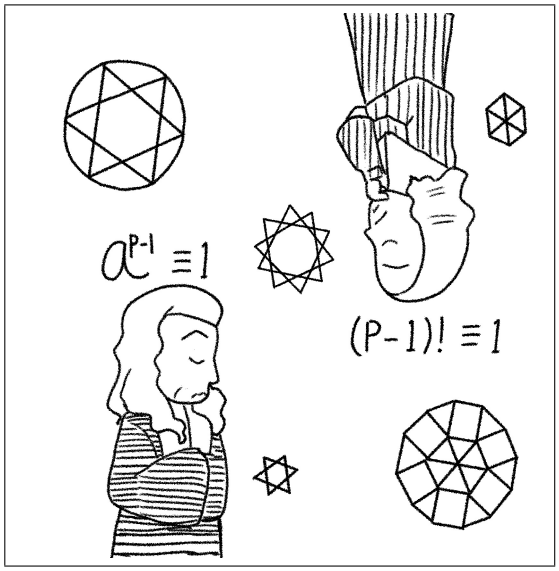
『数学セミナー』2019年6月号 「高校数学ではじめる整数論」

連載●第 3 回

あまりたちのなすサイクル　付録

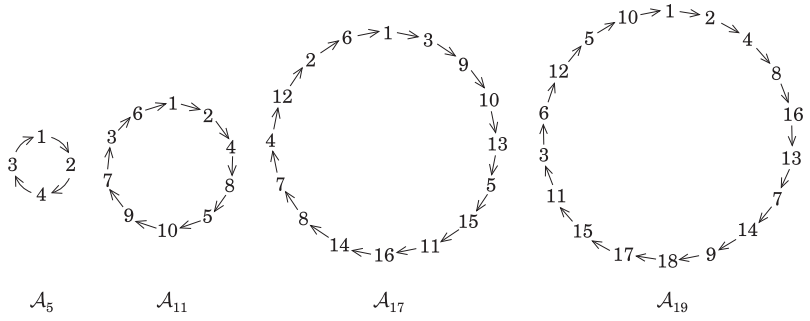
谷口 隆◎神戸大学大学院理学研究科



※ 式番号などは本誌 2019 年 6 月号の連載と通しで振っています.

◎—— (a)

冪 a^n が $\mathcal{A}_p$ 全体になるものを，小さい a から順に探してみると，$p = 5, 11, 17, 19$ それぞれで，$a = 2, 2, 3, 2$ として，a^n で $\mathcal{A}_p$ 全体が作られることが分かります．$\times a$ のサイクルを図にすると，次のとおりです．



注　原始根は一般に複数あります．たとえば法 5 では 2 のほか，3 も原始根です．法 11 では，$2, 6, 7, 8$ が原始根です．((b) の表で，位数が $p-1$ となる a が原始根になります．)

◎—— (b)

次の通りです．サイクルの図を見ながらだと，求めやすいでしょう．

$\mathcal{A}_5$ の元 a	1	2	3	4
a の位数	1	4	4	2

$\mathcal{A}_{11}$ の元 a	1	2	3	4	5	6	7	8	9	10
a の位数	1	10	5	5	5	10	10	10	5	2

$\mathcal{A}_{17}$ の元 a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
a の位数	1	8	16	4	16	16	16	8	8	16	16	16	4	16	8	2

$\mathcal{A}_{19}$ の元 a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
a の位数	1	18	18	9	9	9	3	6	9	18	3	6	18	18	18	9	9	2

r を法 p の原始根とし，$a = r^n$ とします．d を n と $p-1$ の最大公約数とすると，a の位数は $\dfrac{p-1}{d}$ になります．

◎—— (c)

k を n で割った商を q，余りを t とします．$k = qn + t$，$0 \leqq t < n$ です．

$$a^k = a^{qn+t} = a^{qn} \cdot a^t = (a^n)^q \cdot a^t = 1^q \cdot a^t = a^t$$

なので，$a^k = 1$ より $a^t = 1$ です．もし $t \neq 0$ であれば，n より小さな正の整数 t について $a^t = 1$ となり，a の位数が n であることに反します．よって $t = 0$ であり，$k = qn$ なので，k は n の倍数です．

◎—— (d)

a を $\mathcal{A}_p$ の元とし，その位数を n とします．$a^{p-1} = 1$ なので，(c) より $p-1$ は n の倍数です．つまり，n は $p-1$ の約数です．

◎—— (e)

定理 1 から，ある $0 < n < p-1$ である整数 n によって，$-1 = r^n$ と書けます．両辺を 2 乗して $r^{2n} = 1$ となります．r の位数は $p-1$ なので，(c) によって，$2n$ は $p-1$ の倍数です．$0 < 2n < 2(p-1)$ であり，この範囲にある $p-1$ の倍数は $p-1$ のみだから，$2n = p-1$ となります．よって $-1 = r^n = r^{\frac{p-1}{2}}$ です．

◎—— (f)

r を法 p の原始根とします．a を $\mathcal{A}_p$ の元とすると，$a = r^n$ と表せます．

$$a^{p-1} = (r^n)^{p-1} = r^{n(p-1)} = (r^{p-1})^n = 1^n = 1$$

よりフェルマーの小定理が示されました．ウィルソンの定理は，$p = 2$ のときは $(p-1)! = 1! = 1$ より成立します．p が奇素数のときは，定理 1 より $\mathcal{A}_p$ の元すべての積は，

$$r^{0+1+2+\cdots+(p-1)} = r^{\frac{p(p-1)}{2}} = (r^{\frac{p-1}{2}})^p$$

です．(e) より $r^{\frac{p-1}{2}} = -1$ です．p は奇数だから，上の式は $(-1)^p = -1$ となります．これでウィルソンの定理が示されました．

◎—— (g)

r を法 p の原始根とし，$a = r^{\frac{p-1}{4}}$ とおきます．(条件より $\dfrac{p-1}{4}$ は整数です．)　$a^2+1 = r^{\frac{p-1}{2}}+1 = -1+1 = 0$ なので，これを整数の範囲で考えると，$a^2 + 1 \equiv 0 \pmod{p}$ となります．

具体例は $p = 5, 13, 17, 29, 37, 41, 53, \cdots$ について

$$5 \mid 2^2+1,\ 13 \mid 5^2+1,\ 17 \mid 4^2+1,\ 29 \mid 12^2+1,\ 37 \mid 6^2+1,\ 41 \mid 9^2+1,\ 53 \mid 23^2+1,\ \cdots$$

($a \mid b$ は a が b を割り切ることを意味します．)

◎—— 定理 1 の条件 (i), (ii) の同値性

(i) ⇒ (ii)：$r^0, r^1, \cdots, r^{p-2}$ がすべて異なることを示しましょう．そうすれば，$\mathcal{A}_p$ は $p-1$ 個の元からなるので，これらで $\mathcal{A}_p$ の元全部になるはずです．

$0 \leqq m < n \leqq p-2$ で $r^n = r^m$ だとします．両辺に r^{-1} を m 回かけて，$r^{n-m} = 1$ となります．$0 < n-m < p-1$ なので，r は $p-1$ 乗して初めて 1 になるということに反します．

(ii) ⇒ (i)：$r^0 = 1$ だから，(ii) の条件より $r^1, \cdots, r^{p-2}$ はいずれも 1 ではありません．もし $r^{p-1} \neq 1$ だとすると，r^{p-1} はどれかの r^n $(1 \leqq n \leqq p-2)$ と等しくなります．$r^{p-1} = r^n$ から $r^{p-1-n} = 1 = r^0$ となります．$1 \leqq p-1-n \leqq p-2$ なので，(ii) のすべて異なるという条件に反します．したがって $r^{p-1} = 1$ です． ■

◎—— 定理 1 の証明

4 つのステップ (A), (B), (C), (D) で示します．

(A)　$n \geqq 1$ とする．$\mathcal{A}_p$ の元で $x^n = 1$ の解となるものは n 個以下である． □

証明　$\mathcal{A}_p$ に余り 0 を加えた $\mathbb{F}_p = \mathcal{A}_p \cup \{0\}$ を考えると，$\mathbb{F}_p$ は和と積が定まる集合 (専門用語で「環」) になります．$a, b \in \mathbb{F}_p$ について $ab = 0$ ならば，$a = 0$ または $b = 0$ です．

$\mathcal{A}_p$ の元 a が $x^n = 1$ の解だとします．$x^n - 1$ を，$\mathbb{F}_p$ 係数の多項式として 1 次式 $x - a$ で割り，その商を $f(x)$，余りを α とします．$x^n - 1 = (x-a)f(x) + \alpha$ となります．1 次式で割っているので，余り α は定数です．この式で $x = a$ として $0 = \alpha$ を得ます．つまり $x^n - 1 = (x-a)f(x)$ です．$f(x)$ は $n-1$ 次式です．

$\mathcal{A}_p$ の元 b を，$x^n = 1$ の a と異なる解とします．先ほどの式に $x = b$ を代入すると $0 = (b-a)f(b)$ です．これは $\mathbb{F}_p$ での等式であり，$b - a \neq 0$ だから，$f(b) = 0$ です．つまり，b は $f(x) = 0$ の解です．$f(x)$ を $x - b$ で割ると，同様の議論で，余りは 0 で $f(x) = (x-b)g(x)$ となります．$g(x)$ は $n-2$ 次式で，$x^n - 1 = (x-a)(x-b)g(x)$ となりました．

a, b と異なる c が $x^n = 1$ の解ならば，$(c-a)(c-b)g(c) = 0$ です．$(c-a)(c-b) \neq 0$ より $g(c) = 0$ です．よって c は $g(x) = 0$ の解です．$g(x) = (x-c)h(x)$ となります．

異なる解がある限りこれを繰り返します．$x^n = 1$ に異なる n 個の解が与えられていれば，n 回目は 1 次式を 1 次式で割り，商 $k(x)$ は 0 でない定数になります．$k(x) = 0$ は解をもつことができないから，$x^n = 1$ はその n 個以外には解をもちません． ■

(B)　$a \in \mathcal{A}_p$ の位数 m と $b \in \mathcal{A}_p$ の位数 n が互いに素ならば，$ab \in \mathcal{A}_p$ の位数は mn である． □

証明　まず，$(ab)^{mn} = (a^m)^n (b^n)^m = 1$ です．よって ab の位数は mn 以下です．そこで，正の整数 k について，$(ab)^k = 1$ であるとしましょう．この両辺を m 乗すると，$a^m = 1$ から $a^{km} = 1$，したがって $b^{km} = 1$ となります．b の位数は n なので，問題 (c) より，km は n の倍数です．m と n は互いに素だから，k は n の倍数です．同様に両辺を n 乗して考え，k は m の倍数であることもわかります．したがって，k は mn の倍数です．

以上で，ab の位数は mn と分かりました． ■

(C)　$a \in \mathcal{A}_p$ の位数 m と $b \in \mathcal{A}_p$ の位数 n の最小公倍数を ℓ とする．$\mathcal{A}_p$ に位数 ℓ の元が存在する． □

証明　m の約数 m_1 と n の約数 n_1 であって，

$$m_1\text{と } n_1\text{は互いに素で, } m_1n_1 = \ell$$

となるものが存在します[1)]．$m = m_1m_2$，$n = n_1n_2$ とし，$a' = a^{m_2}$，$b' = b^{n_2}$ とおきます．すると，a' の位数は m_1，b' の位数は n_1 で，m_1 と n_1 は互いに素です．よって (B) から，$a'b'$ の位数は $m_1n_1 = \ell$ です．　■

(D)　$\mathcal{A}_p$ に，位数 $p-1$ の元が存在する．　□

証明　$\mathcal{A}_p$ から元 a を任意に取り，その位数を n とします．n が $p-1$ より小さいとき，$\mathcal{A}_p$ の元で，位数が n より大きいものが必ず存在することを示します．

(A) より $x^n = 1$ の $\mathcal{A}_p$ 内の解の個数は n 個以下です．$\mathcal{A}_p$ は $p-1$ 個の元からなるので，$n < p-1$ ならば，$x^n = 1$ の解ではない $\mathcal{A}_p$ の元 b が存在します．$b^n \neq 1$ だから，b の位数 m は n の約数ではありません．したがって m, n の最小公倍数 ℓ は n より大きくなります．(C) によって，この ℓ を位数にもつ元が存在します．

位数が $p-1$ より小さい限り，より位数の大きな元を見つけるこの操作を繰り返します．有限回の繰り返しの後，必ず位数が $p-1$ の元に到達します．　■

*　　*　　*

いかがでしょうか．やはり少し「難しい」のではないかと思います．個人的にはこの難しさは，証明の長さよりも，出てくる考え方の多様さに根を持つように感じられます．専門用語で言えば，代数学の群・環・体の概念がどれも少しずつ表れているのが特徴的です．「分かりにくさ」があっても，あまり気にするのではなく，むしろ，代数学を学ぶ上で一つの道しるべとしてもらえたら，と思います．

[たにぐち たかし]
[絵／森脇かみん]

[1)] これは m, n の素因数分解を考えて得られます．分解に現れる各素因数 p について，より多く p を素因子にもつ方を m_1 または n_1 に入れます．例えば $(m, n) = (60, 18)$ なら，素因数分解 $m = 2^2 \cdot 3 \cdot 5$，$n = 2 \cdot 3^2$ を見て，$m_1 = 2^2 \cdot 5$，$n_1 = 3^2$ とします．詳細はお任せします．