原始根
Primitive Root

p は素数を表す．その他の文字は全て整数とする．

定義 1 n を法として互いに合同である整数の集合を**剰余類**または単に**類**と呼ぶ.

定義 2 n を法とする互いに異なる n 個の類の中からそれぞれ任意に一つずつ取り出した n 個の整数を**代表の一組**（または**剰余系** Restsystem）を組成するという.

定義 3 n を法とする類の中で n と互いに素である数のみを含む類を n を法としての**既約類**と呼ぶ.

定義 4 n を法とする各既約類を代表する $\phi(n)$ 個の整数の集合を n を法とする**既約の代表の一組（既約剰余系**[*1]**）**と呼ぶ.

n が素数のときは既約類は剰余類から 0（を含む類）を除いたものであるである．同じことが剰余系と既約剰余系についても言える．

定理 1 $(a,n)=1$ のとき一次合同式

$$ax \equiv b \pmod{n} \tag{1}$$

は一つの解（類）を有する.

[証明] 剰余系を

$$x_1, x_2, x_3, \cdots, x_n$$

とすると，

$$ax_1, ax_2, ax_3, \cdots, ax_n \tag{2}$$

も剰余系を組成することは明らかである．もし $ax_i \equiv ax_j$ とすると，$a(x_i - x_j) \equiv 0$ となり，$(a,n)=1$ より $x_i - x_j \equiv 0$ つまり $x_i \equiv x_j$ つまり $i=j$ に限られることになる．よって (2) はそれぞれ不合同である．つまり (1) を満たすということは (2) において

$$ax_i \equiv b$$

となる x_i が唯一の解ということである． [証明おわり]

定義 5 $a_0 \neq 0$ のとき

$$a_0x^n + a_1x^{n-2} + a_2x^{n-3} + \cdots + a_n \equiv 0 \pmod{m}$$

を n **次合同式**と呼ぶ.

定理 2

$$x^n - a^n = (x-a)(x^{n-1} + x^{n-2}a + x^{n-3}a^2 + \cdots + a^{n-1})$$

である.

[*1] reduced system of residues，直訳すれば，縮小された剰余系である．縮小とは既約でないものを除外するという意味である.

[証明] 右辺を展開すると

$$\begin{aligned} & x^n + x^{n-1}a + x^{n-1}a^2 + \cdots + xa^{n-1} \\ & \quad - x^{n-1}a - x^{n-2}a^2 - x^{n-3}a^3 - \cdots - a^n \\ & \quad = x^n - a^n \end{aligned}$$

[証明おわり]

定理 3 n 次合同式

$$f(x) \equiv 0 \pmod{p} \tag{3}$$

は最大で n 個（類）の解をもつ.

[証明](3) が解を持たないとき，0 個の解をもつということであるから，条件を満たす.
(3) が一つ以上の解をもつとき，そのうちの一つの解を a とする．つまり

$$f(a) \equiv 0$$

である．今，整式 $f(x)$ を $x - a$ で割ることを考える．整式の除法は一意的であり，かつ因数定理より，

$$f(x) = (x - a)g(x) + f(a) \tag{4}$$

と表せる．$g(x)$ が商で $f(a)$ が余りである．つまり (3) は

$$(x - a)g(x) + f(a) \equiv 0$$

と同値である．さらに

$$(x - a)g(x) \equiv 0 \tag{5}$$

と同値である．p は素数なので (5) を満たすということは $x - a \equiv 0$ または $g(x) \equiv 0$ を満たすということである．よって (5) の $x \equiv a$ 以外の解は

$$g(x) \equiv 0 \tag{6}$$

の解である．(6) はどんな合同式であろうか．(4) を変形すると

$$(x - a)g(x) = f(x) - f(a)$$

ここで

$$f(x) = \sum_{i=0}^{n} a_i x^{n-i}$$

とすると，

$$\begin{aligned} (x - a)g(x) &= \sum_{i=0}^{n} a_i (x^{n-i} - a^{n-i}) \\ &= \sum_{i=0}^{n-1} a_i (x^{n-i} - a^{n-i}) \end{aligned}$$

定理 2 より

$$\begin{aligned}(x-a)g(x) &= \sum_{i=0}^{n-1} a_i(x-a) \sum_{j=0}^{n-i-1} (a^j x^{n-i-j-1}) \\ &= (x-a) \sum_{i=0}^{n-1} a_i \sum_{j=0}^{n-i-1} (a^j x^{n-i-j-1}) \\ \therefore g(x) &= \sum_{i=0}^{n-1} a_i \sum_{j=0}^{n-i-1} (a^j x^{n-i-j-1}) \end{aligned} \tag{7}$$

ゆえに $g(x)$ は整数係数の整式であり[*2]，最高次の項は (7) において $i=j=0$ の場合で

$$a_0 x^{n-1}$$

である．つまり $a_0 \neq 0$ なので $g(x)$ は $n-1$ 次式である．つまり，n 次合同式が解を持つ場合，その解は一つの解と $n-1$ 次合同式の解とで構成される．（前者の解が後者の解のいずれかと重なる可能性はある．）

定理 1 から，p を法とする一次合同式の解は一つであることがわかっている．これらのことから，数学的帰納法により (3) の解は n 個以下であることが示された． [証明おわり]

定義 6 n を法とする合同式において，m が

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

となる最小の 正の 指数であるとき，m を a に**対応する指数**と呼ぶ．あるいは a は指数 m に対応すると言う．[*3]

定理 4 a が法 n に関して指数 m に対応するとき

$$a^k \equiv 1$$

となる必要十分条件は k が m の倍数であることである．

[証明]

$$k = qm + r(0 \leq r < m)$$

とすると，

$$(a^m)^q a^r \equiv 1$$

$$a^r \equiv 1$$

1 と合同になる正の指数で m より小さいものはないので，

$$r = 0$$

$$\therefore k = qm$$

[*2] [1] においてこの部分の記述が無い

[*3] この言い表し方は，必ずしもわかりやすいとは言えないが [1] にならった．他の表し方も色々ある．[2] においては「m は法 n に関して a が属する**ベキ数**である」と表現している．また n を法とする a の位数（multiplicative order of a modulo n）と呼び，$\mathrm{ord}_n(a)$ や $\mathrm{O}_n(a)$ などと記す場合もある．

逆に $k = qm$ であると，

$$a^k = a^{qm} = (a^m)^q \equiv 1$$

[証明おわり]

定理 5 n を法とする場合，a に対応する指数が m であるとき，a^k に対応する指数は

$$\frac{m}{(k,m)}$$

である．

[証明]$(m,k) = d, m = m_0 d, k = k_0 d$ とすると，

$$\left(a^k\right)^{\frac{m}{d}} = a^{\frac{km}{d}} = a^{k_0 m} = (a^m)^{k_0} \equiv 1$$

逆に

$$\left(a^k\right)^x \equiv 1$$

とおくと，定理 4 より kx は m の倍数である．つまり

$$kx = lm$$

とおける

$$k_0 dx = lm_0 d$$

より

$$x = \frac{lm_0}{k_0}$$

$(k_0, m_0) = 1$ であるから，x に最小の自然数解を与えるのは $l = k_0$ のときで，解は

$$x = m_0 = \frac{m}{d}$$

[証明おわり]

補題 1 $(a,b) = d$ とするとき，$d = a_0 b_0$ となる a_0, b_0 を適当に選び，

$$\left(\frac{a}{a_0}, \frac{b}{b_0}\right) = 1$$

とすることができる．

[証明]

$$a = a_1 d, b = b_1 d$$

とする．当然

$$(a_1, b_1) = 1$$

である．よって，d を構成する素因数が a_1, b_1 のどちらかに含まれる可能性はあるが，両方に含まれる可能性はない．よって d の素因数のうち a_1 に含まれるものを全て b_0 に含め，b_1 に含まれるものを全て a_0 に含め

る．どちらにも含まれない素因数はどちらか一方に含める．そうすると，a_1 と $\dfrac{d}{b_0}$ に共通因数はない．b_1 と $\dfrac{d}{a_0}$ も共通因数をもたない．よって，$\dfrac{a_1 d}{a_0}$ と $\dfrac{b_1 d}{b_0}$ も共通因数をもたない．つまり，

$$\left(\frac{a}{a_0}, \frac{b}{b_0}\right) = 1$$

とすることができる． [証明おわり]

定義 7 p を法とするとき，a に対応する指数が $p-1$ であるとき a を p を法としての**原始根**[*4]と呼ぶ．または略して p の原始根ともいう．

定理 6 p を法とする原始根は必ず存在する．

[証明]m が a に対応する指数であるとき，

$$a^0(=1), a, a^2, a^3, \cdots, a^{m-1} \tag{8}$$

は全て

$$x^m \equiv 1 \pmod{p} \tag{9}$$

の解である．しかもこれらは全て不合同である．なぜならば，もし $a^h \equiv a^k (h > k)$ ならば $a^k(a^{h-k} - 1) \equiv 0$ つまり $a^{h-k} \equiv 1$ となり，m より小さい指数で 1 が実現してしまうこととなりこれは矛盾である．

定理 3 より m 次合同式の解の個数は m 個以下なので，(9) の解は (8) が全てである．

さて，もし $m = p-1$ であるなら，a が原始根なので論ずる必要はない．$m < p-1$ であるとき m より大きい数を対応する指数とする数が必ず存在することが言えればこの定理は証明できたことになる．

$m < p-1$ ならば (8) の類以外の数で p で割り切れない数が一つ以上存在する．そのうちの一つを b とする．また，b に対応する指数を n とする．つまり，n は

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

を実現する最小の正の指数である．(8) 以外なので当然 $n > 1$ である．

1. $(m, n) = 1$ ならば ab に対応する指数は mn であることを証明する．

$$(ab)^{mn} = a^{mn} b^{nm} = (a^m)^n (b^n)^m \equiv 1 \cdot 1 = 1$$

逆に，

$$(ab)^x \equiv 1$$

であるとき，

$$(ab)^{xm} \equiv 1$$

$$(a^m)^x b^{mx} \equiv 1$$

$$b^{mx} \equiv 1$$

[*4] 原始元という言い方もあるが，原子根の方が一般的である．

定理 4 より mx は n の倍数である．同様にして nx は m の倍数である．$(m,n)=1$ なので x は a,b の公倍数である．最小公倍数は

$$x = mn$$

である．

このことにより m よりも大きい指数 mn に対応する数 ab が見つかった．

2. $(m,n)=d>1$ のとき，m,n の最小公倍数を l とする．

$$dl = mn$$

より，

$$l = \frac{mn}{d} \tag{10}$$

補題 1 より，適当に m_0, n_0 を選び，

$$d = m_0 n_0, \left(\frac{m}{m_0}, \frac{n}{n_0}\right) = 1$$

とすることができる．今，

$$(a^{m_0})^x \equiv 1$$

とおくと，定理 4 より

$$m_0 x = km$$

とおける．

$$x = \frac{km}{m_0}$$

x が最小の自然数となるのは $k=1$ のときで，

$$x = \frac{m}{m_0}$$

つまり，a^{m_0} は指数 $\dfrac{m}{m_0}$ に対応する．同様に b^{n_0} は指数 $\dfrac{n}{n_0}$ に対応する．よって 1. と同じ論法により，$a^{m_0}b^{n_0}$ は $\dfrac{mn}{m_0 n_0}$ に対応する．(10) より $a^{m_0}b^{n_0}$ は l に対応する．n が m の約数であると $l=m$ となるが，そのようなことはない．なぜならば $m=in$ とすると $b^m=(b^n)^1\equiv 1$ となり，b は (9) の解の一つ，つまり (8) のどれかと合同であることになるが，これは (8) 以外から b を選んだということと矛盾するからである．よって，

$$l > m$$

である．

1. および 2. より，常に m より大きい指数に対応する整数を見つけることができ，有限回でいずれ原始根に達する． [証明おわり]

これらのことから次の定理がいえる．

定理 7 p と互いに素である 任意の 整数 a について

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

が成り立つのは n が $p-1$ の倍数であるときに限られる.

問題 1 41 を法とする原始根を一つ求めよ.

[解]

$$2^6 = 64 \equiv 23$$

$$2^7 \equiv 46 \equiv 5$$

$$2^{10} \equiv 40 \equiv -1$$

$$\therefore 2^{20} \equiv 1$$

2^k と合同でない 3 を選ぶと,

$$3^4 = 81 \equiv -1$$

$$3^8 \equiv 1$$

$$(20, 8) = 4$$

また 20 と 8 の最小公倍数は 40 である.

$$m_0 = 4, n_0 = 1$$

とすると,

$$\left(\frac{20}{m_0}, \frac{8}{n_0}\right) = 1$$

とすることができ,

$$2^4 3^1 = 48 \equiv 7$$

となり 7 が原始根の一つである. この方法で必ずしも最小原始根が求まるとは限らない.

定理 8 p を法とする原始根を r とすると,

$$1, r, r^2, \cdots, r^{p-2}$$

は既約剰余系（既約代表の一組）である.

[証明略] 定理 6 の冒頭の部分より明らか. [証明おわり]

定理 9 p を法とする原始根を r とすると, r^k が原始根であるための条件は

$$(k, p-1) = 1$$

である.

[証明] 定理 5 より r は指数 $p-1$ に対応するので, r^k は指数

$$\frac{p-1}{(k, p-1)}$$

に対応する. よって, $(k, p-1) = 1$ のときこれは原始根である. 逆に原始根であるとき $(k, p-1) = 1$ である. [証明おわり]

定理 10 p を法とする原始根は $\phi(p-1)$ 個ある．

[証明略] 定理 9 より明らか

問題 2 41 を法とする原始根を全て求めよ．

[解] 問題 1 より 7 は原始根である．40 と互いに素である数を指数に選び

$$
\begin{aligned}
7^3 &\equiv 8 \times 7 = 56 \equiv 15 \\
7^7 &\equiv 15^2 \times 7 = 225 \times 7 \equiv 20 \times 7 \equiv 17 \\
7^9 &\equiv 17 \times 8 = 136 \equiv 13 \\
7^{11} &\equiv 13 \times 8 = 104 \equiv 22 \\
7^{13} &\equiv 22 \times 8 = 176 \equiv 12 \\
7^{17} &\equiv 12 \times 23 = 276 \equiv 30 \\
7^{19} &\equiv 30 \times 8 = 240 \equiv -6 \equiv 35 \\
7^{21} &\equiv 35 \times 8 \equiv -48 \equiv -7 \equiv 34 \\
7^{23} &\equiv -56 \equiv -15 \equiv 26 \\
7^{27} &\equiv 26 \times 23 \equiv 24 \\
7^{29} &\equiv 24 \times 8 = 28 \\
7^{31} &\equiv 28 \times 8 \equiv 19 \\
7^{33} &\equiv 19 \times 8 = 152 \equiv 29 \\
7^{37} &\equiv 29 \times 23 = 232 \equiv 11 \\
7^{39} &\equiv 11 \times 8 = 88 \equiv 6
\end{aligned}
$$

定理 10 を拡張すると次の定理になる．

定理 11 $p-1$ の任意の約数を d とすると，指数 d に対応する数（類）の個数は

$$\phi\left(\frac{p-1}{d}\right)$$

である．

[証明] 定理 5 より，指数 $\dfrac{p-1}{(k,p-1)}$ は r^k に対応する．r^k は互いに不合同であるので，$d=(k,p-1)$ である k の個数が指数 d に対応する数（類）の個数である．オイラー関数の性質により，これは

$$\phi\left(\frac{p-1}{d}\right) \text{個}$$

である． [証明おわり]

19 を法とするべき（累乗）を表 1 に示す．1 となった後は同じことを繰り返す．原始根は 6 個である．各数のべきが最初に 1 となる指数は 18 の約数つまり 1,2,3,6,9,18 のどれかになっていることがわかる．またその指数に対応する数（類）の個数はそれぞれ $\phi(1),\phi(2),\phi(3),\phi(6),\phi(9),\phi(18)$, つまり 1,1,2,2,6,6（個）であることもわかる．

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
a^2		4	9	16	6	17	11	7	5	5	7	11	17	6	16	9	4	1
a^3		8	8	7	11	7	1	18	7	12	1	18	12	8	12	11	11	
a^4		16	5	9	17	4		11	6	6		7	4	17	9	5	16	
a^5		13	15	17	9	5		12	16	3		8	14	10	2	4	6	
a^6		7	7	11	7	11		1	11	11		1	11	7	11	7	7	
a^7		14	2	6	16	9			4	15			10	3	13	17	5	
a^8		9	6	5	4	16			17	17			16	4	5	6	9	
a^9		18	18	1	1	1			1	18			18	18	18	1	1	
a^{10}		17	16							9			6	5	4			
a^{11}		15	10							14			2	13	3			
a^{12}		11	11							7			7	11	7			
a^{13}		3	14							13			15	2	10			
a^{14}		6	4							16			5	9	17			
a^{15}		12	12							8			8	12	8			
a^{16}		5	17							4			9	16	6			
a^{17}		10	13							2			3	15	14			
a^{18}	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

表 1

定理 12 p_1 を法とする原始根であり，p_1 と異なる p_2 を法とする原始根でもある数が存在する．

[証明]　p_1 を法とする原始根の一つを r_1，p_2 を法とする原始根の一つを r_2 とする．中国剰余定理より連立合同式

$$\begin{cases} x \equiv r_1 \pmod{p_1} \\ x \equiv r_2 \pmod{p_2} \end{cases}$$

を満たす x が p_1p_2 を法として一つある．　[証明おわり]

一つの素数を法とする複数の原始根同士はいかなる法においても不合同であるので，p_1 を法とする原始根が k 個，p_2 を法とする原始根が l 個あるとすると，両方の原始根である数は p_1p_2 を法として kl 個ある．以上は 2 個の素数についてであるが，それ以上の個数の素数についても同じことが言える．

参考文献

[1] 高木貞治『初等整数論講義第 2 版」（共立出版社，1997 年）

[2] ИМ ヴィノグラードフ著三瓶与右衛門・山中健訳『整数論入門』（共立出版，1981 年）