

平方剰余の相互法則

電波通信

2021 年 2 月 2 日

TeX で

$$a \equiv b \pmod{p}$$

という式を入力するのがとても面倒だと思ったので、この文章では、この式を

$$a =_p b$$

と書くことにする。 $x \in \mathbb{Z}$ と素数 p に対して $x =_p a^2$ となる a が存在する時 x を p の平方剰余という。平方剰余でない数を平方非剰余と呼ぶ。

可換環 R に対して $R^\times$ で、 R の可逆元全体からなる群を表す。

素数 p に対して $\mathbb{F}_p$ で $\mathbb{Z}/p\mathbb{Z}$ を表す。商写像 $\mathbb{Z} \rightarrow \mathbb{F}_p$ を π_p で表す。 $\mathbb{F}_p$ は標数が p の体のになる。また、 $\mathbb{F}_p^\times$ は巡回群になる。この巡回群の生成元を p の原始根という。

写像 $s: \mathbb{F}_p^\times \rightarrow \mathbb{F}_p^\times$ を $s(x) = x^2$ で定義する。 $\mathbb{F}_p^\times$ は可換なので、 f は準同型になるので、 $s(\mathbb{F}_p^\times)$ は $\mathbb{F}_p^\times$ の部分群である。この群を S_p と書くことにする。乗法群 $\mathbb{F}_p^\times$ は可換なのでもちろん S は正規部分群である。 $p \neq 2$ ならば、体の一般論から $a \in \mathbb{F}_p$ に対して $x^2 = a$ となる $x \in \mathbb{F}_p$ はちょうど 2 つあるので、 S の位数は $(p-1)/2$ である。よって $p \neq 2$ の時、剰余群 $\mathbb{F}_p^\times/S_p$ は位数が 2 の群になる。位数が 2 の群は全て同型なので、同型写像 $e_p: \mathbb{F}_p^\times/S_p \rightarrow \{1, -1\}$ をとる。この時、 $a \in \mathbb{Z}$ に対してルジャンドル記号を $(a|p) := e_p \circ s \circ \pi_p(a)$ と定義する。 $\left(\frac{a}{p}\right)$ は $(a|p)$ と同じ意味である。ルジャンドル記号は次のように明示できる。

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & a \text{ は } p \text{ の平方剰余,} \\ -1 & a \text{ は } p \text{ の平方非剰余.} \end{cases}$$

つまり、平方剰余が 1 であるか、 -1 であるかに応じて、平方剰余かそうでないかがわかる。

定義から次のことがわかる。

命題 1. 任意の $a \in \mathbb{Z}$ に対して、

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

が成り立つ。

今からルジャンドル記号の計算方法を説明してゆく。まず次のオイラーの基準が基本的である。

命題 2. p を奇素数とする。このとき任意の $a \in \mathbb{Z}$ に対して

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

が成り立つ。

証明. 最初に注意するが, p が奇数なので, $\frac{p-1}{2}$ は整数である. まず, フェルマーの小定理から, 任意の $x \in \mathbb{F}_p^\times$ に対して

$$x^{p-1} = 1$$

が成り立つ. つまり, 任意の $a \in \mathbb{F}_p^\times$ は多項式 $x^{p-1} - 1$ の根になっている. さらに

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

と因数分解できる. さて, $S_p = \{y^2 \mid y \in \mathbb{F}_p^\times\}$ であるが, 任意の $x \in S_p$ に対して, $x = y^2$ であるとして, 再びフェルマーの小定理から $x^{\frac{p-1}{2}} = y^{p-1} = 1$ なので, $x^{\frac{p-1}{2}} - 1 = 0$ である. 体の一般論から, 多項式 $x^{\frac{p-1}{2}} - 1$ の根は高々 $\frac{p-1}{2}$ 個であり, $\text{card}(S_p) = \frac{p-1}{2}$ なので,

$$(2) \quad S_p = \{x \mid x^{\frac{p-1}{2}} - 1 = 0\}$$

である. $x \in \mathbb{F}_p \setminus S_p$ は平方非剰余の剰余類だが, $x^{p-1} - 1 = 0$ を満たすということと, 式 (1), (2) から, $x^{\frac{p-1}{2}} + 1 = 0$ を満たさなければならない. (体には零因子は 0 しかない.) よって, オイラーの基準が示された. $\square$

このオイラーの基準を使って直ちに平方剰余の相互法則の第一補充則がわかる.

命題 3. 奇素数 p と整数について,

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

が成り立つ.

証明. オイラーの基準から, $(a|p) = (-1)^{\frac{p-1}{2}}$ である. この両辺は 1 か -1 の値しか取らず, また, p が奇素数であることから, $2 \neq_p 0$ なので, 実際の等式として $(a|p) = (-1)^{\frac{p-1}{2}}$ を得る. $\square$

平方剰余の相互法則の第二補充則は次のものである.

命題 4. 奇素数 p に対して

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

証明. $A = \{1, \dots, \frac{p-1}{2}\}$ とおく. 任意の $a \in A$ についてももちろん

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

が成り立つ. よって

$$\begin{aligned} \prod_{a \in A} a &= \prod_{a \in A} ((-1)^a a)(-1)^a \\ &= \prod_{a \in A} ((-1)^a a) \prod_{a \in A} (-1)^a = (-1)^{\sum_{a \in A} a} \prod_{a \in A} ((-1)^a a) \\ &= (-1)^{\frac{p^2-1}{8}} \prod_{a \in A} ((-1)^a a) \end{aligned}$$

ここで等差数列の和の公式から $\sum_{a \in A} a = \frac{p^2-1}{8}$ であることを用いている. $B = \{2i \mid 0 < 2i \in A, i \in \mathbb{Z}\}$, $C = A \setminus B$ とおく. B は A に属する偶数全体の集合で, C は A に属する奇数の集合である. もちろん

$A = B \sqcup C$ である。 $D = \{2i \mid \frac{p}{2} < 2i < p, i \in \mathbb{Z}\}$ とおく。 D は $\frac{p}{2}$ より大きく、 p よりも小さい偶数全体の集合である。 簡単にわかることだが、 任意の $d \in D$ に対して、 $c \in C$ が存在して、 $p - c = d$ となる。 D と C の濃度は等しいことに注意しよう。 よって、

$$\prod_{a \in B} (-a) =_p \prod_{2i \in D} 2i = 2^{\text{card } C} \prod_{\frac{p}{4} < i < \frac{p}{2}} i$$

となる。 また、

$$\prod_{a \in B} a = \prod_{2i \in B} 2i = 2^{\text{card } B} \prod_{0 < i < \frac{p}{4}} i$$

となる。 よって、

$$\begin{aligned} \prod_{a \in A} ((-1)^a a) &= {}_p \left(2^{\text{card } C} \prod_{\frac{p}{4} < i < \frac{p}{2}} i \right) \left(2^{\text{card } B} \prod_{0 < i < \frac{p}{4}} i \right) \\ &= {}_p 2^{\text{card}(B) + \text{card}(C)} \prod_{0 < i < \frac{p}{2}} i \\ &= {}_p 2^{\text{card}(A)} \prod_{a \in A} a = {}_p 2^{\frac{p-1}{2}} \prod_{a \in A} a \end{aligned}$$

よって以上の式を合わせて、

$$\prod_{a \in A} a = {}_p (-1)^{\frac{p^2-1}{8}} 2^{\frac{p-1}{2}} \prod_{a \in A} a$$

を得る。 $\prod_{a \in A} a$ は $\mathbb{F}_p$ の中で 0 ではないので、

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

よって、オイラーの基準から、

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

を得るが、両辺は 1 か -1 の値しか取らず、 $2 \neq {}_p 0$ なので、結局

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

を得る。 □

平方剰余の相互法則は次のものである。

命題 5. 2つの異なる奇素数 p, q に対して、

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

証明. 中国剰余定理を用いた証明を紹介する。 p, q は異なる奇素数なので、特に互いに素である。 よって中国剰余定理から可逆元の間の同型

$$(\mathbb{Z}/pq\mathbb{Z})^\times \cong (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times$$

を得る。 さらに詳しくいうと、写像

$$\delta: (\mathbb{Z}/pq\mathbb{Z})^\times \rightarrow (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times; [k]_{pq} \mapsto ([k]_p, [k]_q)$$

は well-defined だし、同型写像である。さて、

$$A = \{[a]_{pq} \in (\mathbb{Z}/pq\mathbb{Z}) \mid 0 < a < pq/2\},$$

$$B = \{([a]_p, [b]_q) \in (\mathbb{Z}/p\mathbb{Z})^\times \times (\mathbb{Z}/q\mathbb{Z})^\times \mid a \in \mathbb{Z}, 0 < b < q/2\}$$

とする。任意の $(a, b) \in B$ に対して $k \in A$ が存在して $\delta(k) = (a, b)$ かもしくは $\delta(k) = -(a, b)$ のどちらか一方のみが成り立つ。よって、ある $\epsilon \in \{1, -1\}$ が存在して、

$$\prod_{(x,y) \in B} (x, y) = \epsilon \prod_{k \in A} \delta(k)$$

が成り立つ。さて、

$$\begin{aligned} \prod_{(x,y) \in B} (x, y) &= \prod_{0 < a < p, 0 < b < q/2} ([a]_p, [b]_q) = \prod_{0 < b < q/2} \prod_{0 < a < p} ([a]_p, [b]_q) \\ &= \prod_{0 < b < q/2} ([(p-1)!]_p, [b^{p-1}]_q) = \left(\left[((p-1)!)^{\frac{q-1}{2}} \right]_p, \left[\left(\left(\frac{q-1}{2} \right)! \right)^{p-1} \right]_q \right) \end{aligned}$$

である。ここで、ウィルソンの定理から $[(p-1)!]_p = [-1]_p$ であり、

$$((\frac{q-1}{2})!)^2 =_q (q-1)!(-1)^{\frac{q-1}{2}} =_q (-1)(-1)^{\frac{q-1}{2}}$$

なので、

$$(3) \quad \prod_{(x,y) \in B} (x, y) = [(-1)^{\frac{q-1}{2}}]_p, [(-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2} \frac{q-1}{2}}]_q$$

である。そして

$$\begin{aligned} \prod_{k \in A} k &= \prod_{1 \leq k < pq/2, \gcd(k, pq)=1} k \\ &= \left(\prod_{1 \leq k < pq/2, p \nmid k} k \right) \cdot \left(\prod_{1 \leq k < pq/2, q \nmid k} k \right)^{-1} \\ &= \left(\prod_{0 < k < p} k \right) \left(\prod_{p < k < 2q} k \right) \cdots \left(\prod_{(Q-1)p < k < Qp} k \right) \left(\prod_{Qp < k < pq/2} k \right) \left(\prod_{1 \leq k < pq/2, q \nmid k} k \right)^{-1} \end{aligned}$$

ここで、今からこの量の p を法とした値を考える。

$$\prod_{(i-1)p < k < ip} k =_p (p-1)! =_p -1$$

であり、 $\{k \in \mathbb{Z} \mid Qp < k < pq/2\} = \{k \in \mathbb{Z} \mid Qp+1 \leq k \leq (pq-1)/2\} = \{Qp+1, Qp+2, \dots, Qp+P\}$ なので

$$\prod_{Qp < k < pq/2} k =_p P!$$

また、 $\{k \in \mathbb{Z} \mid 1 \leq k < pq/2\} = \{k \in \mathbb{Z} \mid 1 \leq k \leq (pq-1)/2\} = \{1, 2, \dots, (pq-1)/2\}$ であるから、 $\{k \in \mathbb{Z} \mid 1 \leq k < pq/2\} = \{q, 2q, \dots, Pq\}$ なので

$$\prod_{1 \leq k < pq/2, q \nmid k} k = \prod_{1 \leq i \leq P} (qi) = q^P P!$$

となる。よって、

$$\prod_{k \in A} k =_p \frac{(-1)^Q \cdot P!}{q^P P!}$$

であるが、オイラーの基準から

$$\prod_{k \in A} k =_p (-1)^Q \left(\frac{q}{p} \right)$$

今の議論を、 p と q の役割を入れ替えて適用すると、同様にして

$$\prod_{k \in A} k =_q (-1)^P \left(\frac{p}{q} \right)$$

よって (3) と比較すると、

$$(-1)^Q \left(\frac{q}{p} \right) =_p \epsilon (-1)^Q$$

と

$$(-1)^P \left(\frac{p}{q} \right) =_q \epsilon (-1)^P (-1)^{PQ}$$

これら二式の両辺も 1 か -1 のどちらかの値しか取らず^s, $2 \neq_p 0$, $2 \neq_q 0$ なので、実際の等式として

$$\left(\frac{q}{p} \right) = \epsilon$$

と

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

を得る。この二式から、

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

を得る。 □

参考文献

- [1] S. Y. Kim, *An elementary proof of the quadratic reciprocity law*, Amer. Math. Soc. 111 (2004), no. 1, 48–50.
- [2] G. Rousseau, *On the quadratic reciprocity law*, J. Austral. Math. Soc. (Series A), 51 (1991), 423–425.