円分 – 昔とこの頃*

アンドレ・ヴェイユ

0. 文字通り,「円分*1」とは「円を分ける」ことである. ギリシャの幾何学者たちは, N が 2^n, $2^n \cdot 3$, $2^n \cdot 5$, $2^n \cdot 15$ の形の場合に, 定規とコンパスを用いて円を N 等分できることを教えてくれた.

Euler によって三角関数と指数関数の関係が発見され, 円の等分の問題は $X^n = 1$ という形の二項方程式を解くことに帰着された. Gauss は 19 歳のときに方程式 $X^{17} = 1$ を平方根の繰り返しによって解き, フィールズ賞を受賞した (より正確には, もしそれが存在したら受賞していた) が, それは円の 17 等分が定規とコンパスでできたということである. この結果は世間を驚かせたが, もちろん Gauss にとっては二項方程式の理論における初めの一歩にすぎなかった.

1. したがって, $\mathbb{Q}$ 上で 1 のべき根によって生成される体やその部分体を「円分的*2」と形容することは正当だし, それらに関わることすべてに「円分」という語を用いてもよいだろう — ところで, Kronecker 以降知られていることだが, これらの体は $\mathbb{Q}$ の Abel 拡大にほかならない. しかし, この語 (ドイツ語で Kreist(h)eilung) は, Jacobi 以降 19 世紀を通じて, ある種の重要な 1 のべき根の和の研究に限って用いられていた. それは「Gauss 和」と (おそらく Hasse 以降) 我々が呼ぶようになったものである — この用語は慣用なので認めることにするが, 歴史的にはあまり正当でない. より正確には, $q = p^n$ 個の元をもつ有限体 $\mathbb{F}_q$ に関する Gauss 和 とは

$$G = G(\chi, \psi) = \sum_{x \in \mathbb{F}_q^\times} \chi(x)\psi(x) \tag{1}$$

のこととする. ここで, χ は乗法群 $\mathbb{F}_q^\times$ の指標, ψ は加法群 $\mathbb{F}_q$ の非自明な指標である. もし ε が $X^p = 1$ の原始的な根ならば, ψ の値は $\{1, \varepsilon, \dots, \varepsilon^{p-1}\}$ である. もし χ の位数が m ならば, m は $q-1$ を割り, $q - 1 = m\nu$ と書け, このとき G は 位数 m であるということにする. $m = 1$ ならば $G = -1$ である. もし r が巡回群 $\mathbb{F}_q^\times$ の生成元ならば, χ は $\zeta = \chi(r)$ を与えることで定義され, ζ は $X^m = 1$ の原始的な根であるが, このとき

$$G = \sum_{i=0}^{q-2} \zeta^i \psi(r^i) = \sum_{i=0}^{m-1} \zeta^i \sum_{j=0}^{\nu-1} \psi(r^{i+mj}) \tag{2}$$

---

* André Weil, *La cyclotomie jadis et naguère*, Séminaire BOURBAKI, 26e année, 1973/74, n°452, Juin 1974. In: Springer Lecture Notes in Math. 431 (1975), 318-338, Œuvres Scientifiques (全集), Vol. III, 311-327. (大坪紀之による私家版日本語訳, 2012)

*1 訳注, 以下同様 : 仏 cyclotomie

*2 仏 cyclotomique

と書ける. まず目に飛び込んでくる $G(\chi,\psi)$ の第一の性質は, これが体 $\mathbb{Q}(\zeta,\varepsilon)$ の代数的整数であり, その $\mathbb{Q}$ 上のすべての共役もまた Gauss 和であることである — $\mathbb{Q}(\zeta,\varepsilon)$ の自己同形が ζ を ζ^t に, ε を ε^u に置き換えるならば, それは $G(\chi,\psi)$ を $G(\chi^t,\psi^u)$ に置き換える. さらに, 明らかな「記号の乱用」により $\psi^u(x)=\psi(ux)$ であり, 従って

$$G(\chi,\psi^u)=\chi^{-1}(u)G(\chi,\psi), \tag{3}$$

これより直ちに, $G(\chi,\psi)^m$ は $\mathbb{Q}(\zeta)$ に入る.

またここですぐに注意すると, (1) で定義された G に対して

$$\begin{aligned} G\overline{G} &= \sum_{x,y}\chi(xy^{-1})\psi(x-y)=\sum_{z\neq 0}\chi(z)\sum_{y\neq 0}\psi(y(z-1)) \\ &= q-1-\sum_{z\neq 0,1}\chi(z)=\begin{cases} q & (\chi\neq 1\text{ のとき}) \\ 1 & (\chi=1\text{ のとき}) \end{cases} \end{aligned} \tag{4}$$

が成り立つ. もし $\mathbb{F}_q$ が素体 $\mathbb{F}_p=\mathbb{Z}/p\mathbb{Z}$ ならば, $\psi(x)=\varepsilon^x$ と取ることができ, 次を得る:

$$G=\sum_{x=1}^{p-1}\chi(x)\varepsilon^x=\sum_{i=0}^{p-2}\zeta^i\varepsilon^{r^i}=\sum_{i=0}^{m-1}\zeta^i\sum_{j=0}^{\nu-1}\varepsilon^{r^{i+mj}}. \tag{5}$$

2. 歴史的な順序について先に触れたが, もう一度そこに戻ろう. 和 (5) は, Lagrange によって, 方程式の代数的な理論 (「あの手紙以前」の Galois 理論) についての大論文 ([1 a]) において導入された和の, 特別な場合である. とりわけそこで Lagrange が示したのは, 必要ならば 1 の m 乗根を付け加えた後, m 乗根を用いて m 次の巡回拡大 (生成的に言うと「Kummer 拡大」, もちろん誤りだが) がどのように生成されるかである. 彼は和

$$y=x_1+\alpha x_2+\cdots+\alpha^{m-1}x_m, \tag{6}$$

ただし $\alpha^m=1$ であり $x_1,\ldots,x_m$ はある m 次の方程式の根たちである, を導入し, y^m が x_i たちのすべての巡回置換で不変であることを見てとった. 彼はたとえば, そのようにしてべき根による 3 次と 4 次の方程式の古典的な公式が「説明される」ことを示した. 彼は 1808 年の 論文 ([1 b], Note XIII) でも改めてその方法を説明し, (6) の和を「分解式[*3]」と名付けており, その名は 19 世紀を通して使われ続けた.

3. 1801 年に Gauss は, 研究 ([2 a]) の第 VII 章において, $\mathbb{Q}(\varepsilon)$ を $\mathbb{Q}$ の $p-1$ 次巡回拡大とみなし, その「Galois 理論」を完全に説明している. とくに彼が示しているのは, $p-1=m\nu$ に対して, $\mathbb{Q}(\varepsilon)$ は $\mathbb{Q}$ 上 m 次の (唯一の) 部分体 k_m をもち, それが「位数 m の周期」

$$\eta_i=\sum_{j=0}^{\nu-1}\varepsilon^{r^{i+mj}}\quad(0\leq i<m) \tag{7}$$

[*3] 仏 résolvente

のうちの任意の 1 つによって生成され, これらの「周期」は $\mathbb{Q}(\varepsilon)$ の $\mathbb{Q}$ 上の自己同形によって巡回的に置換されるということである.

べき根による解法という問題は Gauss の思考にあまりにも根付いていたため, 完全に脇においておくことができた. 彼は Lagrange の方法を直接的または間接的に知ることになったのかもしれない (それはありそうなことである) し, 彼自身が再発見したのかもしれない (それは可能なことだ) が, それを $\mathbb{Q}$ と $\mathbb{Q}(\varepsilon)$ の中間体に応用した — k_m を上の通りとし, k が k_m の部分体ならば, η_i と補助的な位数 $< p$ の 1 のべき根を用いた Lagrange 分解式を考えることになる. $k = \mathbb{Q}$ のとき, この分解式は和 (5) にほかならない. しかし, Gauss はこれらの重要性を認めていないようだ — 彼はついでに関係式 $G\overline{G} = p$ に言及しているが, それもただ, 根 $(G^m)^{1/m}$ を求めるにはその平方根と, ある円弧の m 等分を求めればよいと言うためだけである. 少し後に Lagrange は 論説 ([1 b], Note XIV) で, Gauss の結果について主に和 (5) に基づいた解説したが, 位数 $< p$ の 1 のべき根を用いることによって生じる曖昧さを十分に考慮していないということで, Gauss による厳しい批判を受けることになった.

4. Gauss が示したように, 周期 η_i から乗法表

$$\eta_i \eta_j = \sum_k N_{ijk} \eta_k, \tag{8}$$

ができる. ここで, N_{ijk} は自然数であり, 合同式 $AX^m + BX^m = C \pmod{p}$ の解の数と縁がある. この事実は重要な数論的な結果をもたらすが, Gauss は早くも 研究 でそのいくつか ($m = 3$ の場合) に気がついている. 後に $m = 4$ について ([2 d]) 同様の結果を展開している. しかし, とりわけ彼が興味を持っていたのは $m = 2$ の場合である — 彼はそれが「周期」ではないく「Gauss 和」を用いることができる唯一の場合だと (間違いなく, 付加的な非有理性を導入する必要がないという理由から) 信じていた. このときは,

$$G = \eta_0 - \eta_1 = 1 + 2\eta_0 = \sum_{x=0}^{p-1} \varepsilon^{x^2}. \tag{9}$$

ここで, (3) より $\overline{G} = \pm G$, よって (4) より $G^2 = \pm p$ であるが, この符号は $p \equiv \pm 1 \pmod{4}$ で決まる. したがって, $\mathbb{Q}(\varepsilon)$ に含まれる 2 次体 k_2 は $\mathbb{Q}(\sqrt{\pm p})$ である.

5. Gauss がすでに 研究 で注意しているように, この結果は和

$$G = \sum_{x=0}^{N-1} \alpha^{x^2},$$

ただし N は任意の奇数で α は 1 の原始 N 乗根である, に一般化され, $G^2 = \pm N$ である. ここから G の符号を, たとえば $\alpha = e^{2\pi i/N}$ として決定するという問題が提起されるが, この形で述べるとこの問題は代数的ではなくなる. 「観察によると」と Gauss が 研究 で (間違いなく意図的な曖昧さをもって) 言うには, いつもそれぞれ $G = +\sqrt{N}, +i\sqrt{N}$ である. 実際, 彼がその証明を得たの

は 1805 年になってからであり, 出版されたのは 1811 年 ([2 b]) であるが, それが彼の (出版されなかった) テータ関数についての研究と地続きであることが, 我々にははっきりと見て取れる. Gauss は $N = pq$, p, q は素数, の場合から, 平方剰余の相互法則の第 4 の証明を導いている. この仕事をきっかけに, またつい最近の時代まで, 重要な一般化がなされたが, それについては全く触れないことにする.

6. 1818 年に Gauss は平方剰余の相互法則の第 6 の証明を出版した ([2 c]) — それもまた位数 2 の Gauss 和に基づいたものであるが, 厳密に代数数論的な観点から考察されている. G が (9) で定義されているとする. q は $\neq p$ なる奇素数とし, $p = 2p' + 1$, $q = 2q' + 1$ とする. Legendre 記号を用いると, 相互法則は

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

と書ける. すでに見たように, $G^2 = (-1)^{p'} \cdot p$, よって

$$G^{q-1} = (-1)^{p'q'} \cdot p^{q'} \equiv (-1)^{p'q'} \left(\frac{p}{q}\right) \mod q.$$

ところが一方で, 二項公式より

$$G^q \equiv \sum_x \varepsilon^{qx^2} = \left(\frac{q}{p}\right) G \mod q$$

であり, G は q と素なので, 相互法則が従う. もっとも, Gauss は環 $\mathbb{Z}[\varepsilon]$ 内での合同を書くことは (あからさまに) 拒み, 代わりに, 環 $\mathbb{Z}[X]$ において $(q, 1 + x + \cdots + X^{p-1})$ を法とした合同で書いている. しかし理解できないのは, Jacobi, Cauchy, Eisenstein らが本質的に上のものと同一の証明を次々に出版した (しかも, この件について誰に優先権があるかという問題を提起し合ったりもした) ことだが, 結局 Eisenstein が, 表現の差を除けばどれも Gauss の第 6 の証明とかわらないということを見てとった.

7. 研究 の第 VII 章に続く仕事の中で Gauss は, 単に $G\overline{G} = q$ の証明を与えるだけでなく, Gauss 和の乗法公式を与えている. (1) より,

$$\begin{aligned} G(\chi, \psi)G(\chi', \psi) &= \sum_{x,y\neq 0} \chi(x)\chi'(y)\psi(x+y) \\ &= \sum_{z\neq 0} \psi(z)\Big[\sum_{\substack{x+y=z \\ x,y\neq 0}} \chi(x)\chi'(y)\Big] + \sum_{x\neq 0} \chi(x)\chi'(-x) \end{aligned}$$

と書ける. $\chi'' = \chi\chi'$ とおくと, 最後の和は $\chi'' \neq 1$ ならば 0 であり, $\chi'' = 1$ ならば $(q-1)\chi(-1)$ である. もう一方は,

$$J = J(\chi, \chi') = \sum_{x\neq 0,1} \chi(x)\chi'(1-x) \tag{10}$$

とおくと, $J\cdot G(\chi'',\psi)$ と書ける. $\chi''=1$ の場合は, $x\mapsto x(1-x)^{-1}$ が $\mathbb{F}_q-\{0,1\}$ から $\mathbb{F}_q-\{0,-1\}$ への全単射であることより, J の値は $\chi\neq 1$ ならば $-\chi(-1)$, $\chi=\chi'=1$ ならば $q-2$ であることが分かるので, もし $\chi\neq 1$ ならば

$$G(\chi,\psi)G(\chi^{-1},\psi)=q\chi(-1) \tag{11}$$

である. $\chi=1$ または $\chi'=1$ の場合は自明である. χ, χ', χ'' が $\neq 1$ の場合は,

$$G(\chi,\psi)G(\chi',\psi)=J(\chi,\chi')\cdot G(\chi'',\psi) \tag{12}$$

を得る. 上と同様に ζ を $Z^m=1$ の原始的な根とし, χ, χ' の位数が m もしくは m の約数とすると, (10) より $J=J(\chi,\chi')$ は $\mathbb{Z}[\zeta]$ に入り, (12) と (4) より, $J\overline{J}=q$ である.

帰納的に, (12) から次の式を得る:

$$\prod_{i=1}^{n}G(\chi_i,\psi)=J\cdot G\left(\prod_{i=1}^{n}\chi_i,\psi\right), \tag{13}$$

ここで, もし χ_i の位数が m を割れば, J はやはり $\mathbb{Q}(\zeta)$ の整数である. $\chi_0=\prod_i\chi_i^{-1}$ とおくと, (12) と (11) より

$$\prod_{i=0}^{n}G(\chi_i,\psi)=q\chi_0(-1)\cdot J \tag{14}$$

を得るが, これは $\chi_0(-1)J$ が, 条件 $\chi_0\chi_1\cdots\chi_n=1$ の下で, $\chi_0,\chi_1,\ldots,\chi_n$ について対称的であることを示している. たとえば, $\mathbb{Q}(\zeta)$ の自己同形 τ を考え, これが ζ を ζ^t に換えるとすれば χ_i は χ_i^t に換わるので, もし $(\chi_0^t,\ldots,\chi_n^t)$ が $(\chi_0,\ldots,\chi_n)$ の置換ならば J は τ で不変になる. このようにして, J が $\mathbb{Q}(\zeta)$ の与えられた部分体に入るようにすることができる.

8. 自然なことだが, Gauss とその直後の後続者たちから Kummer まで, 素体 $\mathbb{F}_p$ に関する Gauss 和とそれに対応する J のみが扱われた. Gauss 自身が整数 J の数論的な重要性を認めていなかったようだ. しかしながら彼も, すでに $m=3$ と $m=4$ の場合に, この整数たちが $\mathbb{Q}(j)$, $\mathbb{Q}(i)$, ただし $j^3=1$, $i^4=1$, における有理素数の分解を与えるという事実を知ったら驚いたことだろう— 彼はこの事実を別の形で知っていた (「周期」を用いて記述していた) . 実際, $p\equiv 1$ mod. 3 (または mod. 4) であり, χ は $\mathbb{F}_q^\times$ の指標で位数が 3 (または位数が 4) であるもの 2 つのうちの 1 つならば, $J(\chi,\chi')$ は $\mathbb{Q}(j)$ における (または $\mathbb{Q}(i)$ における) p の素因子であり, さらに, 重要な合同式をみたす. これは Jacobi が発見したことであるが, 彼はまた大胆にも 1827 年にそれを Gauss に知らせている ([3 a]). そこで Gauss は励ましの態度を (ほんの少しの尊大さとともに) 見せたが, 少し後の楕円関数についての出来事の時のように, 若い象が自分の花壇に踏み込んだと感じたかもしれない.

9. Gauss と異なり, Jacobi は直ちにこの「円分的」な方法がおよぶ範囲の広さを認めた. これによって, 今日我々が整数 J を呼ぶ「Jacobi 和」という名前が正当化される — もっとも, すでに

見たとおり Gauss の秘密の論文たちにすでに姿を現しているし, Cauchy が 1829 年から (Jacobi と独立に) いくつかの予稿の中で, とくに 1940 年に注釈が追加されて出版された 1830 年の数論についての大報告 ([4]) の中で, それを紹介し広く用いているのではいるのだが. Cauchy がとくに驚いたのは, 与えられた $\mathbb{Q}$ の 2 次拡大に含まれるような J が構成できるということ (これは $n°7$ の最後の注意から従う) である. たとえば, $\ell = 2n+3$ を素数, $r_0, \ldots, r_n$ を 2 次剰余 mod. ℓ とする. $p \equiv 1$ mod. ℓ, χ を $\mathbb{F}_p^\times$ の位数 ℓ の指標とし, $0 \le i \le n$ に対して $\chi_i = \chi^{r_i}$ とすると, (14) は体 $k = \mathbb{Q}(\sqrt{-\ell})$ の整数 J を定め, $J\overline{J} = p^{n-1}$ である. 一方, Cauchy は p のべき p^ν で J を割る最大のものを求めており, それより, $4p^{n-1-2\nu}$ が $x^2 + \ell y^2$ の形で書けることがわかる. 現代の言葉では, k において $(J) = p^\nu \mathfrak{p}^{n-1-2\nu}$, ただし $\mathfrak{p}$ は p の 2 つの素因子のうちの 1 つ, と書けるということである. ここに, k のイデアル類群についての, 当時の言葉で言えば判別式 $-\ell$ の 2 次形式の類群についての, 非自明な結果がある. Jacobi は (Cauchy とは独立に) 同じ議論で, この類の数に関する正しい予想を与えてもいるが, それはしばらく後に Dirichlet がかの有名な仕事 (やはり Gauss の「秘密の論文」でかなり予見されている) のなかで確かめることになる.

10. Jacobi がとりわけ「円分的な方法」を応用しようとしたのは当時の数論で最も熱かった問題, つまり, $n > 2$ に対する n べきの相互法則の研究であった. 双平方[*4]剰余の相互法則については Gauss が重要な結果を, すこし大げさな言葉で ("mysterium maxime reconditum[*5]") 発表したところだった. Jacobi がそれらは自分の方法から「とても単純に, とても簡単に」従うと主張するのを見て, 彼は気を悪くしただろうか? いつもの通り彼は決して証明を発表しなかったが, それはまったく別の原理に基づいたものだった. 一方 Jacobi もまたそうで, 彼の証明もケーニヒスベルクでの講義ノート (1836-37) の中に埋もれたままだった — Jacobi によるとそれは, 少し後にまだ学生だった Eisenstein が独立に得たものと同じであった. 3 次剰余については ([5 a]), その本質的な部分を次のように述べることができる.

$\mathbb{Z}[j]$ において, 3 は素因子 $\rho = j-1$ をもつ. 任意の素数 π で 3 と素なものに対し, $q = N(\pi) = 3n+1$ とする. π と素な x に対し, (x/π) は 1 のべき根 $1, j, j^2$ のうちで $\equiv x^n$ mod. π をみたすものを表すが, この「Legendre 記号」を規則 $(x/\alpha\beta) = (x/\alpha)\cdot(x/\beta)$ によって拡張したのが「Jacobi 記号」である. $p = 3\nu + 1$ を有理素数, π を $\mathbb{Z}[j]$ におけるその素因子の 1 つとすると, π にあるただ 1 つの 1 のべき根 (6 乗根) をかけることで, π が「準素[*6]」, つまり $\equiv 1$ mod. 3 であるようにできる. $x \in \mathbb{F}_p^\times$ に対して, $\chi(x) = (x/\pi)$ とおくと, これは $\mathbb{F}_p^\times$ の位数 3 の指標である. $\mathbb{F}_p$ については $\psi(x) = e^{2\pi i x/p}$ ととる. $G = G(\chi, \psi)$, $J = J(\chi, \chi)$ とおく. このとき, $G(\chi^{-1}, \psi) = \overline{G}$, $G^2 = J\overline{G}$, $G^3 = pJ$, $G\overline{G} = J\overline{J} = p$ であり, さらに

$$J = \sum_{x=2}^{p-1} \chi(x)\chi(1-x) \equiv \sum_{x=1}^{p-1} x^\nu (1-x)^\nu \mod \pi \tag{15}$$

[*4] 仏 biquadratique
[*5] 羅 最も隠された神秘
[*6] 仏 primaire

である．しかし, $n \not\equiv 0 \bmod (p-1)$ に対しては $\sum_1^{p-1} x^n \equiv 0 \bmod p$, よって $J \equiv 0 \bmod \pi$ である．$J\overline{J} = p$ なので J/π は 1 の 6 乗根であるが, これは次のように求められる．$\rho = j - 1$ とおいたので $\rho^2 = -3j$, $j^a = (1+\rho)^a \equiv 1 + \rho a \bmod 3$ である．$\chi(x) = j^{i(x)}$ とおくと, $i(xy) \equiv i(x) + i(y) \bmod 3$, よって

$$J \equiv p - 2 + \rho \left[\sum_2^{p-1} i(x) + \sum_2^{p-1} i(1-x) \right] \equiv -1 + 2\rho \sum_1^{p-1} i(x) \equiv -1 \mod 3,$$

したがって, $J = -\pi$ である．

ここで, σ を $\mathbb{Z}[j]$ の素元で $3p$ と素なもの, $s = N(\sigma) = \sigma\overline{\sigma}$ とすると, $s \equiv 1 \bmod 3$, $\chi^s = \chi$, よって

$$G^s \equiv \sum \chi(x)\psi(sx) \equiv \chi(s)^{-1} G \equiv (s/\pi)^{-1} G \mod \sigma$$

である．しかし一方で, $s = 3t + 1$ とすると

$$G^{s-1} = (G^3)^t = (-p\pi)^t \equiv (-\pi^2\overline{\pi}/\sigma) \mod \sigma$$

である．$(-1/\sigma) = (-1/\sigma)^3 = 1$, また, 構造の移送[*7]より $(\overline{\pi}/\sigma) = (\pi/\overline{\sigma})^{-1}$ である．よって, G は σ と素なので, 上の関係式を組み合わせて $(s/\pi) = (\pi/s)$ を得る．これが「Eisenstein の法則」である．いま, 有理素数 p' で $\neq p$, $\equiv 1 \bmod 3$ であるものをとり, π' を準素な p' の素因子とすると, 上の議論で π, s を π, p' で, また π', p で順に置き換えることができ, それらの結果を組み合わせる．するとまず $(\pi/\pi')^2 = (\pi'/\pi)^2$ を得, よって明らかに $(\pi/\pi') = (\pi'/\pi)$ である．

これで, $\mathbb{Z}[j]$ における 3 次の相互法則の本質的な部分がすべて得られた — 補助法則は容易に得られる．ここで, 上の例に対して, J の性質で Jacobi とその時代の数学者たちが非常に重要視したものについても触れよう．$x \in \mathbb{F}_p^\times$ に対して, $\chi(x) = (x/\overline{\pi})^{-1} = (x^{-1}/\overline{\pi}) \equiv x^{p-1-\nu} \bmod \overline{\pi}$ であり, よって (15) より,

$$J \equiv \sum_{x=1}^{p-1} x^{2\nu}(1-x)^{2\nu} \equiv -\binom{2\nu}{\nu} \mod \overline{\pi}\ .$$

この合同式は, $J \equiv 0 \bmod \pi$ と合わせると, $J \bmod p$ を二項係数 $\binom{2\nu}{\nu}$ で完全に決定する．自明な不等式を考えると, その合同式が J, よって π を一意的に決定することも言える．

11. $n°10$ の例はすでに「円分」論, つまり 19 世紀に発展した Gauss 和と Jacobi 和の理論, を性格づける特徴をすべて含んでいる．

まず第一に, これらの和を用いるには, それらが属する円分体におけるそれらの素因子分解を決定しなければいけない．上では位数 3 の和に関する解法を見たが, 位数 4 の場合も同様であるし, Jacobi は位数 5, 8, 12 についても, それらに対応する体は主イデアルしかもたないという (彼

[*7] 仏 transport de structure (決まった日本語訳はないようだ)

がこのとき見つけた) 事実を用いて, 試みている. さらに先に進むには明らかに, (1845 年からの Kummer による) イデアル論という創造が必要であった. 少しのあいだ範囲を狭めることになったが, Kummer は, まず奇素数 ℓ に対する $\mathbb{Q}(\zeta)$, ただし $\zeta^\ell = 1$, のみを扱った (問題の体に付値を具体的に構成することで前進した). 彼の最初の大成功の一つはまさに, G^ℓ の $\mathbb{Z}[\zeta]$, ただし $\zeta^\ell = 1$, における素イデアル分解を, p が素数 $\equiv 1 \bmod. \ell$ で G が $\mathbb{F}_p$ に関する位数 ℓ の Gauss 和の場合に得たことであった. 少し後に彼は (Gauss 和ではなく, 同じことなのだが Jacobi 和について) , 有限体 $\mathbb{F}_q$ で $\mathbb{Z}[\zeta]$ の次数 > 1 の (ℓ と素な) 素イデアル $\mathfrak{p}$ を法とする剰余体として得られるものについても, 同様に扱えるということを発見している ([6] 参照).

12. 素因子への分解は問題の和を単数倍を除いてしか決定しなく, それはすでに位数 3, 4 の場合でも不十分であるが, 位数 ℓ の和の場合にはより強い理由でそうである. なぜなら, このとき (1846 年に出版された) Dirichlet の定理より, $\mathbb{Z}[\zeta]$ における単数は無限にあるからである.

また, 合同式の形でのさらなる精密さを求めよう. $n°11$ のように, これには二つの種類がある:
(a) $\mathbb{F}_p$ (または $q = p^n$ として $\mathbb{F}_q$) に関する和について, p の素因子によって決まる素点[*8]において, その位数のみならず主要部分も与えるようなもの,
(b) より重要だが, これらの和の $\mathbb{Q}_\ell(\zeta)$ における — より一般的には素数でない位数 m の和を考えるとき, $\zeta^m = 1$ として, $\mathbb{Q}(\zeta)$ における m の素因子に対応する素点での — 局所的な振る舞いに関するもの.

これらの問いは Kummer と Eisenstein をして, p 進解析の非常に洗練された技法を発展させたのだが, 不幸なことに, その後それらは深い忘却に追いやられてしまった.

13. とにかく, 改めて強調するが, Eisenstein と Kummer にとって円分とは, 何よりも相互法則の問題に取り組むための手段であり, その枠組みは Hilbert にいたるまで変わらない. m べきの相互法則について Gauss による例が示唆するのは, $\mathbb{Q}(\zeta)$ にとどまり, そこを超えないということである. ここで ζ は, いつもの通り $Z^m = 1$ の原始的な根である. $\mathfrak{p}$ は $\mathbb{Z}[\zeta]$ において m と素でノルムが q であるもの, $\mathfrak{p}$ と素な x に対して, $(x/\mathfrak{p})$ はべき根 ζ^i のうちで $\equiv x^{(q-1)/m} \bmod. \mathfrak{p}$ をみたすものを表す — この「Legendre 記号」を「Jacobi 記号」に, 規則 $(x/\alpha\beta) = (x/\alpha) \cdot (x/\beta)$ によって拡張する. ここで目的になるのは, $(x/y) \cdot (y/x)^{-1}$ のできるだけ明示的な表現を得ること, それから, x が単数のとき, または m を割るときに $(x/\mathfrak{p})$ を与える「補助法則」を得ることである.

ついにここで, Jacobi, Eisenstein, Kummer らが円分に期待したことが, 部分的にしか実現しなかったのである. 円分は「Eisenstein の法則」, つまり $(x/y) \cdot (y/x)^{-1}$ の値を, x (または y) が $\mathbb{Z}$ に入る場合に与える. これはすでに豊かな結果である. ここから, $m = 4$ のときは幸運な偶然によって, 双平方の相互法則の完全な主張を導くことができる. それは記号 (x/y) の「自明な」公理的な性質, つまり, 今日我々が K 理論と呼ぶものを用いてできるのだが, これは間違いなく Jacobi がケーニヒスベルクの講義で行ったことだし, 後に Eisenstein も, K 理論上の着想をもっと一般的な問題に応用している. しかし, 彼の短い人生の最後まで, Eisenstein がますます没頭するよう

[*8] 仏 place

になったのは, むしろ, 数論的な応用をめざした楕円関数の理論の推進だったし, そこから特に, $m = 8$ の場合の相互法則が導かれた. 同じ頃 Kummer は, ℓ が奇素数の場合 (さらに実際は「正則[*9]」な場合) の ℓ べきの相互法則に専心し, 円分を「補助法則」の研究に用いて多くの成果をあげた. しかしながら, 彼が 1853 年頃に大きな嘆きとともに述べざるを得なかったのは, それらの結果と Eisennstein の法則をもって, 円分によってできることはすべて出尽くしたということであった.

14. 1890 年に Stickelberger は, Gauss 和, Jacobi 和の主要部分を与える Jacobi, Kummer, Eisenstein らの結果に再び取り組み, 完成させた. 彼の仕事を p 進の言葉でまとめよう — そうすることで, 本質は変わらないが簡潔になる.

p を素数, $q = p^n$, ω を $W^{q-1} = 1$ の原始的な根とすると, $k = \mathbb{Q}_p(\omega)$ は $\mathbb{Q}_p$ の n 次不分岐拡大である. $\mathbb{F}_q$ を $\mathbb{Z}_p[\omega]/(p)$ と, $\mathbb{F}_p$ を $\mathbb{Z}_p/(p)$ と同一視できる. k の $\mathbb{Q}_p$ 上の自己同形は ω を ω^{p^ν}, ただし $0 \le \nu < n$, に換えるので, t を $k/\mathbb{Q}_p$ における跡[*10]とすると,

$$t(\omega^i) = \omega^i + \omega^{ip} + \cdots + \omega^{ip^{n-1}} \tag{16}$$

であり, $t(\omega^i)$ は $\mathbb{Z}_p$ に入る.

ε を k のある拡大における $X^p = 1$ の原始的な根とし, $a \in \mathbb{Z}_p$ に対して ε^a を明らかな方法 (p 進連続性によってと言ってもよい) で定義する. このとき, $x \in \mathbb{Z}_p[\omega]$ に対して $x \mapsto \varepsilon^{t(x)}$ は, 商を経由して加法群 $\mathbb{F}_q$ の指標 ψ を定める. 一方, k における $X^q = X$ の根の集合は $M = \{0, 1, \omega, \ldots, \omega^{q-2}\}$ であり, これは $\mathbb{F}_q$ の k における乗法的な代表系である. よって, $x \in \mathbb{Z}_p[\omega]$ に対して μ_x を M の元で $\equiv x \bmod p$ をみたすものとすると, $x \mapsto \mu_x$ は商を経由して $\mathbb{F}_q^\times$ の k に値をもつ指標を定め, $\mathbb{F}_q^\times$ の k に値をもつ任意の指標は $x \mapsto \mu_x^{-a}$ の形である. $\mathbb{F}_q$ に関する任意の Gauss 和は, 値が -1 である自明なものを除いて, $k(\varepsilon)$ において次の形で書ける:

$$g_a = \sum_\mu \mu^{-a} \varepsilon^{t(\mu)} \quad (0 < a < q-1), \tag{17}$$

ただし, 和は $\mu \in M^\times = M - \{0\}$ にわたる.

$k(\varepsilon)$ において, $\pi = \varepsilon - 1$ は素元であり, 任意の $z \in \mathbb{Z}_p$ に対して

$$\varepsilon^z = (1+\pi)^z = \sum_0^\infty \pi^i \binom{z}{i}, \tag{18}$$

よって, g_a は収束級数

$$g_a = \sum_{i=0}^\infty A_{a,i} \pi^i, \quad A_{a,i} = \sum_\mu \mu^{-a} \binom{t(\mu)}{i}, \tag{19}$$

で表される. $t(\mu)$ を (16) で表し, 形式的な等式 $(1+T)^{\sum x_\rho} = \prod (1+T)^{x_\rho}$ から得られる

$$\binom{\sum x_\rho}{i} = \sum_{\sum i_\rho = i} \left(\prod_\rho \binom{x_\rho}{i_\rho} \right)$$

[*9] 仏 régulier

[*10] 仏 trace

により, 次を得る:

$$A_{a,i} = \sum_{(i_\rho)} \sum_{\mu} \mu^{-a} \prod_{\rho} \binom{\mu^{p^\rho}}{i_\rho}. \tag{20}$$

ここで, $0 \le \rho < n$, 第 2 の和は $\mu \in M^\times$ をわたり, 第 1 の和は添字の系 $(i_0, \dots, i_{n-1})$ で $\sum i_\rho = i$ をみたすものをわたる. 与えられた a に対して, $A_{a,i} \neq 0$ であるような i の最小の値を決定する. 右辺に現れる二項係数は μ の $\mathbb{Q}$ 係数多項式であり, 一方, $\sum \mu^b$ は b が $q-1$ の倍数かどうかで値 $q-1$ または 0 をとる.

$0 < a < q-1$ なので, $a = \sum a_\rho p^\rho$, ただし $0 \le \rho < n$ に対して $0 \le a_\rho < p$, と書ける. よって,

$$\sum a_\rho = \min \Big(\sum j_\rho \mid \sum j_\rho p^\rho \equiv a \text{ mod. } q-1;\ j_\rho \ge 0\ (0 \le \rho < n) \Big) \tag{21}$$

だが, 最小値は $j_0 = a_0, \dots, j_{n-1} = a_{n-1}$ でのみ実現される. 実際, j_ρ の 1 つ, たとえば j_λ が $> p$ ならば, j_λ を $j_\lambda - p$ で置き換え, $j_{\lambda+1}$ を $j_{\lambda+1} + 1$ で ($\lambda = n-1$ ならば j_0 を $j_0 + 1$ で) 置き換えて, $\sum j_\rho$ を小さくすることができるが, もしすべての j_ρ が $< p$ ならば, $\sum j_\rho p^\rho = a$, よって, すべての ρ で $j_\rho = a_\rho$ である.

ここで $A_{a,i} \neq 0$ と仮定しよう. すると, (20) の右辺は次数 $\equiv 0$ mod. $q-1$ の項を含まなくてはいけなく, これは整数 i_ρ, j_ρ で $\sum i_\rho = i$, $0 \le j_\rho \le i_\rho$, $\sum j_\rho p^\rho \equiv a$ mod. $q-1$ をみたすものがが存在することになり, よって (21) より $i \ge \sum a_\rho$ である. さらに $i = \sum a_\rho$ ならば, これらの条件より, すべての ρ で $i_\rho = j_\rho = a_\rho$ であり,

$$A_{a,i} = (q-1) \prod_{\rho} (a_\rho!)^{-1}. \tag{22}$$

よって, g_a の主要部分は $-\prod_\rho (\pi^{a_\rho}/a_\rho!)$ である. これはこの問題に対する決定的な結果であるが, その本質はすでに Kummer の仕事に現れていたと言うことができる. もちろんこれから Jacobi 和の主要部分がわかるが, それはすでに Jacobi がかなり一般的な場合に計算していた ([3 b]). Stickelberger と Kummer の方法, また間違いなく Jacobi の方法も, いま我々が説明したものと本質的には変わらない. この結果は $\mathbb{F}_q$ に関するすべての Gauss 和 (Jacobi 和) の, すべての p 進的な素点での位数を与え, よって明らかに, これらすべての和の素因子分解を含んでいる.

15. このことはまったく $n°12$ の問題 (b) には触れないが, そのかわり, まず Eisenstein の法則の証明と, 一方で Jacobi 和が Hecke 指標を定義するという性質と, 結びついている. まず第一のものから, もっとも一般的な状況下で始めよう — Eisenstein ([5 b]) を自由に, しかし十分近くをたどる.

ζ を $Z^m = 1$ の原始的な根, $k = \mathbb{Q}(\zeta)$ とする. $\mathfrak{p}$ を k の (m と素な) 素イデアル, そのノルムを $q = p^n$ とする. $\mathbb{F}_q$ を $\mathbb{Z}[\zeta]/\mathfrak{p}$ と同一視すると, $(x/\mathfrak{p})$ は $\mathbb{F}_q^\times$ の位数 m の指標を定める. ε を $X^p = 1$ の原始的な根とし, t を $\mathbb{F}_q/\mathbb{F}_p$ における跡とすると, $x \mapsto \varepsilon^{t(x)}$ は $\mathbb{F}_q$ の加法的な指標 ψ を定める. $\Phi(\mathfrak{p}) = (-1)^m G(\chi, \psi)^m$ とおくと, Φ は ε の選び方によらない. これを, 規則 $\Phi(\mathfrak{a}\mathfrak{b}) = \Phi(\mathfrak{a})\Phi(\mathfrak{b})$ によって, k のイデアルで m と素なもの全体に拡張する. $n°14$ の結果を $G(\chi, \psi)$ に対して, $\mathfrak{p}$ が定

める素点とその共役たちにおいて適用して, 主イデアル $(\Phi(\mathfrak{p}))$, さらに $(\Phi(\mathfrak{a}))$, の素イデアル分解を容易に得る. 形式的なべきの記号で表すと

$$(\Psi(\mathfrak{a})) = \mathfrak{a}^{\Theta}, \tag{23}$$

ここで Θ は $k/\mathbb{Q}$ の Galois 群の群環の元であり, 次のように定義されるものである. 任意の $t \in (\mathbb{Z}/m\mathbb{Z})^{\times}$ に対して, σ_t を k の自己同形で ζ を ζ^t に換えるものとする. このとき,

$$\Theta = \sum_{\substack{0<t<m \\ (t,m)=1}} t \cdot \sigma_{-t}^{-1}. \tag{24}$$

である (m が素数の場合は Kummer による結果である).

特に, (23) を主イデアル $\mathfrak{a} = (\alpha)$ に適用することができ, すると

$$\Phi(\alpha) = \varepsilon(\alpha) \cdot \alpha^{\Theta}, \tag{24}$$

ただし $\varepsilon(\alpha)$ は k の単数, と書くことができる. しかし, 一方で Gauss 和の絶対値は (4) で与えられ, よって直ちに $|\Phi(\mathfrak{a})|^2 = N(\mathfrak{a})^m$ であり, (23) と (24) を考慮すると, 単数 $\varepsilon(\alpha)$ とその k におけるすべての共役の絶対値が 1 であることが従う. よって, Kronecker の定理より, $\varepsilon(\alpha)$ は $\pm\zeta^i$ の形の 1 のべき根である.

ここで, $\mathfrak{p}'$ を m と素な素イデアル, そのノルムを $q' = p'^{n'} = m\nu + 1$ とする. 先と同様の $\mathfrak{p}$, χ, ψ で $\mathfrak{p}$ が $\mathfrak{p}'$ と素なものに対して $G = G(\chi, \psi)$ とおくと,

$$G^{q'} \equiv \sum \chi(x)\psi(q'x) = \chi(q')^{-1}G \equiv \left(\frac{N(\mathfrak{p}')}{\mathfrak{p}}\right)^{-1} G \mod p'.$$

しかしまた ($m = 3$ の場合は $n°10$ を参照),

$$G^{q'-1} = (G^m)^{\nu} \equiv \left(\frac{(-1)^m \Phi(\mathfrak{p})}{\mathfrak{p}'}\right) \equiv \left(\frac{\Phi(\mathfrak{p})}{\mathfrak{p}'}\right) \mod \mathfrak{p}'.$$

よって, $N(\mathfrak{a})$, $N(\mathfrak{b})$ が互いに, また m と素なとき,

$$\left(\frac{N(\mathfrak{b})}{\mathfrak{a}}\right) = \left(\frac{\Phi(\mathfrak{a})}{\mathfrak{b}}\right)^{-1}$$

であることが, $\mathfrak{a} = \mathfrak{p}$, $\mathfrak{b} = \mathfrak{p}'$ の場合から従う. $\mathfrak{a} = (\alpha)$ として (24) を適用すると, 構造の移送により $tu \equiv 1 \bmod m$, つまり $\sigma_u = \sigma_t^{-1}$ のとき

$$\left(\frac{\alpha^{\sigma_u}}{\mathfrak{b}}\right) = \left(\frac{\alpha}{\mathfrak{b}^{\sigma_t}}\right)^{\sigma_u} = \left(\frac{\alpha}{\mathfrak{b}^{\sigma_t}}\right)^{u}$$

であることに注意して, 次を得る:

$$\left(\frac{N(\mathfrak{b})}{\alpha}\right) = \left(\frac{\varepsilon(\alpha)}{\mathfrak{b}}\right)^{-1} \cdot \left(\frac{\alpha}{N(\mathfrak{b})}\right). \tag{25}$$

16. ここから Eisenstein の相互法則を導くために, (Eisenstein が初めからそうしたように) m が奇素数 ℓ である場合に限定する. この場合, $G = G(\chi, \psi)$ をすぐ前と同じものとして,

$$(-G)^\ell \equiv -\sum_{x\neq 0} \chi(x)^\ell \psi(\ell x) \equiv -\sum_{x\neq 0} \psi(\ell x) = 1 \mod \ell\ ,$$

よって, どんな $\mathfrak{a}$ に対しても $\Phi(\mathfrak{a}) \equiv 1 \mod \ell$ であり (これは $n°12$ の問題 (b) に答える), したがって, α が $\alpha^\Theta \equiv \pm 1 \mod (\zeta-1)^2$ をみたせば, $\varepsilon(\alpha) = \pm 1$ である— 実際は, $x \in \mathbb{Z} - \ell\mathbb{Z}$ に対して $\alpha \equiv x \mod (\zeta-1)^2$ であれば十分で, このとき α は「準素」であると Eisenstein は呼んでいる. これらの結果を現代の言葉で見ると, $\mathfrak{a} \mapsto \Phi(\mathfrak{a})$ は $(\zeta-1)^2$ を導手とする「Hecke 指標」(「量指標[*11]」) だということである. もし (25) で α を「準素」なもの, $\mathfrak{b}$ を素イデアル $\mathfrak{p}$ でノルム $q = p^n$ なものとすると, $(p/\alpha)^n = (\alpha/p)^n$ を得る. しかし, n は $\ell - 1$ を割るので ℓ と素である. したがって $(p/\alpha) = (\alpha/p)$ であり, 結局, a が ℓ と素な有理整数で α が $\mathfrak{a}$ と素かつ「準素」ならばいつでも, $(a/\alpha) = (\alpha/a)$. これが Eisenstein の法則である.

17. より最近の発展に関しては非常に手短かに述べる. 参考までに思い出しておくと, Gauss 和は L 関数の関数等式における局所定数因子の中にも現れる — この因子は「根数[*12]」("root-numbers", "Wurzelzahlen") とも呼ばれるが, これは, 悪い命名の才能といったものを持っていた Hilbert が, 彼以前は "Lagrange 分解式" または "Lagrange'sche Wurzelzahl" と呼ばれていたもの, ここで我々が Gauss 和と呼んでいるものを, "Wurzelzahl" と名付けてやろうという気を起こしたからに違いない. Dirichlet L 級数に対して関数等式の局所定数因子が初めて現れたのは, Dirichlet による $L(1)$ の計算においてであるが, この計算は, 実質的に $L(1)$ と $L(0)$ を繋ぐ関数等式を確かめるものであった. 自然なことだが, これは Hecke や Artin の L 関数の関数等式に, より一般的な形で再び現れる. それについて Dwork や Langlands は著しい仕事をし, それは最終的には Deligne によって完成された. Langlands はこれらの因子が表現論において果たす本質的な役割を明らかにした. この一文の著者は, この問題の因子に最もよい命名を提案した人にメダル (フィールズではなくショコラの) を贈呈しよう.

18. 代数的整数でそれとその全ての共役の絶対値が $p^{n/2}$ の形であるものに出会ったとき, 今や我々はそれが標数 p のゼータ関数の根かどうかを問わずにはいられない. 実際 Gauss 和と Jacobi 和がそうであるということを, Hasse と Davenport が 1934 年に発見した ([8], cf. [9 a]) — 彼らの名前を冠する Gauss 和の間の重要な関係式が発見されたのもこのときである. とくに, 位数 m の Jacobi 和は多様体 $\sum a_i X_i^m = 0$ のゼータ関数の根 (または極, 次元による) であるが, 思い返してみれば, その特別な場合は, 別の言葉で表現されてはいるが, Gauss によって知られていたし, かなり一般的な場合が Kummer の仕事に隠れていたのであった. 歴史的好奇心のためについでに言っておくと, 名高い Gauss の 日記[*13]は円分について開いたり閉じたりしている — それは 1796 年 3

[*11] 独 Grössencharakter
[*12] 仏 nombres radiciels
[*13] 独 Tagebuch

月 30 日に円の 17 等分から始まり, 1814 年 7 月 9 日に「双平方剰余の理論」と (よって次数 4 の「周期」と) 関係する $1 = x^2 + y^2 + x^2y^2$ の $\mathbb{F}_p$ における解の数に関するノートで終わっている.

Hasse-Davenport 関係式について述べると, それは $\mathbb{F}_q$ における位数 m の Gauss 和と, $\mathbb{F}_q$ の拡大 $\mathbb{F}_Q$ におけるそれとを関係づけるものである — $Q = q^N$ とし, t, n を $\mathbb{F}_Q/\mathbb{F}_q$ における跡とノルム, $G = G(\chi, \psi)$ を $\mathbb{F}_q$ に関する Gauss 和, G' を $\mathbb{F}_Q$ に関する Gauss 和 $G(\chi \circ n, \psi \circ t)$ とする. このとき, $-G' = (-G)^n$ である. ついでに言うと, このことからもまた, Gauss 和の通常の記号では「悪い符号」を選んでしまったことが分かる. もちろん, この誤りを正すのにまだ遅すぎはしない.

19. 多様体 $\sum a_i X_i^m = 0$ (ついでに言うと, その有限群による商として定義できるすべての多様体) のゼータ関数に関して $n°18$ で引用した結果を, 同じ多様体を代数体上で考えたもののゼータ関数の計算に応用することができる. この関数は Hecke L 関数の積である, つまり, Jacobi 和は円分体の Hecke 指標を定めるということが分かる. すでに $n°16$ で見たように, 重要な特別の場合 (G を位数が奇素数 ℓ の Gauss 和として和 $(-G)^\ell$ に関するもの) は Eisenstein による相互法則の証明の基礎となった. 実際, そこでは「円分的」な $\mathbb{Q}$ 上のすべての Abel 体の Hecke 指標についての非常に一般的な結果が述べられている ([9 b, c] 参照) — この観点から面白いのは当然, 総虚な体である.

このような指標が得られたら, まずそれと対応する Hecke L 関数, とくにその整数 s での値 $L(s)$ を調べることが目標になる. この主題に関しては, Chowla と Selberg による驚くべき結果 ([10] 参照) を引用せねばなるまい — これを適切に解釈すると, $\mathbb{Q}(\sqrt{-n})$ 上のある種の「円分」指標 (n が素数 $\equiv 3$ mod. 4 のときは, Cauchy に従って $n°9$ で定義したもの) が定義する L 関数の $s = 1$ における値が, π と関数 $\Gamma(s)$ の $s = a/n$, $0 < a < n$ における値を用いて初等的に表される. 間違いなく, この道はもっと先まで進むことができるだろう.

参考文献

[1] LAGRANGE — (a) Réflections sur la résolution algébrique des équations, N$^{\text{eau}}$ Mém. de Acad. R. des Sc. et B.-L. de Berlin, 1770-1771 = Oeuvres, vol. III, p. 332;

(b) Traité de la résolutions numériques des équations, 2e éd., Paris 1808, Notes XIII-XIV = Oeuvres, vol. VIII, p. 295-367.

[2] GAUSS — (a) Disquisitiones arithmeticae, 1801 = Werke, vol. I;

(b) Summatio serierum quorundam singularium, 1811 = Werke, vol. II, p. 11;

(c) Theorematis fundamentalis in doctrina de residuis quadraticis demonstrationes et ampliationes novae, 1818 = Werke, vol. II, p. 51;

(d) Theoria residuorum biquadraticorum, Commentation prima, 1828 = Werke, vol. II, p. 65;

(e) Disquisitionum circa aequationes puras ulterior evolutio, Werke, vol. II, p. 243.

[3] JACOBI — (a) Briefe an Gauss, Werke, vol. VII, p. 391-400;

(b) Über die Kreistheilung und ihre Anwendung auf die Zahlentheorie, Berl. Monatsber. 1837, p. 127 = Crelles J. Vol. 30 (1846), p. 166 = Werke, vol. VI, p. 254.

[4] CAUCHY — Mémoire sur la Théorie des Nombres, Mém. Ac. Sc. XVII (1840) = Oeuvres (I), vol. III.

[5] EISENSTEIN — (a) Beweis des Reciprocitätssatzes für die cubischen Reste in der Theorie der aus dritten Wurzeln der Einheit zusammengesetzen complexen Zahlen, Crelles J. 27 (1844), p. 289;

(b) Beweis der allgemeinsten Reciprocitätsgesetze zweischen reellen und complexen Zahlen, Monatsber. d. k. Akad. d. Wiss. zu Berlin, 1850, p. 189.

[6] KUMMER — Über die Ergänzungssätze zu den allgemeinen Reciprocitätsgesetzen, Crelles J. 44 (1851), p. 93.

[7] L. STICKELBERGER — Ueber eine Verallgemeinerung der Kreistheilung, Math. Ann. 37 (1890), p. 321.

[8] H. DAVENPORT - H. HASSE — Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen, Crelles J. 172 (1935), p. 151.

[9] A. WEIL — (a) Numbers of solutions of equations in finite fields, Bull. Am. Math. Soc. 55 (1949), p. 497[*14];

(b) Jacobi sums as "Grössencharaktere", Trans. Am. Math. Soc. 73 (1952), p. 487[*15];

(c) Sommes de Jacobi et caractères de Hecke, Gött. Nachr. (à paraître)[*16]

[10] A. SELBERG and S. CHOWLA — On Epstein's Zeta-Function, Crelles J. 227 (1967), p. 86.

[*14] Œuvres Scientifiques, Vol. I, 399-409.

[*15] Œuvres Scientifiques, Vol. II, 63-71.

[*16] Nachr. Aka. Wiss. Göttingen Math.-Phys. Kl. II (1974), no.1, 1-14. Œuvres Scientifiques, Vol. III, 329-342.