平成30年度公開講座「数学の散歩道」の報告

岸 康弘　(愛知教育大学教育学部)

2019年8月22日

序

愛知教育大学主催の公開講座「数学の散歩道」が, 2018年7月24日と25日の2日間にかけて行われました. 高校生対象の公開講座の中で整数の性質を学ぶ本シリーズは, 平成27年度より始まり今回で4回目を迎えました. 参加者は附属高等学校から22名, その他の高等学校から1名の計23名でした. 積極的な学生が集まり, 活気のある講座となりました. 本稿は, 筆者が2日目に担当した『整数を学ぼう』(以下『本講義』という) の報告になります.

現在, 学習指導要領は改訂に伴い移行期間中ですが, 旧学習指導要領では「素数」という用語は小学校第5学年で導入され「素因数分解」は中学校第3学年で学習します. また, 新学習指導要領ではどちらも中学校第1学年で学習することになっています. いずれにせよ,

· 素数の判定の難しさ

· 素因数分解の難しさ

を学ぶことはありません. 本講義における目的は, 特別な素数が持つ性質について学ぶこととしていますが, 上記2点についても言及します.

本稿の各節は本講義と同じ見出しを付けました. 各節で, どのような内容を講義したのかを述べていきたいと思います.

1　素数の無限性

まず初めに素数および合成数の定義を行います. そして2 ∼ 15までの整数について正の約数をすべて挙げてもらい, 小さな素数を見つけます. この作業には素数を身近に感じてもらう狙いがありますが, 想定した通り, 全員がすぐに計算をし, 正しく素数を見つけ出していました.

次に, ユークリッドと同様の方法で素数の無限性を証明します. 本講義で唯一の「証明」のため, 時間をかけて丁寧に行いました. 証明した後, 補足として, 証明内に現れる関数

$$N = \prod_{p_i \leq p} p_i + 1 = p_1 p_2 \cdots p_n + 1^{1}$$

を計算してもらいました. 具体的には次のような表を作ってもらいます:

p	N
2	$2+1=3$
3	$2\times 3+1=7$
5	$2\times 3\times 5+1=31$
7	$2\times 3\times 5\times 7+1=211$
11	$2\times 3\times 5\times 7\times 11+1=2311$
13	$2\times 3\times 5\times 7\times 11\times 13+1=30031=59\times 509$

[1] もちろん, 本講義では $\prod$ という記号は用いていません.

$p = 13$ の例を見てもらい, N が合成数になる場合があることを確認することが目的です. 素数となる N がユークリッド素数と呼ばれること, またユークリッド素数の無限の存在性が未解決であることについても, 本講義では触れました.

続いて, 素数を与えられた整数で割った余りによって分類し, それらが $an+b$ の形に表されることを確認します. そして, 次に述べる算術級数定理を紹介して第 1 節を終えました.

算術級数定理 (Dirichlet, 1837)**.** $a, b \in \mathbb{Z}\,(a \neq 0)$ に対し, $(a, b) = 1$ ならば, $an+b$ の形の素数は無限に存在する.

この算術級数定理は代数的整数論においてとても深い定理であり, 類体論によって任意の代数体へ「任意の合同類別に関して, 各類に 1 次の素イデアルが無数に存在する」という主張に拡張されています.

2　二平方和定理

この節では, どのような素数が 2 つの平方の和で表せるかを考察します. まずは実例を見るため, 次の表を埋めてもらいました:

p	
2	$2 = 1^2 + 1^2$
3	$3 =$　　$\times$
5	$5 =$
7	$7 =$

p	
11	$11 =$
13	$13 =$
17	$17 =$
19	$19 =$

p	
23	$23 =$
29	$29 =$
31	$31 =$
37	$37 =$

前節で扱った $4n+3$ の形の素数が 2 つの平方の和で表せないことを, ヒントを出しながら気づかせます. そして, 次の定理を紹介します.

二平方和定理[2] (Euler, 1747)**.** 2 つの平方数の和で表せる素数は, 2 または $4n+1$ の形をしたものに限る.

さらに補足として, 3 つの性質

$$\cdot\ p = x^2 + 2y^2 \iff p = 8n+1 \text{ または } p = 8n+3$$
$$\cdot\ p = x^2 + 3y^2 \iff p = 3n+1$$
$$\cdot\ p = x^2 + 5y^2 \iff p = 20n+1 \text{ または } p = 20n+9$$

を述べました. これらは, 2 次体の数論における分岐理論より得られる興味深い結果です.

この節の最後には, x^2+1 の素因子について実験と共に考察し, 素因子として現れるものが 2 または $4n+1$ の形をしたものに限ることを解説しました. なお, 本講義では述べませんでしたが, 一般に次が成り立ちます:

定理. $a, b \in \mathbb{Z}$ に対し, $(a, b) = 1$ ならば, a^2+b^2 の素因子は 2 または $4n+1$ の形をしたものに限る.

[2]証明はオイラーによってなされましたが, 問題自体はフェルマーによって提起されたため, フェルマーの二平方和定理と呼ばれることもあります.

3　ペル方程式

まず初めにペル方程式の定義を与えます.

定義. 平方数でない正の整数 N に対し, 方程式

$$x^2 - Ny^2 = \pm 1$$

を**ペル方程式**と呼ぶ.

ペル方程式は 2 変数の方程式で, 解として整数のものだけを考えます. 本講義では, 簡単のため N を $4n+3$ の形の素数に限定し (この場合, $x^2 - Ny^2 = -1$ に解はありません), $x^2 - Ny^2 = 1$ を扱います. まずは具体例を使ってペル方程式の 1 つの解 (最小解) の見つけ方を説明します. そして, 多くの時間を割いていくつかのペル方程式を解いてもらいます. その際, 解 $(x, y) = (s, t)$ が見つかれば, 別の解が $s + t\sqrt{N}$ のべきを使って見つかることや, 任意の N に対して無限個の整数解が存在することを解説しました. 最終的には, 次の表を完成させます[3]:

N	ペル方程式	整数解 (x, y)
3	$x^2 - 3y^2 = 1$	$(x, y) = (2, 1), (7, 4), (26, 15)$
7	$x^2 - 7y^2 = 1$	$(x, y) = (8, 3), (127, 48)$
11	$x^2 - 11y^2 = 1$	$(x, y) = (10, 3)$
19	$x^2 - 19y^2 = 1$	$(x, y) = (170, 39)$
23	$x^2 - 23y^2 = 1$	$(x, y) = (24, 5)$
31	$x^2 - 31y^2 = 1$	$(x, y) = (1520, 273)$
43	$x^2 - 43y^2 = 1$	$(x, y) = (3482, 531)$
47	$x^2 - 47y^2 = 1$	$(x, y) = (48, 7)$
⋮	⋮	⋮
199	$x^2 - 199y^2 = 1$	$(x, y) = (16266196520, 1153080099)$
⋮	⋮	⋮
223	$x^2 - 223y^2 = 1$	$(x, y) = (224, 15)$

第 3 節はこの表を作ったところで終わります. ペル方程式や前節の二平方和定理の問題 ($x^2 + y^2 = p$) は不定方程式という整数論の 1 つのトピックスであり, もう少し内容を充実させたかったのですが, 時間の都合上組み込むことができませんでした. 機会があれば, その他の不定方程式についても講義したいと思っています.

4　メルセンヌ素数

メルセンヌ素数の定義は次の通りです.

定義. 素数 p に対し,

$$M_p = 2^p - 1$$

が素数になるとき, M_p を**メルセンヌ素数**と呼ぶ.

[3] $N = 199$ のときのように起こる巨大な最小解のことを本講義では「爆発解」と呼びました. このような爆発解を持つ素数 N を見つけることが著者の研究の 1 つであることも伝えました.

これまでの節と同様, まずは実験から入り, 次の表を完成させます:

p	M_p	素数？	p	M_p	素数？
2	$2^2-1=3$	○	11	$2^{11}-1=2047=23\times 89$	×
3	$2^3-1=7$	○	13	$2^{13}-1=8191$	○
5	$2^5-1=31$	○	17	$2^{17}-1=131071$	○
7	$2^7-1=127$	○	19	$2^{19}-1=524287$	○

根拠なく 2047 を素数とする受講生も少なくありません. 合成数であることを伝えると騒めきます. 最初の数例を観察するとほとんどの M_p が素数になりますが, メルセンヌは次のように予想を立てました.

メルセンヌの予想. $19<p\leq 257$ の範囲にある素数 p に対し, M_p が素数となるのは $p=31$, 67, 127, 257 の 4 つだけである.

このうち, $p=67$, 257 の場合は素数ではなく, メルセンヌの予想は誤りでした[4]. 78 桁の数 $M_{257}=2^{257}-1$ について, 素数でないことが判明したのは 1930 年, 素因数分解が完了したのは 1980 年になります. 50 年もの隔たりがあることが, 素因数分解が素数判定よりも難しいことを物語っています.

最後に, 現在見つかっている 50 個のメルセンヌ素数のうち大きなもの 5 つについて, それぞれの指数および桁数, 見つかった年月, 発見した人の名を紹介し, この節は終了です[5].

5 完全数

最後のトピックスは, メルセンヌ数と関連する完全数です. 完全数の定義は次になります:

定義. 正の整数 n に対し, n の正の約数のうち n 以外のものの和がちょうど n となるとき, n を**完全数**と呼ぶ.

最初に, いくつかの計算をさせ, 小さな完全数 6, 28 を見つけてもらいます. そして次の完全数は 496 であることを伝え, この 3 つの完全数の素因数分解を見せます. ここから法則は見つかるでしょうか. 3 つの完全数の奇数の素因子 3, 7, 31 に着目させた後, 次の定理を述べます:

ユークリッドの完全数公式. M_p がメルセンヌ素数ならば, $2^{p-1}M_p$ は完全数となる.

本講義も終わりに近づいていますが, 隣同士で騒ついてくれます. そして, この逆についての結果も述べます:

オイラーの完全数定理. 偶数の完全数は $2^{p-1}M_p$ (M_p はメルセンヌ素数) の形に限る.

これにより, 偶数の完全数についてはメルセンヌ素数に問題が帰着されました.

そして最後に, 奇数の完全数がまだ見つかっていないこと, また存在するかどうかは未解決であることを述べて講義は終了しました.

残念ながら, 時間がなく解説できませんでしたが, 配布プリントには, 次のような奇数の完全数に関する結果を載せています:

[4] さらに, メルセンヌ予想には 3 つのメルセンヌ素数 M_{61}, M_{89}, M_{107} の漏れがありました.
[5] 2018 年 12 月に新しいものが 1 つ見つかったため, 現在では 51 個のメルセンヌ素数が知られています.

補足. 奇数の完全数は 1 つも見つかっていないが, もし存在するならば, 次のことが知られている:

- 奇数の完全数は 10^{300} より大きい. (Brent, Cohen and te Riele, 1991 年)
- 奇数の完全数は 75 個以上の素因子を持つ. (Hare, 2005 年)
- 奇数の完全数は 9 個以上の異なる素因子を持つ. (Nielsen, 2007 年)
- 奇数の完全数の最大の素因子は 10^8 より大きい. (Goto and Ohno, 2008 年)
- 奇数の完全数は $p^{4x+1}a^2$ (ただし, p は $4n+1$ の形の素数) の形をしている.

6 終わりに

講義終了後, 参加者に修了証を渡します. 少し物々しく, 1 人ずつ表情を見ながら修了証を手渡していきました. 修了証を受け取る参加者の笑顔と「ありがとうございました」という言葉に, 講義の疲れは吹っ飛びました. 次年度以降も, 数学の面白さが伝えられるような公開講座を行っていきたいと思います.