平方数の和で表される素数について

伊藤 哲史*

京都大学大学院理学研究科数学教室

The problem of the representation of an integer n as the sum of a given number k of integral squares is one of the most celebrated in the theory of numbers... Almost every arithmetician of note since Fermat has contributed to the solution of the problem, and it has its puzzles for us still.

G. H. Hardy

1 はじめに

これは「城崎新人セミナー」の原稿なので，まずは，“新人”の皆さんに身近な問題を「解く」ことについて述べたいと思う．試験問題を「解く」ことについての説明は不要であろう．別解があるかもしれないが，試験では，適切な順序で考えれば制限時間内に解けることが保証されている問題しか与えられない．ところが，研究者が問題を「解く」ことの意味は異なる．研究者が挑戦する問題は「解ける」ことが保証されていない．もしかしたら，一生懸命考えている問題は「解けない」かもしれないし，解く意味が無いものかもしれない．そもそも「解く」とはどういうことかすら不明確なこともある．研究者の場合，問題を「解く」行為そのものよりも，その問題の背後にある「理論」や「構造」を理解することが重視される．問題が解ける「仕組み」を深く理解することで，より見通しよく解けることもあるし，思わぬ方向に一般化できることもある．理論が進展して問題に対する理解が深まった結果，「解けない」理由が分かることで「解ける」問題も多い（単なる「否定的解決」とは異なる）．

おなじみの例として，方程式の「解の公式」について思い出そう．2 次方程式は解ける．3 次方程式は難しいが，頑張れば解ける．4 次方程式になるとかなり複雑だが，辛抱強く計算すれば，とにかく解けることは理解できる．しかし，2 次の場合はともかく，3 次・4 次方程式の解の公式そのものが重視されることはほとんどない．そんなことより，ガロア理論により方程式の解の「対称性」（**ガロア群**）を理解することの方が大切である．ガロア理論によって，3 次・4 次方程式の解の公式の「仕組み」を，対称群 $\mathfrak{S}_3$，$\mathfrak{S}_4$ の構造（組成列）を用いて理解することができる．さらに， 5 次以上の方程式が「解けない」ことも理解できる．こうして，

問題　方程式が「解ける」のはいつか？

という問題に対する

答え　方程式が「解ける」のは，ガロア群が「可解群」（“解ける群”）のときであり，そのときに限る．

が得られる．

さて，ここでは，整数論の話題から，もう少し違った例を取り上げてみることにしよう．ここで考察するのは，

問題　素数を平方数の和で表せ．

* tetsushi@math.kyoto-u.ac.jp

という素朴な問題である．ひょっとしたら，方程式の「解の公式」よりも古くから考えられている伝統的な問題かもしれない．

まずは，この問題には「解ける」場合があることを説明する．素数 p がいつ 2 つの平方数の和で書けるか，すなわち，方程式 $p = x^2 + y^2$ $(x, y \in \mathbb{Z})$ がいつ解を持つかを簡単に判定することができる（フェルマーの二平方定式）．また，この場合に，解の個数を具体的に求めることもできる．この問題の背後には**類体論**と呼ばれる理論がある．次に，この問題には「解けない」場合があることを説明する．「解けない」理由を理解することは，「解く」ことよりも難しい．そして，「解けない」場合であっても，この問題が**ガロア表現の保型性**に関する**非可換類体論**により統一的に理解できることを説明する．結論を言うと，この問題の背後には（いくつかの）ガロア表現がある．ここで関係するガロア表現は（いくつかの） 1 次元または 2 次元の既約表現である（これは二面体群の既約表現が 1 次元または 2 次元であるという表現論的事実に対応する）．これらがすべて 1 次元表現であること（すなわち対応するガロア表現の像がアーベル群であること）と，問題が「解ける」ことは同値となる．最後に，最近の佐藤 - テイト予想の進展に関連して，素数を 12 個の平方数の和で表す方法の個数について最近分かってきたことを紹介する．

2 「解ける」場合 — フェルマーの二平方定理

1 と自分自身でしか割り切れない 2 以上の自然数を**素数**という．素数

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, \ldots$$

は一見バラバラに存在するように見えるが（**グロタンディーク素数** 57 はもちろん素数ではない），素数の集合はその定義からは想像もできない精緻な「法則」にしたがうことが明らかになってきた．そのような法則は**相互法則**と呼ばれる．以下に説明する「フェルマーの二平方定理」は相互法則の一例である．

準備として，剰余に関する記号を導入しよう．整数 a, b および自然数 n に対し，$a - b$ が n で割り切れることを $a \equiv b \pmod{n}$ と書き，『a と b は n を法として**合同**である』という．

定理 2.1 (フェルマーの二平方定理)**.** p を奇素数とする．p が $p = x^2 + y^2$（$x, y \in \mathbb{Z}$）のように 2 つの平方数の和で書けるための必要十分条件は，$p \equiv 1 \pmod{4}$ である．

フェルマー自身はこの定理の証明を書き残していない．定理 2.1 を最初に証明したのはオイラーであると言われている（ゴールドバッハへの手紙（1749 年 4 月 12 日））．定理 2.1 の非自明なところは，奇素数 p に対し，

1. $p = x^2 + y^2$ $(\exists x, y \in \mathbb{Z})$
2. $p \equiv 1 \pmod{4}$

という全く異なる 2 つの条件の同値性を主張するところにある．(1) ⇒ (2) はやさしい（補題 2.2）が，(2) ⇒ (1) はそれほどやさしくはない．今日では，定理 2.1 には様々な証明が知られているが，いずれの証明も一工夫必要である．素数 p を統一的に表すうまい式があって，その式を少し変形すれば $x^2 + y^2$ が出てくるというわけにはいかない．

例を挙げよう．100 以下の素数のうち 4 で割って 1 余るものを調べてみると，

$$5 = 1^2 + 2^2,\ 13 = 2^2 + 3^2,\ 17 = 1^2 + 4^2,\ 29 = 2^2 + 5^2,\ 37 = 1^2 + 6^2,\ 41 = 4^2 + 5^2,$$
$$53 = 2^2 + 7^2,\ 61 = 5^2 + 6^2,\ 73 = 3^2 + 8^2,\ 89 = 5^2 + 8^2,\ 97 = 4^2 + 9^2$$

となって定理 2.1 は確かに成り立っている．しかし，$p = x^2 + y^2$ と書いたときの x, y を求める簡単な規則は見つかりそうもない．一方で，p が 4 で割って 3 余る素数のときは，$p = 3,\ 7,\ 11,\ 19,\ 23, \ldots$ と考えてみると，確かに $p = x^2 + y^2$ とは書けそうもない．実際そのように書けないことは，次の補題から分かる．

補題 2.2. x, y を整数とすると，$x^2 + y^2 \not\equiv 3 \pmod 4$ が成り立つ．

証明. $x \equiv 0 \pmod 4$ なら，$x^2 \equiv 0 \pmod 4$ である．$x \equiv 1 \pmod 4$ なら，$x^2 \equiv 1^2 \equiv 1 \pmod 4$ である．$x \equiv 2 \pmod 4$ なら，$x^2 \equiv 2^2 \equiv 4 \equiv 0 \pmod 4$ である．$x \equiv 3 \pmod 4$ なら，$x^2 \equiv 3^2 \equiv 9 \equiv 1 \pmod 4$ である．よって，$x^2 \equiv 0$ または 1．同様に，$y^2 \equiv 0$ または 1．したがって，$x^2 + y^2 \equiv 0$ または 1 または 2 であるから，$x^2 + y^2 \not\equiv 3 \pmod 4$. □

この「城崎新人セミナー」は 2010 年 2 月 15 日から始まったので，試しに 20100215 を素因数分解してみよう．

$$20100215 = 5 \times 1171 \times 3433$$

5, 1171, 3433 は素数である．1171 は 4 で割って 3 余る素数だから，補題 2.2 により，$1171 = x^2 + y^2$ とは書けない．3433 は 4 で割って 1 余る素数だから，定理 2.1 によれば $3433 = x^2 + y^2$ と書けるはずである．少し計算すれば $3433 = 27^2 + 52^2$ が確かめられる．

定理 2.1 には様々な証明が知られている．初等的な証明を 3 通り紹介しよう．

ザギエーの「一文証明」

以下は [Za] からの引用である（記号を少し変えた以外は原文のまま）．

> 有限集合 $S = \{(x, y, z) \in \mathbb{Z}^3 \mid x, y, z > 0,\ x^2 + 4yz = p\}$ 上の対合 f を
>
> $$f\colon (x, y, z) \mapsto \begin{cases} (x + 2z,\ z,\ y - x - z) & x < y - z \\ (2y - x,\ y,\ x - y + z) & y - z < x < 2y \\ (x - 2y,\ x - y + z,\ y) & x > 2y \end{cases}$$
>
> で定めると，これはただ一つの固定点を持つから，$\#S$ は奇数であり，したがって対合 $g\colon (x, y, z) \mapsto (x, z, y)$ もまた一つの固定点を持つ．

確かに一文である．ここで，**対合**とは 2 回合成すると恒等写像になる写像のことで，$\#S$ は集合 S の位数を表す．S は有限集合であること，写像 f が対合になること（つまり，$f(f(x, y, z)) = (x, y, z)$），$f$ がただ一つの固定点を持つこと（つまり，$f(x, y, z) = (x, y, z)$ をみたす $(x, y, z) \in S$ がただ一つ存在すること）は容易に確かめられる．素数 p が $4k + 1$ の形のとき f の固定点は $(1, 1, k)$ である．

「鳩の巣論法」による証明

次の定理を用いる．

定理 2.3 (平方剰余の相互法則の第一補充法則)**.** p を奇素数とする．$r^2 \equiv -1 \pmod p$ をみたす整数 r が存在することと，$p \equiv 1 \pmod 4$ は同値である．

証明. $r^2 \equiv -1 \pmod p$ をみたす整数 r が存在することは，有限体 $\mathbb{F}_p$ の中に 1 の 4 乗根が 4 個含まれていることと同値．$\mathbb{F}_p^\times$ は位数 $p - 1$ の巡回群なので，これは $p - 1$ が 4 で割り切れること，すなわち $p \equiv 1 \pmod 4$ と同値である． □

定理 2.1 を証明しよう．p を $p \equiv 1 \pmod 4$ をみたす素数とする．定理 2.3 より $r^2 \equiv -1 \pmod p$ をみたす $r \in \mathbb{Z}$ が存在する．$0 \le a, b < \sqrt{p}$ をみたす整数の組 (a, b) は全部で $(\lfloor \sqrt{p} \rfloor + 1)^2$ 個ある（$\lfloor \alpha \rfloor$ は α を越えない最大の整数）．$\lfloor \sqrt{p} \rfloor + 1 > \sqrt{p}$ だから，$(\lfloor \sqrt{p} \rfloor + 1)^2 > p$ である．この不等式の両辺は整数なので，$(\lfloor \sqrt{p} \rfloor + 1)^2 \ge p + 1$ である．$0 \le a, b < \sqrt{p}$ をみたす整数の組 (a, b) は $p + 1$ 個以上あり，

$a-rb$ を p で割った余りは p 通りしかないから，$a_1-rb_1\equiv a_2-rb_2 \pmod p$ をみたす $(a_1,b_1)\neq(a_2,b_2)$ $(0\leq a_1,a_2,b_1,b_2<\sqrt{p})$ が存在する（鳩の巣論法）．$x=|a_1-a_2|$，$y=|b_1-b_2|$ とおく．$(x,y)\neq(0,0)$ である．$x^2\equiv(a_1-a_2)^2\equiv r^2(b_1-b_2)^2\equiv -y^2 \pmod p$ だから，$x^2+y^2\equiv 0 \pmod p$．$x,y<\sqrt{p}$ より $0<x^2+y^2<2p$ である．x^2+y^2 は 0 より大きく $2p$ より小さい p の倍数だから，$x^2+y^2=p$ である．

「降下法」による証明

p を $p\equiv 1 \pmod 4$ をみたす素数とする．$p=x^2+y^2$ を直接解く代わりに，様々な m についての方程式 $mp=x^2+y^2$ $(0<m<p)$ を考察する．この方程式は少なくとも一組の解 (x,y,m) を持つ（証明: 定理 2.3 より $a^2+1\equiv 0 \pmod p$ となる a $(1\leq a<p)$ が存在する．必要なら $p-a$ を a に置き換えることで，$1\leq a<\frac{p}{2}$ と仮定してよい．このとき，$a^2+1<\frac{p^2}{4}+1<p^2$ だから，$a^2+1=mp$ $(0<m<p)$ と書ける）．$mp=x^2+y^2$ $(0<m<p)$ が解を持つような m の最小値を m_0 とおく．

$m_0>1$ と仮定する．$m_0p=x^2+y^2$ の解 (x,y) をとる．整数 r,s であって，$x'=x-rm_0$，$y'=y-sm_0$，$|x'|\leq\frac{m_0}{2}$，$|y'|\leq\frac{m_0}{2}$ をみたすものをとる．$(x')^2+(y')^2\equiv x^2+y^2\equiv 0 \pmod{m_0}$ だから，$(x')^2+(y')^2$ は m_0 で割り切れる．$m_1=\frac{(x')^2+(y')^2}{m_0}$ とおく．$(x')^2+(y')^2\leq\frac{m_0^2}{4}+\frac{m_0^2}{4}=\frac{m_0^2}{2}$ より，$m_1\leq\frac{m_0}{2}$．x,y が両方とも m_0 で割り切れることはないので（証明: x,y が両方とも m_0 で割り切れたら，m_0p は m_0^2 で割り切れることになるが，$0<m_0<p$ だからそれはあり得ない），$(x')^2+(y')^2\neq 0$．よって $m_1\neq 0$．ここで，等式

$$(xx'+yy')^2+(xy'-x'y)^2=(x^2+y^2)\big((x')^2+(y')^2\big)=m_0^2m_1p$$

に注目する．$x\equiv x' \pmod{m_0}$，$y\equiv y' \pmod{m_0}$ だから，$xx'+yy'\equiv x^2+y^2\equiv 0 \pmod{m_0}$，$xy'-x'y\equiv xy-xy\equiv 0 \pmod{m_0}$ である．$xx'+yy'=m_0\alpha$，$xy'-x'y=m_0\beta$ とおくと，$\alpha^2+\beta^2=m_1p$ となる．$m_1\leq\frac{m_0}{2}$ なので，これは m_0 の最小性に反する．

したがって，$m_0=1$ が分かり，定理 2.1 は示された．

このように，一つの解から出発してより「小さい」解を作ることで矛盾を導く方法を**降下法**という（**無限降下法**ともいう）．フェルマーが好んで用いた方法であると言われている．

3　2 つの平方数の和と類体論

初等的証明は「鑑賞」には適しているが，技巧的すぎて，定理の背後にある「理論」や「構造」が見えにくいという欠点がある．

そこで，定理 2.1 にもう少し「難しい」証明を与えることにする．ここで紹介する定理 2.1 の証明には代数学の知識が必要である．整数環 $\mathbb{Z}$ に -1 の平方根 $\sqrt{-1}$ を添加して得られる環 $\mathbb{Z}[\sqrt{-1}]$（**ガウス整数環**）を使う．$\mathbb{Z}[\sqrt{-1}]$ はユークリッド整域であり，したがって素元分解整域である．高校数学でおなじみの公式 $A^2-B^2=(A+B)(A-B)$ に $A=x$，$B=y\sqrt{-1}$ を代入すると，$x^2+y^2=(x+y\sqrt{-1})(x-y\sqrt{-1})$ が得られるから，定理 2.1 の主張（のうち非自明な方向）は，4 で割って 1 余る素数 p が

$$p=(x+y\sqrt{-1})(x-y\sqrt{-1})$$

と書けること，すなわち，p が $\mathbb{Z}[\sqrt{-1}]$ において “素数”（素元）でなくなってしまうことである（このとき，素数 p は $\mathbb{Q}(\sqrt{-1})$ で**完全分解する**という）．

このような問題は**類体論**により理解することができる．この問題の初等的・古典的な解説は初等整数論の「定番」であり，多くの優れた教科書があるのでここでは深入りしない（[Ta1], [HW], [Co]）．

以下では，非可換類体論を見越して，ガロア表現を使ったより現代的な説明を試みることにしよう．「p が完全分解する」ことをフロベニウス元の共役類に注目して表現論的にとらえることが鍵となる．

$\mathbb{Q}$ の絶対ガロア群 $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ は副有限群としての自然な位相に関してコンパクト群となる．素数 p ごとに体の埋め込み $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ を固定する．これにより，自然な写像 $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \to \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ が得られ，これは単射であることが示せるから，$\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \subset \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ と思える．一方，自然な全射 $\mathrm{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p) \to \mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ があり，その核 I_p を p における**惰性群**という．$\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p)$ は**幾何的フロベニウス元** $\mathrm{Frob}_p\colon \overline{\mathbb{F}}_p \ni x \mapsto x^{1/p} \in \overline{\mathbb{F}}_p$ で位相的に生成される．Frob_p の逆像を一つ固定し，その $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ における像も同じ記号 Frob_p で表す．こうして，絶対ガロア群 $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ は，各素数 p ごとに**幾何的フロベニウス元**とよばれる特別な元

$$\mathrm{Frob}_p \in \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$$

を持つことが分かる．ここで説明した Frob_p は well-defined ではないが，任意の有限次ガロア拡大 $K/\mathbb{Q}$ に対し，$K/\mathbb{Q}$ で**分岐する**有限個の素数 p を除き（惰性群 I_p の $\mathrm{Gal}(K/\mathbb{Q})$ における像が自明のとき p は $K/\mathbb{Q}$ で**不分岐である**といい，そうでないとき**分岐する**という），$\mathrm{Frob}_p \in \mathrm{Gal}(K/\mathbb{Q})$ の共役類は well-defined である（以下では，ガロア表現に対し，不分岐な p における Frob_p の跡に注目する．跡は共役類にしかよらないから，これから述べることは体の埋め込み $\overline{\mathbb{Q}} \hookrightarrow \overline{\mathbb{Q}}_p$ や Frob_p の逆像の取り方によらない）．

連続準同型

$$\rho\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_n(\mathbb{C})$$

を $\mathbb{Q}$ の n 次元**ガロア表現**という．p における惰性群の像 $\rho(I_p)$ が自明なとき，ρ は p で**不分岐である**といい，そうでないとき**分岐する**という．

2 次拡大 $\mathbb{Q}(\sqrt{-1})/\mathbb{Q}$ は 1 次元ガロア表現

$$\rho_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Gal}(\mathbb{Q}(\sqrt{-1})/\mathbb{Q}) \cong \{\pm 1\} \hookrightarrow \mathbb{C}^\times = \mathrm{GL}_1(\mathbb{C})$$

を定める．$\rho_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}$ が分岐する素数は 2 のみなので，奇素数 p に対して，幾何的フロベニウス元の行き先

$$\rho_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(\mathrm{Frob}_p) \in \mathrm{GL}_1(\mathbb{C})$$

は well-defined である（$\mathrm{GL}_1(\mathbb{C})$ はアーベル群なので，各元の共役類は 1 つの元からなる）．

ここで，

$$p \text{ が } \mathbb{Q}(\sqrt{-1})/\mathbb{Q} \text{ で}\textbf{完全分解}\text{する} \iff \rho_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(\mathrm{Frob}_p) = 1$$

が成り立つ．したがって，問題は

問題　奇素数 p に対し，$\rho_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(\mathrm{Frob}_p) \in \mathrm{GL}_1(\mathbb{C})$ を決定せよ．

に言い換えられる．$\rho_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}$ の像はアーベル群なので，$\rho_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(\mathrm{Frob}_p)$ の共役類を決定せよと言っても同じことである．こうして，$p = x^2 + y^2$ という方程式に関する「整数論の問題」が，ガロア表現において幾何的フロベニウス元の像の共役類を決定するという「表現論の問題」に翻訳される．

$\mathbb{Q}$ の類体論（円分体論）の主定理をガロア表現を用いて述べよう．

定理 3.1 ($\mathbb{Q}$ の**類体論 (円分体論)**)**.**　1. n 次元ガロア表現 $\rho\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_n(\mathbb{C})$ の像がアーベル群なら，**導手**と呼ばれる正整数 N が存在し，N を割り切らない素数 p に対して，ρ は p で不分岐で，$\rho(\mathrm{Frob}_p)$ の共役類は $p \pmod N$ にしかよらない．

2. もし ρ の像がアーベル群でなければ，(1) のような N は存在しない．

3. N が (1) の条件をみたすことと，ρ が $\mathrm{Gal}(\mathbb{Q}(\zeta_N)/\mathbb{Q})$ を経由することは同値（ここで $\zeta_N = \exp(2\pi\sqrt{-1}/N)$ は 1 の原始 N 乗根）．

高木貞治，アルチンによって 1920〜30 年頃に確立された類体論により，定理 3.1 の自然な一般化が任意の代数体で成り立つ．(3) の $\mathbb{Q}(\zeta_N)$ にあたる体を導手 N の**類体**という．ただし，類体を解析関数（$\mathbb{Q}$ の場合は

$\exp(2\pi\sqrt{-1}z)$) の特殊値を用いて具体的に構成する問題は，**類体の構成問題**と呼ばれ，虚二次体などの特別な体以外では現在も未解決である．

ガロア表現 $\rho\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_n(\mathbb{C})$ に対し，$\rho(\mathrm{Frob}_p)$ の共役類のしたがう法則が**相互法則**である．像がアーベル群の場合（特に $n=1$ の場合）の相互法則は類体論であり，$\rho(\mathrm{Frob}_p)$ の共役類は “$p \pmod N$” (N は導手) で決まる．ρ の像が非可換な場合は，$\rho(\mathrm{Frob}_p)$ の共役類はどのような「法則」にしたがうのだろうか？これを研究するのが次節以降で説明する「非可換類体論」である．

さて，類体論を用いた定理 2.1 の「現代的証明」を与えよう．$\mathbb{Q}(\sqrt{-1}) = \mathbb{Q}(\zeta_4)$ だから，定理 3.1 より，$\rho_{\mathbb{Q}(\sqrt{-1})/\mathbb{Q}}(\mathrm{Frob}_p)$ は $p \pmod 4$ にしかよらない．定理 2.1 はこれから直ちにしたがう．

定理 2.1 の類似として，

1. 奇素数 p に対し，$\exists x, y \in \mathbb{Z},\ p = x^2 + 2y^2 \iff p \equiv 1, 3 \pmod 8$
2. 3 以外の素数 p に対し，$\exists x, y \in \mathbb{Z},\ p = x^2 + 3y^2 \iff p \equiv 1 \pmod 3$
3. 奇素数 p に対し，$\exists x, y \in \mathbb{Z},\ p = x^2 + 5y^2 \iff p \equiv 1, 9 \pmod{20}$

などの様々な結果があるが，これらも定理 3.1 を用いることで統一的に理解・証明することができる．(1)〜(3) のいずれの場合も，p の分解を考えるべき拡大体（$\mathbb{Q}$ の 2 次拡大のヒルベルト類体）が $\mathbb{Q}$ のアーベル拡大であることが本質的である．もちろん，二次体の整数環は素元分解環とは限らないので，実際に具体的公式を書き下すとなると，それほど単純ではない（[Ta1], [HW], [Co]）．

4 「解けない」場合 — 類体論の限界

類体論を用いることで，$p = x^2 + y^2$ やいくつかの類似の問題を統一的に理解できる．しかし，類体論の効用はそれだけではない．類体論を用いることで，ある種の問題が「解けない」ことを理解することもできる．

天下り的だが，次の問題を考えてみよう．

> **問題**　どのような素数 p が $p = 6x^2 + xy + y^2$ $(x, y \in \mathbb{Z})$ の形に書けるか？

結論から言うと，

$$\exists x, y \in \mathbb{Z},\ p = 6x^2 + xy + y^2 \iff p \equiv a_1, \ldots, a_r \pmod N$$

という形の判定法は**存在しない**．この意味で，この問題は「解けない」．これは，（証明できるはずなのに）証明できていないということではない．どんな整数 $a_1, \ldots, a_r, N$ をもってきても上の “$\iff$” が決して成り立たないことが証明できる（ガロア理論で『方程式が解けない』ことを学んだことを思い出そう！）．

いくつか例を挙げよう．1000 以下の素数のうち $p = 6x^2 + xy + y^2$ の形に書けるものは，

> 23, 59, 101, 167, 173, 211, 223, 271, 307, 317, 347, 449, 463, 593, 599, 607, 691, 719, 809, 821, 829, 853, 877, 883, 991, 997

の 26 個である．実際，

$$\begin{aligned} 23 &= 6 \times 2^2 + 2 \times (-1) + (-1)^2 \\ 59 &= 6 \times 2^2 + 2 \times (-7) + (-7)^2 = 6 \times 2^2 + 2 \times 5 + 5^2 \\ 101 &= 6 \times 4^2 + 4 \times (-5) + (-5)^2 = 6 \times 4^2 + 4 \times 1 + 1^2 \end{aligned}$$

となることが確かめられる．

この問題が「解けない」ことの理由は，$p = 6x^2 + xy + y^2$ が，（後で説明するように）本質的に非可換ガロア表現の相互法則の問題であることによる．したがって，「可換類体論」の立場では，これは「解けない」．

この問題に対する「非可換類体論」の立場からの「答え」を述べよう.

定理 4.1. 無限積の展開

$$f=\prod_{n=1}^{\infty}(1-q^n)(1-q^{23n})=\sum_{n=1}^{\infty}a_nq^n$$

により a_n を定める．素数 $p\neq 23$ に対し,

$$\exists x,y\in\mathbb{Z},\ p=6n^2+nm+m^2\iff a_p=2$$

が成り立つ.

ここに挙げた f は，重さ 1，レベル 23 の**保型形式**のフーリエ展開である．定理 4.1 は『どのような素数 p が $p=6x^2+xy+y^2$ の形に書けるか』という整数論的問題の答えを，保型形式 f のフーリエ係数が知っていることを主張している（実は，定理 4.1 の証明そのものはそれほど難しくない（非可換類体論を知らなくても証明はできる)．大切なのは，この定理 4.1 が，非可換類体論によって「自然に」理解できることである)．

無限積の展開を具体的に計算して，定理 4.1 を確かめてみよう.

$$f(q)=q\prod_{n=1}^{\infty}(1-q^n)(1-q^{23n})=\sum_{n=1}^{\infty}a_nq^n=q-q^2-q^3+q^6+q^8-q^{13}-q^{16}+\mathbf{q^{23}}-q^{24}+q^{25}+q^{26}+q^{27}-q^{29}-q^{31}+q^{39}-q^{41}-q^{46}-q^{47}+q^{48}+q^{49}-q^{50}-q^{54}+q^{58}+\mathbf{2\,q^{59}}+q^{62}+q^{64}-q^{69}-q^{71}-q^{73}-q^{75}-q^{78}-q^{81}+q^{82}+q^{87}+q^{93}+q^{94}-q^{98}+\mathbf{2\,q^{101}}-q^{104}-2\,q^{118}+q^{121}+q^{123}-q^{127}-q^{128}-q^{131}+q^{138}-q^{139}+q^{141}+q^{142}+q^{146}-q^{147}+q^{150}-q^{151}+q^{162}-q^{163}+\mathbf{2\,q^{167}}+\mathbf{2\,q^{173}}-q^{174}-2\,q^{177}-q^{179}+q^{184}-q^{186}-q^{192}-q^{193}-q^{197}+q^{200}-2\,q^{202}+q^{208}+\mathbf{2\,q^{211}}+q^{213}+q^{216}+q^{219}+\mathbf{2\,q^{223}}-q^{232}-q^{233}-q^{239}-q^{242}-q^{246}-q^{248}+q^{254}-q^{257}+q^{262}-q^{269}+\mathbf{2\,q^{271}}-q^{277}+q^{278}-q^{282}+q^{289}+q^{294}-q^{299}+q^{302}-2\,q^{303}+\mathbf{2\,q^{307}}-q^{311}+q^{312}+\mathbf{2\,q^{317}}-q^{325}+q^{326}-q^{328}-q^{331}-2\,q^{334}-2\,q^{346}+\mathbf{2\,q^{347}}-q^{349}-q^{351}-q^{353}+2\,q^{354}+q^{358}+q^{361}-q^{363}-q^{368}-q^{376}+q^{377}+q^{381}+q^{384}+q^{386}+q^{392}+q^{393}+q^{394}-q^{397}-q^{400}+q^{403}-q^{409}+q^{417}-2\,q^{422}-q^{426}-q^{432}-q^{438}-q^{439}-q^{443}-2\,q^{446}+\mathbf{2\,q^{449}}+q^{453}-q^{461}+\mathbf{2\,q^{463}}+q^{464}+q^{466}+2\,q^{472}+q^{478}-q^{487}+q^{489}-q^{491}+q^{496}-q^{499}-2\,q^{501}-q^{509}+q^{512}+q^{514}-2\,q^{519}+q^{529}+q^{533}+q^{537}+q^{538}-q^{541}-2\,q^{542}-q^{547}-q^{552}+q^{554}-q^{568}+q^{575}-q^{577}-q^{578}+q^{579}-q^{584}-q^{587}+q^{591}+\mathbf{2\,q^{593}}+q^{598}+\mathbf{2\,q^{599}}-q^{600}-q^{601}+2\,q^{606}+2\,q^{607}+q^{611}-2\,q^{614}+q^{621}+q^{622}-q^{624}+q^{625}-2\,q^{633}-2\,q^{634}-q^{637}-q^{647}-q^{648}+q^{650}-q^{653}+q^{656}+q^{662}-q^{667}-2\,q^{669}-q^{673}+q^{675}-q^{683}+\mathbf{2\,q^{691}}-2\,q^{694}+q^{696}+q^{698}+q^{699}+q^{702}+q^{706}-q^{713}+q^{717}+\mathbf{2\,q^{719}}-q^{722}-q^{725}+q^{726}+q^{729}-q^{739}+q^{744}+q^{752}-q^{754}-q^{761}-q^{762}-2\,q^{767}+q^{771}-q^{775}-q^{783}-q^{784}-q^{786}+q^{794}-q^{806}+q^{807}+2\,q^{808}+\mathbf{2\,q^{809}}-q^{811}-2\,q^{813}+q^{818}+\mathbf{2\,q^{821}}-q^{823}+\mathbf{2\,q^{829}}+q^{831}-q^{832}-q^{834}-q^{837}+\mathbf{2\,q^{853}}-q^{857}-q^{859}-q^{863}-q^{867}+\mathbf{2\,q^{877}}+q^{878}+\mathbf{2\,q^{883}}+q^{886}-q^{887}+q^{897}-2\,q^{898}+q^{899}-q^{906}-2\,q^{921}+q^{922}+q^{923}-2\,q^{926}-q^{929}+q^{933}-q^{943}-2\,q^{944}-q^{947}+q^{949}-2\,q^{951}-q^{967}+q^{968}+q^{974}+q^{975}-q^{978}+q^{982}+q^{984}+\mathbf{2\,q^{991}}+q^{993}+\mathbf{2\,q^{997}}+q^{998}+\cdots$$

定理 4.1 を理解するために，$p=6x^2+xy+y^2$ の問題の背後に非可換ガロア拡大における相互法則が隠れていることを見る．まずは，$6x^2+xy+y^2$ を因数分解することからはじめる．$\alpha=x\cdot\frac{1+\sqrt{-23}}{2}+y\ (x,y\in\mathbb{Z})$ とおくと,

$$\alpha\cdot\overline{\alpha}=\left(x\cdot\tfrac{1+\sqrt{-23}}{2}+y\right)\left(x\cdot\tfrac{1-\sqrt{-23}}{2}+y\right)=6x^2+xy+y^2$$

が成り立つ（$\overline{\alpha}$ は α の複素共役)．虚二次体 $K=\mathbb{Q}(\sqrt{-23})$ の整数環は $\mathcal{O}_K=\mathbb{Z}\left[\frac{1+\sqrt{-23}}{2}\right]$ だから，素数 p が $p=6x^2+xy+y^2$ と書けることと，$\mathcal{O}_K$ において $p=\alpha\cdot\overline{\alpha}$ と分解することは同値である.

$K/\mathbb{Q}$ は二次拡大だからアーベル拡大であり，「$\mathbb{Q}$ の類体論」が使える．これより次のことが分かる．二次拡大 $K/\mathbb{Q}$ から定まる 1 次元ガロア表現を

$$\rho_{K/\mathbb{Q}}\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\longrightarrow \mathrm{Gal}(K/\mathbb{Q})\cong\{\pm1\}\hookrightarrow\mathbb{C}^\times=\mathrm{GL}_1(\mathbb{C})$$

とおくと，$p\neq 23$ に対し

$$p\text{ が }K/\mathbb{Q}\text{ で}\textbf{完全分解}\text{する}\iff\rho_{K/\mathbb{Q}}(\mathrm{Frob}_p)=1$$

が成り立つ（23 は $K/\mathbb{Q}$ で分岐する素数なので除外した）．ここで，p が $K/\mathbb{Q}$ で完全分解するとは，イデアル $(p) \subset \mathcal{O}_K$ が $(p) = Q_1 \cdot Q_2$ のように $\mathcal{O}_K$ の素イデアルの積に分解することをいう．$K \subset \mathbb{Q}(\zeta_{23})$ なので，p が $K/\mathbb{Q}$ で完全分解するかどうかは $p \pmod{23}$ で決まる．しかし，p が $K/\mathbb{Q}$ で完全分解して，$(p) = Q_1 \cdot Q_2$ と書けたとしても，$\mathcal{O}_K$ は単項イデアル整域ではないので（K の類数は 3），Q_1, Q_2 は単項イデアルとは限らない．これだけでは最初の問題に答えることはできない．

Q_1, Q_2 がいつ単項イデアルになるかを調べるために，今度は「K の類体論」を使う．H を K の**ヒルベルト類体**とする．H は K のアーベル拡大で，自然な同型

$$\mathrm{Gal}(H/K) \cong \mathrm{Cl}(K)$$

があり，素イデアル $Q \subset \mathcal{O}_K$ が単項イデアルであることと，Q が H で完全分解することが同値である（$\mathrm{Cl}(K)$ は K の**イデアル類群**）．このようなアーベル拡大 H/K の存在は，類体論の帰結である（今の場合，$K = \mathbb{Q}(\sqrt{-23})$ は虚二次体なので，虚数乗法論により H を “具体的に” 構成することができる）．ヒルベルト類体 H を用いることで，$p \neq 23$ に対し，

$$\begin{aligned}
&\exists x, y \in \mathbb{Z},\ p = 6x^2 + xy + y^2 \\
&\qquad \iff (p) = Q_1 \cdot Q_2, \quad Q_1, Q_2 \text{は単項な素イデアル} \\
&\qquad \iff p \text{ は } K/\mathbb{Q} \text{ で完全分解し，} Q_1, Q_2 \text{ は } H/K \text{ で完全分解する} \\
&\qquad \iff p \text{ は } H/\mathbb{Q} \text{ で完全分解する} \\
&\qquad \iff \mathrm{Gal}(H/\mathbb{Q}) \text{ において } \mathrm{Frob}_p = 1
\end{aligned}$$

が分かる．

具体的には，$K = \mathbb{Q}(\sqrt{-23})$ のヒルベルト類体 H は $X^3 - X - 1$ の分解体であるから，そのガロア群 $\mathrm{Gal}(H/\mathbb{Q}) \cong \mathfrak{S}_3$（3 次対称群）は非可換群である．$p \neq 23$ に対して幾何的フロベニウス元（の共役類）

$$\mathrm{Frob}_p \in \mathrm{Gal}(H/\mathbb{Q})$$

が定まる．非可換群の共役類を調べるためには表現論の手法が有用である．$\mathfrak{S}_3$ はただ一つの既約 2 次元表現 τ を持ち，合成

$$\rho_{H/\mathbb{Q}} \colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Gal}(H/\mathbb{Q}) \cong \mathfrak{S}_3 \overset{\tau}{\hookrightarrow} \mathrm{GL}_2(\mathbb{C})$$

は $\mathbb{Q}$ の 2 次元ガロア表現を定める．$\mathfrak{S}_3$ の指標表より，$x \in \mathfrak{S}_3$ に対し，$\mathrm{Tr}(\tau(x)) = 2$ となる x は単位元のみである．以上より，

$$\exists x, y \in \mathbb{Z},\ p = 6x^2 + xy + y^2 \iff \mathrm{Tr}\, \rho_{H/\mathbb{Q}}(\mathrm{Frob}_p) = 2$$

が分かる．結局，問題は 2 次元ガロア表現の次の問題に帰着される．

問題　2 次元ガロア表現 $\rho_{H/\mathbb{Q}}$ に対し，$\mathrm{Tr}\, \rho_{H/\mathbb{Q}}(\mathrm{Frob}_p) = 2$ となる p を決定せよ．

$\rho_{H/\mathbb{Q}}$ の像は非可換だから，この問題の「答え」を “$p \pmod{N}$” で場合分けして書くことは**できない**．

一方で，定理 4.1 の保型形式 f は尖点形式で，ヘッケ作用素の同時固有形式なので，f に伴うガロア表現が存在する．すなわち，既約な 2 次元ガロア表現

$$\rho_f \colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\mathbb{C})$$

であって，$\mathrm{Tr}\, \rho_f(\mathrm{Frob}_p) = a_p$ をみたすものが存在する．**実は，この ρ_f が $\rho_{H/\mathbb{Q}}$ と同値である**というのが，定理 4.1 の「種明かし」である．

以上の議論をまとめておこう．$p = x^2 + y^2$ の場合は，素数 p の分解を考察すべき虚二次体 $\mathbb{Q}(\sqrt{-1})$ の類数は 1 だから，$\mathbb{Q}(\sqrt{-1})$ のヒルベルト類体は $\mathbb{Q}(\sqrt{-1})$ 自身であり，アーベル拡大 $\mathbb{Q}(\sqrt{-1})/\mathbb{Q}$ における素数の分解法

則を考えればよい．したがって $\mathbb{Q}$ の類体論の範囲で（たまたま）「解ける」．$p = x^2 + 2y^2$, $p = x^2 + 3y^2$, $p = x^2 + 5y^2$ 等も，対応するヒルベルト類体が $\mathbb{Q}$ のアーベル拡大であるから，$\mathbb{Q}$ の類体論の範囲で（たまたま）「解ける」．一方で，$p = 6x^2 + xy + y^2$ の場合は，虚二次体 $\mathbb{Q}(\sqrt{-23})$ のヒルベルト類体 H は $\mathbb{Q}$ の非可換拡大だから（$\mathrm{Gal}(H/\mathbb{Q}) \cong \mathfrak{S}_3$），非可換ガロア表現の相互法則 — 非可換類体論 — を持ち出す必要があったわけである．

この議論は容易に一般化できる．一般に，二次体のヒルベルト類体は $\mathbb{Q}$ の非可換拡大であるから，素数 p を二次式で書く問題を考察する際には非可換類体論が必要である．また，二面体群の既約表現は 1 次元または 2 次元だから，ガロア表現としては，1 次元または 2 次元の表現を考察すれば十分であることも分かる（3 次元以上の既約ガロア表現を持ち出す必要はない — これは**佐藤 - テイト予想**との大きな違いである）．素数を二次式で書く問題は，本質的に 2 次元非可換類体論の問題であった．古典的には，可換類体論の範囲に「たまたま」収まる問題しか扱っていなかったに過ぎない．

最後に，保型形式 f の「由来」について述べておこう．実は，$\mathbb{Q}(\sqrt{-23})$ はヒルベルト類体 H が $\mathbb{Q}$ の非可換拡大となる虚二次体のうち，判別式の絶対値が最小のものである．つまり，$p = 6x^2 + xy + y^2$ は，古典的な方法では「解けない」最初の問題である．この f が無限積（エータ積）で書けるのは「偶然である」（と私は思っているのだが，どうだろうか？）．一般の保型形式はこのようには書けない（ボーチャーズ積のように無限積で書ける保型形式もある）．一方で，保型形式 f は，

$$f = \frac{1}{2}\left\{ \sum_{n,m\in\mathbb{Z}} q^{6n^2+nm+m^2} - \sum_{n,m\in\mathbb{Z}} q^{6n^2+5nm+2m^2} \right\}$$

のように，判別式 23 の 2 次元格子に関する**テータ関数**の差でも書けるが，こちらは「偶然ではない」．$\mathfrak{S}_3$ の既約 2 次元表現が指数 2 の正規部分群の 1 次元表現の誘導で得られることに対応して，f は虚二次体 $\mathbb{Q}(\sqrt{-23})$ の不分岐ヘッケ指標（$\mathrm{GL}(1)/\mathbb{Q}(\sqrt{-23})$ の保型表現）からの**保型誘導**で得られる $\mathrm{GL}(2)/\mathbb{Q}$ の保型表現に対応する．この場合の保型誘導は，表現論的には**テータ対応**によって得られるから，f はテータ関数の線形結合で表されるのである（重さ 1 の保型形式とガロア表現の関係については [Se] を参照）．

5 非可換類体論予想

前節までに見たように，様々な整数論の問題をガロア表現の問題に言い換えることができる．一般に，（代数的）ガロア表現と（代数的）保型表現が対応するというのが非可換類体論予想（$\mathrm{GL}(n)$ のラングランズ予想）であり，その最も基本的な場合が，像が $\mathrm{GL}_n(\mathbb{C})$ に含まれるガロア表現（**アルチン表現**）に対する強アルチン予想である．

予想 5.1 (強アルチン予想)**.** K を代数体とする．$\rho\colon \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{GL}_n(\mathbb{C})$ を n 次元既約ガロア表現とする．このとき，$\mathrm{GL}_n(\mathbb{A}_K)$ の尖点的保型表現 π が存在して，

$$L(s + \tfrac{n-1}{2}, \rho) = L(s, \pi)$$

が成り立つ．

ここでは保型表現の定義はしないが，大ざっぱに言うと，保型表現とはヘッケ指標や保型形式を表現論的に定式化したものである．予想 5.1 には，正則でない保型形式に対応する保型表現も含まれる．

予想 5.1 ではかなり狭い範囲の保型表現しかとらえることができない．例えば，正則保型形式に対応する保型表現の場合，アルチン表現に対応するのは「重さ 1」の場合だけである．重さが 2 以上の保型形式に対応する保型表現をとらえるには，ℓ 進表現を考える必要がある．代数体 K に対し，連続準同型

$$\rho\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$$

を K の ℓ **進表現**という．$\mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$ には ℓ 進位相を入れる．体同型 $\iota\colon \overline{\mathbb{Q}}_\ell \cong \mathbb{C}$ を固定すれば，アルチン表現は像が有限な ℓ 進表現と同一視できる．

予想 5.2 (**非可換類体論予想** ($\mathrm{GL}(n)$ の**大域ラングランズ予想**))**.** K を代数体とする．ℓ を素数とし，体同型 $\iota\colon \overline{\mathbb{Q}}_\ell \cong \mathbb{C}$ を固定する．n 次元代数的 ℓ 進表現 $\rho\colon \mathrm{Gal}(\overline{K}/K) \longrightarrow \mathrm{GL}_n(\overline{\mathbb{Q}}_\ell)$ と $\mathrm{GL}_n(\mathbb{A}_K)$ の代数的保型表現 π の間には，一対一の対応であって，

$$L(s+\tfrac{n-1}{2}, \rho) = L(s, \pi)$$

をみたすものがただ一つ存在する．また，既約な ρ には尖点的な π が対応する．

代数的 ℓ **進表現**とは，半単純で，有限個の素点の外で不分岐で，ℓ を割る素点において**ド・ラーム**という p 進ホッジ理論から来る条件をみたす ℓ 進表現のことをいう．アルチン表現は全て代数的である．また，代数多様体やモチーフのエタールコホモロジーから定まる ℓ 進表現は，（その半単純化が）代数的であることも知られている．

一方，**代数的保型表現**は，保型表現 π を $\pi = \otimes'_v \pi_v$ のように素点ごとの既約許容表現の制限テンソル積に分解したときの，無限素点 v における π_v の無限小指標の条件により定義される（π が尖点的でないときは**等圧的** (isobaric) というラングランズ分類から来る条件も課す（[Cl], p.84））．GL(1) の代数的保型表現は代数的ヘッケ指標（A_0 型量指標）に他ならない．正則保型形式に対応する保型表現は代数的である．また，実解析的保型形式（マース波動形式）でラプラス作用素の固有値が $\frac{1}{4}$ となるものも代数的保型表現に対応する．

予想 5.1 や予想 5.2 が証明されている場合はそれほど多くはない．$n = 1$ の場合は本質的に類体論である．$n \geq 2$ の場合は二つの方向— 与えられた保型表現に対応する（伴う）ℓ 進表現を構成する方向（**保型表現に伴うガロア表現の構成**）と，与えられた ℓ 進表現が保型表現に伴うことを示す方向（**ガロア表現の保型性**） — がある．

最近になって，いずれの方向についても，大きな進展があった．保型表現に伴うガロア表現の構成は，志村多様体のエタールコホモロジーをヘッケ作用素で分解することで行われる（保型表現の “合同” を使う方法もある）．エタールコホモロジーをアーサー - セルバーグ安定跡公式で計算する際に，**基本補題**が重要な役割を果たす．ガロア表現の保型性は，2 次元ガロア表現の像が有限可解群の場合（ラングランズ，タンネル）（4 次元で像が可解群の場合の部分的結果もある（ラマクリシュナン）），n 次元ガロア表現の像が有限巾零群の場合（アーサー - クローゼル），**底変換・保型誘導**に対応する場合（アーサー - クローゼル）といった像が「小さい」場合の結果と，テイラー - ワイルズ - キシンの方法によるいわゆる $R^{\mathrm{red}} = T$ 定理の応用として得られる結果がある（こちらは主に像が「大きい」場合の結果である）．$K = \mathbb{Q}$, $n = 2$ で ρ が楕円曲線のテイト加群から定まる ℓ 進表現の場合の保型性予想の解決は，ワイルズによるフェルマーの最終定理の証明の鍵となった（[Sa]）．その後，カーレ，ヴァンテンベルジェ，キシンらにより，$K = \mathbb{Q}$, $n = 2$ で「奇」な場合のアルチン予想やセール予想 ($\mathrm{mod}\ \ell$ ガロア表現の保型性予想）が解決された．$n \geqq 2$ の場合も，特別な ρ に対する「潜保型性」（ある有限次拡大 L/K に対して $\rho|_{\mathrm{Gal}(\overline{K}/L)}$ が保型的であること）が証明されており，佐藤 - テイト予想等への応用がある ([T], [It2], [It4], [It5]).

6 素数を k 個の平方数の和で書く $(k = 2, 4, 6, 8)$

さて，素数を平方数の和で書く問題に戻ろう．

自然数 n を k 個の平方数の和で書く方法の個数を

$$r_k(n) := \#\left\{(x_1, \ldots, x_k) \in \mathbb{Z}^k \;\middle|\; n = x_1^2 + \cdots + x_k^2\right\}$$

とおく．定理 2.1 から，奇素数 p に対して

$$r_2(p) \neq 0 \iff p \equiv 1 \pmod 4$$

が分かる．より一般に次の問題を考えよう

問題　素数 p に対し，$r_k(p)$ を求めよ．

もちろん合成数 n について $r_k(n)$ を求める問題も大切だが，ここでは素数 p に限定して考えることにする．その理由は，$r_k(p)$（p は素数）の値が非可換類体論と直接関係するということと，一般の $r_k(n)$ の値は $r_k(p)$（p は素数）の値から（原理的には）導かれることが知られているからである（L 関数のオイラー積の帰結）．

この問題は非常に古くから研究されている．ヤコビは

“*Fundamenta Nova Theoriae Functionum Ellipticarum*”（1829 年）

において $r_2(n)$，$r_4(n)$，$r_6(n)$，$r_8(n)$ を計算した．鍵となるのが**ヤコビのテータ関数**

$$\vartheta(q) = \sum_{n=-\infty}^{\infty} q^{n^2}$$

と呼ばれる重さ $\frac{1}{2}$ の保型形式である．$\big(\vartheta(q)\big)^k$ を展開すると

$$\big(\vartheta(q)\big)^k = 1 + \sum_{n=1}^{\infty} r_k(n) q^n$$

となるから，$r_k(n)$ を求める問題は重さ $\frac{k}{2}$ の正則保型形式 $\big(\vartheta(q)\big)^k$ のフーリエ係数を計算する問題に帰着される．$r_k(n)$ の具体的な計算は，[Gl], [Na], [We] 等を参照（保型形式を使わない「初等的証明」は [Na] を参照．その証明は長く技巧的だが，このような公式が初等的に証明できることは驚きである）．

まず，$r_2(p)$ の結果を述べる．定理 2.1 から，$p \equiv 1 \pmod 4$ であれば，$p = x^2 + y^2$ $(x, y \in \mathbb{Z},\ x, y \geq 1)$ の形に書くことができ，x, y は順序を除いて一意的である．このような x, y の組が一つ与えられると，8 個の組 $(\pm x, \pm y)$，$(\pm y, \pm x)$ も $p = x^2 + y^2$ をみたすから，$r_2(p) = 8$ が分かる．

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

とおけば，

$$r_2(p) = 4\big(1 + \chi(p)\big) = \begin{cases} 8 & p \equiv 1 \pmod 4 \\ 0 & p \equiv 3 \pmod 4 \end{cases}$$

となる．

r_4，r_6，r_8 は結果だけ述べる．p を奇素数とすると，

$$\begin{aligned} r_4(p) &= 8(1 + p) \\ r_6(p) &= 16\big(\chi(p) + p^2\big) - 4\big(1 + \chi(p) p^2\big) \\ r_8(p) &= 16(1 + p^3) \end{aligned}$$

が成り立つ．こうして，$r_2(p)$，$r_4(p)$，$r_6(p)$，$r_8(p)$ は「計算できる」．$p \pmod 4$ の値で場合分けすれば，p の多項式で書けることも分かる．

7　$r_{10}(p)$ は「計算できない」？！

$k = 2, 4, 6, 8$ の場合と異なり，$p \pmod{??}$ による場合分けをどんなに用いても $r_{10}(p)$ を p の多項式で書く公式は存在しないことが知られている．その意味で $r_{10}(p)$ は「計算できない」．

一方，リュービルは，$r_{10}(p)$ を表す次のような公式を証明した（1866 年）（リュービルの公式の「初等的証明」は [Na] を参照）．

$$r_{10}(p) = \frac{4}{5}\bigl(1+\chi(p)p^4\bigr) + \frac{64}{5}\bigl(\chi(p)+p^4\bigr) + \frac{8}{5}\sum_{p=x^2+y^2}(x+y\sqrt{-1})^4$$

最後の項は $p = x^2+y^2$ をみたす整数の組 (x,y) に渡る和である．(x,y) が条件をみたせば，$(x,-y)$ もみたすから，$\sum_{p=x^2+y^2}(x+y\sqrt{-1})^4$ は整数である．リュービルの公式は，素数 p の $\mathbb{Q}(\sqrt{-1})$ での分解法則を使って $r_{10}(p)$ を「計算する」公式である．

$p=5$ の場合にリュービルの公式を確かめてみよう．5 を 5 個の $(\pm1)^2$ と 5 個の 0^2 の和で書く方法は $2^5\cdot{}_{10}C_5 = 8064$ 通りあり，5 を 1 個の $(\pm2)^2$ と 1 個の $(\pm1)^2$ と 8 個の 0^2 の和で書く方法は $2^2\cdot10\cdot9 = 360$ 通りあるから，$r_{10}(5) = 8424$ である．一方，$\chi(5)=1$，$\mathrm{Re}\,(x+y\sqrt{-1})^4 = x^4+y^4-6x^2y^2$ だから，リュービルの公式の右辺は

$$\begin{aligned}
&\frac{4}{5}\bigl(1+\chi(5)5^4\bigr) + \frac{64}{5}\bigl(\chi(5)+5^4\bigr) + \frac{8}{5}\sum_{5=x^2+y^2}(x+y\sqrt{-1})^4\\
&\quad= \frac{4}{5}\bigl(1+5^4\bigr) + \frac{64}{5}\bigl(1+5^4\bigr) + \frac{32}{5}\sum_{5=x^2+y^2,\,x,y\geqq0}(x^4+y^4-6x^2y^2)\\
&\quad= \frac{42568}{5} + \frac{32}{5}\cdot2\cdot(2^4+1^4-6\cdot2^2\cdot1^2)\\
&\quad= \frac{42568-448}{5} = 8424
\end{aligned}$$

となる．

リュービルにより $r_{10}(p)$ の「公式」は得られた．しかしその公式は $\mathbb{Q}(\sqrt{-1})$ における素数 p の分解法則を含むものである．これで $r_{10}(p)$ は「計算できた」と言えるのだろうか？そもそも $r_{10}(p)$ を「計算する」とはどういうことなのだろうか？

8 非可換類体論の視点から — ガロア表現を使って「数える」

$r_{12}(p)$ の場合，問題はさらに深刻である．$p \pmod{??}$ での場合分けをどんなに用いても，また，p の多項式や $K/\mathbb{Q}$ での分解法則（K は代数体）をどんなに組み合わせても，$r_{12}(p)$ の公式は得られない．$r_{12}(p)$ は $r_{10}(p)$ よりもさらに強い意味で「計算できない」．しかし，$r_{12}(p)$ の定義をどんなに眺めていても，それが「計算できない」理由はなかなか見えてこない．

そこで，非可換類体論の視点から $r_k(p)$ を考察しよう．$k\geq2$ を正の**偶数**とする．$\bigl(\vartheta(q)\bigr)^k$ は重さ $\frac{k}{2}$ の正則保型形式である．正則保型形式の空間はヘッケ作用素の同時固有形式で生成されるから，ヘッケ作用素の同時固有形式 $f_1,\dots,f_r$ と定数 $\alpha_1,\dots,\alpha_r\in\mathbb{C}$ をうまく選べば，

$$\bigl(\vartheta(q)\bigr)^k = \sum_{i=1}^{r}\alpha_i f_i$$

と書ける．f_i に伴う 2 次元 ℓ 進表現を

$$\rho_{f_i}\colon \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{GL}_2(\overline{\mathbb{Q}}_\ell)$$

とおく．モジュラー曲線のエタールコホモロジー（と重さの異なる保型形式の合同）を用いることで，2 次元 ℓ 進表現 ρ_{f_i} が構成されている（アイヒラー，志村，ドリーニュ，セール）．p を奇素数とすると，

$$r_k(p) = \sum_{i=1}^{r}\alpha_i\ \mathrm{Tr}\,\rho_{f_i}(\mathrm{Frob}_p)$$

が成り立つから，$r_k(p)$ を「ガロア表現を使って数える公式」が得られたことになる．こうして，$r_k(p)$ を計算する問題は，

- 係数 α_i を計算する問題（保型形式の空間の基底の計算から分かる）
- 2 次元 ℓ 進表現 ρ_{f_i} に対して $\operatorname{Tr}\rho_{f_i}(\mathrm{Frob}_p)$ を計算する問題

という 2 つの問題に帰着される．

ガロア表現を使って，k が小さい場合の古典的結果を解釈してみよう．

$k=2,4,6,8$ の場合，$\big(\vartheta(q)\big)^k$ は**アイゼンシュタイン級数**と呼ばれる特別な保型形式の線形結合で表される．f がアイゼンシュタイン級数のとき，f に伴う 2 次元 ℓ 進表現 ρ_f は可約で，その（半単純化の）像はアーベル群であるから，類体論が使えて，$\operatorname{Tr}\rho_f(\mathrm{Frob}_p)$ は $p \pmod{??}$ での場合分けや p の多項式を用いて「計算できる」ことが分かる．$\chi(p)=(-1)^{(p-1)/2}$ は二次拡大 $\mathbb{Q}(\sqrt{-1})/\mathbb{Q}$ に対応する 1 次元ガロア表現に対応し，p^n はテイト捻り $\overline{\mathbb{Q}}_\ell(-n)$ に対応する．

$r_{10}(p)$ の場合は少々複雑である．$\big(\vartheta(q)\big)^{10}$ はアイゼンシュタイン級数と $\mathbb{Q}(\sqrt{-1})$ で虚数乗法を持つ尖点形式の線形結合で書ける．リュービルによる $r_{10}(p)$ の公式のうち，

$$\sum_{p=x^2+y^2}(x+y\sqrt{-1})^4$$

の項が，虚数乗法を持つ尖点形式のフーリエ係数の寄与である．虚数乗法を持つ尖点形式 f に伴う ℓ 進表現 ρ_f の像は非可換だから，$\mathbb{Q}$ の類体論では「計算できない」．しかし，ρ_f は指数 2 の部分群 $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\sqrt{-1}))\subset\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ に制限するとアーベルになるので，$\mathbb{Q}(\sqrt{-1})$ における分解法則を組み合わせれば「計算できる」．これが，リュービルの公式の「仕組み」である（ρ_f は $\mathrm{Gal}\big(\overline{\mathbb{Q}}/\mathbb{Q}(\sqrt{-1})\big)$ の 1 次元表現からの誘導表現だから f は保型誘導で得られる．定理 4.1 と比較すると面白いだろう）．

$r_{12}(p)$ はどうだろうか．$\big(\vartheta(q)\big)^{12}$ は，アイゼンシュタイン級数と虚数乗法を持つ尖点形式の線形結合では書けないことが，重さ 6 の保型形式の空間の具体的計算から分かる．虚数乗法を持たない保型形式が必要である．具体的には，$\Gamma_0(4)$ に関する重さ 6 の尖点形式

$$g=q\prod_{n=1}^{\infty}(1-q^{2n})^{12}=\sum_{n=1}^{\infty}b_nq^n$$

のフーリエ係数で b_n を定義すると，

$$r_{12}(p)=8(1+p^5)+32\,b_p$$

が成り立つ．g は虚数乗法を持たない尖点形式なので b_p は「計算できない」が，g に伴う 2 次元 ℓ 進表現 $\rho_g\colon\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})\longrightarrow\mathrm{GL}_2(\overline{\mathbb{Q}}_\ell)$ を使って $r_{12}(p)$ を「計算する」ことはできる．

$$r_{12}(p)=8(1+p^5)+32\ \operatorname{Tr}\rho_g(\mathrm{Frob}_p)$$

最近の正則保型形式に対する**佐藤 - テイト予想**の解決により（[BLGHT]），$\operatorname{Tr}\rho_g(\mathrm{Frob}_p)$ は「計算できない」ものの，その「分布」を正確に求めることができるようになった（ヒルベルト保型形式に対する佐藤 - テイト予想の類似も解決されている（[BGG]））．

定理 8.1 (正則保型形式 g に対する佐藤 - テイト予想)**.** $0\le\alpha<\beta\le\pi$ とおく．N 以下の奇素数 p であって，

$$\cos\beta\le\frac{\operatorname{Tr}\rho_g(\mathrm{Frob}_p)}{2p^{5/2}}\le\cos\alpha$$

をみたすものの個数を $C(N,\alpha,\beta)$ とおくと，

$$\lim_{N\to\infty}\frac{C(N,\alpha,\beta)}{(N\text{ 以下の奇素数 p の個数})}=\frac{2}{\pi}\int_\alpha^\beta\sin^2\theta\,d\theta$$

が成り立つ.

ラマヌジャン - ピーターセン予想（ドリーニュが解決, 1974 年）により，不等式

$$-1 \leq \frac{\operatorname{Tr}\rho_g(\mathrm{Frob}_p)}{2p^{5/2}} \leq 1$$

が奇素数 p で成り立つ．佐藤 - テイト予想は，比 $\dfrac{\operatorname{Tr}\rho_g(\mathrm{Frob}_p)}{2p^{5/2}}$ が区間 $[-1,1]$ の中でどのように分布しているかを表す予想である（1963 年に佐藤幹夫が予想）．この分布のグラフが $\sin^2\theta$ のような「連続的」な形をしていることからも，$p \pmod{??}$ での場合分けや，代数体 $K/\mathbb{Q}$ での分解法則といった「離散的」な条件をいくら組み合わせても，$r_{12}(p)$ の公式は得られないことが分かる．そういう意味で，$r_{12}(p)$ は「計算できない」のである．

補足：k が奇数のときの $r_k(n)$ について

ここでは k が偶数の時に限って説明したが，k が**奇数**のときの $r_k(n)$ も整数論的にはもちろん大切である．k が奇数のときは $\big(\vartheta(q)\big)^k$ は重さ半整数の保型形式になるので，そのフーリエ係数 $r_k(n)$ は k が偶数の時とは異なる原理にしたがうと考えられている．重さ半整数の保型形式の非可換類体論における解釈（二重被覆群 $\widetilde{\mathrm{SL}}_2(\mathbb{A})$ におけるラングランズ関手性）は謎が多く，まだきちんと理解されているとは言い難い．$k=3$ のときの古典的な結果として，n が平方数で割り切れず，$n>4$ なら

$$r_3(n) = \begin{cases} 24h(-n) & n \equiv 3 \pmod 8 \\ 12h(-4n) & n \equiv 1,2,5,6 \pmod 8 \\ 0 & n \equiv 7 \pmod 8 \end{cases}$$

がガウスによって証明されている（$h(-d)$ は判別式 $-d$ の二元二次形式の類数）．このように，重さ半整数の保型形式のフーリエ係数は，**志村対応**（重さ半整数の保型形式と重さ整数の保型形式の対応）を通じて，類数や L 関数の特殊値などの深い整数論的不変量と結びつく．重さ半整数の保型形式については [Ko] を参照．また，[O] には，ラマヌジャンも深く研究した三元二次形式 $x^2+y^2+10z^2$ に関する最新の結果と，楕円曲線に対するバーチ - スイナートン＝ダイヤー予想との関係の解説がある．[OS] では $x^2+y^2+10z^2$ の形で表すことが**できない**奇数が 3, 7, 21, 31, 33, 43, 67, 79, 87, 133, 217, 219, 223, 253, 307, 391, 679, 2719 のみであることが，一般化されたリーマン予想の仮定の下で証明されている．

参考文献

[BLGHT] Barnet-Lamb, T., Geraghty, D., Harris, M., Taylor, R., *A family of Calabi-Yau varieties and potential automorphy II*, preprint, to appear P.R.I.M.S. `http://www.math.harvard.edu/~rtaylor/`

[BGG] Barnet-Lamb, T., Gee, T., Geraghty, D., *The Sato-Tate conjecture for Hilbert modular forms*, preprint (`http://arxiv.org/abs/0912.1054`)

[Cl] Clozel, L., *Motifs et formes automorphes: applications du principe de fonctorialité*, Automorphic forms, Shimura varieties, and L-functions, Vol. I (Ann Arbor, MI, 1988), 77–159.

[Co] Cox, D. A., *Primes of the form x^2+ny^2. Fermat, class field theory and complex multiplication*, A Wiley-Interscience Publication. John Wiley & Sons, Inc., New York, 1989.

[Gl] Glaisher, J. W. L., *On the numbers of representations of a number as a sum of 2r squares, where 2r does not exceed eighteen*, Proc. London Math. Soc. (2) **5** (1907), 479–490.

[HW] Hardy, G. H., Wright, E. M., *An Introduction to the Theory of Numbers*, 5th ed., Oxford University Press, Oxford, 1979（邦訳 : G. H. ハーディ, E. M. ライト,『数論入門 I,II』, シュプリンガー数学クラシックス, シュプリンガーフェアラーク東京, 2001 年）

[Ko] Koblitz, N., *Introduction to elliptic curves and modular forms*, Graduate Texts in Mathematics, 97. Springer-Verlag, New York, 1993. (邦訳 : N. コブリッツ (上田勝, 浜畑芳紀訳),『楕円曲線と保型形式』, シュプリンガー・ジャパン, 2006 年)

[Na] Nathanson, M. B., *Elementary Methods in Number Theory*, Graduate Texts in Mathematics, 195. Springer-Verlag, New York, 2000.

[Neu] Neukirch, J., *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften, 322. Springer-Verlag, Berlin, 1999.（邦訳 : J. ノイキルヒ (足立恒雄 (監修), 梅垣敦紀 (翻訳)),『代数的整数論』, シュプリンガーフェアラーク東京, 2003 年)

[O] Ono, K., *Ramanujan, taxicabs, birthdates, ZIP codes, and twists*, Amer. Math. Monthly 104 (1997), no. 10, 912–917.

[OS] Ono, K., Soundararajan, K., *Ramanujan's ternary quadratic form*. Invent. math. 130 (1997), no. 3, 415–454.

[Sa] 斎藤毅,『フェルマー予想』, 岩波書店, 2009 年.

[Se] Serre, J-P., *Modular forms of weight one and Galois representations*, Algebraic number fields: *L*-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), pp. 193–268. Academic Press, London, 1977.

[We] Weisstein, E. W., *Sum of Squares Function*, From MathWorld–A Wolfram Web Resource. `http://mathworld.wolfram.com/SumofSquaresFunction.html`

[Za] Zagier, D, *A one-sentence proof that every prime p equiv (mod 4) is a sum of two squares*, Amer Math Monthly 97 (1990).

[It2] 伊藤哲史,『[速報] 佐藤 - テイト予想，ついに完全解決か？！』, 数学セミナー 2009 年 9 月号， 34–35, 日本評論社.

[It3] 伊藤哲史,『直角三角形の不思議な世界』, 大学への数学 2011 年 1 月号， 64–67, 東京出版.

[It4] 伊藤哲史,『非可換類体論の現状 — ゼータ関数の解析接続法』, 数理科学 2011 年 1 月号, 特集:数論の探求 ゼータからその世界に迫る, 2011 年 1 月号, 40–45, サイエンス社.

[It5] 伊藤哲史,『特集 この 20 年で数学に何が起こったか — 1995 年 : フェルマー予想解決』, 数学セミナー 2011 年 4 月号（掲載予定）, 日本評論社.

[Ta1] 高木貞治，初等整数論講義 第 2 版, 共立出版, 1971 年.

[T] フォーラム:現代数学のひろがり「佐藤 - テイト予想の解決と展望」,『数学のたのしみ』2008 最終号，日本評論社.