奇素数の冪を法とする原始根

オイラーは素数を法とする原始根を発見し，それが $\phi(p-1)$ 個存在することを示した．オイラー自身は任意の素数についてその原始根の存在を証明することができなかった．ガウスは『整数論』でこれを証明し，さらに任意の奇素数の冪を法とする場合も原始根が存在すること，2 の冪が法の場合は原始根が存在しないことを示した[*1]．

定義 1 素数冪 p^h を法とするとき，a に対応する指数が $\phi(p^h) = p^{h-1}(p-1)$ であるとき a を p^h を法としての**原始根**と呼ぶ．または略して p^h の原始根ともいう．

補題 1 奇素数 p について，$(k,p) = 1$ のとき

$$(1+kp)^p = 1 + k'p^2 \tag{1}$$

と表され，

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

である．

[証明](1) の左辺を展開すると

$$\begin{aligned}(1+kp)^p &= 1 + kp^2 + k^2\frac{p^3(p-1)}{2} + \cdots + k^p p^p \\ &= 1 + p^2\left(k + k^2\frac{p(p-1)}{2} + k^3\frac{p^2(p-1)p-2)}{6} + \cdots + k^p p^{p-2}\right)\end{aligned}$$

$k' = k + k^2\dfrac{p(p-1)}{2} + k^3\dfrac{p^2(p-1)(p-2)}{6} + \cdots + k^p p^{p-2}$ とおくと，$p > 2$ なので

$$k \equiv k' \pmod{p}$$

$$\therefore (k',p) = 1$$

[証明おわり]

この場合 p は奇素数なのでこの補題は成り立ったが，$p = 2$ では成り立たない．

補題 2 素数 p について，$e > 1, (k,p) = 1$ のとき

$$(1+kp^e)^p = 1 + k'p^{e+1} \tag{2}$$

と表され，

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

である．

[*1] 参考文献 [2]

[証明] 補題 1 と同様に (2) の左辺を展開すると

$$\begin{aligned}(1+kp^e)^p &= 1+kp^{e+1}+k^2\frac{p^{2e+1}(p-1)}{2}+\cdots+k^pp^{ep}\\ &= 1+p^{e+1}\left(k+k^2\frac{p^e(p-1)}{2}+k^3\frac{p^{2e}(p-1)(p-2)}{6}+\cdots+k^pp^{ep-e-1}\right)\end{aligned}$$

$k'=k+k^2\dfrac{p^e(p-1)}{2}+k^3\dfrac{p^{2e}(p-1)(p-2)}{6}+\cdots+k^pp^{ep-e-1}$ とおくと，$e>1$ なので

$$k\equiv k' \pmod p$$

$$\therefore (k',p)=1$$

[証明おわり]

補題 3 奇素数 p について，$(k,p)=1$ のとき

$$(1+kp)^{p^n}=1+k^{(n)}p^{n+1}$$

と表され,

$$\left(k^{(n)},p\right)=1$$

である.

[証明] 補題 1,2 より

$$\begin{aligned}(1+kp)^p &= 1+k'p^2, \quad (k',p)=1,\\ (1+kp)^{p^2} &= \left(1+k'p^2\right)^p = 1+k''p^3, \quad (k'',p)=1,\\ (1+kp)^{p^3} &= \left(1+k''p^3\right)^p = 1+k'''p^4, \quad (k''',p)=1,\\ &\cdots\cdots\cdots\cdots\cdots\cdots\cdots\\ (1+kp)^{p^n} &= \left(1+k^{(n-1)}p^{n-1}\right)^p = 1+k^{(n)}p^{n+1}, \quad \left(k^{(n)},p\right)=1\end{aligned}$$

[証明おわり]

定理 1 r が奇素数 p を法とする原始根であり，$r^{p-1}=1+kp,(k,p)=1$ であるとき，r は p^h を法とする原始根でもある.

[証明] 当然のことながら $r^{p^{h-1}(p-1)}\equiv 1 \pmod{p^h}$ であるから r^{p-1} は p^h を法として指数 p^{h-1} の約数に対応するが，補題 3 の証明の過程より，p^{h-1} より小さい指数では $1 \pmod{p^h}$ になりえない．よって指数 p^{h-1} に対応する．よって r は $p^{h-1}(p-1)$ 乗して始めて $1 \pmod{p^h}$ となる．よって r は p^h の原始根である.
[証明おわり]

定理 2 r が奇素数 p を法とする原始根であり，$r^{p-1}=1+kp^v, v>1$ であるとき，$r+p$ は p^h を法とする原始根である.

[証明]

$$\begin{aligned}(r+p)^{p-1} &= r^{p-1} + (p-1)r^{p-2}p + \frac{(p-1)(p-2)}{2}r^{p-3}p^2 + \cdots + p^{p-1} \\ &= 1 + kp^v + (p-1)r^{p-2}p + \frac{(p-1)(p-2)}{2}r^{p-3}p^2 + \cdots + p^{p-1} \\ &= 1 + p\left(kp^{v-1} + (p-1)r^{p-2} + \frac{(p-1)(p-2)}{2}r^{p-3}p^{+} \cdots + p^{p-2}\right)\end{aligned}$$

$k' = kp^{v-1} + (p-1)r^{p-2} + \dfrac{(p-1)(p-2)}{2}r^{p-3}p^{+} \cdots + p^{p-2}$ とおくと

$$k' \equiv -r^{p-2} \not\equiv 0 \pmod{p}$$

$$\therefore (k', p) = 1$$

あとは定理 1 と同様の証明によって $r+p$ は p^h を法とする原始根であるということがいえる． [証明おわり]
定理 1,2 より，p を法とする原始根 r はそれ自身が p^h の原始根であるか，または $r+p$ が p^h の原始根となる．ちなみに定理 2 における r は，それ自身は p^h の原始根にはなりえない．それは補題 3 と同じ過程を踏むことによって，$r^{p^h(p-1)}$ になる前に 1 となってしまうからである．

問題 1 27 の原始根を求めよ．

[解]3 の原始根は 2,5,8,11,14,17,20,23,26 である．これらの 2 乗が 9 を法として 1 にならなければ 27 の原子根である．1 になれば次の数が原始根である．

$$\begin{aligned}2^{3-1} &\equiv 4 \pmod{3^2} \\ 5^{3-1} &= 25 \equiv 7 \pmod{3^2} \\ 8^{3-1} &= 64 \equiv 1 \pmod{3^2} \\ 11^{3-1} &\equiv \text{略} \\ 14^{3-1} &\equiv 5^2 \pmod{3^2} \\ 17^{3-1} &\equiv 8^2 \equiv 1 \pmod{3^2} \\ 20^{3-1} &\equiv \text{略} \\ 23^{3-1} &\equiv 5^2 \pmod{3^2} \\ 26^{3-1} &\equiv 1 \pmod{3^2}\end{aligned}$$

よって原始根は 2,5,11,14,20,23 の 6 個である．27 を法とする冪（累乗）を表 1 に示す（3 の倍数は省いてある）．

また，一つの原始根を求めそれを $\phi(27) = 18$ と互いに素である数で冪乗することによっても他の原始根を求めることもできる．つまり

$$\begin{aligned}2^5 &= 32 \equiv 5 \pmod{27} \\ 2^7 &\equiv 5 \times 4 = 20 \pmod{27} \\ 2^{11} &\equiv 20 \times 16 \equiv 23 \pmod{27} \\ 2^{13} &\equiv 23 \times 4 \equiv 11 \pmod{27} \\ 2^{17} &\equiv 11 \times 16 \equiv 14 \pmod{27}\end{aligned}$$

a	1	2	4	5	7	8	10	11	13	14	16	17	19	20	22	23	25	26
a^2		4	16	25	22	10	19	13	7	7	13	19	10	22	25	16	4	1
a^3		8	10	17	19	26	1	8	10	17	19	26	1	8	10	17	19	
a^4		16	13	4	25	19		7	22	22	7	10		25	4	13	16	
a^5		5	25	20	13	17		23	16	11	4	8		14	7	2	22	
a^6		10	19	19	10	1		10	19	19	10	1		10	19	19	10	
a^7		20	22	14	16			2	4	23	25			11	13	5	7	
a^8		13	7	16	4			22	25	25	22			4	16	7	13	
a^9		26	1	26	1			26	1	26	1			26	1	26	1	
a^{10}		25		22				16		13				7		4		
a^{11}		23		2				14		20				5		11		
a^{12}		19		10				19		10				19		10		
a^{13}		11		23				20		5				2		14		
a^{14}		22		7				4		16				13		25		
a^{15}		17		8				17		8				17		8		
a^{16}		7		13				25		4				16		22		
a^{17}		14		11				5		2				23		20		
a^{18}	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

表 1

定理 3 奇素数冪 p^h を法とする原始根の一つを r とすると，

$$1 = r^0, r, r^2, \cdots, r^{\phi(p^h)-1} \tag{3}$$

は法 p^h の既約類を代表する．

[証明] まず明らかに $r^x \not\equiv 0 \pmod{p} (0 \leq x < \phi(p^h))$．もし $r^x \equiv 0$ なら $r^{\phi(p^h)} \equiv 1$ となりえない．よって (3) にあげた数は全て p^h と互いに素である．またそれぞれはお互いに不合同である．もし $r^x \equiv r^y (0 \leq x < y < \phi(p^h))$ であるとすれば $r^x(1 - r^{y-x}) \equiv 0$ となり $r^{\phi(p^h)}$ ではじめて 1 となることと矛盾する．よって，(3) は $\phi(p^h)$ 個の既約類全てである． [証明おわり]

問題 2 25 の原始根を一つ求めよ．

[解]$2^2 \equiv -1 \pmod{5}$ であるから 2 は 5 の原始根である．また $2^4 = 16 = 1 + 3 \times 5$ であるから，2 は 25 の

原始根でもある．他の原始根は

$$\begin{aligned}
2^3 &= 8 \\
2^7 &\equiv 3 \pmod{25} \\
2^9 &\equiv 12 \pmod{25} \\
2^{11} &\equiv 48 \equiv 23 \pmod{25} \\
2^{13} &\equiv 17 \pmod{25} \\
2^{17} &\equiv 22 \pmod{25} \\
2^{19} &\equiv 88 \equiv 13 \pmod{25}
\end{aligned}$$

である．素数を法とする場合と同じように指数表を作ることもできる．

$$N = 2^I \pmod{25}$$

N	1	2	3	4	6	7	8	9	11	12	13	14	16	17	18	19	21	22	23	24
I	0	1	7	2	8	5	3	14	16	9	19	6	4	13	15	18	12	17	11	10

表 2

定理 4 奇素数 p の冪 p^n を法とする原始根の個数は

$$\phi(\phi(p^n)) = p^{n-2}(p-1)\phi(p-1)$$

である．

[証明]r を法 p^n の原始根とすると，r は指数

$$\phi(p^n)$$

に対応する．r^x が指数 $\phi(p^n)$ に対応するための必要十分条件は

$$(x, \phi(p^n)) = 1$$

である．このような x は $\phi(\phi(p^n))$ 個ある． [証明おわり]

2 を法とする原始根は 1 である．4 を法とする原始根は 3 である．$2^h (h > 2)$ を法とする場合は原始根はない．今仮に

$$r = 1 + 2k, (k, 2) = 1$$

とすると，

$$r^2 = 1 + 4k(k+1) = 1 + 8k'$$

となり，2 乗することで既に 2^3 を法として 1 になってしまう．さらに $e > 1$ のとき

$$(1 + 2^e k)^2 = 1 + 2^{e+1} k', (k', 2) = 1$$

が成り立つので $2^{\phi(2^h)}$ となる手前で法 2^h に対して 1 となってしまうからである．

問題 3 奇素数 p と p を法とする原始根 $r(1 < r < p < 100)$ の組 (p, r) で，r が法 p^2 に関して原始根でないものを求めよ．

[解] おそらくコンピュータの助けを借りないと無理だと思われる．アルゴリズムとしては

1. 100 未満の自然数全体から p を素数に絞る．
2. p 未満の原始根を探す．
3. $r^{p-1} \equiv 1 \pmod{p^2}$ であるものを探す．

という手順で行えば見つかるが，実際は 3. を一等先にやるとかなり絞られ，2. の条件を満たすものを選べば求まる．解は 4 組あって，

$$(29, 14), (37, 18)(43, 19), (71, 11)$$

である．

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] 「具象数学初級」<http://math.pisan-dub.jp/concrete/>