

2013年1月25日、分散コンピューティングを用いた素数の探査プロジェクト GIMPS (Great Internet Mersenne Prime Search) に参加する(米)セントラルミズーリ大学の C. Cooper 博士が過去最大の素数を発見した。発見した素数は、2 の 57,885,161 乗から 1 を引いた数で 17,425,170 桁になり、暫定値で小さい方から 48 番目のメルセンヌ素数である。GIMPS は、1996 年以降メルセンヌ素数の探査と検証を行っており、今回で 14 個目の発見となった。素数自身やその分布は現代数学にも関係し、素数分布の解明は重要な課題である。メルセンヌ素数自身にも数学的未解決問題が存在するが、GIMPS による一連の発見は現代数学への寄与も期待できる。

## トピックス 2 過去最大の新たな素数を発見

2013年1月25日、分散コンピューティングを用いた素数の探査プロジェクト GIMPS (Great Internet Mersenne Prime Search) は、過去最大の素数を発見した<sup>1)</sup>。発見した素数は、2 の 57,885,161 乗から 1 を引いた数で、17,425,170 桁になる。この素数は、プロジェクトに参加している(米)セントラルミズーリ大学の数学教授 Curtis Cooper 博士が発見したもので<sup>2)</sup>、同博士は、3,000ドルの賞金をプロジェクトから受け取る予定である。

素数とは、1 とその数自身でしか割り切れない自然数(但し、1 を除く)のことであり、素因数分解やそれを使った公開鍵暗号にとって重要な数である。2、3、5、7、11、13、17……と無限に存在することは、紀元前 3 世紀頃の古代ギリシャの数学者ユークリッドによって証明されているが、その分布の様子は現在も非自明である。素数自身およびその分布は、リーマン予想や ABC 予想<sup>3)</sup>などの現代数学にも関係しており、素数の分布を解明することは重要な課題となっている。

そこで、大きな素数の発見を目的としたプロジェクト GIMPS が 1996 年に発足し、参加者のコンピュータの余剰処理能力をネットワークで結んで、メルセンヌ素数の探査と検証を行ってきた。同プロジェクトは、13 個の素数を既に発見しており、今回は 14 個目の発見となる。この素数は、小さい方から 48 番目(但し、暫定値)のメルセンヌ素数である。なお、1996 年以降に発見された大きな素数は、全て同プロジェクトによって発見されたものである(図表 1)。

自然数  $M_p = 2^p - 1$  (但し、 $p$  は自然数) が素数になる場合をメルセンヌ素数<sup>注)</sup>と呼び、 $2^2 - 1 = 3$ 、 $2^3 - 1 = 7$ 、 $2^5 - 1 = 31$ 、 $2^7 - 1 = 127$  のように、 $p$  が素数であれば  $M_p$  が素数になる可能性が高い。メルセンヌ素数以外にもフェルマー素数やオイラー素数などが存在し、メルセンヌ素数が全ての素数を網羅するわけではない。しかし、 $M_p$  が素数であれば  $p$  は素数であることが証明されており、素数かどうかの判定法も確立していることから、最

近発見された大きな素数は全てメルセンヌ素数である。

しかし、42 番目から 48 番目までのメルセンヌ素数の間に、他のメルセンヌ素数が存在しないことが証明されておらず、43 番目以降の番号は暫定番号である。事実、47 番目のメルセンヌ素数の発見後に、45 番目と 46 番目のメルセンヌ素数が発見された。47 番目のメルセンヌ素数は、(米)カリフォルニア大学ロサンゼルス校 (UCLA) のグループが発見したもので、初めて 1 千万桁を超えたため、100,000ドルの賞金を受け取った。

メルセンヌ素数自身に対しても、「メルセンヌ素数は無数に存在するか?」などの数学的未解決問題が存在する。GIMPS による一連の大きな素数の発見は、現代数学への寄与も期待できる。

図表 1 GIMPS が発見したメルセンヌ素数

番号	$p$	$M_p$ の桁数	発見年	発見者
35	1,398,269	420,921	1996	J. Armengaud
36	2,976,221	895,932	1997	G. Spence
37	3,021,377	909,526	1998	R. Clarkson
38	6,972,593	2,098,960	1999	N. Hajratwala
39	13,466,917	4,053,946	2001	M. Cameron
40	20,996,011	6,320,430	2003	M. Shafer
41	24,036,583	7,235,733	2004	J. Findley
42	25,964,951	7,816,230	2005	M. Nowak
43	30,402,457	9,152,052	2005	C. Cooper & S. Boone
44	32,582,657	9,808,358	2006	C. Cooper & S. Boone
45	37,156,667	11,185,272	2008	H-M. Elvenich
46	42,643,801	12,837,064	2009	O.M. Strindmo
47	43,112,609	12,978,189	2008	E. Smith, et al.
48	57,885,161	17,425,170	2013	C. Cooper

出典：参考 1

注：フランスの神学者 Marin Mersenne (1588-1648) は、 $2^p - 1$  ( $p \leq 257$ ) が素数になるのは、 $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$  だけであると主張したが、他にも素数が存在するなどその主張の一部は誤りであることが後に分かった。

- 参 考 1) GIMPS ホームページ：<http://www.mersenne.org/>  
 2) (米)セントラルミズーリ大学ニュース発表：<http://www.ucmo.edu/news/prime.cooper.2013.cfm>  
 3) 科学技術動向誌 No.132 (2012 年 11・12 月号)「数学上の未解決問題 ABC 予想を証明」