

研究員の 眼

最大のメルセンヌ素数が 6年ぶりに更新されました ー52個目の完全数及びメルセンヌ素数の発見ー

客員研究員 中村 亮一
E-mail: nryoichi@nli-research.co.jp

はじめに

メルセンヌ素数については、これまでに2回の研究員の眼で紹介してきた。まずは、完全数との関係で、研究員の眼「[完全数とその魅力についてー「博士の愛した数式」を観て、改めて数字の持つ奥深さに魅せられましたー](#)」(2017.2.13)の中で紹介した。その時点では、49個の完全数及びメルセンヌ素数があると述べたが、研究員の眼「[最大のメルセンヌ素数が2年ぶりに更新されましたー50個目の完全数及びメルセンヌ素数の発見ー](#)」(2018.2.26)において、2018年1月3日に、新たなメルセンヌ素数を探索するプロジェクトサイトである GIMPS (Great Internet Mersenne Prime Search)¹が、2017年12月26日に50個目の完全数及びメルセンヌ素数が発見されたと公表したことを紹介した。今回、GIMPS は、2024年10月21日に、2024年10月12日に52個目の完全数及びメルセンヌ素数が発見されたことを公表²した。これは、これまでに特定された最大のメルセンヌ素数³ということになる。今回は、その内容を紹介する⁴。

完全数及びメルセンヌ素数とは

完全数及びメルセンヌ素数の詳しい内容については、以前の研究員の眼も参照していただくことにして、ここでは簡単に説明しておく。

¹ GIMPS の Web サイトは以下の通り

<https://www.mersenne.org/>

35 番目以降のメルセンヌ素数の発見は GIMPS によっている。

² プレスリリース

<https://www.mersenne.org/primes/?press=M136279841>

³ GIMPS の公表資料では、今回の最大のメルセンヌ素数について、「the largest known prime number (最大の既知の素数)」と表現されている。なお、素数自体は無限に存在しており、これは例えば背理法で証明される(素数が有限個しか存在しないと仮定すれば、それらの有限個の全ての素数を掛け合わせた数字に1を加えた数は、それまでのどの素数でも割り切れないので素数となる、ことから矛盾が発生する)。

⁴ 先の GIMPS の Web サイトに加えて、以下の「メルセンヌ素数」に関する Web サイトからの情報等に基づいて記述している。

Mersenne Primes:History, Theorems and Lists <http://primes.utm.edu/mersenne/index.html>

「完全数 (Perfect number)」とは、「その数字自身を除く約数の和がその数字自身に等しい自然数」のことをいう。例えば、6 の約数は、1、2、3、6 の 4 つで、6 以外の約数の和が、 $1+2+3=6$ となるので、6 は完全数である。28 も完全数で、 $1+2+4+7+14=28$ となっている。

「メルセンヌ数 (Mersenne number)」とは、 $2^n - 1$ という形の数（これは、 M_n と表現される）であり、素数のメルセンヌ数を「メルセンヌ素数 (Mersenne prime number)」⁵と呼んでいる。

この時、以下のことが知られている⁶。

- ・ $2^n - 1$ が素数（即ち、メルセンヌ素数）であるような正の整数 n を用いて、 $2^{n-1} \times (2^n - 1)$ という形で表される数は完全数である。さらに、 $n \geq 2$ となるので、 $2^{n-1} \times (2^n - 1)$ は偶数となる。
- ・ 逆に、偶数の完全数は、全て $2^{n-1} \times (2^n - 1)$ の形となる。
- ・ 即ち、「メルセンヌ素数と偶数の完全数は 1 対 1 に対応」している。

現時点で確認されているメルセンヌ素数は限られており、2018 年 12 月に 51 個目が発見されていたが、今回 6 年ぶりに新たに発見されたものは、それに続く 52 個目となっている。

新たなメルセンヌ素数

今回新たに発見されたメルセンヌ素数は、「 $2^{136279841} - 1$ 」で、「M136279841」と呼ばれている。

この「M136279841」は、4102 万 4320 桁の数字で、これまで最大だった 51 個目のメルセンヌ素数「M82589933(= $2^{82589933} - 1$)」の 2486 万 2048 桁と比べて、1600 万桁以上大きくなっている。

実は、以前の研究員の眼で紹介した 50 個目のメルセンヌ素数や 51 個目のメルセンヌ素数等は、以下の通りとなっており、今回の新たなメルセンヌ素数はそれまでのものに比べて格段に桁数が大きくなった数となっている。

48 個目	M57885161	1742 万 5170 桁
49 個目	M74297281	2233 万 8618 桁
50 個目	M77232917	2324 万 9425 桁
51 個目	M82589933	2486 万 2048 桁

今回の新たなメルセンヌ素数の発見について

今回の新たなメルセンヌ素数は、カリフォルニア州サンノゼの 36 歳の研究者で、元 NVIDIA 社員のルーク・デュラント (Luke Durant) 氏によって、10 月 12 日に発見された。ルーク・デュラント氏は、何千人もの GIMPS ボランティアの 1 人である。

2017 年に、ミハイ・ブレダ (Mihai Preda) 氏が PC (パソコン) の GPU (Graphics Processing Unit) のパワーがますます高まっていることに対応して、メルセンヌ数の素数性をテストする GpuOwl プログラムを作成し、そのソフトウェアを全ての GIMPS ユーザーに提供した。ルーク・デュラント氏は、一連の GIMPS ソフトウェアを多数の GPU サーバーで実行及び維持するためのイ

⁵ 350 年以上前にこれらの数字を研究していたフランスの修道士マリヌ・メルセンヌ (Marin Mersenne) (1588-1648) に因んで名付けられている。

⁶ 全てのメルセンヌ素数が完全数を形成することは、紀元前 3 世紀のユークリッド原論において証明されている。また、全ての偶数の完全数がメルセンヌ素数から形成されることは、18 世紀にレオンハルト・オイラーによって証明された。

ンフラストラクチャを開発し、17 か国にわたる 24 のデータセンター地域における数千のサーバー GPU 構成された「クラウドスーパーコンピューター」で、約 1 年間のテストの結果、M136279841 を発見している。

10 月 12 日に、リュカ-レーマー・テスト (Lucas-Lehmer test) と呼ばれる素数判定法で、素数であることが確認され、その後、GIMPS が複数のプログラムを実行して、素数であることを検証し、素数であることを認めた。

なお、ルーク・デュラント氏は、自らが設計に携わった GPU が、基礎的な数学や科学の研究にも適しており、新しいメルセンヌ素数の発見は GPU が AI (人工知能) 以外にも使用できることを示す素晴らしいデモンストレーションになると判断した、としている。

今回の発見で、ルーク・デュラント氏には、GIMPS から賞金として 3000 ドルが贈られることになるようだ。3000 ドルという賞金は、費やされた時間と労力に十分見合った金額とはいえないように思われるが、52 個目のメルセンヌ素数の発見者として、その歴史に名前が刻まれるという名誉がより重要なことになる。彼は賞金をアラバマ数学科学学校の数学科に寄付する予定とのことである。

なお、電子フロンティア財団 (Electronic Frontier Foundation) は、1 億桁の素数の発見に対して 150,000 ドルの賞金 (匿名の寄付者による資金提供) を支払うとしている。

メルセンヌ素数の順番

今回 52 個目の、これまでで最大のメルセンヌ素数が発見されたと述べたが、これが 52 番目に小さなメルセンヌ素数であるとは限らない。

以前の 50 番目のメルセンヌ素数発見に関する研究員の眼において、「2016 年 9 月に、現在の 45 番目までのメルセンヌ素数より小さいものは存在しないことが確認されているが、46 番目から今回の 50 個目の最大のメルセンヌ素数までの間に、新たなメルセンヌ素数が存在しないことは未だ確認されておらず、新たなメルセンヌ素数が発見されるかもしれない。その意味で、今回発見されたメルセンヌ素数は、現段階ではあくまでも「50 個目」のメルセンヌ素数であり、「50 番目」のメルセンヌ素数とは言い切れないものとなっている。」と述べていたが、その後、48 番目までの順番が確定している。

ただし、49 番目以降の順番は確定していないため、49 番目のメルセンヌ素数よりも小さいメルセンヌ素数が発見されるかもしれないことになっている。過去においては、45 番目のメルセンヌ素数は、46 番目のメルセンヌ素数の後に発見されている。

メルセンヌ素数の用途

それでは、これらのメルセンヌ素数は、どのような形で社会に役立っているのだろうか。なぜ、このような大きな時間と労力をかけて、より大きなメルセンヌ素数を探そうとしているのだろうかと疑問に思われるかもしれない。

これについては、正直言って、現時点においては、メルセンヌ素数自体そのものに、実用的な用途は殆どないものとされているようだ。それでも、人々の単純な探求心に加えて、素数を発見するためのプログラムはハードウェアのテストとして使用されているし、過去のユークリッドやオイラーやフェルマー等の著名な数学者の素数等に関する研究は新たな理論等を生み出してきており、メルセンヌ

素数の発見に向けた各種の研究等は、間接的には社会に役立ってきているといえるだろう。

そもそも、重要な暗号化アルゴリズムが素数に基づいて開発されるまで、大きな素数を探す理由についても、数十年前に同様な疑問が持たれていた。

完全数やメルセンヌ素数を巡る予想や未解決問題

さて、先に述べたように、お互いに深く関係している完全数とメルセンヌ素数（メルセンヌ素数と偶数の完全数は1対1に対応）については、いまだ解明されていない問題も多い。例えば、以下の通りである。

- ・奇数の完全数は存在するのか。
- ・完全数は無数に存在するのか、メルセンヌ素数は無数に存在するのか。
- ・1の位が6か8以外の完全数は存在するのか。
- ・メルセンヌ合成数（素数 p に対するメルセンヌ数 $2^p - 1$ で合成数⁷）は無数に存在するのか。
- ・二重メルセンヌ素数（double-Mersenne primes）（メルセンヌ数 $p = M_n (= 2^n - 1)$ が素数かつメルセンヌ数 $M_p (= 2^p - 1)$ も素数）（これを MM_n と表記）は、以下の4つ以外にあるのか。

$$MM_2 = 2^3 - 1 = 7$$

$$M_2 = 2^2 - 1 = 3$$

$$MM_3 = 2^7 - 1 = 127$$

$$M_3 = 2^3 - 1 = 7$$

$$MM_5 = 2^{31} - 1 = 2147483647$$

$$M_5 = 2^5 - 1 = 31$$

$$MM_7 = 2^{127} - 1 = 170141183460469231731687303715884105727$$

$$M_7 = 2^7 - 1 = 127$$

最後に

今回、新たに52個目のメルセンヌ素数が発見されたが、これもあくまでも1つのステップでしかない。今回の発見においては、クラウドでのGPUのパワーの向上と利用可能性の爆発的な成長が多大な貢献をしている。今後は、量子コンピュータ等の開発でコンピュータの処理能力がより一層向上していけば、さらなるメルセンヌ素数の発見が急速に進んでいくことになるのかもしれない。

数学や科学の発展がコンピュータ技術の開発や発展を促すとともに、逆にこれらの発展が数学上の問題の解決に寄与してくるという相互に貢献し合う形になっている。

これまでの数学上の未解決とされている問題等は、基本的には紙と鉛筆の世界において、人間の頭の中で理論的に証明されてきたものと思われるが、これからは四色問題の証明等のように、コンピュータやAIも駆使して解決されていくことも多くなっていくのかもしれない。それでも、それらのコンピュータやAIの使用に至るまでのプロセスにおいては、人間が頭で考えた理論やモデルがベースとして重要なままであり続けるということなのであろう。

こうした時代の到来により、これまでの多くの未解決問題が解決されていくことになれば、それは大変興味深くかつ喜ばしいことであり、そうした好循環が生まれてくることを大いに期待していきたいと思っている。

⁷ 2以上の自然数で素数でない数。自然数は1と素数と合成数に区分されることになる。