\text{ 個}}$$

$$\overline{B} = \frac{1}{q} \cdot \underbrace{\overline{A}\,\overline{A}\cdots\cdots\overline{A}}_{n\text{ 個}}$$

即ち $\frac{1}{pq}$ の循環節を求めるには $\frac{1}{p}$ の循環節を $q$ で始めてわりきれるまで並べて書いたときの商をとればよい。

例

$$\frac{1}{21} = \frac{1}{3\times 7} = 0.\dot{0}47619\dot{}$$

$$\frac{1}{3} = 0.\dot{3}$$

$$7)\overline{333333}\ \overline{047619}$$

参考文献

WILLIAM JUDSON LEVEQUE: Topics In Number Theory (1)

## II. 最小公倍数の求め方について

例えば，120, 504, 882 の $L\cdot C\cdot M\cdot$ は普通下のようにやって求める。その根拠は素因数分解によって説明される。

| | | | |
|---|---|---|---|
| 2 | 120 | 504 | 882 |
| 2 | 60 | 252 | 441 |
| 2 | 30 | 126 | 441 |
| 3 | 15 | 63 | 441 |
| 3 | 5 | 21 | 147 |
| 7 | 5 | 7 | 49 |
| | 5 | 1 | 7 |

$L.\ C.\ M. = 2^3 \times 3^2 \times 5 \times 7^2 = 17640$

次に素因数分解の理論を用いないで，やや一般的な方法を導いてみよう。よく行われる証明法については省略することがある。

〔定理〕1. $d \mid a,\ d \mid b \rightarrow d \mid (ma \pm nb)$

〔定理〕2. $(a, b) = (a - bq, b) = (r, b)$

ここに $r$ は $a$ を $b$ でわった剰余

これから Euclid の互除法が，又次の定理が導かれる。

〔定理〕3. $(ka, kb) = k\,(a, b)$

〔定理〕4. $(a, b, c) = ((a, b), c)$

（系） $(ka, kb, kc) = k\,(a, b, c)$

〔定理〕5. $b \mid ac,\ (b, a) = 1 \rightarrow b \mid c$

（証明）

$(b, a) = 1$ より 〔定理〕3. から

$$(bc, ac) = c$$

$b \mid ac$ より $bd = ac$ なる $d$ があるから

$$(bc, bd) = c$$

$$\therefore \quad b\,(c, d) = c \qquad \therefore\ b \mid c$$

〔定理〕6. $a \mid m,\ b \mid m,\ (a, b) = 1 \rightarrow ab \mid m$

（証明）

$a \mid m,\ b \mid m$ より $aa' = bb' = m$ なる $a', b'$ がある。

$$\therefore \quad a \mid bb' \text{ 又 } (a, b) = 1$$

よって〔定理〕5 から

$$a \mid b', \text{ 即ち } b' = aa''$$

$$\therefore \quad m = bb' = baa'', \text{ 即ち } ab \mid m$$

〔定理〕7. $(a, c) = 1,\ (b, c) = 1 \rightarrow (ab, c) = 1$

（証明）

$$(ab, c) = (ab, c\,(b, 1)) = (ab, (cb, c))$$
$$= ((ab, cb), c) = (b\,(a, c), c)$$
$$= (b \times 1, c) = (b, c) = 1$$

〔定理〕8. $(a, b) = G,\ a = Ga',\ d = Gb' \rightarrow (a', b') = 1$

（証明）

$(a, b) = G$ より $(Ga', Gb') = G$

$$G\,(a', b') = G$$

$$\therefore \quad (a', b') = 1$$

〔定理〕9. $a = Ga',\ b = Gb',\ (a', b') = 1 \rightarrow (a, b) = G$

（証明）

$$(a, b) = (Ga', Gb') = G\,(a', b') = G.$$

〔定理〕10. $a \mid m,\ b \mid m \rightarrow \{a, b\} \mid m$

（証明）

$\{a, b\} = L.$ を $m$ でわった商を $q$，余りを $r$ とすると

$$m = Lq + r \qquad 0 \leqq r < L$$

$$\therefore \quad r = m - Lq$$

$m$, $L$ 共に $a$, $b$ の公倍数だから明らかに $r$ も亦 $a$, $b$ の公倍数である。従って $r \neq 0$ とすると $L$. の最小性に矛盾する。

$$\therefore \qquad r = 0,\ m = Lq,\ L \mid m$$

即ち $$\{a, b\} \mid m$$

〔定理〕 11. $(a, b) = 1 \rightarrow \{a, b\} = ab.$

（証明）

$a \mid \{a, b\}$, $b \mid \{a, b\}$, $(a,b) = 1$ であるから〔定理〕6 により

$$ab \mid \{a, b\}$$

又前定理から $\{a, b\} \mid ab$

$$\therefore \qquad \{a, b\} = ab$$

〔定理〕 12. $\{ka, kb\} = k\{a, b\}$

（証明）

$a$, $b$ の公倍数を $m$ とすると

$$m = aa' = bb'$$

なる $a'$, $b'$ がある。

$$\therefore \qquad km = ka.\ a' = kb.b'$$

即ち $a$, $b$ の公倍数の $k$ 倍は $ka$, $kb$ の公倍数である。

逆に ka, $kb$ の公倍数を $M$ とすると

$$M = ka.\ a' = kb.\ b'$$

なる $a'$, $b'$ がある。

$$\therefore \qquad aa' = bb' = m \text{ とおくと}$$

$m$ は $a$, $b$ の公倍数で，上式から

$$M = km$$

即ち $ka$, $kb$ の公倍数は $a$, $b$ の公倍数の $k$ 倍である。

よって，$a$, $b$ の公倍数の $k$ 倍の全体と，$ka$, $kb$ の公倍数の全体とは一致する。故に各の最小のものも亦一致する。よって

$$\{ka, kb\} = k\{a, b\}$$

〔定理〕 13. $(a, b)\{a, b\} = ab$

（証明）

$(a, b) = G$, $a = Ga'$, $b = Gp'$ とすると

$$(a', b') = 1 \cdots\cdots\cdots\cdots\cdots\cdots〔定理〕\ 9$$

$$\therefore \qquad \{a', b'\} = a'b' \cdots\cdots\cdots\cdots\cdots\cdots〔定理〕\ 11$$

$$\therefore \qquad \{Ga', Gb'\} = Ga'b' \cdots\cdots〔定理〕\ 12$$

$$\{a, b\} = Ga'b'$$

$$(a, b)\{a, b\} = Ga', Gb' = ab$$

これは又一つ $L.\ C.\ M.$ のの求め方を与える。

$$\{a, b\} = \frac{a}{(a, b)} \cdot b = \frac{b}{(a, b)} \cdot a$$

〔定理〕 14. $\{a, b, c\} = \{\{a, b\}, c\}$

$$\{a, b, c, d,\} = \{\{a, b\}, \{c, d\}\cdots\cdots\}$$

〔定理〕 15. $\{ka, kb, kc,\} = k\{a, b, c,\cdots\cdots\}$

次に

$c \mid \{a, b\} \rightarrow \{a, b, c\} = \{\{a, b\}, c\} = \{a, b\}$……(1)

に注意すれば，〔定理〕12. は更に次のように拡張することができる。

〔定理〕16. $(k, c) = 1 \rightarrow \{ka, kb, c\} = k\{a, b, c\}$

（証明）

$k \mid \{ka, kb, c\}$, $c \mid \{ka, kb, c\}$, $(k, c) = 1$ より

$kc \mid \{ka, kb, c\}$……〔定理〕6.

よって上の注意 (1) により

$$\begin{aligned}\{ka, kb, c\} &= \{\{ka, kb, c\}, kc\}\\ &= \{ka, kb, \{c, kc\}\}\\ &= \{ka, kb, c\{1, k\}\}\\ &= \{ka, kb, kc\}\\ &= k\{a, b, c\}\end{aligned}$$

これは更に一般化されて

〔定理〕17, $(k, c) = 1, (k, d) = 1, \cdots\cdots \rightarrow$

$\{ka, kb, c, d, \cdots\cdots\} = k\{a, b, c, d, \cdots\cdots\}$

次に〔定理〕11. の一般化に当たる定理をつけ加えておく。

〔定理〕18. $(a, b) = (a, c) = (b, c) = 1 \rightarrow \{a, b, c\} = abc$

（証明）

$(a, b) = 1$ より $\{a, b, c\} = \{\{a, b\}, c\} = \{ab, c\}$

$(a, c) = (b, c) = 1$ より $(ab, c) = 1$

$\therefore \quad \{ab, c\} = abc$

即ち $\{a, b, c\} = abc$

四つ以上の数についても同様。

以上の定理から，次のような求め方が得られる。

| | | | |
|---|---|---|---|
| 6 | 120 | 504 | 882 |
| 4 | 20 | 84 | 147 |
| 3 | 5 | 21 | 147 |
| 7 | 5 | 7 | 49 |
| | 5 | 1 | 7 |

$L = 6 \cdot 4 \cdot 3 \cdot 7 \cdot 5 \cdot 7$

$= 17640$

| | | | |
|---|---|---|---|
| 100 | 300 | 400 | 21 |
| 3 | 3 | 4 | 21 |
| | 1 | 4 | 7 |

$L = 100 \cdot 3 \cdot 4 \cdot 7$

$= 8400$

**Résumé**

# On The Two Problems of The Number Theory

I. On The Order of An Element belonging to Several Reduced Residue Systems

When $a$ is an element common to reduced residue systems modulo $p$, $q$ and $pq$, the order of $a$ modulo $pq$ is a function of the order of $a$, modulo $p$, and $q$;

$$\mathrm{ord}_{pq}\ a = \{\mathrm{ord}_p a,\ \mathrm{ord}_q a\}$$

under the coudition of $(p, q) = 1$. It is an object of this paper to generalize the theorem.

II. On The Theorem of L. C. M.

The step-method of L. C. M. is explained generally on the prime-factorizing, but here a little generalized method is constructed without using prime-factorization.