フェルマーの小定理について

才野瀬（さいのせ）　一郎（いちろう）

§1. はじめに

参考文献〔1〕(改訂版 チャート式 基礎からの数学Ⅰ＋A) の整数分野が書き換えられて，次の興味深い事項①～⑤が掲載されている。

実は，これらを組み合わせると⑥のフェルマーの小定理が証明できる。〔1〕では数学Ⅱで学ぶ二項定理を持ち出して証明をしているが，この方法は本質的で興味深い証明ではあるが，唐突な感は否めない。そこで以下のように数学Aの範囲で証明を完結させよう。

なお，この方法は参考文献〔2〕による。

① P482 検討

n は自然数とする。1 から n までの自然数の中で，n と互いに素であるものの個数を $\phi(n)$ と表す。$\phi(n)$ をオイラー関数と呼ぶ。

なお $n \geqq 2$ の場合は，0 から $n-1$ までの整数の中で考えても同じである。

このとき，p が素数で k が自然数とすると
$\phi(p^k)=p^k-p^{k-1}$ が成り立つ。
特に $\phi(p)=p-1$ である。

② P494 演習例題 121(1)

整数 a と自然数 m が互いに素なとき

$$ax \equiv ay \pmod{m} \Rightarrow x \equiv y \pmod{m}$$

③ P501 解説

a，b (>0)，q，r が整数で $a=bq+r$，
すなわち $a \equiv r \pmod{b}$ のとき，
特に a を b で割った余りが r のとき，
$(a,\ b)=(b,\ r)$ が成り立つ。

ここで，x と y の最大公約数を $(x,\ y)$ と表す。

④ P512 補足事項 (※)

0 でない整数 a，b に対して，
$ax+by=1$ となる整数 x，y が存在する
$\iff$ a と b が互いに素

⑤ P512 定理

a と b は互いに素な自然数とするとき，b 個の整数 $a\cdot1$，$a\cdot2$，$a\cdot3$，……，ab をそれぞれ b で割った余りは互いに異なる。すなわち，余りには 0 以上 $b-1$ 以下の整数が 1 回ずつ現れる。

なお，a を b で割った余りと，$a+qb$ (q は整数) を b で割った余りは等しいので，a は整数としてよい。また，ab と 0 を b で割った余りはともに 0 で等しいことに注意。

⑥ P500 フェルマーの小定理

p が素数で a が p と互いに素な整数のとき，
$a^{p-1} \equiv 1 \pmod{p}$ が成り立つ。

§2. 証明

以下では，①～⑤を用いて次の命題と定理を示そう。

[命題]

b を 2 以上の自然数とし，b のオイラー関数の値を $m=\phi(b)$ とおく。また，0 以上 $b-1$ 以下の整数 (b 個) を並び替えて，x_1，x_2，……，x_m は b と互いに素な数，x_{m+1}，x_{m+2}，……，x_b はそうでない数 (1 と b 以外の公約数をもつ) とする。さらに，a を b と互いに素な整数とし，各 ax_k を b で割った余りを y_k とおく。

(1) x_1，x_2，……，x_b と y_1，y_2，……，y_b は，ともに 0 以上 $b-1$ 以下の整数全体 (相異なる b 個) を表す。

(2) $x_1, x_2, \cdots\cdots, x_m$ と $y_1, y_2, \cdots\cdots, y_m$ は順序を除いて一致する。

(3) c を b と互いに素な整数とすると，ac も b と互いに素である。

(4) $z=x_1x_2\cdots\cdots x_m$ とおくと $z=y_1y_2\cdots\cdots y_m$ が成り立つ。さらに，z は b と互いに素である。

証明 (1) x_j は自明。y_j は⑤による。

(2) 「各 $y_k\,(m+1\leqq k\leqq b)$ が $x_j\,(m+1\leqq j\leqq b)$ のいずれかに等しい」……(※)

が成り立てば，(1)により y_k は相異なるので，

$y_k\,(m+1\leqq k\leqq b)$ 全体は同じ $(b-m)$ 個の

$x_j\,(m+1\leqq j\leqq b)$ 全体と順序を除いて一致する。

すると再度(1)により，各 y_k $(1\leqq k\leqq m)$ は

x_j $(1\leqq j\leqq m)$ のいずれかに等しい。

ここで直前と同じ議論をすれば，結論が従う。

以下 (※) を示す。

$m+1\leqq k\leqq b$ のとき，x_k と b はある公約数 $d\,(\neq 1,\ b)$ をもつから，ax_k も d を約数にもつ。

ここで③により $(ax_k,\ b)=(y_k,\ b)$ であるから，

y_k と b も公約数 d をもち，(※) が示された。

(3) c を b で割った余りを x_k とする。

仮定と③により，$1=(b,\ c)=(b,\ x_k)$ となり，x_k も b と互いに素であるから $k\leqq m$ である。

すると(2)より，y_k と b が互いに素となる。

これと，$ac\equiv ax_k\equiv y_k\pmod b$ に③を用いて

$$(ac,\ b)=(y_k,\ b)=1$$

(4) 前半は(2)，後半は(3)を繰り返し使う。

(補足) 技巧的ではあるが，(1)の後に④を用いて(3)(2)の順に示す手短かな別証明が可能。

(3)：仮定に④を用いると，$ax+by=1$，$cz+bw=1$ となる整数 x，y，z，w が存在する。

$ax=1-by$，$cz=1-bw$ の辺々を掛けて

$$ax\cdot cz=(1-by)(1-bw)$$

よって $ac\cdot xz+b(y+w-byw)=1$

再び④によれば，ac と b は互いに素。

(2)：すると $k\leqq m$ のときに，ax_k は b と互いに素であるから，③により y_k が b と互いに素となる。

(1)により y_k は相異なる m 個の整数であるから，結論が従う。

[定理]

(1) **オイラーの定理**

b は自然数とし，$m=\phi(b)$ とおく。このとき，a が b と互いに素な整数ならば，$a^m\equiv 1\pmod b$ が成り立つ。

(2) **フェルマーの小定理** (⑥) が成り立つ。

(3) p を素数とすると，整数 a に対して $a^p\equiv a\pmod p$ が成り立つ。

(4) **ラグランジュの定理**

b は自然数とし，$\phi(b)=m$ とおく。a が b と互いに素な整数のとき，(1)によれば $a^d\equiv 1\pmod b$ となる最小の自然数 d が $1\leqq d\leqq m$ の範囲にあることがわかる。

この最小値 d を $\bmod b$ における a の位数と呼ぶ。

このとき，$a^k\equiv 1\pmod b$ ならば，k は d の倍数となる。

特に，位数 d は m の約数である。

証明 (1) $b=1$ のときは $\phi(1)=1$ より明らかなので，$b\geqq 2$ の場合を考える。

命題において，$\bmod b$ で考えると，

$k=1,\ 2,\ \cdots\cdots,\ m$ のとき $ax_k\equiv y_k$

辺々を掛け合わせて命題(4)の z を用いると

$$(ax_1)(ax_2)\cdots\cdots(ax_m)\equiv y_1y_2\cdots\cdots y_m$$

すなわち $a^mx_1x_2\cdots\cdots x_m\equiv y_1y_2\cdots\cdots y_m$

よって $a^m\cdot z\equiv 1\cdot z$

さらに，命題(4)により z は b と互いに素であるから，②を用いて $a^m\equiv 1$ を得る。

(2) (1)と $\phi(p)=p-1$ $(\because ①)$ による。

(3) a が p と互いに素なときは，⑥の両辺を a 倍すればよい。

そうでないときは，a は p の倍数であり

$a\equiv 0\pmod p$ より $a^p\equiv 0\equiv a\pmod p$

(4) k を d で割った商を q，余りを r とおくと

$$k=dq+r,\quad 0\leqq r<d$$

ここで，$\bmod b$ において

$$1\equiv a^k=a^{dq+r}=(a^d)^qa^r\equiv 1^q\cdot a^r=a^r$$

であるが，d の最小性から $r=0$ が従うので，k は d の倍数である。

「特に」は前半と(1)による。

§3. 例題

最後に，典型的な例題を掲げよう。

［**例題**］

(1)　a が整数のとき，a^5-a が 3 の倍数となることを示せ。(〔1〕P497 演習例題 124(2) 改題)

(2)　a が整数のとき，a^9-a^3 が 9 の倍数となることを示せ。　(京都大 2001 年)

(3)　数列 $\{2^n\}$ の下 3 桁を表す整数はあるところから循環する。循環が始まる番号 N と循環の長さ M を求めよ。　(広島大 2016 年改題)

解答　(1)　定理(3)より　$a^3\equiv a\pmod 3$

両辺に a^2 を掛けて直前の合同式を使うと

$a^5\equiv a^3\equiv a\pmod 3$ となり　$a^5-a\equiv 0\pmod 3$

(2)　$\phi(3^2)=3^2-3^1=6$ ($\because$①) より，a が 9 と互いに素なときは，定理(1)から $a^6\equiv 1\pmod 9$ となり $a^6-1\equiv 0\pmod 9$ を満たす。

a が 9 と互いに素でないときは，a は 3 の倍数であるから a^2 は 9 の倍数となり，$a^2\equiv 0\pmod 9$ を満たす。

いずれにしても

$$a^9-a^3=a\cdot a^2(a^6-1)\equiv 0\pmod 9$$

よって，a^9-a^3 は 9 の倍数である。

(**補足**)　全く同様にして，p が素数で n が自然数のとき，整数 a に対して次を得る。

$$a^n(a^{p^n-p^{n-1}}-1)\equiv 0\pmod{p^n}$$

特に　$a^{p^n}-a^{p^{n-1}}\equiv 0\pmod{p^n}$

(3)　$n\geqq N$ において，

$$2^{n+M}\equiv 2^n\pmod{1000}\qquad\cdots\cdots(ア)$$

となる自然数 M，N の最小値を求めればよい。

$1000=2^3\cdot 5^3$ より

(ア) $\iff$ $2^{n+M}-2^n$ が 1000 の倍数

$\iff$ $2^{n+M}-2^n$ が 5^3 の倍数かつ 2^3 の倍数

$$\iff \begin{cases} 2^{n+M}\equiv 2^n\pmod{125} & \cdots\cdots(イ)\\ 2^{n+M}\equiv 2^n\pmod 8 & \cdots\cdots(ウ)\end{cases}$$

に注意する。

(i)　以下，mod125 で考える。(イ)において

2^n ($n\geqq 1$) は 125 と互いに素であるから，②より

(イ) $\iff$ $2^n\cdot 2^M\equiv 2^n\cdot 1$ $\iff$ $2^M\equiv 1$

したがって，(イ)を満たす M の最小値は mod125 における 2 の位数である。

なお，M が位数のとき，(イ)は $n\geqq 1$ に対して成り立つことを注意しておく。

そこで位数が 100 であることを示す。

$\phi(125)=5^3-5^2=100$ ($\because$①) より定理(4)によれば，位数は 100 の約数。

これから，k が 100 と異なる 100 の約数のとき $2^k\not\equiv 1$ を示せばよい。そのためには「$2^{20}\not\equiv 1$ かつ $2^{50}\not\equiv 1$」を示せば十分。

ここで，$k=1$，2 のとき，二項定理から

$$\begin{aligned}(5^k-1)^5&=(5^k)^5-{}_5C_1(5^k)^4+{}_5C_2(5^k)^3\\&\qquad-{}_5C_3(5^k)^2+{}_5C_4(5^k)-1\\&=5^{5k}-5^{4k+1}+2\cdot 5^{3k+1}\\&\qquad-2\cdot 5^{2k+1}+5^{k+1}-1\\&\equiv 5^{k+1}-1\end{aligned}$$

ゆえに　$4^5=(5-1)^5\equiv 5^2-1$ ($k=1$) となり

$2^{50}=(4^5)^5\equiv(5^2-1)^5\equiv 5^3-1\equiv -1\not\equiv 1$ ($k=2$)

$2^{20}=(4^5)^2\equiv(5^2-1)^2=5^4-2\cdot 5^2+1$

$\equiv -2\cdot 5^2+1=-49\not\equiv 1$

(ii)　続いて，$M=100$ として(ウ)を考える。

mod8 において，

$2^{n+100}\equiv 2^n$ $\iff$ $2^n\equiv 2^{100}\cdot 2^n$

$\iff$ $2^n\equiv 0$ $\iff$ $n\geqq 3$

以上(i)(ii)から，M，N の最小値はそれぞれ 100，3 であることがわかる。

《参考文献》

〔1〕　改訂版チャート式　基礎からの数学Ⅰ＋A　数研出版　P500　他

〔2〕　金子昌信，境隆一　暗号の整数論―素数研究が生きるセキュリティ技術　講談社　P34～P37

(広島県広島市立基町高等学校)