平方剰余の相互法則の証明

宮川　幸隆

1　序文

平方剰余の相互法則は初等整数論の宝玉である。 GAUSS は、その著書 DISQUISITIONES ARITHMETICAE（参考文献 [2]）の緒言の中で、「 …… 私はそのころ、ある別の研究に没頭していた。ところが、そのような日々の中で、私はゆくりなくあるすばらしいアリトメティカの真理（もし私が思い違いをしているのでなければ、それは第１０８条の定理であった）に出会ったのである。私はその真理自体にもこの上もない美しさを感じたが、そればかりではなく、それはなおいっそうすばらしい他の数々の真理とも関連があるように思われた。…… （邦訳、高瀬 正仁 氏）」と語っているが、第１０８条の定理とは今日、平方剰余の相互法則の第一補充法則と呼ばれているものに他ならない。平方剰余相互法則の第一補充法則は Euler の基準から直ちに従うが、Euler の基準の現代的な証明は、例えば、参考文献 [4] の中にある。

「それはなおいっそうすばらしい他の数々の真理とも関連があるように思われた。」の数々の真理の一つとして、平方剰余の相互法則は初等整数論の宝玉であるのだと思う。

本稿は、その平方剰余相互法則の最もイケている証明を紹介するものである。尚、本稿は、参考文献 [5] の内容の一部に厳密な証明を付け加えたものであることを申し添えておく。

2　双曲線関数の背後に潜む多項式、双曲多項式

本節では、まず、二つの関数 cw, sw を

$$cw(z) = z + \frac{1}{z}, \quad sw(z) = z - \frac{1}{z}$$

と定義する。$\mathbb{C}$ を複素数全体の集合とするとき、$\mathbb{C}$ から 0 のみを除いた集合 $\mathbb{C} - \{0\}$ のことを $\mathbb{C}$ の乗法群と呼び、$\mathbb{C}^\times$ という記号で表わした： $\mathbb{C}^\times = \mathbb{C} - \{0\}$.

$cw(z)$, $sw(z)$ の定義域は $\mathbb{C}^\times = \mathbb{C} - \{0\}$ と考えることにする。この cw, sw に対して、次のような定理が成立する：

2.1　定理（$cw(z^n) = P_n(cw(z))$, $sw(z^n) = Q_n(cw(z))sw(z)$, n は奇数）

n は奇数とする。

(i) 0 でないすべての複素数 z に対し

$$cw(z^n) = P_n(cw(z)), \quad sw(z^n) = Q_n(cw(z))sw(z)$$

を満たし、係数が共にすべて整数である n 次式 $P_n(x)$ と $n-1$ 次式 $Q_n(x)$ が存在する。

(ii) $P_n'(x) = nQ_n(x)$ である。

(iii) p を奇素数とするとき、$P_p(x)$ の $p-1$ 次以下の係数はすべて p で割り切れる。

証明に先立ち、具体例に当たって見よう：

$P_1(x) = x$ と $Q_1(x) = 1$ は明らかであろう。

また $cw(z^2) = cw^2(z) - 2$, $\quad sw(z^2) = cw(z)sw(z)$ から、

$$P_2(x) = x^2 - 2, \quad Q_2(x) = x,$$

である。さて、$cw(z^{k+1}) = cw(z^k)cw(z) - cw(z^{k-1})$, $\quad sw(z^{k+1}) = sw(z^k)cw(z) - sw(z^{k-1})$ であるから、

$$P_{k+1}(x) = xP_k(x) - P_{k-1}(x), \quad Q_{k+1}(x) = xQ_k(x) - Q_{k-1}(x)$$

となって、

$$P_3(x) = x(x^2-2) - x = x^3 - 3x, \quad Q_3(x) = x \cdot x - 1 = x^2 - 1.$$

このように、この定理の (i) は確かに成り立ちそうであるが、もう少し具体例に当たって見よう：

$$P_4(x) = x(x^3 - 3x) - (x^2 - 2) = x^4 - 4x^2 + 2,$$

$$Q_4(x) = x(x^2 - 1) - x = x^3 - 2x,$$

$$P_5(x) = x(x^4 - 4x^2 + 2) - (x^3 - 3x) = x^5 - 5x^3 + 5x,$$

$$Q_5(x) = x(x^3 - 2x) - (x^2 - 1) = x^4 - 3x^2 + 1$$

等々となるから、この定理の (i) は確かに成り立ちそうである。

さらに、$P_1(x) = x$ と $Q_1(x) = 1$ から、

$$P_1'(x) = Q_1(x),$$

$P_2(x) = x^2 - 2$, $\quad Q_2(x) = x$ から、

$$P_2'(x) = 2Q_2(x),$$

$P_3(x) = x^3 - 3x$, $\quad Q_3(x) = x^2 - 1$ から、

$$P_3'(x) = 3Q_3(x),$$

$P_4(x) = x^4 - 4x^2 + 2$, $\quad Q_4(x) = x^3 - 2x$ から、

$$P_4'(x) = 4Q_4(x),$$

$P_5(x) = x^5 - 5x^3 + 5x$, $\quad Q_5(x) = x^4 - 3x^2 + 1$ から、

$$P_5'(x) = 5Q_5(x),$$

等々となるから、この定理の (ii) も確かに成り立ちそうである。

さらに、$P_3(x)=x^3-3x$, $P_5(x)=x^5-5x^3+5x$, 等々から、この定理の（iii）も確かに成り立ちそうである。

さて、この定理を証明して見よう：

証明] (i) まず、0でないすべての複素数 z と奇数 n とに対し

$$sw(z^n)=sw(z)W_n(sw^2(z))$$

を満たし、係数が共にすべて整数である $(n-1)/2$ 次式 $W_n(X)$ が存在することを示そう。

このことは、次の事実によって示される：

Fact 1.1

$$W_1(X)=1.$$

Fact 1.2

$$W_3(X)=X+3.$$

Proof.

$$sw(z^3)=z^3-\frac{1}{z^3}=\left(z-\frac{1}{z}\right)\left(z^2+1+\frac{1}{z^2}\right)=sw(z)\left\{\left(z-\frac{1}{z}\right)^2+3\right\}=sw(z)\{sw^2(z)+3\}$$

であるから、

$$W_3(X)=X+3.$$

q.e.d.

Fact 1.3 $k>2$ なる奇数 k に対して、

$$W_{k+2}(X)=(X+2)W_k(X)-W_{k-2}(X).$$

Proof.

$n=k$, $k-2$ のとき、W_n が存在すると仮定すると、

$$sw(z^{k+2})=z^{k+2}-\frac{1}{z^{k+2}}=\left(z^k-\frac{1}{z^k}\right)\left(z^2+\frac{1}{z^2}\right)-\left(z^{k-2}-\frac{1}{z^{k-2}}\right)=sw(z^k)\left\{\left(z-\frac{1}{z}\right)^2+2\right\}-sw(z^{k-2})$$

$$=sw(z)W_k(sw^2(z))\{sw^2(z)+2\}-sw(z)W_{k-2}(sw^2(z))=sw(z)[\{sw^2(z)+2\}W_k(sw^2(z))-W_{k-2}(sw^2(z))].$$

よって、$n=k+2$ のときも、W_n が存在して、

$$W_{k+2}(X)=(X+2)W_k(X)-W_{k-2}(X).$$

Fact 1.1 と Fact 1.2 によって、W_1, W_3 は存在するから、すべての奇数 n に対して、W_n が存在する。

q.e.d.

このWnを第n双曲多項式と呼ぼう：
0でないすべての複素数zに対し

$$sw(z^n) = sw(z)W_n(sw^2(z))$$

を満たし、係数が共にすべて整数である$(n-1)/2$次式$W_n(X)$が存在することが示されたから、

$$sw^2(z) = cw^2(z) - 4$$

とから、

$$W_n(sw^2(z)) = W_n(cw^2(z) - 4) = Q_n(cw(z))$$

とおくと、0でないすべての複素数zに対し

$$sw(z^n) = Q_n(cw(z))sw(z)$$

を満たし、係数が共にすべて整数であるn−1次式$Q_n(x)$が存在することが示された。
次に、

$$P_1(x) = x,$$

$$cw(z^2) = cw^2(z) - 2, \quad i.e., \quad P_2(x) = x^2 - 2$$

であるから、$n = 1, 2$のとき、(i) は示される。さて、

$$cw(z^{k+1}) = cw(z^k)cw(z) - cw(z^{k-1})$$

であるから、$n = k, k-1$のとき (i) が示されると仮定すると、

2.1.1

$$P_{k+1}(x) = xP_k(x) - P_{k-1}(x)$$

となって、$n = k+1$のときも (i) は示される。以上によって、(i) は示された。

(ii) $cw(z^n) = P_n(cw(z))$の両辺をzで微分すると、

$$nsw(z^n) = P_n'(cw(z))sw(z), \quad i.e.,$$

$$nQ_n(cw(z))sw(z) = P_n'(cw(z))sw(z)$$

これが0でない任意のzに対して成り立つから、両辺を$sw(z)$で割って$cw(z) = x$とおいた$nQ_n(x) = P_n'(x)$も成り立つ。

(iii) (ii) により、$P_p'(x) = pQ_p(x)$であり、一方、(i) により$Q_p(x)$の係数は整数であるから、$P_p'(x)$の係数はpの倍数である。そこで、

$$P_p'(x) = pa_px^{p-1} + pa_{p-1}x^{p-2} + \cdots\cdots + pa_1 \quad (a_p, a_{p-1}, \cdots\cdots, a_1 \in \mathbb{Z})$$

とおく。このとき、

$$P_p(x) = a_px^p + \frac{pa_{p-1}}{p-1}x^{p-1} + \cdots\cdots + pa_1x + a_0$$

これの$x^i (i = 1, 2, \cdots\cdots, p-1)$の係数

2.1.2

$$\frac{pa_i}{i}$$

は整数であるが、pは素数なのでpとiとは互いに素となり、

$$\frac{a_i}{i}$$

が整数となって2.1.2はpの倍数である。また、$a_0 = P_p(0)$であるが、2.1.1　$P_{k+1}(x) = xP_k(x) - P_{k-1}(x)$から、$a_0 = P_p(0) = 0 \cdot P_{p-1}(0) - P_{p-2}(0) = -P_{p-2}(0) = \cdots = (-1)^{\frac{p-1}{2}} P_1(0) = 0$により、$a_0$も$p$の倍数となって（iii）も示された。
（定理2.1の証明終わり）

さて、

$$sm(z) = sw(e^z)$$

によって、関数smを定義すると、その定義域は$\mathbb{C}$であって、

2.1.3

$$sm(z) = 2\sinh(z)$$

に他ならない。そして、定理2.1の（i）の証明で見たように、sw関数の背後には双曲多項式が潜んでいるのである。

3　双曲多項式のExamples

$W_5(X) = (X+2)W_3(X) - W_1(X)$

[Fact 1.3による。]

$= (X+2)(X+3) - 1$

[Fact 1.2,　1.1による。]

$= X^2 + 5X + 5,$

$W_7(X) = (X+2)W_5(X) - W_3(X)$

[Fact 1.3による。]

$= (X+2)(X^2+5X+5) - (X+3)$

[Fact 1.2による。]

$= X^3 + 7X^2 + 14X + 7,$

$W_9(X) = (X+2)W_7(X) - W_5(X)$

[Fact 1.3による。]

$= (X+2)(X^3+7X^2+14X+7) - (X^2+5X+5)$
$= X^4+9X^3+27X^2+30X+9,$

$W_{11}(X) = (X+2)W_9(X) - W_7(X)$

[Fact 1.3 による。]

$= (X+2)(X^4+9X^3+27X^2+30X+9) - (X^3+7X^2+14X+7)$
$= X^5+11X^4+44X^3+77X^2+55X+11,$

.....,

等々となる。このように、p を奇素数とするとき、$W_p(X)$ の最高次の項以外の項の係数はすべて p の倍数となるという著しい整数論的性質が成り立つ。このことは定理 2.1 において cw と sw とを交換して得られる次の定理 3.1 を用いて証明される：

3.1 定理（$sw(z^n) = P_n(sw(z))$, $cw(z^n) = Q_n(sw(z))cw(z)$, n は奇数）

n は奇数とする。

(i) 0 でないすべての複素数 z に対し

$$sw(z^n) = P_n(sw(z)), \quad cw(z^n) = Q_n(sw(z))cw(z)$$

を満たし、係数が共にすべて整数である n 次式 $P_n(x)$ と $n-1$ 次式 $Q_n(x)$ が存在する。

(ii) $P_n'(x) = nQ_n(x)$ である。

(iii) p を奇素数とするとき、$P_p(x)$ の $p-1$ 次以下の係数はすべて p で割り切れる。

証明に先立ち、具体例に当たって見よう：

$P_1(x) = x$ と $Q_1(x) = 1$ は明らかであろう。

また $sw(z^3) = sw(z)[sw(z)^2+3]$, $cw(z^3) = [sw^2(z)+1]cw(z)$ から、

$$P_3(x) = x(x^2+3) = x^3+3x, \quad Q_3(x) = x^2+1,$$

である。さて、$sw(z^{k+2}) = sw(z^k)[sw^2(z)+2] - sw(z^{k-2})$, $cw(z^{k+2}) = cw(z^k)[sw^2(z)+2] - cw(z^{k-2})$ であるから、

$$P_{k+2}(x) = (x^2+2)P_k(x) - P_{k-2}(x), \quad Q_{k+2}(x) = (x^2+2)Q_k(x) - Q_{k-2}(x)$$

となって、

$$P_5(x) = (x^2+2)(x^3+3x) - x = x^5+5x^3+5x, \quad Q_5(x) = (x^2+2)(x^2+1) - 1 = x^4+3x^2+1.$$

このように、この定理の (i) は確かに成り立ちそうであるが、もう少し具体例に当たって見よう：

$$P_7(x) = (x^2+2)(x^5+5x^3+5x) - (x^3+3x) = x^7+7x^5+14x^3+7x,$$

$$Q_7(x) = (x^2+2)(x^4+3x^2+1) - (x^2+1) = x^6+5x^4+6x^2+1,$$

$$P_9(x) = (x^2+2)(x^7+7x^5+14x^3+7x) - (x^5+5x^3+5x) = x^9+9x^7+27x^5+30x^3+9x,$$

$$Q_9(x)=(x^2+2)(x^6+5x^4+6x^2+1)-(x^4+3x^2+1)=x^8+7x^6+15x^4+10x^2+1$$

等々となるから、この定理の（i）は確かに成り立ちそうである。

さらに、$P_1(x)=x$ と $Q_1(x)=1$ から、

$$P_1'(x)=Q_1(x),$$

$P_3(x)=x^3+3x$, $Q_3(x)=x^2+1$ から、

$$P_3'(x)=3Q_3(x),$$

$P_5(x)=x^5+5x^3+5x$, $Q_5(x)=x^4+3x^2+1$ から、

$$P_5'(x)=5Q_5(x),$$

$P_7(x)=x^7+7x^5+14x^3+7x$, $Q_7(x)=x^6+5x^4+6x^2+1$ から、

$$P_7'(x)=7Q_7(x),$$

$P_9(x)=x^9+9x^7+27x^5+30x^3+9x$, $Q_9(x)=x^8+7x^6+15x^4+10x^2+1$ から、

$$P_9'(x)=9Q_9(x),$$

等々となるから、この定理の（ii）も確かに成り立ちそうである。

さらに、$P_3(x)=x^3+3x$, $P_5(x)=x^5+5x^3+5x$, $P_7(x)=x^7+7x^5+14x^3+7x$, 等々から、この定理の（iii）も確かに成り立ちそうである。

さて、この定理を証明して見よう：

証明] （i）$n=1$ のとき、

3.1.1

$$P_1(x)=x, \quad Q_1(x)=1.$$

$n=3$ のとき、

3.1.2

$$sw(z^3)=sw(z)[sw^2(z)+3], \quad i.e., \quad P_3(x)=x(x^2+3);$$
$$cw(z^3)=[sw^2(z)+1]cw(z), \quad i.e., \quad Q_3(x)=x^2+1$$

であるから、$n=1,3$ のとき、（i）は示される。さて、$n=k, k-2$ のとき（i）が示されると仮定すると、

$$sw(z^{k+2})=P_k(sw(z))[sw^2(z)+2]-P_{k-2}(sw(z))$$

であるから、

3.1.3

$$P_{k+2}(x) = (x^2+2)P_k(x) - P_{k-2}(x),$$

となり、

$$cw(z^{k+2}) = Q_k(sw(z))cw(z)[sw^2(z)+2] - Q_{k-2}(sw(z))cw(z)$$

であるから、

$$Q_{k+2}(x) = (x^2+2)Q_k(x) - Q_{k-2}(x)$$

となって、$n = k+2$ のときも (i) は示される。以上によって、(i) は示された。

(ii) $sw(z^n) = P_n(sw(z))$ の両辺を z で微分すると、

$$ncw(z^n) = P_n'(sw(z))cw(z), \quad i.e.,$$

$$nQ_n(sw(z))cw(z) = P_n'(sw(z))cw(z)$$

これが 0 でない任意の z に対して成り立つから、両辺を $cw(z)$ で割って $sw(z) = x$ とおいた $nQ_n(x) = P_n'(x)$ も成り立つ。

(iii) (ii) により、$P_p'(x) = pQ_p(x)$ であり、一方、(i) により $Q_p(x)$ の係数は整数であるから、$P_p'(x)$ の係数は p の倍数である。そこで、

$$P_p'(x) = pa_px^{p-1} + pa_{p-1}x^{p-2} + \cdots\cdots + pa_1 \quad (a_p, a_{p-1}, \cdots\cdots, a_1 \in \mathbb{Z})$$

とおく。このとき、

$$P_p(x) = a_px^p + \frac{pa_{p-1}}{p-1}x^{p-1} + \cdots\cdots + pa_1x + a_0$$

これの $x^i (i = 1, 2, \cdots\cdots, p-1)$ の係数

3.1.4

$$\frac{pa_i}{i}$$

は整数であるが、p は素数なので p と i とは互いに素となり、

$$\frac{a_i}{i}$$

が整数となって 3.1.4 は p の倍数である。また、$a_0 = P_p(0)$ であるが、p が奇素数のときは、3.1.3 $P_{k+2}(x) = (x^2+2)P_k(x) - P_{k-2}(x)$ から、$a_0 = P_p(0) = 2 \cdot P_{p-2}(0) - P_{p-4}(0)$ であり、3.1.1 により、$P_1(0) = 0$, 3.1.2 により、$P_3(0) = 0$ であるから、$a_0 = 0$ も p の倍数となって (iii) も示された。

(定理 3.1 の証明終わり)

この定理 3.1 における $P_n(x)$ と双曲多項式 $W_n(X)$ との間には

3.1.5

$$P_n(x) = xW_n(x^2)$$

という関係が成り立つので、p を奇素数とするとき、$W_p(X)$ の最高次の項以外の項の係数はすべて p の倍数となるという著しい整数論的性質が成り立つのである：

$W_1(X) = 1,$

$W_3(X) = X + 3,$

$W_5(X) = X^2 + 5X + 5,$

$W_7(X) = X^3 + 7X^2 + 14X + 7,$

$W_9(X) = X^4 + 9X^3 + 27X^2 + 30X + 9,$

$W_{11}(X) = X^5 + 11X^4 + 44X^3 + 77X^2 + 55X + 11,$

.....

4 sm 関数と、双曲多項式の因数分解

双曲多項式 $W_n(X)$ に関しては、定理 2.1 の証明] の (i) から判るように、奇数 n に対して、$W_n(X)$ は X の

$$\frac{n-1}{2}$$

次の多項式であり、その最高次の係数は **1** である。そして、双曲多項式 $W_n(X)$ を因数分解することを考えて見ると、3 以上の奇数 l に対して、

4.0.6

$$\frac{sm(lz)}{sm(z)} = W_l(sm^2(z)) = \prod_{j=1}^{\frac{l-1}{2}} \left(sm^2(z) - sm^2\left(\frac{2j\pi i}{l}\right)\right)$$

が成り立つ。例えば、$l = 3$ のときは、双曲多項式の Examples から、

$$W_3(X) = X + 3$$

であって、

$$\prod_{j=1}^{\frac{3-1}{2}} \left(sm^2(z) - sm^2\left(\frac{2j\pi i}{3}\right)\right) = sm^2(z) - sm^2\left(\frac{2\pi i}{3}\right)$$

であるから、

$W_3(X) = X + 3 = X - (\sqrt{3}i)^2 = X - \left(2i \sin\left(\frac{2\pi}{3}\right)\right)^2 = X - \left(\exp\left(\frac{2\pi i}{3}\right) - \exp\left(-\frac{2\pi i}{3}\right)\right)^2$

$= X - sm^2\left(\frac{2\pi i}{3}\right)$ である。このように、$W_3(x)$ の零点は、関数 sm の特殊値の二乗である。

$l=5$ のときは、やはり双曲多項式の Examples から、

$$W_5(X)=X^2+5X+5$$

であって、

$$\prod_{j=1}^{\frac{5-1}{2}}\Big(sm^2(z)-sm^2\Big(\frac{2j\pi i}{5}\Big)\Big)=\Big(sm^2(z)-sm^2\Big(\frac{2\pi i}{5}\Big)\Big)\Big(sm^2(z)-sm^2\Big(\frac{4\pi i}{5}\Big)\Big)$$

であるから、

$$W_5(X)=X^2+5X+5=\Big(X-sm^2\Big(\frac{2\pi i}{5}\Big)\Big)\Big(X-sm^2\Big(\frac{4\pi i}{5}\Big)\Big)$$

であり、$W_5(x)$ の零点は、やはり関数 sm の特殊値の二乗であるが、ここでは、

4.0.7

$$\frac{sm(5z)}{sm(z)}=\Big(sm^2(z)-sm^2\Big(\frac{2\pi i}{5}\Big)\Big)\Big(sm^2(z)-sm^2\Big(\frac{4\pi i}{5}\Big)\Big)$$

を示しておく必要があるであろう：然るに、

$$\frac{sm(5z)}{sm(z)}$$

は $sm^2(z)$ の 2 次多項式であり、その最高次の係数は 1 である。そして、

$$z=\frac{2\pi i}{5}$$

と

$$z=\frac{4\pi i}{5}$$

は、共に

$$\frac{sm(5z)}{sm(z)}=0$$

を満たすから、4.0.7 は確かに成り立つのである。

$l=7$ のときは、やはり双曲多項式の Examples から、

$$W_7(X)=X^3+7X^2+14X+7$$

であって、

$$\prod_{j=1}^{\frac{7-1}{2}}\Big(sm^2(z)-sm^2\Big(\frac{2j\pi i}{7}\Big)\Big)=\Big(sm^2(z)-sm^2\Big(\frac{2\pi i}{7}\Big)\Big)\Big(sm^2(z)-sm^2\Big(\frac{4\pi i}{7}\Big)\Big)\Big(sm^2(z)-sm^2\Big(\frac{6\pi i}{7}\Big)\Big)$$

であるから、

$$W_7(X)=X^3+7X^2+14X+7=\Big(X-sm^2\Big(\frac{2\pi i}{7}\Big)\Big)\Big(X-sm^2\Big(\frac{4\pi i}{7}\Big)\Big)\Big(X-sm^2\Big(\frac{6\pi i}{7}\Big)\Big)$$

であり、$W_7(X)$ の零点は、やはり関数 sm の特殊値の二乗であるが、ここでは、

4.0.8

$$\frac{sm(7z)}{sm(z)}=\Big(sm^2(z)-sm^2\Big(\frac{2\pi i}{7}\Big)\Big)\Big(sm^2(z)-sm^2\Big(\frac{4\pi i}{7}\Big)\Big)\Big(sm^2(z)-sm^2\Big(\frac{6\pi i}{7}\Big)\Big)$$

を示しておく必要があるであろう：然るに、

$$\frac{sm(7z)}{sm(z)}$$

は $sm^2(z)$ の3次多項式であり、その最高次の係数は1である。そして、

$$z=\frac{2\pi i}{7}$$

と

$$z=\frac{4\pi i}{7}$$

と

$$z=\frac{6\pi i}{7}$$

は、共に

$$\frac{sm(7z)}{sm(z)}=0$$

を満たすから、4.0.8は確かに成り立つのである。

$l=9,\quad l=11,\quad \cdots\cdots\cdots$ のときも以下同様である。
そして、4.0.6は平方剰余の相互法則の証明に応用される。

4.0.6の証明]　3以上の奇数 l に対して、

$$\frac{sm(lz)}{sm(z)}=W_l(sm^2(z))=\prod_{j=1}^{\frac{l-1}{2}}\Big(sm^2(z)-sm^2\Big(\frac{2j\pi i}{l}\Big)\Big)$$

が成り立つことを示すのであるが、定理2.1 の証明] の (i) と sm 関数の定義によって、まず、$z\neq ni\pi(n\in \boldsymbol{Z})$ なる任意の複素数 z に対して、

4.0.9

$$\frac{sm(lz)}{sm(z)}=W_l(sm^2(z))$$

は成り立つ。そこで、後は、3以上の奇数 l に対して、

4.0.10

$$W_l(sm^2(z)) = \prod_{j=1}^{\frac{l-1}{2}} \Big(sm^2(z) - sm^2\Big(\frac{2j\pi i}{l}\Big)\Big)$$

が成り立つことを示すのであるが、まず、
$j = 1, 2, \cdots\cdots, \frac{l-1}{2}$ に対して、

$$0 < \frac{2j\pi}{l} < \pi, \quad \frac{sm(2j\pi i)}{sm(\frac{2j\pi i}{l})} = 0$$

であるから、4.0.9 とから、

$$W_l\Big(sm^2\Big(\frac{2j\pi i}{l}\Big)\Big) = 0, \quad \Big(j = 1, 2, \cdots, \frac{l-1}{2}\Big)$$

が成り立つ。よって、$W_l(X)$ が X の

$$\frac{l-1}{2}$$

次の多項式であったことと、その最高次の係数が 1 であったこととから、

$$W_l(sm^2(z)) = \prod_{j=1}^{\frac{l-1}{2}} \Big(sm^2(z) - sm^2\Big(\frac{2j\pi i}{l}\Big)\Big).$$

よって、4.0.10 は示された。
（4.0.6 の証明終り）

5　平方剰余の相互法則と、4.0.6 を用いたその証明

まず、sm 関数の定義から、容易に次の定理を得る：

5.1　定理（sm 関数の性質）

任意の複素数 z に対して、

$$sm(-z) = -sm(z), \quad sm(z + 2\pi i) = sm(z).$$

（定理 5.1 終り）

さて、Legendre 記号

$$\Big(\frac{a}{p}\Big)$$

に於いて、もし a も奇素数であって、$a \neq p$ であれば、

$$\Big(\frac{p}{a}\Big)$$

もLegendre記号である。即ち、二つの相異なる奇素数p, qに対して、

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

も

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

もLegendre記号であるが、これらの間には、

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

という簡明な相互依存関係が成立する。これが平方剰余の相互法則である。即ち、

5.2 定理（平方剰余の相互法則）

二つの相異なる奇素数p, qに対して、

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

という相互依存関係が成立する。

証明]

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

を示せばよい。

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

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

は法pに関する一つの既約剰余系である。

$q\neq p$から、

$$qj\not\equiv 0 \pmod p,\quad \left(j=1,2,3,\cdots,\frac{p-1}{2}\right),$$

よって、各jに対して、

$$qj\equiv(-1)^{\mu}j' \pmod p$$

を満たすようなj'が一意的に存在して、

$$j\neq k \text{ ならば } j'\neq k'$$

である。このとき、

$$\frac{qj}{p}-\frac{(-1)^{\mu}j'}{p}\in\mathbb{Z}$$

であるから、上の定理5.1（sm関数の性質）とから、

$$sm\left(\frac{qj\cdot 2\pi i}{p}\right)=sm\left(\frac{qj\cdot 2\pi i}{p}+2\left(\frac{(-1)^{\mu}j'}{p}-\frac{qj}{p}\right)\pi i\right)=(-1)^{\mu}sm\left(\frac{2j'\pi i}{p}\right).$$

それゆえ、

$$qj \equiv j' \cdot \frac{sm\left(\frac{q\cdot 2j\pi i}{p}\right)}{sm\left(\frac{2j'\pi i}{p}\right)} \pmod{p},$$

よって、

$$(1) \quad q^{\frac{p-1}{2}} \equiv \prod_{j=1}^{\frac{p-1}{2}} \left\{ \frac{sm\left(\frac{q\cdot 2j\pi i}{p}\right)}{sm\left(\frac{2j\pi i}{p}\right)} \right\} \pmod{p}.$$

(1) の右辺は $+1$ か -1 であるから、Euler の基準によって、次の (2) を得る：

$$(2) \quad \left(\frac{q}{p}\right) = \prod_{j=1}^{\frac{p-1}{2}} \left\{ \frac{sm\left(\frac{q\cdot 2j\pi i}{p}\right)}{sm\left(\frac{2j\pi i}{p}\right)} \right\}.$$

この (2) に 4.0.6 を用いると、次の (3) を得る：

$$(3) \quad \left(\frac{q}{p}\right) = \prod_{j=1}^{\frac{p-1}{2}} \prod_{k=1}^{\frac{q-1}{2}} \left\{ sm^2\left(\frac{2j\pi i}{p}\right) - sm^2\left(\frac{2k\pi i}{q}\right) \right\}.$$

p と q を交換することによって、同様に次の (4) を得る：

$$(4) \quad \left(\frac{p}{q}\right) = \prod_{j=1}^{\frac{p-1}{2}} \prod_{k=1}^{\frac{q-1}{2}} \left\{ sm^2\left(\frac{2k\pi i}{q}\right) - sm^2\left(\frac{2j\pi i}{p}\right) \right\}.$$

(3) と (4) から、次を得る：

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

これで、定理は示された。

（定理 5.2 の証明終り）

6 参考文献

[1] 高木 貞治、初等整数論講義　第二版、共立出版、１９３１年。

[2] D. CAROLO FRIDERICO GAUSS.　DISQUISITIONES ARITHMETICAE　１８０１年。

邦訳、高瀬 正仁　訳、ガウス整数論、朝倉書店、１９９５年。

[3] 平松 豊一、数論を学ぶ人のための相互法則入門、牧野書店。

[4] 宮川 幸隆、電子書籍「代数の基礎と初等整数論」、みんなの本屋さん in App ストア in iPhone or iPad、２０１２年１月。

[5] 宮川 幸隆、双曲多項式の諸性質、日本数学会編集の雑誌「数学」第５８巻、第３号、２００６年７月、夏季号。