

2017 年度数学特別セミナー

有限体上の方程式を通して見る現代整数論

(Modern number theory from the viewpoint of equations on finite fields)

述: 三枝 洋一^{*} / 記: 穂坂 秀昭[†]

2019 年 7 月

概要

開成学園では毎年、現役の数学者に講演していただく「数学特別セミナー」を開催しています。2017 年度は東京大学大学院数理科学研究科の三枝洋一先生をお招きし、「有限体上の方程式を通して見る現代整数論」というテーマでセミナーをしていただきました。このノートは、その講演の内容をまとめたものです。

なお脚注、参考文献及び演習問題解答はいずれも穂坂が付け足したものです。三枝先生にお話していただいた内容は全て本文中に含めています。

目次

0	今回のセミナーの内容	2
1	準備: 有限体 $\mathbb{F}_p$	2
2	$\mathbb{F}_p$ で方程式を考えよう!	4
2.1	1 次方程式	4
2.2	2 次方程式	4
2.3	3 次方程式における 2 つのタイプ	9
2.4	2 つの方程式のタイプの違い	10
2.5	$x^3 - 2 = 0$ の解の個数を記述する無限積	11
2.6	保型形式	13
3	保型形式の限界, そして...	17
4	練習問題の解答	18
5	参考文献	20

^{*} 東京大学大学院 数理科学研究科 准教授

[†] 開成中学校・高等学校 数学科 教諭

0 今回のセミナーの内容

皆さんが方程式を考えるときには、実数や複素数の範囲で解を探すことがほとんどだと思いますが、今回は、素数 p を固定して、整数を p で割った余りのみに注目する世界（「有限体」という名前が付いています）で方程式を考えてみたいと思います。例えば 2 次方程式 $x^2 = 3$ は、2 乗して p で割ると余りが 3 になるような整数 x を探す問題となりますが、この種の問題についてはガウスによる 200 年以上も前の研究があり、「平方剰余の相互法則」という美しい結果が知られています。その一方で、方程式の形を少し変更すると、問題も一気に難しくなり、現在においても魅力あるテーマとして盛んに研究が行われています。

今回のセミナーでは、平方剰余の相互法則等の古典的な話題から始めて、有限体上の方程式について最近ようやく分かってきたこと、今でも分かっていないことなど、現代整数論の最前線の様子をお伝えすることを目標としたいと思います。できるだけ平易な説明を心がけるつもりですので、予備知識は初等整数論の初歩（素数とは何か、素因数分解など）のみで十分だと思います。複素数範囲での方程式（2 次方程式や 3 次方程式など）を解いた経験があると話が聞きやすいかもしれません。

1 準備: 有限体 $\mathbb{F}_p$

まず、今回のテーマに登場する**有限体**と呼ばれるものが何であるか、説明しましょう。

今回の話を通して、 p は常に素数（たとえば $2, 3, 5, 7, \dots$ ）を表すとしします。素数 p を 1 つ固定し、有限体を定義します。これは、集合としては $\mathbb{F}_p = \{0, 1, 2, \dots, p-1\}$ という数の集まりです*¹。ただし $\mathbb{F}_p$ は単なる集合というだけでなく、その中で $+$, $-$, $\times$ という計算ができます。どうするかというと、整数だと思って計算して、その後 p で割った余りを取れば良いのです。整数として計算すると $0, 1, \dots, p-1$ の範囲に収まらないかもしれませんが、 p で割った余りを取れば、再び $\mathbb{F}_p$ の範囲に入ります。

例 1. $p = 5$ として、 $\mathbb{F}_5$ という数の世界で計算を考えます。 $\mathbb{F}_5 = \{0, 1, 2, 3, 4\}$ 内で $(3+4) \times 3$ を求めてみましょう。普通に整数として計算すると $3+4=7$ ですが、これは $\mathbb{F}_5$ からはみ出してしまうので、5 で割った余りを取ります。そうすると $3+4=2$ となるので、 $(3+4) \times 3 = 2 \times 3 = 6$ となります。するとまた $\mathbb{F}_5$ からはみ出してしまうので、再び余りを取って 1 にします。このようにして

$$(3+4) \times 3 = 7 \times 3 = 2 \times 3 = 6 = 1$$

が得られます。なお、今の計算では途中で 2 回余りを取りましたが、最後にまとめて余りを取って $(3+4) \times 3 = 21 = 1$ としても結果は同じです。一般に、余りを取るの好きなタイミングで構いません（このことは、もちろん証明を要します）。

ところで $2 \times 3 = 1$ という式は、見方を変えたと “ $2 = 1 \div 3$ ” とも見えます。すなわち、割り算ができているのです。

*¹ 有限体を表すときは、普通にアルファベットを使って F_p と書くのではなく、太字の $\mathbb{F}$ を使って $\mathbb{F}_p$ と書くことがしばしばあります。これは有理数、実数、複素数全体の集合をそれぞれ $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ と表すのと同じ慣習です。

一般に $\mathbb{F}_p$ では、0 でない元（要素）による割り算^{*2}もできます。正確に述べると、 $a, b \in \mathbb{F}_p$ かつ $a \neq 0$ ならば、 $ax = b$ となる $x \in \mathbb{F}_p$ が唯一存在します。実は、ここで「 p が素数」という仮定が効いています。その理由を説明しましょう。

証明 a と b を固定して、 a を何倍かしたら b になることをいう。

a の元に $\mathbb{F}_p$ のそれぞれの元をかけて $a \cdot 0, a \cdot 1, \dots, a \cdot (p-1)$ を考える。 $a \cdot 0 = 0$ と $a \cdot 1 = a$ は分かるが、他の元がどうなるかは分からない。ただ、これらは相異なる $\mathbb{F}_p$ の元である。なぜなら同じ数が現れる、すなわち $0 \leq i < j \leq p-1$ に対し $\mathbb{F}_p$ の中で $a \cdot i = a \cdot j$ が成り立ったとすると、整数の中で $a \cdot i$ と $a \cdot j$ を p で割った余りは同じである。すなわち整数として $a \cdot j - a \cdot i = a(j-i)$ は p の倍数である。 p は素数なので、 a か $j-i$ は p の倍数である。（もし p が素数でない、たとえば $p = 4$ の場合、 a と $j-i$ が 2 の倍数であれば、それぞれが 4 の倍数でなくても $a(j-i)$ が 4 の倍数になったりする）。一方 $1 \leq a \leq p-1$ かつ $1 \leq j-i \leq p-1$ なので、 a と $j-i$ のどちらも p の倍数でない。これは矛盾である。

したがって $a \cdot 0, a \cdot 1, \dots, a \cdot (p-1)$ という p 個の数が全て異なることが分かり、 $a \cdot 0, a \cdot 1, \dots, a \cdot (p-1)$ は $0, 1, \dots, p-1$ の並び替えになっている。特に $ax = b$ となる x が唯一存在する。□

■**注意** この証明からは、もう少し詳しい事実を導き出せます。

$a \cdot 0, a \cdot 1, \dots, a \cdot (p-1)$ は $0, 1, \dots, p-1$ の並び替えでしたが、 $a \cdot 0 = 0$ となっています。よって $a \cdot 1, a \cdot 2, \dots, a \cdot (p-1)$ は $1, 2, \dots, p-1$ の並び替えなので、 $\mathbb{F}_p$ で

$$(a \cdot 1) \times (a \cdot 2) \times \cdots \times (a \cdot (p-1)) = 1 \cdot 2 \cdots (p-1) \quad (*)$$

です。この右辺に現れる数はいずれも p の倍数でないから、この値は $\mathbb{F}_p$ において 0 ではありません。

一方、等式 (*) の左辺から a を全てくり出すと $(a \cdot 1) \times (a \cdot 2) \times \cdots \times (a \cdot (p-1)) = a^{p-1} 1 \cdot 2 \cdots (p-1)$ になります。すなわち (* の左辺) = a^{p-1} × (* の右辺) だから、(* の右辺) = a^{p-1} (* の右辺) です。等式 (*) の右辺が 0 でないことに注意すると、両辺割り算して $a^{p-1} = 1$ を得ます。

この結果は **Fermat の小定理**と呼ばれています^{*3}。普通の整数では、何乗かして 1 になる数は ± 1 の 2 つしかありません。しかし $\mathbb{F}_p$ では、0 でないどんな数も $p-1$ 乗したら 1 になるという際立った性質があるのです。

話を元に戻し、割り算の計算例を見てみましょう。

例 2. 先ほどと同じ $\mathbb{F}_5$ 内で $3 \div 4$ をやってみます。整数の世界では $3 \div 4$ はできませんが、 $\mathbb{F}_5$ の世界ではこれができます。これを行うには 3 を、5 で割った余りが同じであるような 4 の倍数に置き換えます。そうすると $3 \div 4 = 8 \div 4 = 2$ となります。また Fermat の小定理を使えば $4^4 = 4^{5-1} = 1$ が分かりますから、 $3 \div 4 = 3 \times 4^4 \div 4 = 3 \times 4^3 = 192 = 2$ として求めることもできます。

このように、証明は別として、 $\mathbb{F}_p$ での計算は決して難しくありません。コンピュータがあれば、計算はなお容易にできるでしょう。

^{*2} ここでいう「割り算」は、整数における「商と余り」による割り算ではなく、割り切るような割り算のことを指します。

^{*3} 後で登場する Fermat 予想・Fermat-Wiles の定理が「大定理」なので、それと比べて「小定理」と呼ばれます。

2 $\mathbb{F}_p$ で方程式を考えよう！

これで今回のテーマを話す舞台が整ったので、紹介しましょう。今回のテーマは「 $\mathbb{F}_p$ で方程式を考えよう！」です。普段の数学の授業で方程式を解くときは、解の範囲は実数だったり複素数だったり整数だったりです。これを $\mathbb{F}_p$ にしたらどうなるか、ということを考えてみたいと思います。

2.1 1 次方程式

方程式には 1 次方程式、2 次方程式、3 次方程式その他諸々色々なものがありますが、一番簡単な 1 次方程式を最初に考えてみましょう。1 次方程式の場合、解き方は普通と全く同じです。

例 3. $p = 7$ の場合. $\mathbb{F}_7$ で $3x + 5 = 0$ とすると, $3x = -5$ です. $\mathbb{F}_7$ の中で $-5 = 2 = 9$ であることを使えば, $3x = 9$ となります. よって $x = 3$ が解です.

このポイントは $\mathbb{F}_p$ で四則演算ができることです。整数の範囲では一般に割り算ができませんが、 $\mathbb{F}_p$ の範囲では割り算ができ、これが解を求めるときに役立っています。ちなみに、このことを指して $\mathbb{F}_p$ は体であるといいます。

2.2 2 次方程式

次に 2 次方程式を考えてみましょう。 $p \neq 2$ としておきます。なぜこの仮定を設けるかは、すぐに分かります。

$ax^2 + bx + c = 0$ ($a \neq 0$) とすると、平方完成により

$$a\left(x + \frac{b}{2a}\right)^2 = \frac{b^2}{4a} - c \quad \therefore \left(x + \frac{b}{2a}\right)^2 = \frac{b^2 - 4ac}{4a^2}$$

となります。この変形自体は、普通に 2 次方程式を解くときと同じです。ただし $p \neq 2$ としたことにより、2 で割り算が出来ることに注意しましょう。もし $p = 2$ だと $\mathbb{F}_2$ で $2 = 0$ となってしまうので、 $\frac{b}{2a}$ という項が 0 での割り算になってしまいます。このように有限体の世界の話では、2 という数が現れるときに注意しなければいけないのです。興味があれば、 $p = 2$ の場合にどうなるかを考えてみると良いでしょう。

さて $p \neq 2$ という条件のもと、2 次方程式では「 $\sqrt{\quad}$ が取れるか」すなわち $x^2 = a$ という形が本質的な問題であることが分かります。いくつかの場合に解いてみましょう。

■方程式 $x^2 = 1$ $x^2 = 1$ とすると $0 = x^2 - 1 = (x - 1)(x + 1)$ より $x = \pm 1$ です。ゆえに、解は常に 2 つあります。(ただし $p = 2$ のときは $1 = -1$ なので、解が 1 つになってしまいます。) このように因数分解して解を見つける方法は、 $\mathbb{F}_p$ の場合でもいつも通り使えます。が、新しさはありません。

■方程式 $x^2 = -1$ (ここで、 -1 は $\mathbb{F}_p$ における $p - 1$ のことです。) この方程式は、実数の範囲では解を持っていませんでしたが、 $\mathbb{F}_p$ だとどうなるのでしょうか？ $p \neq 2$ としたので、その次に簡単な $\mathbb{F}_3$ と $\mathbb{F}_5$ でやってみます。元が有限個しかないので、全部並べて表を書いてみれば解けます。

例 4. $\mathbb{F}_3$ では $0^2 = 0, 1^2 = 1, 2^2 = 4 = -1$ でした. そして $\mathbb{F}_3$ では $-1 = 2$ であり, 表の中に 2 が出てこないから, 方程式 $x^2 = -1$ は解なしです.

x	0	1	2
x^2	0	1	1

一方 $\mathbb{F}_5$ でも表を書いてみると, $0^2 = 0, 1^2 = 1, 2^2 = 4, 3^2 = 9 = 4, 4^2 = 16 = 1$ となります. $\mathbb{F}_5$ で $-1 = 4$ だから, 解は $x = 2, 3$ の 2 つです.

x	0	1	2	3	4
x^2	0	1	4	4	1

ちなみに, この表が $x = 0$ の列を除いて左右対称になるのは, ある意味当たり前です. $1 = -4, 3 = -2$ だから, 1 と 4, 3 と 2 はそれぞれ, 2 乗すると同じになってしまいます.

このように実数の範囲で解けなかった方程式 $x^2 = -1$ は, 素数 p の値によって $\mathbb{F}_p$ での解があったりなかったりします. $p = 3$ では解がなく, $p = 5$ では解があります. これが $p = 7$ だとどうなるでしょうか? あるいは $p = 65537$ ではどうでしょうか*4? さらに最近, 大きい素数が見つかったという話*5 がありますが, その場合どうでしょうか? いくら有限とはいえ, ものすごく大きい p に対して今のような表を作るのは不可能です. しかし実は, 次のような簡単な判定条件があります.

定理 5 (平方剰余の第 1 補充則). $p \neq 2$ のとき, $x^2 = -1$ となる $x \in \mathbb{F}_p$ の個数は, p を 4 で割った余りで判別できる. $p \neq 2$ なので, p を 4 で割った余りは 1 または 3 であり,

- p を 4 で割って 1 余るとき, $x^2 = -1$ の $\mathbb{F}_p$ における解は 2 個である.
- p を 4 で割って 3 余るとき, $x^2 = -1$ の $\mathbb{F}_p$ における解は 0 個である.

さっき考えた例の場合に, 定理はとうなっているでしょうか.

例 6. $p = 3$ と $p = 5$ の場合では, 確かに定理が成り立っています.

- $p = 3$ は 4 で割って 3 余る数であり, $\mathbb{F}_3$ における方程式 $x^2 = -1$ の解は 0 個になっています.
- $p = 5$ は 4 で割って 1 余る数であり, $\mathbb{F}_5$ における方程式 $x^2 = -1$ の解は 2 個になっています.

*4 これは割と有名な素数です. 一般に $2^{2^n} + 1$ の形の自然数は **Fermat 数** と呼ばれ, その中でも特に素数である Fermat 数は **Fermat 素数** と呼ばれています. そして知られている Fermat 素数の中で一番大きいものが 65537 です. ちなみに, 知られている Fermat 素数の残りは 3, 5, 17, 257 の 4 つです.

*5 本セミナーに先立つ 2018/1/3, GIMPS (Great Internet Mersenne Prime Search) プロジェクトが「知られている最大の素数」として $2^{77232917} - 1$ を発表しました. これは 2324 万 9418 桁の数です.
<https://www.mersenne.org/primes/press/M77232917.html>

この定理の証明はすごく色々知られていますが、そのうちの1つを紹介します。 $\mathbb{F}_p$ では p 個しか数がありませんが、今から行う証明では、これより広い数の範囲を考えます。

このような考え方は、実数に対しても行うものです。実数係数の場合、2次方程式が解を持たないことがありました。たとえば $x^2 = -1$ です。こういうとき、数学では、解が存在するように数の範囲を広げてきました。今の例では $x^2 = -1$ が解を持つように複素数を導入することが、この操作に当たります。そして3次方程式や4次方程式が解を持たなければさらに数の範囲を広げることになるのですが、幸運なことに複素数の範囲では全ての n 次方程式が解を持つことが知られており、複素数より数の範囲を広げる必要はありません（ちなみに、この事実を**代数学の基本定理**といいます）。

これと同じことを $\mathbb{F}_p$ で考えます。 $\mathbb{F}_p$ を含み、かつその中で全ての n 次方程式が解を持つような「数」の集合 Ω_p が存在します^{*6}。有限体の世界においても、複素数のような数があるのです。この事実を受け入れるのには少し抵抗があるかもしれませんが、それは複素数の「2乗すると -1 になる数」を受け入れることと同じです。実際の証明は、大学に入ったら学ぶことになるでしょう。

複素数は $a + bi$ のように表せましたが、 Ω_p の数はどう表せるかよく分かりません。しかし、この問題には立ち入らないことにします。数学では、正体はよく分からなくても「存在する」という事実だけから色々なことが示せることがあります。今回もそのような議論になります。 Ω_p の存在を認めて先に進みましょう。

ただ、 Ω_p の性質はいくつか知っておく必要があります。

- Ω_p では四則演算ができます。さっきの言葉を使うと「 Ω_p は体である」ということです。これは議論を進めるための最低条件ですが、もし商が取れなくても、その数の世界で分数を考えれば^{*7}済む話です。
- $x, y \in \Omega_p$ に対し $(x + y)^p = x^p + y^p$ が成り立ちます。普通の計算で $(x + y)^2 = x^2 + y^2$ としたら当然間違いですが、 Ω_p では p 乗のときだけ、このような計算が許されます。この原理はそんなに難しくありません。たとえば $p = 3$ のとき、 Ω_3 は $\mathbb{F}_3$ を広げた世界なので、 $3 = 0$ です。これより $(x + y)^3 = x^3 + 3x^2y + 3xy^2 + y^3 = x^3 + y^3$ となります^{*8}。一般の p でも同じことです。二項定理を使えば、 $(x + y)^p$ の $x^{p-k}y^k$ ($0 \leq k \leq p$) の係数に ${}_pC_k$ が現れます。 $k \neq 0, p$ である限り、この ${}_pC_k$ が p の倍数になり、 $\mathbb{F}_p$ では消えます。
- 最後に、拡大された Ω_p と元の $\mathbb{F}_p$ との関係を捉えるための性質を述べます。 $x \in \Omega_p$ に対して、 $x \in \mathbb{F}_p$ と $x^p = x$ が同値です。これは複素数の場合に「 $z = x + yi$ が実数である $\iff$ 共役複素数 $\bar{z}$ と z が一致する」ということの類似です。複素数の場合には、実数であるかは複素共役を取ると分かりました。 Ω_p では、 $x \in \Omega_p$ が $\mathbb{F}_p$ に属しているかは、 p 乗して元に戻るかを調べればよいのです。

最後の性質も簡単なので証明しておきましょう。もし難しければ、事実を認めて先に行っても構いません。

証明 $x \in \mathbb{F}_p$ とする。 $x = 0$ なら $x^p = 0 = x$ である。また $x \neq 0$ なら、Fermat の小定理より $x^{p-1} = 1$ である。よって $x^p = x \cdot x^{p-1} = x \cdot 1 = x$ である。

逆を示す。 $x^p = x$ は p 次方程式なので、解は p 個以下である。一方いま計算したように、 $\mathbb{F}_p$ の p 個の元は全て $x^p = x$ を満たす。よって p 次方程式 $x^p = x$ の解は $\mathbb{F}_p$ の元たちで尽くされている。□

^{*6} この Ω_p は、 $\mathbb{F}_p$ の**代数閉包**と呼ばれています。より一般に、 $\mathbb{F}_p$ の場合に限らずどんな体であっても「それを含む代数閉包」が存在するという、**Steinitz の定理**が知られています。

^{*7} 整数に対して「分数」を考えると、有理数が作れました。四則演算のうち $+$, $-$, $\times$ の3つができ、かつ0でないもの同士の積が0でないような数の範囲に対しては、それと同じことができます。こうして作られる数の体系は、元の数の**商体**と呼ばれます。

^{*8} x^3 や y^3 の肩に現れる3は「かける個数」を表す**自然数**なので、 $\mathbb{F}_p$ の元ではありません。注意してください。

これらの性質を使って、定理の証明をしましょう。

定理の証明 方程式 $x^2 = -1$ が $\mathbb{F}_p$ 内に解を持つかが問題ではあるが、少なくとも Ω_p 内で見れば、解が存在する。その解 a を 1 つ取ると、 $a^2 = -1$ を満たすから

$$x^2 = -1 \iff x^2 = a^2 \iff (x-a)(x+a) = 0 \iff x = \pm a$$

である。よって $x = \pm a$ が、 Ω_p 内の方程式 $x^2 = -1$ の解である。

こうすれば、残る問題はこれらの解 $x = \pm a$ が $x \in \mathbb{F}_p$ を満たすかどうかになる。そこで $\mathbb{F}_p$ と Ω_p の関係を使い、 $a^p = a$ かどうかを考える。 a という数はよく分からないが、 $a^2 = -1$ は分かっている。そして $p-1$ が偶数であるから、 $\frac{p-1}{2}$ は整数であり

$$a^p = a^{2 \times \frac{p-1}{2} + 1} = (a^2)^{\frac{p-1}{2}} \times a = (-1)^{\frac{p-1}{2}} a$$

となる。よって $\frac{p-1}{2}$ が偶数なら $a^p = a$ で、そうでないなら $a^p = -a$ である。すなわち p を 4 で割った余りが 1 なら $a^p = a$ で、4 で割った余りが 3 なら $a^p = -a$ である。そしていま、 $a \neq -a$ である。実際 $a = -a$ とすると $2a = 0$ となるが、 $p \neq 2$ より $2 \neq 0$ だから $a = 0$ となってしまう。これは $a^2 = -1$ に矛盾する。

以上より $a \in \mathbb{F}_p$ は、 p を 4 で割ったとき 1 余ることと同値である。□

ちょっと不思議な感じがしますが、 Ω_p という数の範囲や a という数のことが良く分からなくても、 a という数の存在だけで証明ができてしまいました。物事を具体的に理解するのは大事なことです、そうでないこともあるものです。

もう少し別の場合でも試してみましょう。

■方程式 $x^2 = 2$ いくつかの p で実験してみても良いのですが、いきなり定理を書いてしまいましょう。

定理 7 (平方剰余の第 2 補充則). $p \neq 2$ のとき、 $x^2 = 2$ となる $x \in \mathbb{F}_p$ は、 p を 8 で割った余りが 1, 7 のとき 2 個、余りが 3, 5 のとき 0 個である。

さっきは 4 で割った余りを考えましたが、今度は 8 で割った余りを考えます。この違いが何故現れるのかを考えながら、証明を追ってみてください。これも、さっきと同様 Ω_p で新しい数を考えることでできます。ちなみに $p = 2$ のときは方程式が $x^2 = 0$ になるので、その解は $x = 0$ の 1 つだけです。

証明 $a^4 = -1$ となる $a \in \Omega_p$ を 1 つ取る。つまり a は、4 次方程式 $x^4 = -1$ の解である。 Ω_p ではどんな方程式も解けるので、このような a が (正体はよく分からないが) 取れる。今度は 2 乗して 2 になる $\sqrt{2}$ のような数を作らなければいけない。そこで複素平面での考察をすると、 $a + a^{-1}$ を使えば良いことが分かる。実際 $a^4 = -1$ だから、

$$(a + a^{-1})^2 = a^2 + 2 + a^{-2} = \frac{a^4 + 1}{a^2} + 2 = 2$$

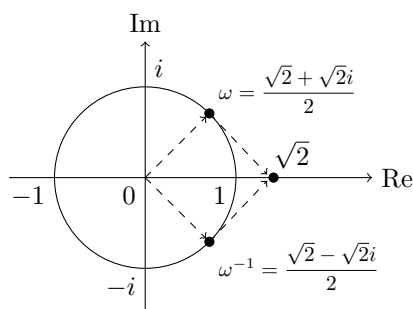
となっている。よって方程式 $x^2 = 2$ は、 Ω_p 内で 2 解 $\pm(a + a^{-1})$ を持つ。

この解 $a + a^{-1}$ が $\mathbb{F}_p$ の元かどうか、つまり $(a + a^{-1})^p = a + a^{-1}$ かどうかを考える。ここで和の p 乗が出てきたので、 $(a + a^{-1})^p = a^p + a^{-p}$ という計算ができる。また $a^4 = -1$ だから $a^8 = 1$ なので、 $(a + a^{-1})^p$ は p を 8 で割った余りで決まっている。そして p を 8 で割った余りに応じて

- 余りが 1 なら、 $a^p = a$ より $a^p + a^{-p} = a + a^{-1}$.
- 余りが 3 なら、 $a^p = a^3 = a^4 a^{-1} = -a^{-1}$ より $a^p + a^{-p} = -a^{-1} - a = -(a + a^{-1})$.
- 余りが 5 なら、 $a^p = a^5 = a^4 a = -a$ より $a^p + a^{-p} = -a - a^{-1} = -(a + a^{-1})$.
- 余りが 7 なら、 $a^p = a^7 = a^8 a^{-1} = a^{-1}$ より $a^p + a^{-p} = a^{-1} + a = a + a^{-1}$.

となる。故に $x^2 = 2$ の解が $\mathbb{F}_p$ 内に存在するのは、 p を 8 で割った余りが 1 または 7 の場合である。□

■注意 これは複素平面で考えると、次のように作り方が分かります。実軸正の向きから単位円周上を正の向きに 45° 移動した点を $\omega = \frac{\sqrt{2} + \sqrt{2}i}{2}$ とします。すると $\omega^{-1} = \frac{\sqrt{2} - \sqrt{2}i}{2}$ で、これを使うと $\omega + \omega^{-1} = \sqrt{2}$ が得られます。



この ω は 2 乗すると $\omega^2 = i$ となるので、 $\omega^4 = -1$ となります。よって ω が、上の証明中における a と同じ役割を果たしているわけです*9。

より一般に、次の結果が知られています。これも、Gauss によって得られた結果です。

定理 8 ([Gauss 1801]). 整数 a に対し整数 $N > 0$ を上手く選ぶと、 $x^2 = a$ となる $x \in \mathbb{F}_p$ の個数は p を N で割った余りで決まる。

かくして 2 次方程式がいつ解けるのかが、綺麗に分かりました。これを決定する具体的なアルゴリズムもあり、それは**平方剰余の相互法則**と呼ばれています。ここでは詳細は述べませんが、非常に面白い定理です。興味がある人は調べてみてください。なお、いま行った議論は、平方剰余の相互法則を示すだけの力があります。平方剰余の相互法則の証明も、同様のアイデアでできます。

自分で練習してみたい人のために、1 つ問題を挙げておきます。 $x^2 = -3$ の $\mathbb{F}_p$ における解は、いつ存在するのでしょうか？（ヒント：何乗かして 1 になる数を用いて、 $\sqrt{-3}$ にあたるものを複素平面で作みましょう。）

*9 $\mathbb{Z}$ に 4 乗して -1 になる数を付け加えた環 $\mathbb{Z}[x]/(x^4 + 1)$ を考えると、 x を -1 の原始 4 乗根に対応させることで、ここから自然に環準同型 $\mathbb{Z}[x]/(x^4 + 1) \rightarrow \mathbb{C}$ と $\mathbb{Z}[x]/(x^4 + 1) \rightarrow \Omega_p$ が作れます。そして $\mathbb{C}$ は標数 0 だから、 $\mathbb{Z}[x]/(x^4 + 1) \rightarrow \mathbb{C}$ は単射です。よって $\sqrt{2}$ を表すような -1 の原始 4 乗根の整数係数多項式を $\mathbb{C}$ の中で作っておけば、 $\mathbb{C} \leftarrow \mathbb{Z}[x]/(x^4 + 1) \rightarrow \Omega_p$ という対応を通して、 $\mathbb{C}$ で作った式が Ω_p で同じ振る舞いを示すわけです。

2.3 3 次方程式における 2 つのタイプ

2 次方程式に関する Gauss の結果は 1800 年頃に得られていました。さらに一歩進んで、3 次方程式を考えてみましょう。ここでは 2 つの例を考えます。1 つは $x^3 - 3x + 1 = 0$ で、もう 1 つは $x^3 - 2 = 0$ です。一見すると適当に選んだようにも感じられますが、なぜ 2 つの例を選んだかは、あとで説明します。実はこれら 2 つの方程式は、かなり性格が異なっているのです。また $\sqrt[3]{2}$ が $x^3 - 2 = 0$ の実数解なのはすぐ分かります。もう一つの方程式 $x^3 - 3x + 1 = 0$ の意味も、後で明らかになります。

では、これらの方程式が $\mathbb{F}_p$ に解を持つかを調べていきましょう。

■ $x^3 - 3x + 1 = 0$ これは 2 次方程式の場合と似ていて、次の定理が成り立ちます。

定理 9. $x^3 - 3x + 1 = 0$ となる $x \in \mathbb{F}_p$ は $p = 2$ のとき 0 個、 $p = 3$ のとき 1 個で、 p を 9 で割った余りが 1, 8 のとき 3 個、2, 4, 5, 7 のとき 0 個である。

このように解の個数が、 $p = 2, p = 3$ のときを例外として、 p を 9 で割った余りで決まります。 p を 9 で割った余りは 0 から 8 までですが、 p が素数ですから、余りとして現れるのは 1, 2, 3, 4, 5, 7, 8 のいずれかです。さらに余りが 3 になるのは $p = 3$ のときに限ります。これで分類が完了していることが分かります。

証明のやり方は 2 次方程式のときとほとんど同じなので、ヒントだけ与えておきます。この方程式がどういう方程式なのか問題で、ぱっと見ただけで解を見抜くのは難しいのですが、実は実数範囲で $x^3 - 3x + 1 = 0$ の解は $x = 2 \cos \frac{2}{9}\pi, 2 \cos \frac{4}{9}\pi, 2 \cos \frac{8}{9}\pi$ です。 x を $2x$ で置き換えた $8x^3 - 6x + 1 = 0$ の方が、ピンとくる人がいるかもしれません。 x に $2 \cos \theta$ を代入して 3 倍角の公式を使うと $\cos 3\theta = -\frac{1}{2}$ になるので、そこから解が得られます。

これで、複素平面上で解を表せるようになります。1 を含むように単位円周を 9 等分する点を取り、1 に隣り合う点を $\zeta := \cos \frac{2}{9}\pi + i \sin \frac{2}{9}\pi$ と置きます。そうすると $\zeta + \zeta^{-1} = 2 \cos \frac{2}{9}\pi$ が解の 1 つになります。これはさっきと似たパターンです。そして ζ は単位円周を 9 等分する点の 1 つだから、 $x^9 - 1 = 0$ 、つまり $(x^3 - 1)(x^6 + x^3 + 1) = 0$ の解です。しかし $\zeta^3 \neq 1$ なので $\zeta^6 + \zeta^3 + 1 = 0$ が得られます。これを参考に $a^6 + a^3 + 1 = 0$ となる $a \in \Omega_p$ を取ると、 $x^3 - 3x + 1 = 0$ の Ω_p での解は $a + a^{-1}, a^2 + a^{-2}, a^4 + a^{-4}$ と分かります。これらが $\mathbb{F}_p$ の元になっているかを、今までと同様に調べれば良いわけです。 p 乗したときの様子が分かりやすい数は、何乗かして 1 になるような数を用いて表せるもので、そうした表示が出来れば 2 次方程式のときと同様の議論ができます。興味のある人は、各自でやってみてください。

■ $x^3 - 2 = 0$ 一方で、こちらの方程式は上手くいきません。実は $x^3 - 2 = 0$ の $\mathbb{F}_p$ 内での解の個数は、 p をある整数 $N > 0$ で割った余りでは決まらないことが知られています。

このように 3 次方程式では、 $\mathbb{F}_p$ における解の個数が p を整数で割った余りで分かるときと分からないときがあります。すると自然に、次の問が出てきます。

- ケース 1 とケース 2 の違いは何故起こるのか？
- ケース 2 の場合に、解の個数を記述する方法はないのか？

これらの問題を、続けて考えてみましょう。ケース 2 はかなり意外な形をしていて、話の流れが変わります。

2.4 2つの方程式のタイプの違い

因数分解できない整数係数の3次方程式 $f(x) = 0$ には2種類あります。先ほどの1番と2番を、それぞれタイプ1、タイプ2と書きましょう。これらは何が違うのでしょうか？

タイプ1 解の1つを α とすると、他の解が α の有理数係数多項式で書けるもの

タイプ2 タイプ1以外

タイプ1の場合、3つの解はある意味で緊密な関係にあります。

先ほどの例で確認してみます。 α を $x^3 - 3x + 1 = 0$ の解とすると、 $\alpha^2 - 2$ も解になっています。何故かという $\alpha = 2 \cos \theta$ ならば、 $\alpha^2 - 2 = 4 \cos^2 \theta - 2 = 2 \cos 2\theta$ になるからです（もちろん、直に代入して計算しても分かります）。このように、1つの解があれば別の解が作れます。これを繰り返して、 $x^3 - 3x + 1 = 0$ の解は $\alpha, \alpha^2 - 1, (\alpha^2 - 2)^2 - 2$ と分かります。これらの中に同じ物が現れないことはチェックする必要がありますが、それは $\alpha = 2 \cos \frac{2}{9}\pi$ などの表示を確かめれば分かります。

一方、 $x^3 - 2 = 0$ の3解は $\sqrt[3]{2}$ と $\sqrt[3]{2} \times \frac{-1 \pm \sqrt{3}i}{2}$ です。 $\sqrt[3]{2}$ は実数解で、残り2つは虚数解です。よって $\alpha = \sqrt[3]{2}$ とすると、 α の有理数係数多項式は実数なので、決して残り2つの解にはなりません。

一般に $f(x) = 0$ がタイプ1の場合には、次を満たす整数 $N > 0$ が存在します*10。

$$\zeta_N := \cos \frac{2\pi}{N} + i \sin \frac{2\pi}{N} \text{ とすると、} f(x) = 0 \text{ の解は、} \zeta_N \text{ の有理数係数多項式}$$

2次方程式の例 $x^2 = 2$ では、 $\sqrt{2} = \zeta_8 + \zeta_8^{-1} = \zeta_8 + \zeta_8^7$ を使いました。この類似がタイプ1では成り立つわけですが。したがってタイプ1では、先ほどと同じ証明を繰り返すことでさらに、 $f(x) = 0$ の $\mathbb{F}_p$ 内での解の個数が p を N で割った余りで決まることも分かります。複素数の範囲で解を ζ_N の有理数係数多項式で表せば、それを参考にして Ω_p 内での解を、何乗かして1になる元の多項式で表すことができます。それが $\mathbb{F}_p$ に入っているかどうかを p 乗して確かめれば良いのです。

今のは3次方程式の話でしたが、より次数が高い方程式に対してもタイプ1の類似が定義できます。タイプ1の類似の方程式は **Abel 方程式** と呼ばれ、これを定義するのに使う数学は **Galois 理論** と呼ばれています。さらに Abel 方程式に対しても上で述べたこと、すなわち方程式の解がある特別な数の有理数係数多項式で表せることや、解の個数が p を適当な自然数 N で割った余りで判定できることが成り立ちます。こういうものは **類体論** と呼ばれます。これは20世紀前半の整数論の花形で、一つの大きな成果です。ここで述べたのは一般の類体論に比べて非常に簡単ではあるのですが、そうした内容も含めて20世紀前半に分かったことです。

ちなみに Galois 理論は、解の間にどれくらい関係があるかを定量的に考える理論です。たとえば3次方程式にも解の公式がありますが、なぜ解の公式があるのかについて、Galois 理論は答えてくれます。こういう立場に立つとタイプ1、2は解の公式とも非常に深い関係があるのですが、ここではその話はしません。興味がある人は勉強してください。当時の Galois 理論は今の形とは大分異なっていたのですが、Galois が決闘で死んだのは1832年なので、これは19世紀前半（平方剰余の相互法則が示された少し後）の数学です。

*10 これは有理数体 $\mathbb{Q}$ を含む体に対し「タイプ1の方程式が解ける最小の体（Abel 体）であることと、1のとある冪乗根を $\mathbb{Q}$ に付け加えた体（円分体）に含まれることが同値」だと主張する **Kronecker-Weber の定理** の一部です。

2.5 $x^3 - 2 = 0$ の解の個数を記述する無限積

基本的には「良い方程式に対しては、その $\mathbb{F}_p$ 内における解の個数が p を N で割った余りで決まる」というのが類体論です。ということは、 $x^3 - 2 = 0$ の $\mathbb{F}_p$ における解の個数が分からないことは類体論の限界を示しています。ここからはその限界を超えた話をしましょう。

解の個数が p を何かで割った余りで決まらない状況では、どのようにすれば良いのでしょうか？以下伝統的な理由で、いつも使っている x の代わりに文字 q を使います。非常に唐突ですが、次のような無限積を考えます。

$$q \prod_{n=1}^{\infty} (1 - q^{6n})(1 - q^{18n})$$

この $\prod$ で表しているのは、掛け算の記号です。上の式を $\prod$ 記号なしで具体的に書けば

$$q(1 - q^6)(1 - q^{18})(1 - q^{12})(1 - q^{36})(1 - q^{18})(1 - q^{54}) \cdots$$

となります。 $\sum$ を知っている人は、その掛け算バージョンだと思ってください。こんな無限な掛け算をして良いのだろうかと思うのは当然ですが、1 個 n を止めて q^n の係数を求めるのだと考えてみます、たとえば q^7 の係数を求めるのだと考えてこの式を眺めると、2 つ目のカッコ以降に現れる q の冪乗は全て無視すれば良いと分かります。そうすれば有限回の計算でちゃんと、 q^7 の係数が求まります。このようなことを考えます。これを展開した結果を $a_1q + a_2q^2 + a_3q^3 + \cdots$ という無限和で表します。この式で数列 $(a_n)_{n=1}^{\infty}$ を定めます。このような計算に慣れていない人がほとんどだと思いますので、例をやってみましょう。

例 10. 次のような感じで、展開ができます。

- a_1 を求めてみましょう。最初の q を除くと、残りの部分を展開して出てくるのは定数項 1 か q^6 以上の次数の項です。よって $a_1 = 1$ です。
- 次に a_2 を考えると、この式を展開して q^2 が出てくることはありません。よって $a_2 = 0$ です。同様に q^3, q^4, q^5, q^6 も現れないので、 $a_3 = a_4 = a_5 = a_6 = 0$ です。
- a_7 はどうかというと、 $q(1 - q^6) = q - q^7$ という展開で $-q^7$ が現れます。よって $a_7 = -1$ です。
- かっこの中で q^6 の次に現れるのは q^{12} ですから、 $a_8 = a_9 = a_{10} = a_{11} = a_{12} = 0$ です。
- $(1 - q^{12})$ があるから、 $a_{13} = -1$ です。
- q^{12} の次に出てくるのは q^{18} なので、 $a_{13} = a_{14} = a_{15} = a_{16} = a_{17} = a_{18} = 0$ です。
- a_{19} は状況が変わります。展開して q^{19} を作るわけですが、まず q と $1 - q^{18}$ から $-q^{19}$ が 2 個作れる一方、これ以外にも $(1 - q^6)$ と $(1 - q^{12})$ から q^{18} が作れます。よって $a_{19} = (-1) \times 2 + 1 = -1$ と分かります。

この展開と元の問題との間にどういう関係があるかということ、次の定理が成り立ちます。

定理 11. $p \neq 2, 3$ のとき、方程式 $x^3 - 2 = 0$ の $\mathbb{F}_p$ 内での解の個数は $1 + a_p$ である。

ここから特に、 a_p は $-1, 0, 2$ のいずれかであることが従います。実際 3 次方程式の解は高々 3 個ですから、 $1 + a_p = 0, 1, 2, 3$ です。そして解の個数が 2 になるのは重解を持つケースですが、方程式 $x^3 - 2 = 0$ は $p \neq 2, 3$ のとき重解を持ちません。そうすると $1 + a_p$ は $0, 1, 3$ のいずれかで、 $a_p = -1, 0, 2$ のどれかが必ず成り立ちます。

結局このことから、謎の無限積 $q \prod_{n=1}^{\infty} (1 - q^{6n})(1 - q^{18n})$ における素数次の項の係数には $-1, 0, 2$ のいずれかしか現れないことが分かります。この事実はおそらく、初等的にパズルで示すのは不可能だと思います。そしてさらに、その係数が方程式 $x^3 - 2 = 0$ の解の個数を知っているということです。

にわかには信じられないので、例を計算してみましょう。

例 12. $p = 2, 3$ は例外なので、一番簡単な場合は $p = 5$ です。最初にやったように表を書いてみます。

$\mathbb{F}_5$ で $0^3 = 0, 1^3 = 1, 2^3 = 8 = 3, 3^3 = 27 = 2, 4^3 = 64 = 4$ です。3 乗して 2 になる数は 3 だけなので、方程式 $x^3 = 2$ の解は 1 個です。かたや先ほどの展開で、 $1 + a_5 = 1 + 0 = 1$ でした。

x	0	1	2	3	4
x^3	0	1	3	2	4

次に簡単なのは $p = 7$ の場合です。 $\mathbb{F}_7$ で $0^3 = 0, 1^3 = 1, 2^3 = 8 = 1, 3^3 = 27 = 6, 4^3 = 64 = 1, 5^3 = 125 = 6, 6^3 = (-1)^3 = -1 = 6$ です。3 乗して 2 になる数はないから、方程式 $x^3 - 2 = 0$ は $\mathbb{F}_7$ で解を持ちません。かたや $a_7 = -1$ でしたから、 $1 + a_7 = 1 - 1 = 0$ となり、確かに $1 + a_7$ が解の個数と一致しています。

x	0	1	2	3	4	5	6
x^3	0	1	1	6	1	6	6

今挙げたのは解が 0 個か 1 個でしたから、解が 3 つある場合も気になります。ただ、この場合は p がかなり大きくなり、一番簡単な場合でも $p = 31$ になってしまいます。予め計算した答えを言うと、 $\mathbb{F}_{31}$ で $4^3 = 64 = 2, 7^3 = 49 \times 7 = 18 \times 7 = 126 = 2, 20^3 = 4^3 \times 5^3 = 2 \times 125 = 2 \times 1 = 2$ と分かります。かくして $\mathbb{F}_{31}$ で方程式 $x^3 - 2 = 0$ の解は 3 つあるので、 $1 + a_{31} = 3$ 、つまり $a_{31} = 2$ となっているはずです。これを確かめるには、無限積の中から q の冪が 30 乗以下であるような項だけを集めてきて（すなわち、次の波線部を無視して）

$$\begin{aligned} & (1 - q^6)(1 - q^{18})(1 - q^{12})(1 - q^{36})(1 - q^{18})(1 - q^{54})(1 - q^{24})(1 - q^{72})(1 - q^{30})(1 - q^{90}) \cdots \\ &= (1 - q^6)(1 - q^{18})(1 - q^{12})(1 - q^{18})(1 - q^{24})(1 - q^{30}) \cdots \end{aligned}$$

における q^{30} の係数を求める必要があります。次数の組合せは $30, 6 + 24, 12 + 18$ の 3 通りです。それぞれの係数がどうなるかというと、 q^{30} 単独では -1 、 $q^6 \times q^{24}$ では $(-1) \times (-1) = 1$ 、 $q^{12} \times q^{18}$ では $(-1) \times (-1) = 1$ が 2 つで 2 です。足すと $-1 + 1 + 2 = 2$ となっています。

これはかなりすごい事実だと思います。いかがでしょうか？

2.6 保型形式

このように解の個数を無限積を用いて表してみたわけですが、この無限積の正体が分らないと、現象が分かった気がしません。そこで無限積の正体を説明します。少々難しいので、もしかしたら知らない事が出てくるかもしれません。というのも、複素数の関数が出てくるからです。しかし説明しないわけにもいきません。

複素数 $z = x + yi$ ($y > 0$) に対し (少々苦しいですが) $q = e^{2\pi iz}$ とおきます。ここで $e = 2.71828 \dots$ は自然対数の底と呼ばれる、数学で非常に大事な定数です。この肩に複素数を乗せていいのかという話ですが、これは指数法則で計算して肩をばらすと $e^{2\pi iz} = e^{2\pi ix} e^{-2\pi y}$ になります。ここで Euler の公式というものを使うと $e^{2\pi iz} = (\cos 2\pi x + i \sin 2\pi x) e^{-2\pi y}$ となります。大事なのは指数法則が成り立つことと、 $e^{2\pi ix} = \cos 2\pi x + i \sin 2\pi x$ という式です。 $e^{\pi i} = -1$ という式がありますが、それはこの式に $x = \frac{1}{2}$ を代入すると得られます。

ちなみに指数関数と三角関数は、複素数の範囲で考えると同じものになります。三角関数 $\cos z, \sin z$ は 2 回微分すると -1 が付くだけなので、微分しても変わらない指数関数と似ている感じがします。これが複素数の範囲で数学を考えると、本当に同じものになってしまいます^{*11}。このような背景があつて、普段はあまり $\cos, \sin$ を使わなかったりします。

さて先ほどの無限積では q はただの文字でしたが、これを $q = e^{2\pi iz}$ という式で複素関数と思うのが重要な視点です。こうして先ほどの無限積を複素関数と捉え直したとき、 $f(z) = q \prod_{n=1}^{\infty} (1 - q^{6n})(1 - q^{18n})$ は、次のように高い対称性を持っています。単に適当な項をかけただけではなく、非常に良い性質を示すのです。

定理 13. a, b, c, d を、 $ad - bc = 1$ かつ $a - 1, c, d - 1$ が 108 の倍数となる整数とする^{*12}。このとき

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)f(z) \quad (*)$$

が成り立つ。

つまり z を 1 次分数変換^{*13} $\frac{az+b}{cz+d}$ で置き換えても、元とほとんど同じ形になるのです。唐突な式変形に見えるかもしれませんが、この 1 次分数変換という式は非常に由緒正しいものです。

ちなみに a, b, c, d は 4 つバラバラの数として扱うのではなく、

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

のように正方形に並べると捉えやすくなります。こういうものを**行列**といいます。今は高校で習わないことになってしまいましたが、みなさんには、そういうことを考えず勉強して欲しいと思います。また定義に現れる $ad - bc$ は**行列式**と呼ばれるものです。

^{*11} $e^{2\pi iz} = \cos z + i \sin z$ という式から $e^{-2\pi iz} = \cos(-2\pi iz) + i \sin(-2\pi iz) = \cos 2\pi z - i \sin 2\pi z$ が得られます。この 2 つの式を合わせて $\cos 2\pi z = \frac{e^{2\pi iz} + e^{-2\pi iz}}{2}$, $\sin 2\pi z = \frac{e^{2\pi iz} - e^{-2\pi iz}}{2i}$ が得られます

^{*12} 要するに $SL_2(\mathbb{Z})$ の特別な元を考えているわけです。

^{*13} 分子・分母の両方が 1 次式であるような分数式による変換を **1 次分数変換**といいます。

例 14. $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ の場合を考えます. この場合 $\frac{az+b}{cz+d} = z+1$ となります. よって式 (*) は $f(z+1) = f(z)$, すなわち f が周期関数であることを意味しています. ただ, この結果は無限積を見れば自明です. z を $z+1$ に置き換えると, $q(z) = e^{2\pi iz}$ は $q(z+1) = e^{2\pi i(z+1)} = e^{2\pi iz} e^{2\pi i} = e^{2\pi iz} = q(z)$ となります. これと $f(z)$ が $q = q(z)$ の関数で表せていることから, 周期性が従います.

ただ a, b, c, d は条件を満たす中で好きに選べるので, 他の組合せを選べば, もっと非自明な式が現れます. それを 1 つ見てみましょう. 左下の c は 108 の倍数でないといけなから 108 にしてみても, そうすると b が 0 でないと $ad - bc$ の計算が大変になるので $b = 0$ としてみます. あとは左上と右下を 1 にして $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 108 & 1 \end{pmatrix}$ で考えましょう. このとき式 (*) は

$$f\left(\frac{z}{108z+1}\right) = (108z+1)f(z)$$

となります. ここで現れた $\frac{z}{108z+1}$ は q の式で表すことができないので, この式を q の無限積を展開した形だけ見て示すことは非常に難しいです. この式は全く明らかではありません.

他にも色々な a, b, c, d の取り方がありますが, それらの全てに対して式 (*) が成り立つわけでは, これは非常に非自明ですが, 証明することができます.

今現れた不思議な対称性^{*14}を持つ複素関数には, 名前が付いています. 定理中の性質を満たす $f(z)$ を **重さ 1, レベル 108 の保型形式** といいます. 本当は, 保型形式にはもう少し条件がついていて, たとえばさっきの「 q の式で書ける」といった内容が条件に入っています. 他にも複素関数の意味での微分可能性なども課されます. ただ一番本質的なのは, 先ほど現れた謎の対称性の式 (*) です. ちなみに, 1 次分数変換で式がそのまま保たれるわけではなくちょっと掛け算が生じるところが, 保型関数ではなく保型形式と書かれる理由です. またレベル 108 というとすごくレベルが高い感じがしますが, 重さ 1 の保型形式の中では 108 はかなりレベルが低い方で, これ以下のレベルの保型形式はほとんどありません.

より一般に, **重さ w , レベル N の保型形式** とは $ad - bc = 1$ かつ $a - 1, c, d - 1$ が N の倍数となる整数 a, b, c, d に対し,

$$f\left(\frac{az+b}{cz+d}\right) = (cz+d)^w f(z) \quad (*)$$

を満たす複素関数のことをいいます (本によっては, c が N で割り切れる条件だけを課していることもありますが, それは流儀の問題です). 例によってこれに加えていくつかの条件が付きますが, それは省略します.

ちなみに保型形式を特徴付ける条件 (*) はかなり強烈です. たとえば重さ 1, レベル 108 の保型形式は, 先ほど挙げた例の定数倍しかないことが示されます. つまりさっきの保型形式は, 重さ 1, レベル 108 で q の係数が 1 であるような唯一の保型形式です. 対称性だけで, 完全に保型形式が決定されています.

ここまでで 2 つのことを話しました. まず, 類体論では分からないような方程式 $x^3 - 2 = 0$ に対して, 謎の無限積を展開した係数を見ると解の個数に分かるのでした. そしてその謎の無限積の正体は, 保型形式と呼ばれるものでした.

^{*14} たとえば図形の場合, 線対称とは「折り返し操作に対する不変性」のことです. このように対称性とは「ある種の操作に対する不変性」のことなので, 「保型形式は 1 次分数変換に対する対称性を持つ」と表現します.

以上をまとめると「 $x^3 - 2 = 0$ の $\mathbb{F}_p$ 内での解の個数は、重さ 1 の保型形式が知っている！」ということになります。これは偶然ではなく、タイプ 2 の全ての 3 次方程式について成り立ちます。定理の形で書いておきましょう。

定理 15. $f(x) = 0$ をタイプ 2 の 3 次方程式とすると、ある整数 $N > 0$ および重さ 1、レベル N の保型形式 $q + a_2q^2 + a_3q^3 + \cdots$ であって、次を満たすものが存在する：素数 p が N を割り切らないとき、 $f(x) = 0$ の $\mathbb{F}_p$ 内での解の個数は $1 + a_p$ である。

ちなみにさっきは保型形式を無限積で書きましたが、保型形式が無限積で書けるのは珍しいことで、一般には無限積で表せない保型形式もあります。そしてタイプ 2 に関連する定理は無限積のままで一般化することができないので、我々は保型形式の言葉を使わなければいけません。ただ無限積で表せた方が例として説明しやすいので、さっきは無限積を使いました。

というわけで 2 次方程式の解の個数は、 p を N で割った余りで分かりました。3 次方程式の解の個数について、Abel 方程式という良い方程式の場合は p を N で割った余りで分かり、その理論が類体論と呼ばれていました。一方、類体論で分からないものは保型形式を使うと分かりました。

そして保型形式は 3 次方程式に使うだけでは勿体ないものです。他にも色々な方程式の $\mathbb{F}_p$ 内での解の個数を、保型形式が知っています。4 次方程式や 5 次方程式を考えても良いのですが、ちょっと方向を変えて、変数を増やしてみましょう。唐突ですが、 $y^2 + y = x^3 - x^2$ という方程式を考えます。普通このような方程式の解は無限にあって「個数」を考える意味はないのですが、今は考えている数の範囲が有限体 $\mathbb{F}_p$ であるため、解は有限個になります。この個数を、やはり保型形式が知っています。さっき 1 変数の方程式では重さ 1 の保型形式が出てきましたが、2 変数の方程式では重さ 2 の保型形式が登場します。

定理 16. 方程式 $y^2 + y = x^3 - x^2$ を満たす $x, y \in \mathbb{F}_p$ の組 (x, y) の個数を n_p とおく。このとき重さ 2、レベル 11 の保型形式 $q \prod_{n=1}^{\infty} (1 - q^n)^2 (1 - q^{11n})^2 = q + a_2q^2 + a_3q^3 + \cdots$ に対し、 $n_p = n - a_p$ ($p \neq 11$) が成り立つ。

ちなみに重さ 2 の保型形式の中で定数項が 0 のもの（尖点形式）は、レベル 11 が最低です。また無限積の中に 2 乗が現れたことで、1 次分数変換で $(cz + d)^2$ が飛び出すようになって、保型形式の重さが 2 になります。先の例に合わせて $p = 11$ を除きましたが、実は今回に限ってたまたま $p = 11$ でも成り立ちます。

このように、2 変数の方程式であっても保型形式が $\mathbb{F}_p$ における解の個数を知っているという現象が見られます。そして上のように、 x と y の 3 次方程式で定まる平面曲線（で特異点を持たないもの）を楕円曲線といいます。ここで「特異点を持たない」と書いたのは、たとえば「 $(1 \text{ 次式})^3 = 0$ 」という形で直線を表すような 3 次方程式を排除するためのおまじないです。因数分解ができないとか、尖った点がないということを表します。先ほどは 2 次方程式の解の個数が保型形式で分かるという話をしましたが、 $\mathbb{F}_p$ 係数での楕円曲線上の点（これを $\mathbb{F}_p$ 有理点といいます）の個数も、重さ 2 の保型形式が知っています。これは志村-谷山予想と呼ばれるものです。

定理 17 (志村–谷山予想, [Taylor–Wiles 1995, Breuil–Conrad–Diamond–Taylor 2001]). a, b を整数とし, 楕円曲線 $y^2 = x^3 + ax + b$ に対し, 前と同様 $n_p := \#\{(x, y) \in \mathbb{F}_p^2 \mid y^2 = x^3 + ax + b\}$ と定める. このとき, ある整数 $N > 0$ 及び重さ 2, レベル N の保型形式 $q + a_2q^2 + a_3q^3 + \cdots$ であって, $n_p = p - a_p$ が成り立つものが存在する.

例によって a, b には, 曲線が特異点を持たないための条件が付きますが, それは省略します. また一般の楕円曲線は $y^2 = x^3 + ax + b$ という形に変形できるので, この定理は特殊な楕円曲線だけを扱っているわけではありません.

ちなみに, 先ほどから登場している保型形式の重さは「1 を引くと次元になる」という関係の数になっています. この定理の場合, 楕円曲線は 1 次元で $2 - 1 = 1$ となっています. 1 変数の場合だと方程式の解が有限個の点で 0 次元になるので, 重さ 1 が現れます.

この志村–谷山予想は, 名前を聞いたことのある人がいるかもしれません. これは有名な Fermat 予想^{*15}

整数 a, b, c に対し $a^n + b^n = c^n$ かつ $n \geq 3$ ならば, $abc = 0$

の証明に使われたからです. もし $n \geq 3$ で $a^n + b^n = c^n$ かつ $abc \neq 0$ を満たす整数の 3 つ組 (a, b, c) が存在すると, これを使った方程式によって, とある楕円曲線 E が作れます. そうすると志村–谷山予想で対応する保型形式 f が存在するはずですが. ここで現れた楕円曲線 E は非常に特殊な形をしていて, E の形から, 重さ 2, レベル 2 の保型形式 f' で f と関係するものが存在することが言えます. 一方, 重さ 2 の保型形式でレベル 2 のものが存在しないことが, 解析的^{*16}に (大して難しくはなく) 示せます.

このように 350 年前からあった Fermat 予想は, 最終的に有限体上の方程式と関連付けて解かれたのです. Fermat 予想が解けたとき「Fermat 予想の解決ではなく, 志村–谷山予想が解けて嬉しかったんだ」などと言った数学者もいましたが, このように志村–谷山予想を利用して昔からある予想が解けたことも, 大変嬉しいことです.

似た方針で, 次の定理も示せます. Fermat 予想に比べて, こちらはあまり有名ではありません.

定理 18 ([Bugeaud–Mignotte–Siksek 2006, Theorem 1]). 数列 $(F_n)_{n=1}^\infty$ を Fibonacci 数列とする. すなわち $F_1 = F_2 = 1, F_{n+2} = F_{n+1} + F_n$ とする. このとき数列 $(F_n)_{n=1}^\infty$ の項で N^m ($N \geq 1, m \geq 2$) の形のものは $F_1 = F_2 = 1 = 1^2, F_6 = 8 = 2^3$ と $F_{12} = 144 = 12^2$ しかない.

Fibonacci 数列に現れる平方数が 1 と 144 しかないことは割と簡単で, こちらは 1970 年代に証明されています^{*17}. ただ平方数に限らず自然数の冪乗がこれしかないことを示すには, Fermat 予想の証明と同様の議論が必要でした.

^{*15} Fermat が書き残した「この余白は証明を書くには狭すぎる」という言葉は, あまりにも有名です. ただ, 実際に Fermat 予想を証明するのに必要だった数学を眺めてみると, 当時の Fermat に完全な証明ができていたとは思えません.

^{*16} 「複素関数に対する微積分を用いて」という意味です.

^{*17} J. H. E. Cohn, On square Fibonacci numbers, *J. London Math. Soc.* **39** (1964), 537–540 の中で, 割と初等的な計算で示されています.

3 保型形式の限界, そして…

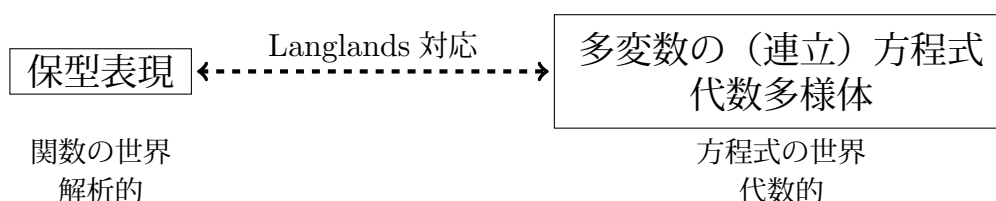
最後に、今我々が考えているこの先の話をしてします。保型形式は万能で何でも分かるのかということ、そうでもありません。今まで考えてきた問題は「2 次方程式の次は 3 次方程式にしてみよう」とか「1 変数から 2 変数にしてみよう」とか、割と安易なものでした。(ちなみにここまでの話で出ませんでした、2 変数の 2 次方程式はもっと簡単です。考えてみてください。) もっと問題を難しくしようとすると、素朴には

- 4 次以上の方程式の $\mathbb{F}_p$ 内における解の個数
- (実は、4 次式を考えるのと 3 次式を考えるのはほとんど変わらないので) $y^2 = (x \text{ の 5 次式})$ という曲線の $\mathbb{F}_p$ 有理点の個数
- もっと変数を増やしたときの、曲面上の $\mathbb{F}_p$ 有理点の個数

が出てきます。実はこの中には、全然分かっていないものも含まれています。これは 2 次方程式から 3 次方程式に話を進めたときと同じような状況になっていて、運が良ければ保型形式で書けることもありますが、一般にはそうではありません。先ほど類体論で分かる方程式を Abel 方程式と言いましたが、保型形式で書けるものにも **GL(2) 型** という名前がついてます。このあたりの記号の説明はしませんが、行列と関係しています。そして実は、Abel 方程式は **GL(1) 型** に他なりません。すなわち **GL(1) 型** は類体論で分かり、**GL(2) 型** は保型形式で分かる、というわけです。そして **GL(2) 型** でないような方程式があります。

ではどうしようもないのかということ、そうではなくて、保型形式を **GL(2) 型** でないものに一般化することが考えられます。保型形式の一般化として、各整数 $n \geq 1$ に対して「**GL(n) の保型表現**」と呼ばれるものがあり、これを使うと上で述べたような全ての問題に答えられると期待されています。これらの期待を含む壮大な予想が **Langlands 予想** と呼ばれています。(実のところ Langlands 予想はもっともっと広いものですので、今のような言い方をしてしまうと、一部の専門家は「そうではない」と言うかもしれません。ただ、それでも「Langlands 予想がどういうものなのか」に関しては、かなり正確な言い方になっています。)

この Langlands 予想について図を描いて終わりにします。



どうなっているかというと、一方には保型表現の世界があって、他方には多変数の(連立)方程式(すなわち、曲線や曲面や、それらを一般化した**代数多様体**)の世界があります。保型表現の世界は関数の世界であり、解析(微積分や、それらの複素バージョンや、あるいは関数解析)をふんだんに使います。代数多様体の世界は方程式の世界で、どちらかという代数的です。それぞれ非常に歴史のある分野で、これまで深い研究がなされてきたわけですが、この間に橋を架けようというのが **Langlands 対応** というものです。この橋渡しの研究が、いま盛んに進行中です。解析と代数を結びつける必要があるのです、ありとあらゆる数学(たとえば幾何学、表現論、物理学など…)を使います。全く違う分野を結びつけるとしてもいかなかった結果が現れたりするの、面白いところです。最近では Taylor さんを中心に議論が進んでいて、色々なことが証明されていますが、今日の話はここまでにしておきます。

4 練習問題の解答

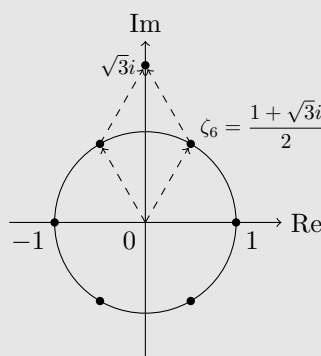
■方程式 $x^2 = -3$ の $\mathbb{F}_p$ における解

例 19. $x^2 = -3$ の $\mathbb{F}_p$ における解がいつ存在するかを調べましょう.

複素平面上で考えて, 1 の冪根を用いて $\sqrt{-3}$ を作ります. $\sqrt{-3} = \sqrt{3}i$ を作るには, 単位円周を 6 等分して ζ_6 を考え

$$\sqrt{3}i = \frac{1 + \sqrt{3}i}{2} + \frac{-1 + \sqrt{3}i}{2} = \zeta_6 + \zeta_6^2$$

とすれば良さそうです.



Ω_p でこの真似をします. $a^3 + 1 = (a + 1)(a^2 - a + 1)$ です. そこで 3 乗して -1 になる元のうち -1 でないものとして, $a^2 - a + 1 = 0$ を満たす複素数 a を取ります. そして $\omega = a + a^2$ とおきます. このとき

$$\omega^2 = a^2 + 2a^3 + a^4 = a^2 - 2 - a = -1 - 2 = -3$$

です. よって $x^2 = -3$ は, 解 $\pm(a + a^2) = \pm(a - a^{-1})$ を持ちます.

かくして Ω_p 内でも同様に, $a^2 - a + 1 = 0$ を満たす a を取れば, 方程式 $x^2 = -3$ の 2 解が $\pm(a - a^{-1})$ と分かります. これが $\mathbb{F}_p$ に属するかを考えましょう. $a^6 = 1$ なので, $(a - a^{-1})^p = a^p + (-1)^p a^{-p}$ は, p を 6 で割った余りで決まります. そして p は素数なので, p を 6 で割った余りは 1, 2, 3, 5 のいずれかです. また 6 で割って 2 余る p は $p = 2$ だけ, 6 で割って 3 余る p は $p = 3$ だけです.

余りが 1 この場合 $(a - a^{-1})^p = a^p - a^{-p} = a - a^{-1}$ だから, $\pm(a - a^{-1})$ が $\mathbb{F}_p$ 内での解になっています.

余りが 2 この場合は $p = 2$ で, $-3 = 1$ です. よって元の方程式は $x^2 = 1$ となり, さらに $1 = -1$ だから, 方程式は重解 $x = 1$ を持ちます.

余りが 3 この場合は $3 = 0$ なので, そもそも元の方程式が $x^2 = 0$ になってしまいます. この解は重解 $x = 0$ です.

余りが 5 この場合は $(a - a^{-1})^p = a^5 - a^{-5} = a^{-1} - a = -(a - a^{-1}) \neq a - a^{-1}$ です. よって解は $\mathbb{F}_p$ 内に存在しません.

■方程式 $x^3 - 3x + 1 = 0$ の $\mathbb{F}_p$ における解

例 20. 方程式 $x^3 - 3x + 1 = 0$ の $\mathbb{F}_p$ における解がいつ存在するかを調べましょう.

まず実数の範囲で方程式を解いてみます. $x = 2 \cos \theta$ を代入すると

$$0 = 8 \cos^3 \theta - 6 \cos \theta + 1 = 2(4 \cos^3 \theta - 3 \cos \theta) + 1 = 2 \cos 3\theta + 1 \quad \therefore \cos 3\theta = -\frac{1}{2}$$

となります. よって $3\theta = \frac{2}{3}\pi, \frac{4}{3}\pi, \frac{8}{3}\pi$ とすれば, 3 解 $x = 2 \cos \frac{2}{9}\pi, 2 \cos \frac{4}{9}\pi, 2 \cos \frac{8}{9}\pi$ が得られます.

ここで, 1 つの解から残りの解を作る方法を調べておきましょう. $\cos$ の倍角公式 $\cos 2\theta = 2 \cos^2 \theta - 1$ より, $2 \cos 2\theta = (2 \cos \theta)^2 - 2$ です. よって α が上記の解のいずれかなら $\alpha^2 - 2$ も解になります.

次に, 複素平面上で 1 の冪乗根を用いて解を表示します. $\zeta = \cos \frac{2}{9}\pi + i \sin \frac{2}{9}\pi$ を考えると, $\zeta + \zeta^{-1} = 2 \cos \frac{2}{9}\pi$ が解の 1 つです. よって残りの 2 解は $(\zeta + \zeta^{-1})^2 - 2 = \zeta^2 + \zeta^{-2}$ と $(\zeta^2 + \zeta^{-2})^2 - 2 = \zeta^4 + \zeta^{-4}$ だとわかります. ちなみに $\zeta^9 = 1$ より $\zeta^8 = \zeta^{-1}$ なので, もう 1 度同じ操作を繰り返すと $(\zeta^4 + \zeta^{-4})^2 - 2 = \zeta^8 + \zeta^{-8} = \zeta^{-1} + \zeta$ となり, 最初の解に戻ります.

これを利用して Ω_p での解を作ります. 今の ζ は, 9 乗して 1 になる数のうち, 1 の 3 乗根でないものとして特徴付けられます. そして $x^9 - 1 = (x^3 - 1)(x^6 + x^3 + 1)$ という因数分解を合わせると, ζ は $\zeta^6 + \zeta^3 + 1 = 0$ を満たします. そこで Ω_p 内で, $a^6 + a^3 + 1 = 0$ を満たす数 a を 1 つ取ります. このとき

- $a + a^{-1}$ は $x^3 - 3x + 1 = 0$ の解です:

$$(a + a^{-1})^3 - 3(a + a^{-1}) + 1 = a^3 + 1 + a^{-3} = \frac{a^6 + a^3 + 1}{a^3} = 0.$$

- $x = \alpha$ が $x^3 - 3x + 1 = 0$ の解なら, $x = \alpha^2 - 2$ も解です. 実際 $\alpha^3 - 3\alpha + 1 = 0$ なら

$$\begin{aligned} (\alpha^2 - 2)^3 - 3(\alpha^2 - 2) + 1 &= \alpha^6 - 6\alpha^4 + 9\alpha^2 - 1 \\ &= \alpha^3(\alpha^3 - 3\alpha + 1) - 3\alpha(\alpha^3 - 3\alpha + 1) - \alpha^3 + 3\alpha - 1 = 0. \end{aligned}$$

これより Ω_p での解 $\omega_0 = a + a^{-1}$, $\omega_1 = a^2 + a^{-2}$, $\omega_2 = a^4 + a^{-4}$ が得られます. これらはいずれも方程式 $x = x^2 - 2$ の解 $2, -1$ ではないので, 全て異なります. そして $\omega_{k+1 \bmod 3} = \omega_k^2 - 2$ だから, どれか 1 つが $\mathbb{F}_p$ に入れば残り全てが $\mathbb{F}_p$ に入ります. そこで $(a + a^{-1})^p = a^p + a^{-p}$ が $\mathbb{F}_p$ に入るか調べましょう. $a^9 - 1 = (a^3 - 1)(a^6 + a^3 + 1) = 0$ より $a^9 = 1$ なので, p を 9 で割った余りを考えます.

余りが 1 or 8 余りが 1 なら $a^p + a^{-p} = a + a^{-1}$, 余りが 8 なら $a^p + a^{-p} = a^{-1} + a$ より, いずれにせよ $(a + a^{-1})^p = a + a^{-1}$ です. よって解は 3 個です.

余りが 2 or 7 余りが 2 なら $a^p + a^{-p} = a^2 + a^{-2}$, 余りが 7 なら $a^p + a^{-p} = a^{-2} + a^2$ より, いずれにせよ $(a + a^{-1})^p = a^2 + a^{-2} \neq a + a^{-1}$ です. よって解は 0 個です.

余りが 4 or 5 余りが 4 なら $a^p + a^{-p} = a^4 + a^{-4}$, 余りが 5 なら $a^p + a^{-p} = a^{-4} + a^4$ より, いずれにせよ $(a + a^{-1})^p = a^4 + a^{-4} \neq a + a^{-1}$ です. よって解は 0 個です.

余りが 3 素数 p を 9 で割った余りが 3 になるのは $p = 3$ のときだけです. このとき元の方程式が $x^3 + 1 = 0$ になります. これを満たす x を総当たりで調べると, $x = 2$ しかないことが分かります. よって解は 1 個です.

5 参考文献

今回のテーマに関する文献をいくつか紹介しておきます.

■論文 今回の講演の中で結果が引用された論文は、以下の通りです.

- C. Breuil, B. Conrad, F. Diamond and R. Taylor, On the Modularity of Elliptic Curves over $\mathbf{Q}$: wild 3-adic exercises, *J. Amer. Math. Soc.* **14** (2001), 843–939.
- Y. Bugeaud, M. Mignotte and S. Siksek, Classical and modular approaches to exponential Diophantine equations I. Fibonacci and Lucas perfect powers, *Ann. Math.* **163** (2006), 969–1018.
- J. H. E. Cohn, On square Fibonacci numbers, *J. London Math. Soc.* **39** (1964), 537–540.
- R. Taylor and A. Wiles, Ring-Theoretic properties of certain Hecke Algebras, *Ann. Math.* **141** (1995), 553–572.
- A. Wiles, Modular elliptic curves and Fermat’s Last Theorem, *Ann. Math.* **141** (1995), 443–551.

Fermat 予想に関係した文献は [Breuil–Conrad–Diamond–Taylor 2001], [Taylor–Wiles 1995] と [Wiles 1995] です. また, これらの論文の手法を整数の冪乗の形をした Fibonacci 数列の項の問題に適用したのが [Bugeaud–Mignotte–Siksek 2006] です. そして [Cohn 1964] は, Fibonacci 数列の中に現れる平方数を決定した論文です.

■書籍

- C. F. Gauss, *Disquisitiones Arithmeticae*, Lipsiae (1965)
- 斎藤毅, 河東泰之, 小林俊行編『数学の現在 i 』(東京大学出版会)
- Jean-Pierre Serre 著, 弥永昌吉訳『数論講義』(岩波書店)

一番最初に挙げた Gauss の著書は, 平方剰余の相互法則に対する最初の証明が記されたものです. この第 4 章に証明が与えられています. 原著は今では当然絶版ですが, Yale University Press や Springer などから再版されているようです.

次に挙げた『数学の現在 i 』という本は, 東京大学理学部数学科の 4 年生向けに最先端の数学を紹介するオムニバス形式の授業「数学講究 XB」のうち, 代数学に関する内容をまとめたものです. この第 6 章に「整数論—モジュラー曲線の背後に潜む数論的現象」という三枝先生の記事があります.

最後に挙げた Serre の『数論講義』は, 定評のある数論の教科書です. 第 7 章で保型形式が扱われています.