平方剰余

文字は全て整数とする．p は 奇素数 とする．

定義 1 $(a,p)=1$ の場合，二次合同式

$$x^2 \equiv a \pmod{p}$$

が解を有するとき，a を p の**平方剰余**，解を有しないとき**平方非剰余**という．
前者を

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

後者を

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

と表す．この記号を**ルジャンドルの記号**という．a は $(a,p)=1$ である 正または負の 整数である．

$(a,p)\neq 1$ の場合，つまり $a\equiv 0 \pmod{p}$ のとき，

$$\left(\frac{a}{p}\right)=0$$

と定義するが，以後 $(a,p)=1$ の場合のみを扱う．

復習をすれば，a が平方剰余であるということは $\mathrm{Ind}.a$ が偶数であることと同値である．底となる原始根は任意である．つまり次のように表せる．

$$\left(\frac{a}{p}\right)=(-1)^{\mathrm{Ind}.a}$$

つまり，p を法とする既約類のうち平方剰余と非平方剰余は半分ずつである．a が平方剰余であるとき，$x^2\equiv a$ の一つの解を α とすれば，$p-\alpha$ も解である．つまり $1,2,3,\cdots,\dfrac{p-1}{2}$ の平方が p の平方剰余を与える．例えば 11 の平方剰余は

$$1^2=1, 2^2=4, 3^2=9, 4^2=16\equiv 5, 5^2=25\equiv 3$$

すなわち，1,3,4,5,9 である．1 はあらゆる奇素数 p の平方剰余である．

定理 1 $a\equiv a' \pmod{p}$ ならば，$\left(\dfrac{a}{p}\right)=\left(\dfrac{a'}{p}\right)$.

[証明略]

定理 2 $\left(\dfrac{abc\cdots}{p}\right)=\left(\dfrac{a}{p}\right)\left(\dfrac{b}{p}\right)\left(\dfrac{c}{p}\right)\cdots$

[証明略]

定理 3（**オイラーの規準**）

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

[証明]　a が平方剰余であるための必要十分条件は

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$$

ゆえに $\left(\frac{a}{p}\right) = 1$ ならば，$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$．また $\left(\frac{a}{p}\right) = -1$ ならば，$a^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$．フェルマーの小定理より $\left(a^{\frac{p-1}{2}}\right)^2 \equiv 1 \pmod{p}$ であるから，$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$　[証明おわり]

定理 4（**ガウスの予備定理**）$(a, p) = 1$ のとき

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

のうち p を法とした絶対最小剰余のうち負のものの数を n 個とすると，

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

[証明]$r = \frac{p-1}{2}$ とする．(1) の絶対最小剰余の絶対値の列を

$$a_1, a_2, a_3, \cdots, a_r$$

とすると，これらのどれも等しくない．なぜならば

$$a_i = aj, i \neq j$$

とすると，絶対剰余の符号が等しいときは

$$ai \equiv aj \pmod{p}$$

つまり

$$i \equiv j \pmod{p}$$

これはありえない．絶対剰余の符号が異なるときは

$$ai \equiv -aj \pmod{p}$$

つまり

$$i + j \equiv 0 \pmod{p}$$

$i + j < p - 1$ であるからこれもありえない．つまり集合

$$\{a_1, a_2, a_3, \cdots, a_r\}$$

と

$$\{1, 2, 3, \cdots, r\}$$

は等しい．つまり (1) の絶対最小剰余の積は

$$(-1)^n r!$$

である．また (1) の全ての積は

$$r! a^r$$

であるから，これらは p を法として等しい，つまり

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

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

左辺も右辺も ± 1 以外の値を取らないので,

$$a^r = (-1)^n$$

オイラーの規準より

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

[証明おわり]

定理 5 （第一補充法則）

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

[証明] オイラーの規準より

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

右辺は必ず ± 1 の値をとるので,

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

[証明おわり]

定理 6 （第二補充法則）

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

[証明] ガウスの予備定理より

$$2, 4, 6, \cdots, p-5, p-3, p-1$$

のなかで $\frac{p}{2}$ より大きいものの数を n とすると

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

n を求めることは困難ではないが，n が偶数であるか奇数であるかが問題となるだけなので，偶奇を求めることにすると,

$$n \equiv 1 + 3 + 5 + \cdots \pmod{2}$$

この級数の末項は p によって変る．$\frac{p-1}{2}$ が奇数であればこれが末項であり，偶数であればそれより 1 小さい整数である．しかしながら偶奇を問題とするだけならば次のように常に $\frac{p-1}{2}$ を，さらに奇数の間に全ての偶数を挿入してもかまわない．

$$n \equiv 1 + 2 + 3 + 4 + 5 + \cdots + \frac{p-1}{2} \pmod{2}$$

この級数は等差級数で初項 1，末項 $\dfrac{p-1}{2}$，項数 $\dfrac{p-1}{2}$ であるから，

$$n \equiv \frac{1}{2} \cdot \frac{p-1}{2}\left(\frac{p-1}{2}+1\right) = \frac{p^2-1}{8} \pmod 2$$

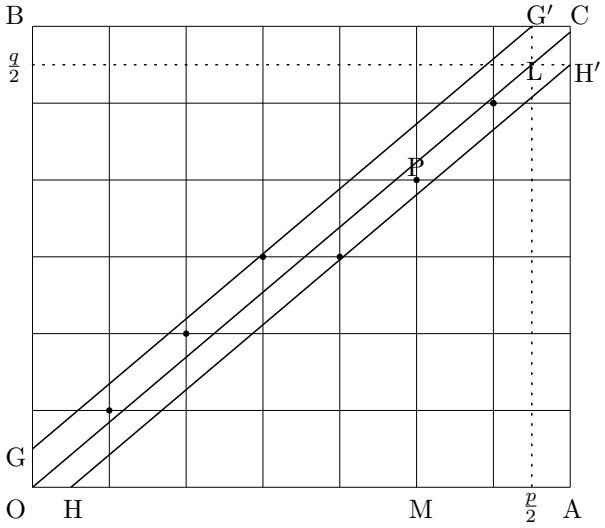
$$\therefore \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$$

[証明おわり]

定理 7 （平方剰余の相互法則）

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

［証明］



qx を p で割った余りが $\dfrac{p}{2}$ より大きいということはどういうことか，調べてみる．

$$qx = ps + r$$

と割り算ができたとすると，

$$r > \frac{p}{2}$$

$$\frac{qx}{p} = s + \frac{r}{p}$$

つまり

$$\frac{r}{p} > \frac{1}{2}$$

上図で言えば，点 P のような点と縦に見て最も近い格子点が上にある場合である．そのような格子点は全て，線分 OC と GG′ の間に存在する．このような格子点の数を n とすると

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

同様に上図を横方向に見ることにより，線分 OC と HH′ の間に存在する格子点の個数を m とすると，

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

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

$m+n$ は六角形 OGG′CH′H の内部の格子点の個数である．よく見ると，この六角形は点対称図形である．よってその対称の中心となる点が格子点でなければ $m+n$ は偶数であり，格子点であれば $m+n$ は奇数である．これは $\dfrac{p+1}{2}, \dfrac{q+1}{2}$ が偶数であるか，奇数であるかで決まる．よって題意は証明されたのである．

［証明おわり］

問題 1 p が $8n+1$ または $8n+3$ のときに限って

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

であることを証明せよ．

［解］

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

$$\frac{p-1}{2}+\frac{p^2-1}{8} = \frac{p^2+4p-5}{8} = \frac{p^2-4p+3}{8}+p-1 \equiv \frac{(p-1)(p-3)}{8} \pmod 2$$

［証明おわり］

問題 2 p が $5n \pm 1$ のときに限って

$$\left(\frac{5}{p}\right) = 1$$

であることを証明せよ．

［解］平方剰余の相互法則より

$$\left(\frac{5}{p}\right)\left(\frac{p}{5}\right) = (-1)^{\frac{p-1}{2}\cdot 2} = (-1)^{p-1} = 1$$

$$\therefore \left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$$

$p \equiv 1 \pmod 5$ のとき

$$\left(\frac{p}{5}\right) = \left(\frac{1}{5}\right) = 1$$

$p \equiv 4 \pmod 5$ のとき第一補充法則より

$$\left(\frac{p}{5}\right) = \left(\frac{-1}{5}\right) = (-1)^4 = 1$$

これらのとき

$$\left(\frac{5}{p}\right) = 1$$

残りの半数は全て非平方剰余なので $p \equiv 2$ または $p \equiv 3 \pmod 5$ のとき

$$\left(\frac{p}{5}\right) = -1$$

よってこれらのとき

$$\left(\frac{5}{p}\right) = -1$$

［証明おわり］

問題 3 p が $12n \pm 1$ のときに限って，$\left(\frac{3}{p}\right) = 1$ であることを証明せよ．

［解］平方剰余の相互法則より

$$\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right)$$

$p = 3m + 1$ のとき

$$\left(\frac{p}{3}\right) = 1$$

$p = 3m + 2$ のとき

$$\left(\frac{p}{3}\right) = -1$$

$p = 4l + 1$ のとき

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

$p = 4l + 3$ のとき

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

よって題意は証明された．［証明おわり］

問題 4 $\left(\frac{17}{23}\right)$ を求めよ．

$\left(\frac{17}{23}\right)\left(\frac{23}{17}\right) = (-1)^{4\cdot 11} = 1$ より

$$\left(\frac{17}{23}\right) = \left(\frac{23}{17}\right) = \left(\frac{6}{17}\right) = \left(\frac{2}{17}\right)\left(\frac{3}{17}\right)$$

第二補充法則より

$$\left(\frac{2}{17}\right) = (-1)^{\frac{288}{8}} = (-1)^3 6 = 1$$

$\left(\frac{17}{3}\right)\left(\frac{3}{17}\right) = 1$ より

$$\left(\frac{3}{17}\right) = \left(\frac{17}{3}\right) = \left(\frac{2}{3}\right)$$

第一または第二補充法則より

$$\left(\frac{2}{3}\right) = -1$$

$$\therefore \text{与式} = -1$$

問題 5 $\left(\dfrac{365}{1847}\right)$ を求めよ.

365 を素因数分解して

$$\left(\frac{365}{1847}\right) = \left(\frac{5}{1847}\right)\left(\frac{73}{1847}\right)$$

$\dfrac{5-1}{2} = 2, \dfrac{73-1}{2} = 36$ なので

$$\left(\frac{5}{1847}\right)\left(\frac{73}{1847}\right) = \left(\frac{1847}{5}\right)\left(\frac{1847}{73}\right) = \left(\frac{2}{5}\right)\left(\frac{22}{73}\right) = \left(\frac{2}{5}\right)\left(\frac{2}{73}\right)\left(\frac{11}{73}\right)$$

第二補充法則より

$$\left(\frac{2}{5}\right)\left(\frac{2}{73}\right)\left(\frac{11}{73}\right) = -\left(\frac{11}{73}\right) = -\left(\frac{73}{11}\right) = -\left(\frac{-4}{11}\right) = -\left(\frac{-1}{11}\right)\left(\frac{2^2}{11}\right) = -\left(\frac{-1}{11}\right)$$

第一補充法則より

$$-\left(\frac{-1}{11}\right) = 1$$

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] 芹沢正三『数論入門』（講談社ブルーバックス，2008 年）