2次体の類数問題

平松豊一・斎藤正顕

1 Dirichlet の類数公式

1.1

Lagrange は整数 m が

$$m = ax^2 + bxy + cy^2, \quad D = b^2 - 4ac$$

と2次形式で表される問題を考え, 2次形式論を展開した（1773）.

$$f(x,y) = ax^2 + bxy + cy^2, \quad (a,b,c) = 1$$

$$\begin{pmatrix} x \\ y \end{pmatrix} \longmapsto \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix}, \quad \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in SL_2(\mathbf{Z})$$

なる変換で, f が

$$f'(x,y) = a'x^2 + b'xy + c'y^2$$

となるとき, f と f' を同値であるという.

$$f \sim f'$$

とかく. このとき, f と f' の判別式は同じで, 同じ整数を表現する. 判別式 D の同値類の個数は有限で, それを類数という. $h = h(D)$ とかく.

D が基本判別式とは

1) $D \equiv 1 \bmod 4$, D: square-free 又は,

2) $D \equiv 0 \bmod 4$, $\frac{D}{4} \equiv 2, 3 \bmod 4$, $\frac{D}{4}$: square-free

のときをいう.

判別式 D の 2次体 $\mathbf{Q}(\sqrt{D}) = K$ の2つのイデアル A, B に対し,

$$B = \rho A, \ \rho \in \mathbf{Q}(\sqrt{D}), \ N(\rho) > 0$$

なる関係があるとき, B と A は同値であるといい,

$$A \sim B$$

と表す. このイデアルの同値類は有限個で, それを K の類数といい, $H(D)$ で表す. 尚, $N(\rho) > 0$ を仮定しないとき, K の広義の類数という. K が虚2次体又は K が $N(\varepsilon) = -1$ なる単数をもつ実2次体の時は, 両者は一致する. また, D : 基本判別式のときは, $h(D) = H(D)$ となる.

さて,

$$ax^2 + bxy + cy^2, \quad D = b^2 - 4ac < 0$$

に対し,

Gauss の類数問題 与えられた類数 h をもつすべての negative disc. を決定する effective algorithm を求めよ.

1.2 Dirichlet の類数公式

mod m の Dirichlet 指標

$$\chi : (\mathbf{Z}/m\mathbf{Z})^\times \longrightarrow S^1 \quad \text{homomorphism}$$

に対し, $\chi : \mathbf{Z} \longrightarrow \mathbf{C}$ st

a) $\chi(n) = 0 \Longleftrightarrow (n, m) > 1$

b) $\chi(kn) = \chi(k)\chi(n)$, $k, n \in \mathbf{Z}$

c) $\chi(n) = \chi(k)$, $k \equiv n \bmod m$

なる χ を対応させる

$$\begin{aligned} L(s,\chi) &= \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \quad (\mathrm{Re}\ s > 1) \\ &= \prod_p (1 - \chi(p)p^{-s})^{-1} \end{aligned}$$

定理 1.1 (Dirichlet) $L(1,\chi) \neq 0$ for $\chi \neq id$.

基本判別式 D に対し,

$$n \longmapsto \left(\frac{D}{n}\right) : \text{Kronecker 記号}$$

は mod $|D|$ の primitive Dirichlet 指標を与える. 任意の primitive real Dirichlet 指標はある基本 disc. に関する指標 $(\frac{D}{\cdot})$ と一致する. さて,

$$w = \begin{cases} 2 & D < -4 \\ 4 & D = -4 \\ 6 & D = -3. \end{cases}$$

とおくとき,

定理 1.2 (Dirichlet)

$$h(D) = \begin{cases} \dfrac{w\sqrt{|D|}}{2\pi} L(1, \left(\dfrac{D}{\cdot}\right)), & D < 0, \\ \dfrac{\sqrt{D}}{\log \varepsilon_0} L(1, \left(\dfrac{D}{\cdot}\right)), & D > 0, \end{cases}$$

ここで, $\varepsilon_0 = \frac{1}{2}(t_0 + u_0\sqrt{D})$ は Pell 方程式

$$t^2 - Du^2 = 4$$

の基本解 ($t_0, u_0 > 0$ 最小) を表す.

Gauss 和を利用して,

定理 1.3 (Dirichlet) D : fundamental disc. として,

$$h(D) = \begin{cases} -\dfrac{w}{2|D|} \displaystyle\sum_{n=1}^{|D|-1} \left(\frac{D}{n}\right) n, & D < 0, \\ -\dfrac{1}{\log \varepsilon_0} \displaystyle\sum_{n=1}^{D-1} \left(\frac{D}{n}\right) \log \sin \frac{\pi n}{D}, & D > 0. \end{cases}$$

<u>**N.B.**</u> Dirichlet′の類数公式の特別な場合 : $x^2 + py^2$, $p \equiv 3 \bmod 4$ は Jacobi によって考察された (1832). また, Gauss もある時期に類数公式を知っていた (Werke , Dedekind) : Bachmann's report, Über Gauss' Zahlentheorische Arbeiten, Material für eine wisenschaftliche Biographie von Gauss (ed. by F. Klein and M. Brendel, Heft 1, Leipzig, Teubner, 1911).

2 Gauss の類数問題

2.1

The Gauss conjecture : The number of negative disc. $D < 0$ which have a given class number h is finite.

定理 2.1 (Hecke-Deuring-Heilbronn)

$$h(D) \to \infty \text{ as } D \to -\infty.$$

しかし, その証明が ineffective だったので, 与えられた類数をもつ虚 2 次体を決定する algorithm を与えることはできなかった. 例えば,

定理 2.2 (Heilbronn-Linfoot) $h(D) = 1$ となる基本判別式 $D < 0$ をもつ虚 2 次体は高々10 個である:

$$D = -3, -4, -7, -8, -11, -19, -43, -67, -163, ?$$

定理 2.3 (Siegel) $\forall \varepsilon > 0$, $\exists$ constant $c > 0$: effectively には計算できない st

$$h(D) > c|D|^{\frac{1}{2}-\varepsilon}, \quad \varepsilon > 0.$$

<u>**N.B.**</u> Tatuzawa は, 高々 1 つの例外を除いて, すべての $D < 0$ に対し c を effective に決めた.

2.2 $h(D) = 1, 2$ 問題の歴史

$$\left.\begin{array}{l} \text{1966 Baker} \\ \text{1966 Stark} \end{array}\right\} \text{第 10 番目の虚 2 次体はない}$$

<u>**N.B.**</u> Baker は Gelfand-Linnik のアイディアを使い, Stark は Heegner's によく似ている.

1968 Deuring : Heegner's proof の gap をうめる

1968 Siegel : another proof

1969 Stark : 2 papers

1970 Chowla : 定理 2.1 と関連する

$$\left.\begin{array}{l}\text{1971 Baker}\\ \\ \text{1971 Stark}\end{array}\right\}\text{類数 2 問題の解決 : 18 個, i.e., } D = \begin{array}{l}-15,-20,-24,-35,-40,-51,\\ -52,-88,-91,-115,-123,-148,\\ -187,-232,-235,-267,-403,-427\end{array}$$

1972 Goldstein

N.B. CM-field : totally real fields の totally complex 2 次拡大 ; Gauss の class number prob. は CM-field に拡張できる.

Stark conjecture 与えられた類数をもつ CM-fields が有限個ある.

cf. H. M. Stark : Class-numbers of CM-fields and Siegel zeros, to be published.

3 虚 2 次体の類数 1 問題

K. Heegner (high school teacher) : Diophantische Analysis und Modulfunktionen, Math. Z., **56** (1952), 227-253.

この証明は, H. Weber : Lehrbuck der Algebra, Vol. 3 (1908) を利用しているが, a gap があった. 以下で, この Heegner method で, 'a gap' を訂正して, 証明を概観する (Stark).

N.B. Baker の証明も, Gelfand-Linnik のアイディア : '3 つの logarithms が 1 次独立なら類数 1 問題は解ける' を base にしている. しかし, 実は 2 つの logarithms が 1 次独立なら類数 1 問題は解けることがわかり (Stark), この問題は実質的に Gelfand-Linnik によって 1949 年に解かれていたことがわかる.

$\operatorname{Im} z > 0$, $q = 2^{2\pi i z}$

$$j(z) = \frac{E_4(z)^3}{\Delta(z)} = \frac{\left\{1 + 240\sum_{n=1}^{\infty}\left(\sum_{d|n} d^3\right) q^n\right\}^3}{q\prod_{n=1}^{\infty}(1-q^n)^{24}} \quad : \text{Elliptic modular inv.}$$

$$\gamma_2(z) = \{j(z)\}^{\frac{1}{3}} \quad \left(\tfrac{1}{3}\text{ 乗は虚軸上 real となる branch}\right) \quad : \Gamma(3)\text{-inv.}$$

$$f(x,y) = ax^2 + bxy + cy^2, \quad a > 0, \quad (a,b,c) = 1$$
$$D = b^2 - 4ac < 0$$

$h'(D)$: 類数

とする.

$|D| \equiv 3 \bmod 8,\ 3 \nmid D$ なら

$h'(D) = h(D)$: $\mathbf{Q}(\sqrt{D})$ の類数.

$$\underset{\text{イデアル}}{\mathfrak{a} = [\alpha, \beta]} \underset{1\text{対}1}{\longleftrightarrow} f(x, y) = \frac{N(\alpha x + \beta y)}{N(\mathfrak{a})}$$

- $h(D) = 1,\ D < -8$ なら, $3 \nmid D,\ |D| \equiv 3 \bmod 8$ (Dickson)

- $j\left(\dfrac{-b+\sqrt{D}}{2a}\right)$, は $\deg h'(D)$ の代数的整数 (Weber III, §122)

以下, $|D| \equiv 3 \bmod 8,\ 3 \nmid D$ とする.

<u>**N.B.**</u> それ以外の D :
$D = -3, -4, -7, -8$ のとき, $h(D) = 1$.

$$f(z) := q^{-\frac{1}{48}} \prod_{n=1}^{\infty} (1 + q^{\frac{2n-1}{2}}) = \frac{q^{-\frac{1}{48}} \eta\left(\frac{z+1}{2}\right)}{\eta(z)}$$

とおく. $f\left(\dfrac{-3+\sqrt{D}}{2}\right)$ は方程式

$$x^{24} + \gamma_2 \left(\frac{-3+\sqrt{D}}{2}\right) x^8 - 16 = 0 \tag{1}$$

の解である (Weber III, §54).

$$f_2(z) := \sqrt{2} q^{\frac{1}{24}} \prod_{n=1}^{\infty} (1 + q^n) = \frac{\sqrt{2}\eta(2z)}{\eta(z)}$$

とおく. $e^{\frac{\pi i}{8}} f_2\left(\dfrac{-3+\sqrt{D}}{2}\right)$ も (1) の解である (Weber III, §54). 以下,

$$J = j(\sqrt{D}), \quad F = f(\sqrt{D}), \quad h = h(D),$$
$$j = j\left(\frac{-3+\sqrt{D}}{2}\right), \quad f_2 = e^{\frac{\pi i}{8}} f_2\left(\frac{-3+\sqrt{D}}{2}\right), \quad \gamma_2 = \gamma_2\left(\frac{-3+\sqrt{D}}{2}\right)$$

と略記する.

1) $f_2^2 = \dfrac{2}{F^2}$ (Weber III, §128)

2) $F^2 \in \mathbf{Q}(j)$ (Weber III, §127)

3) $F \in \mathbf{Q}(j)$ (Weber の予想) $\cdots$ Birch によって証明された.

N.B. Heegner は, この予想 3) を使い, (1) が 6 次の因子をもちその係数が degree h の代数的数であることを示した. ここの部分が 'a gap' に相当する. しかし, 類数 1 問題を解くには, 3) は不要である.

さて,

- ∘ $\mathbf{Q}(f_2^2) = \mathbf{Q}(F^2) = \mathbf{Q}(J)$
- • $J^3 + rJ^2 + sJ + t = 0$ $(r, s, t \in \mathbf{Q}(j))$ (Weber III, §69)

これ等より

$$\begin{aligned}[\mathbf{Q}(j,J):\mathbf{Q}] &= [\mathbf{Q}(j,J):\mathbf{Q}(j)][\mathbf{Q}(j):\mathbf{Q}] \\ &\leq 3h, \\ [\mathbf{Q}(j,J):\mathbf{Q}] &\geq [\mathbf{Q}(J):\mathbf{Q}] = 3h \quad \text{(Dickson)}\end{aligned}$$

従って, $\mathbf{Q}(j,J) = \mathbf{Q}(J)$ は $\mathbf{Q}(j)$ 上 3 次, i.e., $\mathbf{Q}(f_2^2)$ は $\mathbf{Q}(j)$ 上 3 次となる. よって f_2^2 は

$$x^3 + \lambda x^2 + \mu x + \nu = 0, \quad \lambda, \mu, \nu \in \mathbf{Q}(j)$$

の解になる. γ_2 は代数的整数で, f_2^2 は (1) の解だから代数的整数 :

$$\lambda, \mu, \nu : \mathbf{Q}(j) \text{ 内の代数的整数}$$

そこで, f_2^4 のみたす方程式を

$$x^3 + \delta x^2 + \varepsilon x + \phi = 0$$

とするとき,

$$\begin{cases} f_2^{12} + \delta f_2^8 + \varepsilon f_2^4 + \phi = 0 \\ f_2^6 + \lambda f_2^4 + \mu f_2^2 + \nu = 0 \end{cases}$$

これより,

$$\delta = 2\mu - \lambda^2, \quad \varepsilon = \mu^2 - 2\lambda\nu, \quad \phi = -\nu^2.$$

f_2^8 についても同様に,

$$x^3 + (2\varepsilon - \delta^2)x^2 + (\varepsilon^2 - 2\delta\phi)x - \phi^2 = 0$$

をみたす. $\mathbf{Q}(f_2^2) = \mathbf{Q}(f_2^8)$ 故 f_2^8 のみたす方程式は unique で, f_2 が (1) をみたすから,

$$(f_2^8)^3 - \gamma_2(f_2^8) - 16 = 0.$$

これより,

$$\varepsilon^2 - 2\delta\phi = -\gamma_2, \quad \delta^2 = 2\varepsilon, \quad \phi^2 = 16.$$

$\sqrt{D}$ は純虚数 故 $J = j(\sqrt{D})$ は real : ν は real. よって,

$$\phi \leq 0 : \phi = -4, \ \nu = \pm 2.$$

$$(2\mu - \lambda^2)^2 = \delta^2 = 2\varepsilon = 2(\mu^2 \pm 4\lambda).$$

ここで, $h=1$ とすると, λ, μ, ν : 有理整数 故

$$\lambda, \mu : \text{even}$$
$$\pm\lambda = 2\alpha, \ \ \mu = 2\beta \quad (\alpha, \beta \in \mathbf{Z})$$

とおくと,

$$2\alpha(\alpha^3+1) = (\beta - 2\alpha^2)^2$$

なる方程式を得る. これを Heegner の Diophantine 方程式という. これを解いて,

$$(\alpha, \beta) : (1,0),\ (-1,2),\ (2,2),\ (1,4),\ (2,14)$$

i.e.,

$$\gamma_2 = -32, -97, -960, -5280, -64032$$

$\gamma_2 = \gamma_2\left(\dfrac{-3+\sqrt{D}}{2}\right)$ より, Weber III (§125) を使い,

$$D = -11, -19, -43, -67, -163.$$

4　虚 2 次体の類数 2 問題

$\alpha_1 (= -1),\ \alpha_2,\ \ldots,\ \alpha_n\ (n \geq 2)$: 異なる実 2 次体の基本単数

Logarithms は principal values, $\beta^\gamma = e^{\gamma \log \beta}$;

$b_2, \ldots, b_n \in \mathbf{Z}, \quad b_n \neq 0, \quad b_1 = -D\ (D < 0)$

とする.

定理 4.1 $\nu \geq 1$: real, $0 < \varepsilon \leq 1$ とするとき,

$$\exists H_0 = H_0(\varepsilon, \nu, \alpha_1, \ldots, \alpha_{n-1}) : \text{effectively computable number}$$

st $H > H_0$, $|b_j| < H^\nu$ $(j = 1, \ldots, n)$, $\log \alpha_n < H^{1-\varepsilon}$ に対し

$$|b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n| \geq e^{-H}.$$

これより,

定理 4.2 $\exists c$: effectively computable number, st $h(d) = 2$ なら $|d| < c$.

具体的に,

定理 4.3 $h(d) = 2$ なら $|d| < 10^{1100}$.

定理 4.4 $h(d) = 2$ なら $|d| < 10^{1030}$.

5 実2次体の類数1問題

Gauss-Hasse 予想 p : 素数, $p \equiv 1 \bmod 4$, $h(p)$: 実2次体 $\mathbf{Q}(\sqrt{p})$ の類数とするとき, $h(p) = 1$ なる実2次体のすべての実2次体 $\mathbf{Q}(\sqrt{p})$ に関する density は 0 でない.

未解決である！

定理 (Takhtajan-Vinogradov) $\Gamma = \Gamma_0(p)$ (Hecke の合同部分群), $p \equiv 1 \bmod 4$ とするとき,

$$\lambda_1(\Gamma, \chi, 0) = \frac{1}{4} \Longleftrightarrow h(p) > 1.$$

従って,

$$\text{Gauss-Hasse 予想} \Longleftrightarrow \lambda_1 \neq \frac{1}{4} \text{ となる } p \text{ が無数にある.}$$

- 名城紘昭 : $h(p) = 1$ となる素判別式実2次体の個数

	$h = 1$	$p \equiv 1 \bmod 4$	%
$0 \sim 10^7$	256346	332180	77.17
$0 \sim 2 \times 10^7$	489086	635170	77.0
$0 \sim 3 \times 10^7$	714221	928779	76.90
$0 \sim 4 \times 10^7$	934304	1216687	76.79
$0 \sim 5 \times 10^7$	1151373	1500452	76.74
$0 \sim 6 \times 10^7$	1365463	1780670	76.68
$\vdots$	$\vdots$	$\vdots$	$\vdots$

- H. Cohen-H. W. Lenstra, Jr. :
  $p \equiv 1 \bmod 4$, $x \to \infty$

a) $h(p) > x$ となる確率 $\sim \dfrac{1}{2x}$

b) $\displaystyle\sum_{p \leq x} h(p) \sim \frac{x}{8}$

Appendix

Gauss の類数問題 $(D < 0)$ のその後 :

1975 Goldfeld : 十分小さい $\varepsilon > 0$ で

$$h(D) < \frac{\varepsilon\sqrt{|D|}}{\log |D|}$$

のとき,

$$\exists\beta < 1 \text{ st for } \chi \bmod D, \text{ odd, primitive, } L(\beta, \chi) = 0,$$

$$1 - \beta \quad \sim \quad \frac{6}{\pi^2} L(1, \chi) \sum_{\substack{b^2 - 4ac = D \\ -a < b \leq a \leq c \\ \text{or } 0 \leq b \leq a = c}} \frac{1}{a} \quad \text{as } D \to -\infty.$$

β を Siegel zero と呼ぶ.

1983 Gross-Zagier-Goldfeld : $\varepsilon > 0$ に対し,

$$\exists c > 0 \text{ effectively computable constant,}$$

$$\text{st } h(D) > c(\log|D|)^{1-\varepsilon}.$$

Gauss の class number problem はこれで解けたことになる.

1984 Oesterlé :

$$h(D) > \frac{1}{7000}(\log|D|) \prod_{\substack{p\,||\,D| \\ p \neq |D|}} \left(1 - \frac{[2\sqrt{p}]}{p+1}\right)$$

N.B. conductor 5077 の elliptic curve を利用して, $7000 \to 55$ と改良された (Brumer-Kramer-Oesterlé). これと, $h(D) \neq 3$ for $907 < |D| < 10^{2500}$ (Montgomery-Weinberger) より, $h(D) = 3$ なる虚 2 次体の完全リストを得る. また, $h(D) = 1, 2, 4$ の完全リストから,

$$n = x^2 + y^2 + z^2 \quad (x \geq y \geq z \geq 0)$$

と unique に表される n の完全リストが決定される.

References

[1] A.Baker, Linear forms in the logarithms of algebraic numbers, Mathematika **13** (1966), 204–216.

[2] A.Baker, Imaginary quadratic fields with class number two, Ann. of Math. (2) **94** (1971), 139–152.

[3] B.J.Birch, Diophantine analysis and modular functions, in Algebraic Geometry, Oxdford (1969), 35–42.

[4] S.Chowla, The Heegner-Stark-Baker-Deuring-Siegel theorem, J.Reine Angew. Math. **241** (1970), 47-48.

[5] H.Cohen and H.W.Lenstra, Jr., Heuristics on class groups of number fields, Lecture Notes in Math. **1068** (1984), 33–62.

[6] M.Deuring, Imaginäre quadratische Zahlkörper mit der Klassenzahl Eins, Invent. Math. **5** (1968), 169–179.

[7] W.Duke and Y.Tschinkel (Ed.), Analytic Number Theory, A Tribute to Gauss and Dirichlet, Clay Math. Proc. **7**, 2007.

[8] D.M.Goldfeld, The class number of quadratic fields and the conjecture of Birch and Swinnerton-Dyer, Ann. Scuola Norm. Sup. Pisa (4) **3** (1976), 623–663.

[9] D.M.Goldfeld, Gauss' class number problem for imaginary quadratic fields, Bull. of the American Math. Soc. (1) **13** (1985), 23–37.

[10] L.J.Goldstein, Imaginary quadratic fields of class number 2, J. of Number Theory **4** (1972), 286–301.

[11] B.Gross and D.Zagier, Points de Heeger et derivées de fonctions L, C. R. Acad. Sci. Paris **297** (1983), 85–87.

[12] H.Heilbronn, On the class number in imaginary quadratic fileds, Quart. J. Math. Oxford Ser. **25** (1934), 150–160.

[13] H.Heilbronn and E.H.Linfoot, On the imaginary quadratic corpora of class number one, Quart. J. Math. Oxford Ser. **25** (1934), 293–301.

[14] J.Oesterlé, Nombres de classes des corps quadratiques imaginaries, Séminaire N. Bourbaki, 1983-1984, Éxp. 631.

[15] C.L.Siegel, Über die Classenzahl quadratischer Zahlkörper, Acta. Arith. **1** (1935), 83–86.

[16] C.L.Siegel, Zum Beweise des Starkschen Staz, Invent. Math. **5** (1968), 180–191.

[17] H.M.Stark, On complex quadratic fields with class number equal to one, Tras. Amer. Math. Soc. **122** (1966), 112–119.

[18] H.M.Stark, On the "gap" in a theorem of Heegner, J. of Number Theory **1** (1969), 16-27.

[19] H.M.Stark, Class-number problems in quadratic fields, Actes, Congrés intern. Math. Tome **1**., 511–518, 1970.

[20] H.M.Stark, A transcendence theorem for class-number problems, Ann. of Math. (2) **94** (1971), 153-173.

[21] H.M.Stark, A transcendence theorem for class-number problems (II), Ann. of Math. (2) **94** (1971), 174-209.

[22] T.Tatuzawa, On a theorem of Siegel, Japan J. Math. **21** (1951),163–178.

[23] A.I.Vinogradov and L.A.Takhtajan, On the Gauss conjecture for real quadratic fields, Sov. Math. Dokl. **22** (1980), 821–824.

[24] 名城紘昭, 素判別式２次体の類数表, 鳥羽商船高等専門学校紀要 **5** (1983), 73–76.