数理解析研究所講究録
第1625巻 2009年 88-94

Gauss:Disquisitiones Arithmeticae に見られる合同式 $ax^3 - by^3 \equiv 1 \pmod{p}$ について

小柴 洋一 (鹿児島大 (理))

2008年8月6日 (水)

1 はじめに

合同式ゼータ関数は整数論、代数幾何学等の研究現場に現れる重要な概念です。このゼータ関数の場合の「Riemann 予想」の歴史を調べてきました. そのことが標題の Gauss の話につながるのです.

どういう事かといいますと関数体の「Riemann 予想」はしばしば不等式

$$|1 + q^n - N_n| \leqq 2g \cdot q^{\frac{n}{2}} \tag{1}$$

で表現されます.

式 (1) の意味 : 有限体 k を定義体とする代数曲線 C/k があるとき k の個数を q , C の種数を g, k の n 次拡大 k_n での C の k_n 有理点の個数を N_n としています.

Andre Weil によると代数曲線 $ax^3 - by^3 \equiv 1 \pmod{p}$ の場合に Gauss は同じ認識に達していたというのです. Gauss [2] および高瀬 [4] 参照.

2 代数的数体と代数関数体の類似性

合同式ゼータ関数を考えるアイデアは、有限次代数体と1変数代数関数体の類似性にあります。Emile Artin(1924年) 以前にこの類似性に注目した数学者、もしくは論文著作が種々見られます[*1]。

[*1] もちろん、初等的には、整数と多項式の類似といってもよろしいかと思います

特に1変数代数関数体の定数体を有限体にするとその類似性が強められ，ゼータ関数を考えることが出来ます.

3 合同式ゼータ関数

有限体 k を定義体とする代数曲線 C/k があるとき

$$\zeta(s;C/k)=\sum_{\mathfrak{A}>0}N(\mathfrak{A})^{-s} \tag{2}$$

右辺の総和は C/k の全ての正因子 $\mathfrak{A}$ を走るのです.

数体と関数体との類似性で言えば有理数体 Q の正因子 $\mathfrak{A}$ は正整数 n と考えられます. この右辺は

$$\sum_{n=1}^{\infty}n^{-s}$$

でこれは良く知られた Riemann ゼータ関数です.

4 Weil による「Riemann 予想」の証明

式 (2) は現在では

$$\frac{d}{du}\log Z(u)=\sum_{n=1}^{\infty}N_nu^{n-1},\quad u=q^{-s}$$

の形 で述べられることが多い.

Weil [7]70 ページによると

$$Z(u)=\frac{P(u)}{(1-u)(1-qu)}$$

$u=q^{-s}$. ここでは $P(u)$ は $2g$ 次の有理整係数の多項式.

「Riemann 予想」とは $P(u)$ の零点 u の絶対値が $q^{-\frac{1}{2}}$ であることをいいます[*2] .

代数曲線の代数的対応の環を考えます. δ を C の恒等対応の類，ι を C の Frobenius 対応の類とします.

x,y を任意の有理整数として $\xi=x\cdot\delta+y\cdot\iota$. とおく.

$$Castelnuovo\text{の不等式}\quad \sigma(\xi\xi')\geqq 0$$

[*2] ということは s の方で言えば $\Re s=\frac{1}{2}$

より次の不等式を得ます.

$$2g \cdot x^2 + 2\sigma(\iota^n) \cdot xy + 2gq^n \cdot y^2 \geqq 0 \tag{3}$$

式 (3) の正値定符号であることから式 (1) が得られます.

$$d[\log P(u)] = -\sum_{n=1}^{\infty} \sigma(\iota^n) \cdot u^n \cdot \frac{du}{u}.$$

から関数 $\log P(u)$ が $|u| < q^{-\frac{1}{2}}$ で正則，関数等式から $|u| > q^{-\frac{1}{2}}$ でも正則，したがって $P(u)$ の零点は円周 $|u| = q^{-\frac{1}{2}}$ 上になければならないことになります.

5 Weil の引用した Gauss 文献の箇所

文献 Weil [8] によると Gauss は既にある特殊な場合に不等式 (1) を認識していたというのです. もちろん有理整数環を modulo p で考えた場合です[*3]. 正確に述べれば不等式 (1) において $q = p, n = 1, g = 1$ の場合です.

それは 3 つあって

1. $ax^3 - by^3 \equiv 1 \pmod{p}$ $p = 3n + 1$
   Disquisitioes の 3 5 8 節にある. Gauss [3] 第 1 巻 445 ページにあるものです.
2. $ax^4 - by^4 \equiv 1 \pmod{p}$ 4 次剰余についての覚書 (memoir) にある. Gauss [3] 第 2 巻 67 ページから 92 ページにあるものです.
3. $y^2 \equiv ax^4 - b \pmod{p}$ 日記 (Tagebuch) にある. Gauss [3] 第 1 1 巻 571 ページから 572 ページにあるものです.

Gauss 全集で見てみると不等式 $ax^3 - by^3 \equiv 1 \pmod{p}$ が直接，書いてあるわけではありません. これについて更に Gauss 資料の分析が必要かと思います. 別の機会に報告したいと思います.

[*3] p は有理素数

6 Schmidt と Herglotz の文献

文献 Schmidt [9] によると

$$ax^3 - by^3 \equiv 1 \pmod{p} \quad p = 3n+1$$
$$ax^4 - by^4 \equiv 1 \pmod{p} \quad p = 4n+1$$
$$ax^3 - by^3 \equiv 1 \pmod{p}$$

の場合に Gauss は解の個数についての評価式を得ていたという.

Eichler 文献 [5] ３２２ページ によると Gauss は方程式

$$f(x,y) = x^2y^2 + x^2 + y^2 - 1 \equiv 1 \pmod{p}$$

の場合に関数体の「Riemann 予想」すなわち式 (1) を予想した. すなわち,

$$|1 + p - N| \leqq 2 \cdot p^{\frac{1}{2}}$$

を予想したことになる[*4].

Herglotz [*5]はこれを証明している. 文献 Herglotz [6] を参照.

7 解析接続

級数 $\sum_{n=1}^{\infty} n^{-s}$ は $\Re s \leqq 1$ では発散している. 定義域が $\Re s > 1$ でないと意味がない. これを複素変数 s として Riemann はどのように考えたのであろうか?

Cauchy は定積分 $\int_0^{\infty} \frac{\sin x}{x} dx$ を複素積分で捉えています (１８２５年).

定積分 $\int_0^{\infty} x^{s-1}e^{-x}dx$ は平凡な微分積分の計算だが Riemann は複素積分 $\int_C (-x)^{s-1}e^{-x}dx$ と見た. $(-x)^{s-1} = e^{(s-1)\log(-x)}$ として対数関数の Riemann 面上の積分とした. １８５９年の時点で Euler の実数変数の ζ 級数から複素変数 s として考え全平面に定義域を拡張, すなわち解析接続の考えを持つことが出来たというのは大変な飛躍であったといえる. 次は Riemann の原論文 [1] から抜粋してきた. 解析接続の部分です. 本論文の２ページ目にある.

[*4] この曲線は種数が 1 であることに注意

[*5] E.Artin の先生である. Emile Artin 全集による.

⋮

Betrachtet man nun das Integral

$$\int \frac{(-x)^{s-1}\,dx}{e^x-1}$$

von $+\infty$ bis $+\infty$ positiv um ein Grössengebiet erstreckt, welches den Werth 0, aber keinen andern Unstetigkeitswerth der Function unter dem Integralzeichen im Innern enthält, so ergiebt sich dieses leicht gleich

$$(e^{-\pi si}-e^{\pi si})\int_0^\infty \frac{x^{s-1}\,dx}{e^x-1},$$

vorausgesetzt, dass in der vieldeutigen Function $(-x)^{s-1}=e^{(s-1)\log(-x)}$ der Logarithmus von $-x$ so bestimmt worden ist, dass er für ein negatives x reell wird. Man hat daher

$$2\sin\pi s\,\Pi(s-1)\zeta(s)=i\int_\infty^\infty \frac{(-x)^{s-1}\,dx}{e^x-1},$$

das Integral in der eben angegebenen Bedeutung verstanden.
Diese Gleichung giebt nun den Werth der Function $\zeta(s)$ für

⋮

7.1 現代流にとらえると

$\sigma>1$ に対し

$$\Gamma(s)=\int_0^\infty x^{s-1}e^{-x}dx.$$

この積分で x を nx におきかえると

$$n^{-s}\Gamma(s)=\int_0^\infty x^{s-1}e^{-nx}dx$$

が得られ、n について総和をとることにより

$$\zeta(s)\Gamma(s)=\int_0^\infty \frac{x^{s-1}}{e^x-1}dx$$

を得る。今の場合、右辺の積分はその両端で絶対収束し、積分と無限和の交換は許されるからです。

ここで s を複素変数のパラメーターとみなし複素積分を考えよう．正の無限大から実軸に近い直線から始まり帰ってゆく道 C を考えよう。

定理 1. $\sigma > 1$ に対し、正の実軸の補集合において $(-z)^{s-1}$ を $e^{(z-1)\log(-z)}, -\pi < \Im\log(-z) < \pi$ と定義すると、

$$\zeta(s) = -\frac{\Gamma(1-s)}{2\pi i}\int_C \frac{(-z)^{s-1}}{e^z-1}dz$$

が成り立つ。

Proof. 右辺の積分は被積分関数の形より収束することが解る。Cauchy の定理により、複素積分変数 $z = x + yi$ が複素平面上の整数倍の点を囲まないかぎり積分路の形をかえてもかまわない。とくに、円周の半径を 0 に収束させてよい。円周上の積分が $r \to 0$ のときに 0 になることはすぐにわかる。極限においては、結局、正の実軸を往復する積分となる。上半平面側では $\int_\infty^0 \frac{x^{s-1}}{e^x-1}dx$ となり、下半平面側では $\int_0^\infty \frac{(xe^{2\pi i})^{s-1}}{e^x-1}dx$ であり[*6]、ゆえに、

$$\int_C \frac{(-z)^{s-1}}{e^z-1}dz = (e^{2\pi is}-1)\Gamma(s)\zeta(s)$$

をうる。 □

参考文献

[1] B.Riemann. Über die Anzahl der Primzahlen unter einer gegebenen Grösse. *Monats berichte der Berliner Akademie*, November 1859.

[2] C.F.Gauss. *Disqusitiones Arithmeticae.* Springer, 1971.

[3] C.F.Gauss. *Carl Friedrich GAUSS.* Georg Olms Verlag, 1973.

[4] C.F. ガウス. ガウス整数論. 朝倉書店, 1995. 高瀬正仁　訳.

[5] M Eichler. *Einführung in die Theorie der Algebraishen Zahlen und Funktionen.* Birkhauser, 1963.

[6] G.Herglotz. Zur letzen Eintragung im Gaußschen Tagebuch. *Ber. Verh.Sáchs.Akad. Wiss.Leipzig Math.-Phys.*, Vol. Kl.73, pp. 271–276, 1921.

[7] A Weil. *Variétés abeliennes et courbes algébriques.* Hermann, 1948.

[*6] ここのところでいわゆる「Riemann 面」を考えている

[8] A Weil. Numbers of solutions of equations in finite fields. *Bull. Am. Math. Soc.*, Vol. 55, pp. 497–508, 1949.

[9] W.F.Schmidt. *Equations over Finite Fields ,An Elementary Approach*, Vol. 536. Springer, 1975. Lecture Notes.