1.5　整数の謎

古来より「数」というものに関しては，さまざまな研究がなされてきた。それは現実の生活において実用上必要である，という理由もあるが，同時に，数というものがどのような性質を持つのか，ということに多くの人々が惹きつけられた，という理由もあるだろう。「数」が持っている神秘性は，時に，宗教や哲学，占いなどと結びつくこともあった。

紀元前 332 年にアレキサンダー大王によって建設されたアレキサンドリアは，その後，700 年間にもわたって，世界の数学，科学の中心であった。ここに，ムセイオンと呼ばれる大学が作られ，60 万巻にも及ぶパピルス書を蔵する図書館が設置された。最も初期に，ここで数学の学派を率いていたのがユークリッドである。彼が著した「原論」は 13 巻にもなるもので，それまで主にギリシャで発展してきた数学の集大成である。その中には，素数の定義や，2 つの自然数の最大公約数を求めるための，いわゆる「ユークリッド互除法」，また，素数が無限にあることの証明なども書かれている。

数学はその後，アレキサンドリアでさらに発展を遂げ，西暦 250 年頃には，整数に関する研究の集大成とも言える，ディオファントスの「数論」が著された。この中では，整数係数の不定方程式などについても詳しく述べられている。

整数についての研究は，その後，1300 年もの間停滞し，17 世紀頃になってヨーロッパで復活する。西暦 1621 年に，ディオファントスの「数論」のラテン語訳が出版される。フランス，トゥー

ルーズの裁判所顧問だったピエール・ド・フェルマーは，この本を入手し，暇をみては，自分自身で注釈や書き込みを付け加えながら読み進んだ。その書き込みの中で，次のようなものがあった。

「 x, y, z, n が整数で $x^n + y^n = z^n$ を満たすとする。もし $n \geqq 3$ ならば x, y, z のどれかは 0 である。」

そして彼は，この命題の「真に驚くべき証明」を見つけたが,「それを書くための十分な余白がない」と述べている。これが **フェルマー予想** であり，その後，多くの人達が挑戦し，最終的に 1995 年に，アンドリュー・ワイルズによって証明された。

図 1.1: Pierre de Fermat (1601〜1665)

フェルマーの研究は，その後，オイラー，ガウスらによって発展し，整数論の基礎が築かれた。

古くから知られている整数についての問題として，次のようなものがある。

(1) p を素数とする。p は常に $2^{p-1} - 1$ を割り切るか？

(2) p^3 が $2^{p-1} - 1$ を割り切るような素数 p は存在するか？

(3) 2 よりも大きい偶数は，必ず 2 つの素数の和として書けるか？(ゴールドバッハ (Goldbach) の予想)

(4) 8 と 9 以外に，素数の冪が隣り合った数となるものはあるか？(カタラン (Catalan) の予想)

(5) $p, p + 2$ という形の 2 つの素数の組は無限に多くあるか？

(6) 任意の自然数 $n \geqq 1$ に対して，$n + 1$ から $2n$ の中に必ず素数が存在するか？（ベルトラン (Bertrand) の予想）

(7) 任意の自然数 $n \geqq 1$ に対して，n^2 から $(n + 1)^2$ の中に必ず素数が存在するか？

(8) $2^p - 1$ がまた素数であるような素数 p は無限に多くあるか？

(9) $2^{2^n} + 1$ という数は全て素数か？

(10) 自分自身よりも小さな約数を全て加えた和がその数自身と一致する時，それを **完全数** という。 奇数の完全数は存在するか？

これらの問題に関して，現在までのところ，次のようなことが知られている。

(1) については，成立することがフェルマーによって証明された。これが上記のフェルマーの小定理である。

(2) は未解決である。すなわち，p^3 が $2^{p-1}-1$ を割り切るような素数 p は一つも見つかっていないし，そのようなものが存在しないことも証明されてはいない。

(3) も有名な問題であるが，200 年以上にわたって未解決である。

(4) Preda Mihăilescu が 2002 年に解決した。彼は「隣り合った素数の冪は $8=2^3$ と $9=3^2$ 以外には存在しない。」ということを証明した。

(5) は「双子素数問題」として知られているが，やはり未解決である。

(6) チェビシェフ (Chebyshev) が 1850 年に肯定的に証明した。

(7) 未解決である。

(8) も未解決である。 2^n-1 という形の数を **メルセンヌ数** と言い，$M(n)$ あるいは M_n という記号で表す。n が合成数なら，M_n は必ず合成数である。

p が素数の場合，M_p は素数となることもあれば合成数となることもある。M_p が素数になる時，この M_p を **メルセンヌ素数** という。

$$M_2=2^2-1=3 \quad M_3=2^3-1=7 \quad M_5=2^5-1=31 \quad M_7=2^7-1=127$$

はメルセンヌ素数だが，$M_{11}=2^{11}-1=2047=23\times 89$ は素数ではない。

図 1.2: Marin Mersenne (1588〜1648)

p が素数であっても，ほとんどの場合 M_p は素数ではないのだが，非常に大きな素数 p に対して，M_p が素数になることがある。

現在知られている最大の素数は，2008 年 8 月に見つかった，45 番目に発見されたメルセンヌ素数，

$$M_{43,112,609}=2^{43,112,609}-1$$

であり，12,978,189 桁 の数である。（全てのメルセンヌ素数の中で小さい方から 45 番目ということではない。）

これは，GIMPS (The Great Internet Mersenne Prime Search) という，世界中のネットワークに繋がれたＰＣに膨大な計算を分散させることにより，巨大なメルセンヌ素数を見つけ出そうというプロジェクトによって発見された (**http://www.mersenne.org**) 。この 45 番目は，UCLA 数学科の Edson Smith らが発見した。

1000 万桁の素数には，10 万ドルの賞金がかかっていたが，これにより，UCLA 数学科が 50,000 ドルを受け取り，25,000 ドルを，これ以前の 6 個のメルセンヌ素数発見者が受け取り，残り 25,000 ドルはチャリティーに寄付された。

なお，メルセンヌ素数が無限にあるかどうかは知られていない。1000 万桁の数まで探しても，メルセンヌ素数はせいぜい 50 個程度しか見つからない，というのは，かなりの少なさではある。ほとんどの素数 p に対して M_p は合成数になるわけだが,「合成数であることがわかっている」ということと,「その数の素因数が全てわかっている」ということは大きく異なる。

例えば，かなり小さな素数 **971** について M_{971} は素数ではなく合成数であることは，かなり前からわかっていたが，この 290 桁程度の数の 1 つの素因数 (53 桁) が初めて見つかったのは 2004 年である。

(9) まず一般に，a^{b^c} と書いたら，これは，$a^{(b^c)}$ を意味する。なぜなら，もしこれが $(a^b)^c$ なら，それは a^{bc} と等しくなるからである。

さて，$2^{2^n}+1$ という形の数を **フェルマー数** と言い，F_n と書く。というのも，この形の自然数は全て素数であろう，と予想したのがフェルマーだったからである。

しかしこの問題は，オイラーによって否定的に解決された。オイラーは，

$$F_5 = 2^{2^5}+1 \;=\; 2^{32}+1 \;=\; 4294967297 \;=\; 641\times 6700417$$

となること，すなわち $F_5 = 2^{2^5}+1$ は素数ではない，ということを示した。ちなみにこれは素因数分解であり，この 2 つの数は素数である。

実は，フェルマーの予想とは裏腹に，フェルマー数で素数であることがわかっているのは，$n = 0, 1, 2, 3, 4$ の場合だけである。すなわち，

$$F_0 = 2^{2^0}+1 = 3 \qquad F_1 = 2^{2^1}+1 = 5 \qquad F_2 = 2^{2^2}+1 = 17$$
$$F_3 = 2^{2^3}+1 = 257 \qquad F_4 = 2^{2^4}+1 = 65537$$

は素数であるが，それ以外の n について，知られているものは全て合成数である。例えば，

$F_6 = 2^{2^6}+1 \;=\; 18446744073709551617 = 274177\times 67280421310721$

(1880 年に Ｆ. ランドリー (当時 82 歳) が示した。)

$F_7 = 2^{2^7}+1 \;=\; 340282366920938463463374607431768211457$

$\;=\; 59649589127497217\times 5704689200685129054721$

(1975 年に ブリルハートとモリスン が示した。
しかし，この数字は本を見て書いたのではなく，
ＰＣ上の Mathematica で数分計算したら出てきたものである。)

となる。これらもやはり素因数分解である。これを見ると，不思議なことに，フェルマー数は，かなり大きな素因数のみを持ち，なかなか因数分解しずらい数であることがわかる。フェルマーがこれらを合成数であると見抜けなかったことは無理もない。実際フェルマー数は，因数分解プログラムのテストに使われる。

現在までのところ，$5 \leqq n \leqq 32$ については，F_n は合成数であることがわかっているが，完全に因数分解されているのは F_{11} までである。そして F_{14} という，4933 桁 の数については，合成数であることは 1963 年に証明されたが，その素因数は一つも知られていない。

F_{33}, F_{34}, F_{35} については，合成数であるのか素数であるのかすらわかっていないが，F_{36}, F_{37}, F_{38}, F_{39} は合成数であることがわかっている。

現在の時点で，合計 226 個のフェルマー数が合成数であることが知られている。その中で最大のものは $F_{2478782}$ であり約 10^{746187} 桁 の数である。(746187 桁ではないことに注意。ちなみに，賞金がかかっていた素数の 1000 万桁 というのは 10^7 桁 のことである。)

(**http://www.prothsearch.net/fermat.html** 参照)

p を素数とした時，正 p 角形が定規とコンパスだけで作図可能であるためには，p はフェルマー数でなければならない，ということが知られている。すなわち，p が素数で $p < 2^{2^{33}} + 1$ の時，正 p 多角形で作図できるのは，

$$p = 3,\ 5,\ 17,\ 257,\ 65537$$

だけである。ちなみに，正 3 角形，正 5 角形の作図法はユークリッドの時代から知られていたが，正 17 角形の作図法を発見したのは，ガウス (当時 19 歳) である。

(10) 例えば，

$$\begin{aligned} 6 &= 1+2+3 \\ 28 &= 1+2+4+7+14 \\ 496 &= 1+2+4+8+16+31+62+124+248 \end{aligned}$$

などは完全数である。実は，$2^n - 1$ が素数ならば $2^{n-1}(2^n - 1)$ は完全数であることは，紀元前 300 年の「ユークリッド原論」にすでに書かれている。また，偶数の完全数はこの形のもの以外には存在しないことは，オイラーによって証明された。しかし，奇数の完全数はこれまで一つも見つかっていないし，そのようなものが存在しないことも証明されていない。ただ，奇数の完全数があれば，それは 300 桁以上でなければならない，ということはわかっている。

1.6 ユークリッド 互除法

2 つの自然数の最大公約数を計算するための効率的な方法として，**ユークリッド 互除法** というものがある。これはその名のとおり，2300 年前に書かれた「ユークリッド原論」にすでに書かれてある。そのプロセスは以下のとおりである。

(1) まず，$n_0 > n_1$ を 2 つの自然数とする。n_0 を n_1 で割った商を q_1 とし，余りを n_2 とすると，$n_0 = q_1 n_1 + n_2$ であり，$0 \leqq n_2 \leqq n_1 - 1$ である。

(2) $n_2 = 0$ なら $n_0 = q_1\, n_1$ なので，$n_1 = GCD(n_0, n_1)$ である。

(3) $n_2 > 0$ なら，$GCD(n_0, n_1) = GCD(n_1, n_2)$ である。なぜならこの時，$n_0 = q_1\, n_1 + n_2$ なので n_0 は $GCD(n_1, n_2)$ の倍数であり，このことから $GCD(n_0, n_1) \geqq GCD(n_1, n_2)$ がわかる。また，$n_0 - q_1\, n_1 = n_2$ であるから，n_2 は $GCD(n_0, n_1)$ の倍数なので，$GCD(n_0, n_1) \leqq GCD(n_1, n_2)$ でなければならない。従って $GCD(n_0, n_1) = GCD(n_1, n_2)$ でなければならない。

(4) これにより，$GCD(n_0, n_1)$ を求める問題は，より小さな数のペアに対して $GCD(n_1, n_2)$ を求める問題へと置き換えられたことになる。あとは，このプロセスを繰り返せば良い。

(5) $GCD(n_0, n_1) = GCD(n_1, n_2)$ であるから，プロセスを繰り返しても，ペアの最大公約数は変わらない。

$n_i = q_{i+1}\, n_{i+1} + n_{i+2}$ となった時，

$n_{i+2} \neq 0$ **ならば：** $GCD(n_i, n_{i+1}) = GCD(n_{i+1}, n_{i+2})$ となり，その時はプロセスを続けることになる。

$n_{i+2} = 0$ **ならば：** $n_i = q_{i+1}\, n_{i+1}$ なので，$GCD(n_i, n_{i+1}) = n_{i+1}$ となり，n_{i+1} が最大公約数となる。

(6) $n_i > n_{i+1} > n_{i+2}$ なので，プロセスが進めば，数は必ず減少して行くので，このプロセスは有限回で終了する。

最後まで余りが 0 にならないなら，最後は余りが 1，すなわち $n_i = q_{i+1}\, n_{i+1} + 1$ となるが，これは，$GCD(n_i, n_{i+1}) = GCD(n_{i+1}, 1) = 1$ となり，最初の n_0 と n_1 が互いに素であることを示している。

例: $GCD(2397, 64515)$ を求めてみよう。

- $64515 = 26 \cdot 2397 + 2193$ であるから，
  $GCD(2397, 64515) = GCD(2193, 2397)$ である。
- $2397 = 1 \cdot 2193 + 204$ であるから，
  $GCD(2193, 2397) = GCD(204, 2193)$ である。
- $2193 = 10 \cdot 204 + 153$ であるから，
  $GCD(204, 2193) = GCD(153, 204)$ である。
- $204 = 1 \cdot 153 + 51$ であるから，
  $GCD(153, 204) = GCD(51, 153)$ である。
- $153 = 3 \cdot 51$ であるから，$GCD(51, 153) = 51$ である。
- 以上から，$GCD(2397, 64515) = 51$ がわかった。

このアルゴリズムの計算量を考えてみよう。

Case 1: $n_1 > \dfrac{n_0}{2}$ の場合。

この時は明らかに $q_1 = 1$ であり，$n_0 = n_1 + n_2$ となるので，

$$n_2 = n_0 - n_1 < n_0 - \frac{n_0}{2} = \frac{n_0}{2}$$

となる。

Case 2: $n_1 \leqq \dfrac{n_0}{2}$ の場合。

この時も，$n_2 < n_1 \leqq \dfrac{n_0}{2}$ となる。

以上から，どちらの場合であっても，$n_2 < \dfrac{n_0}{2}$ となる。すなわち，このプロセスを 2 回行うことにより，n_{i+2} は n_i の 1/2 倍以下となる。

n_0 が大体 $n_0 = 2^\alpha$ 位の数であるなら，n_2 は $2^{\alpha-1}$ 以下の数であり，n_4 は $2^{\alpha-2}$ 以下の数であり，これが続いて行く。従って，この操作を 2α-回 行えば，$n_{2\alpha}$ は 1 以下となり，どんな場合でも，操作は終了する。

$\alpha = \log_2 n_0$ であるから，多くとも $2\log_2 n_0$ 回の操作で，最初の数の最大公約数に到達する。

例えば，RSA 暗号などで使われる 200 桁くらいの数を考えてみよう。まず，200 桁程度の割り算はほとんど計算時間はかからない。また，10 進数で 200 桁くらいの数は 2 進数で見ると 660 桁くらいなので，これを大きな方とする 2 つの数についてユークリッド互除法を適用すると，多くても 1300 回程度のプロセスで最大公約数が見つかることになる。これは現在の計算機にとっては，極めて短時間で計算できる程度のものである。このアルゴリズムは，以下の既約剰余類の逆元の計算に使われるなど，RSA 暗号を実現する上で最も重要なものである。

演習問題 1.8　2 つの自然数 m, n を入力すると，その最大公約数 $GCD(m, n)$ を出力するプログラムを作れ。可能なものは BigInteger クラスを用いていくらでも大きい自然数に対応可能なものを作れ。