『数学セミナー』2020年2月号 「高校数学ではじめる整数論」

連載●第 11 回

相互律鑑賞会　付録

谷口 隆◎神戸大学大学院理学研究科

※ 式番号は本誌 2020 年 2 月号の連載と通しで振っています.

◎ーー1　(10) の証明

(12) にあるような和と積分の関係は，ポワソンの和公式というフーリエ解析の公式によって分析できます．(12) は正しい式ですが，(11) のように $G(n)$ の和を二つに分けず，$G(n)$ 自体を考察し，(10) を直接証明することが可能です．その証明を通して，(11) のような和の分け方をしたことの意味も分かるので，ここでは (10) を証明します．$e(x) := e^{2\pi ix}$ とおきます．

証明　各奇数 n について，次の条件をみたす $\mathbb{R}$ 上の関数 $\varphi_n(x)$ を取る．

- φ_n は滑らかで，台は区間 $\left(-\dfrac{n}{4}, \dfrac{3n}{4}\right)$ に含まれる．
- $0 \leqq \varphi_n(x) \leqq 1$ であり，また $\left[-\dfrac{n}{4}\right] + 1 \leqq x \leqq \left[\dfrac{3n}{4}\right]$ で $\varphi_n(x) = 1$ である．
- n に依存しない正定数 M_1, M_2 で，$|\varphi_n'(x)| < M_1$, $|\varphi_n''(x)| < M_2$ をみたすものが存在する．

以下，$\varphi_n(x)$ の添字 n を省略して，$\varphi(x)$ と書く．条件から

$$G(n) = \sum_{-\frac{n}{4}<a<\frac{3n}{4}} e\left(\frac{a^2}{n}\right) = \sum_{a\in\mathbb{Z}} \varphi(a) e\left(\frac{a^2}{n}\right)$$

である．ポワソンの和公式によって，

$$G(n) = \sum_{b\in\mathbb{Z}} F(b) \tag{21}$$

ただし

$$F(b)=F_n(b):=\int_{\mathbb{R}}\varphi(x)e\left(\frac{x^2}{n}-bx\right)dx=\int_{-\frac{n}{4}}^{\frac{3n}{4}}\varphi(x)e\left(\frac{x^2}{n}-bx\right)dx$$

である．以下，$F(b)$ について次を示す．

$$F(b)=\begin{cases}\dfrac{1}{1-i}\sqrt{n}+O(1) & b=0\\ \dfrac{i^{-n}}{1-i}\sqrt{n}+O(1) & b=1\\ O\left(\dfrac{1}{b^2}\right) & b\neq 0,1\end{cases}\tag{22}$$

($b\neq 0,1$ のときの $F(b)=O\left(\dfrac{1}{b^2}\right)$ は，$|F(b)|\leqq\dfrac{M'}{b^2}$ となる n,b に依存しない正定数 M' が存在するという意味である．) (22) が得られれば，(10) はすぐにしたがう．実際，(22) を (21) に代入すると，

$$G(n)=\frac{1+i^{-n}}{1-i}\sqrt{n}+O(1)+\sum_{b\neq 0,1}O\left(\frac{1}{b^2}\right)=\frac{1+i^{-n}}{1-i}\sqrt{n}+O(1)$$

である．以下，(22) を考える．

$$\begin{aligned}F(0)&=\int_{-\frac{n}{4}}^{\frac{3n}{4}}\varphi(x)e\left(\frac{x^2}{n}\right)dx=\int_{-\frac{n}{4}}^{\frac{3n}{4}}e\left(\frac{x^2}{n}\right)dx+O(1)\\&=\int_0^{\frac{3n}{4}}e\left(\frac{x^2}{n}\right)dx+\int_0^{\frac{n}{4}}e\left(\frac{x^2}{n}\right)dx+O(1)\end{aligned}$$

である．フレネルの積分公式 (14) より，この一項目の積分は

$$\begin{aligned}\int_0^{\frac{3n}{4}}e\left(\frac{x^2}{n}\right)dx&=\sqrt{n}\int_0^{\frac{3\sqrt{n}}{4}}e(x^2)dx\\&=\sqrt{n}\left(\frac{1+i}{4}+O\left((\sqrt{n})^{-1}\right)\right)=\frac{1}{2(1-i)}\sqrt{n}+O(1)\end{aligned}$$

である．二項目も同様に計算でき，$F(0)=\dfrac{1}{1-i}\sqrt{n}+O(1)$ である．$F(1)$ は積分変数の x を $\dfrac{n}{2}-x$ で置換して，

$$F(1)=e\left(-\frac{n}{4}\right)\int_{-\frac{n}{4}}^{\frac{3n}{4}}e\left(\frac{x^2}{n}\right)dx+O(1)$$

である．積分は $F(0)$ のときと同じだから，$e\left(-\dfrac{n}{4}\right)=i^{-n}$ により，$F(1)=\dfrac{i^{-n}}{1-i}\sqrt{n}+O(1)$ である．

$b\neq 0,1$ とする．x を nx で置換して

$$F(b)=n\int_{-\frac{1}{4}}^{\frac{3}{4}}\varphi(nx)e(n(x^2-bx))dx$$

である．$b \neq 0, 1$ より，$x \in \left[-\frac{1}{4}, \frac{3}{4}\right]$ で $2x - b \neq 0$ であることに注意し，部分積分を 2 回行うと，

$$F(b) = -\frac{1}{2\pi i} \int_{-\frac{1}{4}}^{\frac{3}{4}} \left(\frac{\varphi(nx)}{2x-b}\right)' e(n(x^2 - bx))dx$$

$$= \frac{1}{(2\pi i)^2 n} \int_{-\frac{1}{4}}^{\frac{3}{4}} \left(\frac{\left(\frac{\varphi(nx)}{2x-b}\right)'}{2x-b}\right)' e(n(x^2 - bx))dx$$

である．ただしそれぞれで，積分区間の端点で関数の値が消えていることを用いた．$x \in \left[-\frac{1}{4}, \frac{3}{4}\right]$ で

$$\left(\frac{\left(\frac{\varphi(nx)}{2x-b}\right)'}{2x-b}\right)' = \frac{n^2\varphi''(nx)}{(2x-b)^2} - \frac{6n\varphi'(nx)}{(2x-b)^3} + \frac{12\varphi(nx)}{(2x-b)^4} = \frac{n^2\varphi''(nx)}{(2x-b)^2} + O\left(\frac{n}{|b|^3}\right)$$

より，

$$F(b) = O\left(n \int_{-\frac{1}{4}}^{\frac{3}{4}} \frac{|\varphi''(nx)|}{(2x-b)^2} dx\right) + O\left(\frac{1}{|b|^3}\right)$$

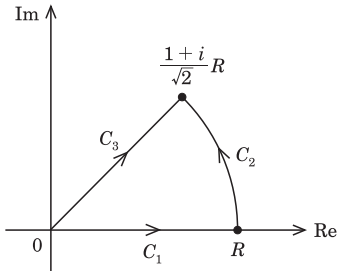
である．$|\varphi''(nx)| < M_2 = O(1)$ であり，また $|\varphi''(nx)|$ は $O\left(\frac{1}{n}\right)$ の長さの区間を除いて値が消えているので，

$$n \int_{-\frac{1}{4}}^{\frac{3}{4}} \frac{|\varphi''(nx)|}{(2x-b)^2} dx = O\left(n \cdot \frac{1}{n} \cdot \frac{1}{b^2}\right) = O\left(\frac{1}{b^2}\right)$$

である．以上で $F(b) = O\left(\frac{1}{b^2}\right)$ が示された． ■

◎一一2　(14) の証明

R を正の実数とし，C_1, C_2, C_3 を複素数平面上の次の積分路とする．C_1, C_3 は原点を端点とする線分で，C_2 は原点を中心とする半径 R の円弧である．



$e^{2\pi i z^2}$ は正則関数なので，コーシーの積分定理から，

$$\int_{C_1} e^{2\pi i z^2} dz + \int_{C_2} e^{2\pi i z^2} dz = \int_{C_3} e^{2\pi i z^2} dz \tag{23}$$

である．$\displaystyle\int_{C_1} e^{2\pi i z^2}dz = \int_0^R e^{2\pi i t^2}dt$ である．C_3 上の積分は，$z = \dfrac{1+i}{2}t$ $(0 \leqq t \leqq \sqrt{2}R)$ とおくと

$$\begin{aligned}\int_{C_3} e^{2\pi i z^2}dz &= \frac{1+i}{2}\int_0^{\sqrt{2}R} e^{-\pi t^2}dt \\ &= \frac{1+i}{2}\int_0^{\infty} e^{-\pi t^2}dt - \frac{1+i}{2}\int_{\sqrt{2}R}^{\infty} e^{-\pi t^2}dt \\ &= \frac{1+i}{4} + O\left(\int_R^{\infty} e^{-t}dt\right) = \frac{1+i}{4} + O(e^{-R})\end{aligned}$$

と計算できる．C_2 上の積分は，$z = Re^{i\theta}$ $(0 \leqq \theta \leqq \dfrac{\pi}{4})$ とおくと，

$$\int_{C_2} e^{2\pi i z^2}dz = Ri\int_0^{\frac{\pi}{4}} e^{2\pi i R^2 e^{2i\theta}}d\theta$$

ここで，$0 \leqq x \leqq \dfrac{\pi}{2}$ で $\sin x \geqq \dfrac{2}{\pi}x$ であることから，

$$|e^{2\pi i R^2 e^{2i\theta}}| = |e^{2\pi i R^2(\cos 2\theta + i\sin 2\theta)}| = e^{-2\pi R^2 \sin 2\theta} \leqq e^{-4R^2\theta}$$

である．したがって

$$\left|\int_{C_2} e^{2\pi i z^2}dz\right| \leqq R\int_0^{\frac{\pi}{4}} e^{-4R^2\theta}d\theta = \frac{1}{4R}\left[-e^{-4R^2\theta}\right]_0^{\frac{\pi}{4}} \leqq \frac{1}{4R}$$

である．(23) にこれらの結果を代入して，

$$\int_0^R e^{2\pi i t^2}dt = \frac{1+i}{4} + O(e^{-R}) + O(R^{-1}) = \frac{1+i}{4} + O(R^{-1})$$

を得る． ■

◎一一3　(16) の証明

これは比較的容易である．$\zeta = e^{\frac{2\pi i}{p}}$ とし，

$$A := \sum_{a\in\mathbb{F}_p^{\times},\left(\frac{a}{p}\right)=1} \zeta^a, \qquad B := \sum_{a\in\mathbb{F}_p^{\times},\left(\frac{a}{p}\right)=-1} \zeta^a$$

と置く．和はそれぞれ，$a \in \mathbb{F}_p^{\times}$ の元で $\left(\dfrac{a}{p}\right) = 1$ をみたすもの全体，$\left(\dfrac{a}{p}\right) = -1$ をみたすもの全体である．

$$A + B = \sum_{a\in\mathbb{F}_p^{\times}} \zeta^a = \sum_{a=1}^{p-1}\zeta^a = -1 + \sum_{a=0}^{p-1}\zeta^a = -1$$

である．

$$G(p) = \sum_{a\in\mathbb{F}_p} \zeta^{a^2} = 1 + \sum_{a\in\mathbb{F}_p^{\times}} \zeta^{a^2} = 1 + 2A = A - B,$$

$$((16)\text{ の左辺}) = \sum_{a\in\mathbb{F}_p} \zeta^{qa^2} = 1 + \sum_{a\in\mathbb{F}_p^{\times}} \zeta^{qa^2} = \begin{cases} 1 + 2A = A - B & \left(\dfrac{q}{p}\right) = 1 \text{ のとき}, \\ 1 + 2B = B - A & \left(\dfrac{q}{p}\right) = -1 \text{ のとき} \end{cases}$$

により (16) がしたがう．

◎——4　証明 A の問題の解答

(a) OT 上の点 $\left(x, \dfrac{qx}{p}\right)$ が格子点であるのは，x が整数かつ qx が p の倍数であるときである．p は素数であり，q は p で割れないから，このとき x は p の倍数となる．しかし，$\mathcal{D}$ 内の点の x 座標は $0 < x < \dfrac{p+1}{2}$ だから，p の倍数になることはない．

(b) $1 \leqq k \leqq \dfrac{p-1}{2}$ とする．kq を p で割ったあまりが $\dfrac{p}{2}$ より大きくなるのは，$\dfrac{kq}{p}$ の分数部分が $\dfrac{1}{2}$ より大きいときである．つまり，$\mathrm{E}\left(k, \dfrac{kq}{p}\right)$ を通る縦線 $x = k$ 上で，E の上側 $\dfrac{1}{2}$ 未満の距離に格子点が存在するときである．線分 RS は線分 OT を縦に $\dfrac{1}{2}$ だけ平行移動したものだから，このような格子点は，$\mathcal{D}$ 内の OT の上側に存在する格子点である．

(c) これは (b) とまったく同様である．

(d) 線分 OC, PS, QR の中点はいずれも M なので，六角形 OPQCSR は M に関して点対称である．よって $\mathcal{D}$ も M に関して点対称である．M についてある格子点と点対称な点は格子点だから，$\mathcal{D}$ 内の格子点は，M に関して二つずつ互いに対称である．したがってその個数は，M が格子点であれば奇数で，そうでなければ偶数である．

(e) 定理 3 より，$\left(\dfrac{q}{p}\right) = (-1)^n$, $\left(\dfrac{p}{q}\right) = (-1)^m$ である．また，(a), (b), (c) より $\mathcal{D}$ 内にある格子点の個数は $m+n$ である．よって (d) から

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{m+n} = \begin{cases} -1 & \text{M が格子点のとき} \\ 1 & \text{M が格子点でないとき} \end{cases}$$

である．$\mathrm{M}\left(\dfrac{p+1}{4}, \dfrac{q+1}{4}\right)$ が格子点であるのは，$p \equiv q \equiv 3 \pmod 4$ のときである．

◎——5　証明 B の問題の解答

(a) $y^n - 1$ は異なる n 個の複素数 $\zeta^0, \zeta^1, \cdots, \zeta^{n-1}$ を根に持つので，因数定理を繰り返し用いて，$y^n - 1 = \prod_{\ell=0}^{n-1}(y - \zeta^\ell)$ である．y を $\dfrac{y}{z}$ で置き換え，両辺を z^n 倍すると，$y^n - z^n = \prod_{\ell=0}^{n-1}(y - \zeta^\ell z)$ である．n は奇数なので，$\ell = 0, 1, \cdots, n-1$ としたときの，-2ℓ の法 n での剰余はすべて異なり，全部を尽くす．したがって

$$y^n - z^n = \prod_{\ell=0}^{n-1}(y - \zeta^{-2\ell} z) = \zeta^{-(0+1+\cdots+(n-1))} \prod_{\ell=0}^{n-1}(\zeta^\ell y - \zeta^{-\ell} z)$$

である．$0 + 1 + \cdots + (n-1) = \dfrac{n-1}{2} \cdot n$ は n の倍数なので，$\zeta^{-(0+1+\cdots+(n-1))} = 1$ である．

(b) (18) で $y = e^{2\pi ix}$, $z = e^{-2\pi ix}$ として，

$$f(nx) = \prod_{\ell=0}^{n-1} f\left(x + \frac{\ell}{n}\right) = f(x) \prod_{\ell=1}^{\frac{n-1}{2}} f\left(x + \frac{\ell}{n}\right) \prod_{\ell=\frac{n+1}{2}}^{n-1} f\left(x + \frac{\ell}{n}\right)$$

である．ℓ が 1 から $\dfrac{n-1}{2}$ までを動くとき，$n - \ell$ は $\dfrac{n+1}{2}$ から $n-1$ まで動くので，

$$\prod_{\ell=\frac{n+1}{2}}^{n-1} f\left(x + \frac{\ell}{n}\right) = \prod_{\ell=1}^{\frac{n-1}{2}} f\left(x + \frac{n-\ell}{n}\right) = \prod_{\ell=1}^{\frac{n-1}{2}} f\left(x - \frac{\ell}{n}\right)$$

だから，(19) が得られる．ただし $f(x) = f(x+1)$ を用いた．

(c) 定理 3 の証明のように，$ka \equiv r_k \pmod p$, $|r_k| < \dfrac{p}{2}$ とする．$\dfrac{ka}{p}$ と $\dfrac{r_k}{p}$ の差は整数なので，$f\left(\dfrac{ka}{p}\right) = f\left(\dfrac{r_k}{p}\right)$ である．よって $\displaystyle\prod_{k=1}^{\frac{p-1}{2}} f\left(\frac{ka}{p}\right) = \prod_{k=1}^{\frac{p-1}{2}} f\left(\frac{r_k}{p}\right)$ である．一方，$r_1, \cdots, r_k$ は，絶対値は全体として $1, 2, \cdots, \dfrac{p-1}{2}$ である．よって，負のものが n 個であるとすると，$f(-x) = -f(x)$ であることから，

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

である．したがって定理 3 より (20) がしたがう．

(d) (19) で $n = q$, $x = \dfrac{k}{p}$ とした式を，$k = 1$ から $k = \dfrac{p-1}{2}$ まで辺ごとにかけると

$$\prod_{k=1}^{\frac{p-1}{2}} \frac{f\left(\dfrac{kq}{p}\right)}{f\left(\dfrac{k}{p}\right)} = \prod_{k=1}^{\frac{p-1}{2}} \prod_{\ell=1}^{\frac{q-1}{2}} f\left(\frac{k}{p} + \frac{\ell}{q}\right) f\left(\frac{k}{p} - \frac{\ell}{q}\right)$$

である．(20) より，この左辺は $\left(\dfrac{q}{p}\right)$ である．

(e) (17) で p と q を置き換えると，$f(-x) = -f(x)$ であることから，次のように示される．

$$\begin{aligned}
\left(\frac{p}{q}\right) &= \prod_{k'=1}^{\frac{q-1}{2}} \prod_{\ell'=1}^{\frac{p-1}{2}} f\left(\frac{k'}{q} + \frac{\ell'}{p}\right) f\left(\frac{k'}{q} - \frac{\ell'}{p}\right) \\
&= \prod_{k'=1}^{\frac{q-1}{2}} \prod_{\ell'=1}^{\frac{p-1}{2}} f\left(\frac{\ell'}{p} + \frac{k'}{q}\right) \left(-f\left(\frac{\ell'}{p} - \frac{k'}{q}\right)\right) \\
&= (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \prod_{k'=1}^{\frac{q-1}{2}} \prod_{\ell'=1}^{\frac{p-1}{2}} f\left(\frac{\ell'}{p} + \frac{k'}{q}\right) f\left(\frac{\ell'}{p} - \frac{k'}{q}\right) \\
&= (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} \left(\frac{q}{p}\right)
\end{aligned}$$

◎一一6　補充律とその証明

ルジャンドル記号には，本体の相互律 (1) のほかに次の公式があります．

定理 4　p を奇素数とする．

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}, \tag{24}$$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} \tag{25}$$

が成り立つ．　□

(24), (25) の右辺がそれぞれ

$$(-1)^{\frac{p-1}{2}} = \begin{cases} 1 & p \equiv 1 \pmod 4 \\ -1 & p \equiv 3 \pmod 4 \end{cases}$$

$$(-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & p \equiv \pm 1 \pmod 8 \\ -1 & p \equiv \pm 3 \pmod 8 \end{cases}$$

となることは簡単に分かります．(24) と (25) はそれぞれ平方剰余の第一補充律，第二補充律と呼ばれ，(1), (24), (25) をまとめて平方剰余の相互律と呼ぶこともあります．

(24) は，オイラーの規準で $a = -1$ とした式です．また，11 月号の命題 3 からもすぐにしたがいます．(25) の証明は，本稿の 1, 2, 3 節のそれぞれの方法でできます．以下，それを紹介します．

6.1　代数的な証明

証明　$X^4 + 1 \in \mathbb{F}_p[X]$ の $\mathbb{F}_p$ 上の最小分解体を $\mathbb{F}_p(\boldsymbol{\mu}_8)$ とし，$X^4 + 1$ の $\mathbb{F}_p(\boldsymbol{\mu}_8)$ 内の根の一つを ζ とする．$x := \zeta + \zeta^{-1} \in \mathbb{F}_p(\boldsymbol{\mu}_8)$ とする．x^2, x^p を計算すると，$\zeta^4 = -1$ であることからそれぞれ，

$$x^2 = \zeta^2 + 2 + \zeta^{-2} = \zeta^2 + 2 - \zeta^2 = 2, \tag{26}$$

$$x^p = \zeta^p + \zeta^{-p} = \begin{cases} x & p \equiv \pm 1 \pmod 8, \\ -x & p \equiv \pm 3 \pmod 8, \end{cases} \tag{27}$$

である．(26) より $x \neq 0$ なので，(27) より

$$x \in \mathbb{F}_p \Longleftrightarrow x^p = x \Longleftrightarrow p \equiv \pm 1 \pmod 8$$

である．一方 (26) より

$$x \in \mathbb{F}_p \Longleftrightarrow \left(\frac{2}{p}\right) = 1$$

である．したがって $\left(\frac{2}{p}\right) = 1 \Longleftrightarrow p \equiv \pm 1 \pmod 8$ であり，(25) が示された．　■

6.2 解析的な証明

定理 5 n を任意の正の整数とする．(7) の $G(n)$ について，

$$G(n) = \frac{1+i^{-n}}{1+i^{-1}}\sqrt{n} = \begin{cases} (1+i)\sqrt{n} & n \equiv 0 \pmod 4, \\ \sqrt{n} & n \equiv 1 \pmod 4, \\ 0 & n \equiv 2 \pmod 4, \\ i\sqrt{n} & n \equiv 3 \pmod 4 \end{cases} \tag{28}$$

が成り立つ． □

証明 n が奇数のときは定理 2 で示したので，n が偶数のときを考える．(7) の和の a を $a+\dfrac{n}{2}$ に置き換えて，

$$G(n) = \sum_{a\in\mathbb{Z}/n\mathbb{Z}} e^{\frac{2\pi i}{n}(a+\frac{n}{2})^2} = \sum_{a\in\mathbb{Z}/n\mathbb{Z}} e^{\frac{2\pi i a^2}{n}} \cdot e^{\frac{\pi i}{2}n} = i^n G(n)$$

である．よって $n \equiv 2 \pmod 4$ ならば，$G(n) = -G(n)$ だから $G(n) = 0$ である．

以下，$n \equiv 0 \pmod 4$ として，(28) を示す．まずやはり，(9) が成り立つことを示す．$G(n^3)$ の $0 \leqq a \leqq n^3-1$ の和を $a = b + c\dfrac{n^2}{2}$, $0 \leqq b \leqq \dfrac{n^2}{2}-1$, $0 \leqq c \leqq 2n-1$ と置き換えて計算すると，

$$G(n^3) = \sum_{b=0}^{\frac{n^2}{2}-1} e^{\frac{2\pi i b^2}{n^3}} \left(\sum_{c=0}^{2n-1} e^{\frac{2\pi i bc}{n}} \right)$$

である．内側の c についての和は，b が n の倍数のとき $2n$ で，そうでないときは 0 である．よって $b = dn$ と置き換えて，

$$G(n^3) = 2n \sum_{d=0}^{\frac{n}{2}-1} e^{\frac{2\pi i d^2}{n}} = n \sum_{d=0}^{n-1} e^{\frac{2\pi i d^2}{n}} = nG(n)$$

である．また，$n \equiv 0 \pmod 4$ のときも (10) が成り立つ．この証明は n が奇数のときとまったく同様である．$\dfrac{n}{4}$ が整数になるので，関数を少しだけ平行移動し，φ_n の台が $\left(-\dfrac{n+1}{4}, \dfrac{3n-1}{4}\right)$ 含まれるようにし，$-\dfrac{n}{4} \leqq x \leqq \dfrac{3n}{4}-1$ では $\varphi_n(x) = 1$ となるように取ればよい．

(9) と (10) から (28) が得られることを示しておく．$E(n) := G(n) - \dfrac{1+i^{-n}}{1+i^{-1}}\sqrt{n}$ とおく．(10) から，すべての n について $|E(n)| \leqq M$ となるような正定数 M が存在する．正の整数 n を固定する．(9) から，整数 $k \geqq 0$ について

$$E(n^{3^k}) = n^{\frac{3^k-1}{2}} E(n)$$

が帰納的に得られる．よって $n^{\frac{3^k-1}{2}}|E(n)| \leqq M$ である．$n > 1$ のとき，これがすべての k について成り立つためには，$E(n) = 0$ でなければならない．

$n = 1$ のときはこの論法は使えないが，$E(1) = G(1) - 1 = 0$ は定義からただちに示される． ■

(25) の証明　$\zeta = e^{\frac{2\pi i}{8}}$ とおく．まず

$$\left(\frac{2}{p}\right) = \frac{G(8p)}{4\zeta^p G(p)} \tag{29}$$

が成り立つことを示す．$\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \ni (b,c) \mapsto 8b + cp \in \mathbb{Z}/8p\mathbb{Z}$ が全単射であることから，

$$G(8p) = \sum_{b \in \mathbb{Z}/p\mathbb{Z}} e^{\frac{2\pi i \cdot 8b^2}{p}} \cdot \sum_{c \in \mathbb{Z}/8\mathbb{Z}} e^{\frac{2\pi i p c^2}{8}}$$

である．右辺の積の第一項は (16) と同様に考えて，$\displaystyle\sum_{b \in \mathbb{Z}/p\mathbb{Z}} e^{\frac{2\pi i \cdot 2(2b)^2}{p}} = \left(\frac{2}{p}\right) G(p)$ である．一方，第二項は

$$\begin{aligned}\sum_{c \in \mathbb{Z}/8\mathbb{Z}} e^{\frac{2\pi i p c^2}{8}} = \sum_{c=0}^{7} \zeta^{pc^2} = 2\sum_{c=0}^{3} \zeta^{pc^2} &= 2(1 + \zeta^p + \zeta^{4p} + \zeta^{9p}) \\ &= 2(1 + \zeta^p - 1 + \zeta^p) = 4\zeta^p\end{aligned}$$

である．これより (29) が得られる．(29) に (28) を代入すると

$$\left(\frac{2}{p}\right) = \frac{2\sqrt{8p}}{4\zeta^p(1 + i^{-p})\sqrt{p}} = \frac{\sqrt{2}}{\zeta^p + \zeta^{-p}} = \begin{cases} 1 & p \equiv \pm 1 \pmod 8, \\ -1 & p \equiv \pm 3 \pmod 8, \end{cases}$$

となる．■

注　n を奇数とすると，(29) を示した方法と同じ議論で，

$$G(4n) = 2(1 + i^n) G(n) \tag{30}$$

を示すことができます．したがって $G(4n) = 2(1+i)\sqrt{n}$ が示されれば，$G(n) = \dfrac{G(4n)}{2(1+i^n)} = \dfrac{1 + i^{-n}}{1 + i^{-1}}\sqrt{n}$ が得られます．この意味で，(28) は実は n が 4 の倍数のときに示せば十分です．ただ，その証明は自然に n が奇数の場合を含めて考えることができるので，ここでは n が 4 の倍数のときと n が奇数のときとの両方を直接示しました．

6.3　初等的な証明

証明　定理 3 より，$2, 4, \cdots, p-1$ のうち $\dfrac{p}{2}$ より大きいものが n 個であるとすると，$\left(\dfrac{2}{p}\right) = (-1)^n$ である．$p = 4k+1$ のとき，$2, 4, \cdots, p-1$ のうち $\dfrac{p}{2}$ より小さいものは k 個だから，$n = \dfrac{p-1}{2} - k = k$ である．$p = 4k+3$ のとき，$2, 4, \cdots, p-1$ のうち $\dfrac{p}{2}$ より小さいものは k 個だから，$n = \dfrac{p-1}{2} - k = k+1$ である．したがって $(-1)^n$ はいずれの場合も k の偶奇によって決まり，結論をまとめると

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv \pm 1 \pmod 8, \\ -1 & p \equiv \pm 3 \pmod 8, \end{cases}$$

となる．■

[たにぐち たかし]
[絵／森脇かみん]