数の世界　～メルセンヌ数編 ～

定義 1 n が自然数のとき, $2^n - 1$ をメルセンヌ数 ***(Mersenne number)*** といい, M_n で表す. 特に, 素数であるメルセンヌ数のことをメルセンヌ素数 ***(Mersenne prime)*** という.

2 の n 乗より 1 だけ小さい形をしている自然数をメルセンヌ数といいます. 最初の方から書き並べていくと,

1, 3, 7, 15, 31, 63, 127, 255, 511, 1023, 2047, 4095, ……

となっています. このようなタイプの数がなぜメルセンヌ数と呼ばれるかというと, フランスのマラン・メルセンヌ (Marin Mersenne, 1588～1648) が, 「n が 257 以下の自然数のとき, $2^n - 1$ が素数となるのは n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257 である.」と主張したことからきています. ちなみに, その後の研究により 67, 257 のときは素数でないこと, さらに, メルセンヌが予想したリストには含まれていなかった n = 61, 89, 107 のときに素数となることが発見されました. メルセンヌ素数については以下のことが知られています.

定理 1 n を自然数とする. $2^n - 1$ が素数であるならば n は素数である.

証明には対偶法と呼ばれる間接証明法を利用します. さて, いつものことですがメルセンヌ素数は無限に存在するのでしょうか. 実は, これも未解決問題になっています. もし, 先ほどの定理の逆である「n を自然数とする. n が素数であるならば $2^n - 1$ は素数である. 」が真であれば, メルセンヌ素数が無限にある (素数は無限にありますよね) ことがわかりますが, これは正しくありません. 成立しない例を見つけてみてください. (「P ならば Q」の逆とは「Q ならば P」のことをさします.)

上の定理からメルセンヌ素数を見つけるために, n に素数を入れて調べていくのですが, 実際に素因数分解をして考えることは, 数が大きくなるにつれ困難になっていきます. そのため, 総当たりで割っていかなくてもメルセンヌ数がメルセンヌ素数かどうかを判定できる素数判定法 (リュカ・テストやリュカ - レーマー・テストなど) が生み出されました. 特に, このリュカ・テストやリュカ - レーマー・テストは, 一般的な数に対する素数判定法に比べ, メルセンヌ数だからこそ少ない処理で素数かどうか判定ができる方法になっています. そのため, ニュースになる最大の素数が更新されたという素数は, ここ最近ではメルセンヌ素数のみとなっています.

では, どのようにメルセンヌ素数を探しているかというと, 世の中には面白い人たちがいるもので, 1996 年に George Woltman により設立された GIMPS (Great Internet Mersenne Prime Search) という世界中の協力者によりメルセンヌ素数を探し出すグループが存在します. 分散型コンピューティングという手法を用いて, 1 台の PC で探しているのではなく協力者の PC をすべて利用し, 問題を複数の部分問題に分割して, たくさんの PC に処理を振り分けて実行することで処理能力をあげて探しています. ここ最近の最大の素数の更新はこのグループの結果によるものです. 現在見つかっている最大の素数は, 第 1 回にも書いた 2486 万 2048 桁のもので, これは n = 82589933 に対応するメルセンヌ素数となっています.

メルセンヌ素数が有名な理由はこれだけではありません. 完全数という特別な数に関係あることが知られています. 次回は完全数のお話をしましょう. では, また来週 !!