原始根の存在定理と平方剰余の相互法則

原始根の存在定理

a は素数 p と互いに素であるとする。

このとき，フェルマーの小定理により $a^{p-1}\equiv 1 \pmod{p}$ が成り立つ。

$a^{e}\equiv 1 \pmod{p}$ が成り立つ，正で最小な整数 e を，a の**位数**という。

e を a の位数とすると， $1\leqq e\leqq p-1$ である。a の位数が $p-1$ であるとき，a を**原始根**という。

以下，素数 p を法とする合同で考える 。

命題 1　位数は $p-1$ の約数である。

証明　位数が e である自然数は存在するとし，その 1 つを a とする。すなわち

$$a^{e}\equiv 1,\quad 0<e\leqq p-1$$

このとき，除法の定理により

$$p-1=eq+r,\quad 0\leqq r<e$$

を満たす　q，r　が存在する。これより

$$a^{p-1}=a^{eq+r}$$

$$a^{p-1}=(a^{e})^{q}\cdot a^{r}$$

$a^{p-1}\equiv 1$，$a^{e}\equiv 1$ であるから

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

$0\leqq r<e$ であるから，位数 e の定義により $r=0$

よって，　$p-1=eq$

したがって，e は $p-1$ の約数である。

□

命題 2　素数 p より小さい自然数で，位数が e であるものの個数は，0 か $\varphi(e)$ のどちらかである。ただし，φ はオイラーの関数である。

（註　自然数 n と互いに素である，n 以下の自然数の個数を $\varphi(n)$ とする。）

証明　a の位数はで e であるとし，合同方程式　$x^{e}\equiv 1$　…①　の解について考える。

$$(a^{k})^{e}=(a^{e})^{k}\equiv 1\quad (0\leqq k<e)$$

よって，　$a^{k}\ (0\leqq k<e)$　…②　は①の解である。

また，　$a^{j}\equiv a^{k}\ (0\leqq j<k<e)$　と仮定すると　$a^{k-j}\equiv 1\ (0<k-j<e)$

これは e の定義により矛盾する。

よって，　$a^{k}\ (0\leqq k<e)$　は，どの 2 つも互いに合同でない。

また，①は e 次の方程式であるから，①の互いに合同でない解は多くても e 個である。

したがって，②が合同方程式　$x^{e}\equiv 1$　の解のすべてである。

$0\leqq k<e$ とする。

$(a^k)^l \equiv 1 \Leftrightarrow a^{kl} \equiv 1 \Leftrightarrow kl$ は e の倍数

であるから，$0<l<e$ のときに $(a^k)^l \equiv 1$ となる l が存在しないための必要十分条件は，kl が e の倍数となるような l が存在しないこと，すなわち，k と e が互いに素であることであり，そのような k の個数は $\varphi(e)$ である。

よって，素数 p より小さい自然数で，位数が e であるものの個数は，0 か $\varphi(e)$ のどちらかである。

特に，p より小さい自然数の原始根の個数は，0 か $\varphi(p-1)$ のどちらかである。

□

補題　自然数 n の正の約数 d について，$\varphi(d)$ の総和は n になる。すなわち　$n=\sum_d \varphi(d)$

証明　n 以下の自然数で，n との最大公約数が d であるものの集合を A_d とする。

また，$\frac{n}{d}$ 以下の自然数で，$\frac{n}{d}$ と互いに素であるものの集合を B_d とする。

$m \in A_d \quad \Rightarrow \quad \frac{m}{d}$ は $\frac{n}{d}$ 以下の自然数で，$\frac{m}{d}$ と $\frac{n}{d}$ は互いに素 $\quad \Rightarrow \quad \frac{m}{d} \in B_d$

逆に，

$k \in B_d \quad \Rightarrow \quad kd$ は n 以下の自然数で，kd と n の最大公約数は $d \quad \Rightarrow \quad kd \in A_d$

よって，　$A_d=\{a_1, a_2, \cdots\cdots, a_l\}$　とすると，　$B_d=\left\{\frac{a_1}{d}, \frac{a_2}{d}, \cdots\cdots, \frac{a_l}{d}\right\}$　であるから，A_d と B_d の要素の個数は等しい。

集合 B_d の要素の個数は　$\varphi\left(\frac{n}{d}\right)$　であるから，集合 A_d の要素の個数を $|A_d|$ とすると，

$$|A_d|=\varphi\left(\frac{n}{d}\right)$$

これより

$$n=\sum_d |A_d|=\sum_d \varphi\left(\frac{n}{d}\right)$$

ここで，自然数 $\frac{n}{d}$ も自然数 n の正の約数であり，その集合は自然数 d の集合に等しい。よって

$$\sum_d \varphi\left(\frac{n}{d}\right)=\sum_d \varphi(d)$$

したがって

$$n=\sum_d \varphi(d)$$

□

註　例えば，　$n=24, d=3$　のとき，　$A_3=\{3, 9, 15, 21\}$　で，$\frac{n}{d}=8$，　$B_3=\{1, 3, 5, 7\}$　である。

定理　p を素数とするとき，$p-1$ の任意の正の約数 d を位数とする $p-1$ 以下の自然数が $\varphi(d)$ 個存在する。

証明　$p-1$ 以下の自然数は，必ずある位数を持つから，位数 e によって分類できる。位数が e である自然数が存在するとき，その個数は，命題２により $\varphi(e)$ であるから

$$p-1=\sum_{e}\varphi(e)$$

命題１により，位数 e は $p-1$ の約数であるから，d を $p-1$ の正の約数とすると

$$\sum_{e}\varphi(e)\leqq\sum_{d}\varphi(d)$$

また，補題により

$$\sum_{d}\varphi(d)=p-1$$

以上より

$$p-1=\sum_{e}\varphi(e)\leqq\sum_{d}\varphi(d)=p-1 \quad \text{であるから} \quad \sum_{e}\varphi(e)=\sum_{d}\varphi(d)$$

したがって，$p-1$ の任意の正の約数 d を位数とする $p-1$ 以下の自然数が $\varphi(d)$ 個存在する。

□

この定理において，特に，位数が $p-1$ である自然数も存在するから，原始根は存在する。

参考　原始根の存在定理の別証明（高木貞二先生の「初等整数論講義」にある証明法）

この証明法では，原始根を見つけるアルゴリズムが与えられます。

補題　a，b の位数がそれぞれ e，f で，e と f が互いに素であるとき，ab の位数は ef である。

証明　$(ab)^{ef}=(a^e)^f\cdot(b^f)^e\equiv1$

ここで，$(ab)^x\equiv1$ となる x について考える。

$(ab)^{ex}=\{(ab)^x\}^e\equiv1$ であるから $b^{ex}\equiv(a^e)^x\cdot b^{ex}=(ab)^{ex}\equiv1$

よって，ex は f の倍数であるが，e と f は互いに素であるから，x は f の倍数である。

同様にして，x は e の倍数である。

ここで，e と f は互いに素であるから，x は ef の倍数である。

したがって ab の位数は ef である。

□

定理　原始根は存在する。

証明　ある自然数 a の位数 e が　$e=p-1$　ならば，定理は証明された。

よって，　$e<p-1$　の場合を考える。

合同方程式　$x^e\equiv1$　の解は e 個しかないから　$x^e\equiv1$　を満たさない　$x=b$　が存在する。b の位数を f とすると，f は e の約数でない。したがって，e と f の最小公倍数を　l　とすると，　$l>e$　である。

ここで，$l=e_0f_0$，$(e_0,f_0)=1$ で，e_0 は e の約数，かつ f_0 は f の約数となる e_0，f_0 をとる。(注)

このとき，$\dfrac{e}{e_0}$ は整数であり，　$\left(a^{\frac{e}{e_0}}\right)^{e_0}=a^e\equiv1$

よって，$a^{\frac{e}{e_0}}$ の位数は e_0 の約数であるが，$a^{\frac{e}{e_0}}$ の位数が e_0 より小さいとすると，a の位数が e より小さくなり矛盾する。したがって，$a^{\frac{e}{e_0}}$ の位数は e_0 である。

同様にして，$b^{\frac{f}{f_0}}$ の位数は f_0 である。

$(e_0, f_0)=1$ であるから，補題により $a^{\frac{e}{e_0}}\cdot b^{\frac{f}{f_0}}$ の位数は $e_0\cdot f_0$ すなわち l である。

$l>e$ であるから，$a^{\frac{e}{e_0}}\cdot b^{\frac{f}{f_0}}$ の位数は e より大きい。

これを繰り返せば，遂には位数が $p-1$ である自然数が見つかるから，原始根は存在する。

□

注　e，f を素因数分解し，素因数の指数の大きい方が e，f のどちらであるかに従って，素因数を e_0，f_0 に分配する。指数が同じときはどちらに分配してもよい。この分配によって，条件を満たす e_0，f_0 が構成できる。

定理　r を原始根とするとき，$r^k\equiv 1 \pmod p$ ならば，k は $p-1$ の倍数。

証明　k を $p-1$ で割った商を s，余りを t とすると，$k=(p-1)s+t$ であるから

$$r^k=r^{(p-1)s+t}=r^{(p-1)s}\cdot r^t$$

$r^k\equiv 1$ ，$r^{p-1}\equiv 1$ であるから，$r^t\equiv 1$

$0<t<p-1$ とすると，原始根の定義に矛盾するから，$t=0$

よって，$k=(p-1)s$ となるから，k は $p-1$ の倍数である。

平方剰余の相互法則

p は 2 以外の素数とする。

$x^2\equiv a \pmod p$ が解を持つときに，a は p の平方剰余，解を持たないときに平方非剰余という。

a が p の倍数でないとき，a が平方剰余であるか，非剰余であるかに従って

$$\left(\frac{a}{p}\right)=1 \quad \text{または} \quad \left(\frac{a}{p}\right)=-1$$

とする。これを Legendre 記号という。

次の定理は，平方剰余と Legendre 記号の定義より明らかである。

定理　$a\equiv b \pmod p$ ならば $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$

定理　r を原始根とし，$a\equiv r^k \pmod p$ とする。このとき，a が平方剰余であるための必要十分条件は，k が偶数であることである。

証明　k が偶数のとき平方剰余であることは明らか。

逆に，　r^k　が平方剰余であると仮定すると，　$r^k \equiv b^2$　となる b が存在する。

b は r を用いて　$b \equiv r^l$　と表されるから　$r^k \equiv r^{2l}$　よって　$r^{k-2l} \equiv 1$

したがって，　$k-2l$　は偶数　$p-1$　の倍数であるから，k は偶数である。

□

系　　r を原始根とし，　$a \equiv r^k \ (mod\ p)$　とするとき，　$\left(\frac{a}{p}\right) = (-1)^k$

この系より，次の定理は明らかである。

定理　$\left(\frac{abc\cdots}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)\left(\frac{c}{p}\right)\cdots\cdots$

定理　(Euler の基準)

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \ (mod\ p)$$

証明

以下で，合同は p を法とする。

$$\left(a^{\frac{p-1}{2}}\right)^2 = a^{p-1} \equiv 1$$

であるから，

$$a^{\frac{p-1}{2}} \equiv 1 \quad \text{または} \quad a^{\frac{p-1}{2}} \equiv -1$$

r を原始根として　$a \equiv r^m$　とすると

$$a^{\frac{p-1}{2}} \equiv r^{m\cdot\frac{p-1}{2}} \qquad \cdots①$$

$a^{\frac{p-1}{2}} \equiv 1$　とすると，　$r^{m\cdot\frac{p-1}{2}} \equiv 1$　であるから，　$m\cdot\frac{p-1}{2}$　は　$p-1$　の倍数。

よって，　$\frac{m}{2}$　は整数であるから，m は偶数である。したがって，a は平方剰余である。

逆に，a が平方剰余であるとすると，m は偶数であるから，　$m\cdot\frac{p-1}{2}$　は　$p-1$　の倍数。

したがって，①より　$a^{\frac{p-1}{2}} \equiv 1$　である。

□

次の法則を，**平方剰余の相互法則**という。

p，q を異なる奇素数とするとき　$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$

与えられた数が平方剰余か否かを調べるには，さらに，次の補充法則を用いる。

第一補充法則　　$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$

第二補充法則　　$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Eulerの基準において，特に $a=-1$ とすると，第一補充法則が得られる。

ガウスの予備定理

a が奇素数 p で割り切れないとき

$$a,2a,3a,\cdots\cdots,\frac{p-1}{2}\cdot a$$

を p で割った絶対値剰余の中に，負であるものが n 個あるとすれば,

$$\left(\frac{a}{p}\right)=(-1)^n$$

証明　以下で，合同は p を法とする。

$1\leqq i<j\leqq\frac{p-1}{2}$ とする。

$ia\equiv ja$ とすると $(i-j)a\equiv 0$

$0<i-j<\frac{(p-1)}{2}$ であるから矛盾する。

$ia\equiv -ja$ とすると $(i+j)a\equiv 0$

$2<i+j<p-1$ であるから矛盾する。

したがって，　$a,2a,3a,\cdots\cdots,\frac{p-1}{2}\cdot a$ の絶対値剰余の絶対値はすべて異なる。

これより $a,2a,3a,\cdots\cdots,\frac{p-1}{2}\cdot a$ の絶対値剰余の絶対値は $1,2,3,\cdots\cdots,\frac{p-1}{2}$ を入れ替えたものである。よって

$$1a\cdot 2a\cdot 3a\cdots\cdots\frac{p-1}{2}a\equiv 1\cdot 2\cdot 3\cdots\cdots\frac{p-1}{2}\cdot(-1)^n$$

$$1\cdot 2\cdot 3\cdots\cdots\frac{p-1}{2}a^{\frac{p-1}{2}}\equiv 1\cdot 2\cdot 3\cdots\cdots\frac{p-1}{2}\cdot(-1)^n$$

$1,2,3,\cdots\cdots,\frac{p-1}{2}$ は p と互いに素であるから

$$a^{\frac{p-1}{2}}\equiv(-1)^n$$

オイラーの基準により

$$\left(\frac{a}{p}\right)\equiv(-1)^n$$

$\left(\frac{a}{p}\right),(-1)^n$ はともに±1 しかとらず，$p>2$ であるから

$$\left(\frac{a}{p}\right)=(-1)^n$$

□

第二補充法則の証明

ガウスの予備定理を用いる。

$2,4,6,\cdots\cdots,p-1$ のうちで絶対値平方剰余が負であるのは，$\frac{p}{2}$ より大きいものである。その個数を求める。

$p=4k+1$ と表されるとき

$\frac{p}{2}+\frac{1}{2}=2k+1$ より $\frac{p}{2}+\frac{1}{2}$ は奇数であるから，求める個数は，

$$\left\{(p-1)-\left(\frac{p}{2}+\frac{3}{2}\right)\right\}\div 2+1=\frac{p-1}{4}$$

奇数を掛けても偶奇は変わらないので，$\frac{p+1}{2}$ を掛けると $\frac{p^2-1}{8}$

$p=4k+3$ と表されるとき

$\frac{p}{2}+\frac{1}{2}=2k+2$ より $\frac{p}{2}+\frac{1}{2}$ は偶数であるから，求める個数は，

$$\left\{(p-1)-\left(\frac{p}{2}+\frac{1}{2}\right)\right\}\div 2+1=\frac{p+1}{4}$$

奇数を掛けても偶奇は変わらないので，$\frac{p-1}{2}$ を掛けると $\frac{p^2-1}{8}$

以上より，

$$\left(\frac{2}{p}\right)=(-1)^{\frac{p^2-1}{8}}$$

平方剰余の相互法則の証明

$1\cdot q,2\cdot q,3\cdot q,\cdots\cdots,\frac{p-1}{2}\cdot q$ のうちで，p で割ったときの絶対値剰余が負であるものの個数を m，

$1\cdot p,2\cdot p,3\cdot p,\cdots\cdots,\frac{q-1}{2}\cdot p$ のうちで，q で割ったときの絶対値剰余が負であるものの個数を n とすると，

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^m(-1)^n=(-1)^{m+n}\qquad\cdots①$$

である。

qk を p で割った絶対値剰余が負

$\Leftrightarrow$ $\frac{p}{2}<qk-ip<p$ となる整数 i が存在する。

$\Leftrightarrow$ $\frac{1}{2}<\frac{qk}{p}-i<1$ となる整数 i が存在する。

$\Leftrightarrow$ $\frac{qk}{p}<i+1<\frac{qk}{p}+\frac{1}{2}$ となる整数 i が存在する。

$\Leftrightarrow$ $\frac{q}{p}k$ と $\frac{q}{p}k+\frac{1}{2}$ の間に整数が存在する。

よって，　$1 \leqq x \leqq \dfrac{p-1}{2}$　の範囲において，直線　$y=\dfrac{q}{p}x$　と直線　$y=\dfrac{q}{p}x+\dfrac{1}{2}$　に挟まれた領域における格子点の個数が m である。

同様に，　$1 \leqq y \leqq \dfrac{q-1}{2}$　の範囲において，直線　$x=\dfrac{p}{q}y$　と直線　$x=\dfrac{p}{q}y+\dfrac{1}{2}$　に挟まれた領域における格子点の個数が n である。

これら2つの領域は重ならないから，2つの領域を合わせた領域の格子点の個数は　$m+n$　である。

p と q は互いに素であるから，　$0<x<p$　の範囲において，直線　$py=qx$　上には格子点はない。

また，　$0<x<1, \dfrac{p-1}{2}<x<\dfrac{p+1}{2}, 0<y<1, \dfrac{q-1}{2}<x<\dfrac{q+1}{2}$　のどの範囲にも格子点はない。

したがって，次の連立不等式が表す領域の格子点の個数も　$m+n$　である。

$$0<x<\frac{p+1}{2}\quad,\quad 0<y<\frac{q+1}{2}\quad,\quad y<\frac{q}{p}x+\frac{1}{2}\quad,\quad x>\frac{p}{q}y+\frac{1}{2}$$

この領域は，点　$\left(\dfrac{p+1}{4}, \dfrac{q+1}{4}\right)$　に関して対称である。

実際，直線　$x=0$　と直線　$x=\dfrac{p+1}{2}$　および，直線　$y=0$　と直線　$y=\dfrac{q+1}{2}$　は，この点に関して対称である。また，点　$\left(\dfrac{p+1}{4}, \dfrac{q+1}{4}\right)$　から平行な2直線　$y=\dfrac{q}{p}x+\dfrac{1}{2}$　，　$x=\dfrac{p}{q}y+\dfrac{1}{2}$　までの距離はともに，　$\dfrac{p+q}{4\sqrt{p^2+q^2}}$　であるから，この2直線もこの点に関して対称である。

ここで，p，q は奇数であるから，　$\dfrac{p+1}{4}, \dfrac{q+1}{4}$　は，整数か，整数$+\dfrac{1}{2}$ の形の数となる。よって，この領域における格子点は，点　$\left(\dfrac{p+1}{4}, \dfrac{q+1}{4}\right)$　に関して対称な位置に，2点が対となって現れる。これより，点　$\left(\dfrac{p+1}{4}, \dfrac{q+1}{4}\right)$　が格子点であるか否かに従って，この領域内にある格子点の個数は，それぞれ，奇数個か偶数個になる。

$m+n$　が奇数

$\Leftrightarrow$ 点　$\left(\dfrac{p+1}{4}, \dfrac{q+1}{4}\right)$　は格子点である

$\Leftrightarrow$ p，q はともに4で割って3余る素数

$\Leftrightarrow$　$\dfrac{p-1}{2}, \dfrac{q-1}{2}$　はともに奇数

$\Leftrightarrow$　$\dfrac{p-1}{2}\cdot\dfrac{q-1}{2}$　は奇数

よって，①より

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right)=(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

が成り立つ。

例 $\left(\frac{38}{41}\right)$ を求める。 $\left(\frac{38}{41}\right)=\left(\frac{2}{41}\right)\left(\frac{19}{41}\right)$ …① であり,

$$\left(\frac{2}{41}\right)=(-1)^{\frac{41^2-1}{8}}=(-1)^{5\cdot 42}=1 \quad \cdots②$$

また,

$\left(\frac{19}{41}\right)\left(\frac{41}{19}\right)=(-1)^{9\cdot 20}=1$ であるから $\left(\frac{19}{41}\right)=\left(\frac{41}{19}\right)=\left(\frac{3}{19}\right)$

$\left(\frac{3}{19}\right)\left(\frac{19}{3}\right)=(-1)^{1\cdot 9}=-1$ であるから $\left(\frac{3}{19}\right)=-\left(\frac{19}{3}\right)=-\left(\frac{1}{3}\right)=-1$

よって $\left(\frac{19}{41}\right)=-1$ …③

①，②，③より $\left(\frac{38}{41}\right)=-1$