約数の和に関する未解決の問題*

京都大学数学教室 山田智宏 (Tomohiro Yamada)

$\sigma(N)$ を N の（自分自身も含めた）約数の和とする。$\sigma(N)$ の性質については、多くの問題が提起され、多くの研究がなされてきた。とくに $\sigma(N)=2N$ を満たす N は完全数と呼ばれ、古くから関心を持たれていた。$N=6,28,496...$ などがその一例である。

Euclid は 2^m-1 （ m は整数）が素数ならば $2^{m-1}(2^m-1)$ は偶数の完全数であることを示し、Euler は偶数の完全数は常にこの形になることを示した。したがって、偶数の完全数の問題は Mersenne 素数の問題に帰着する。これに対して、奇数の完全数は、それが存在するかどうかすら未だ解決されていない。これが $\sigma(N)$ の性質に関する未解決の問題の代表例だろう。

$N=p_1^{e_1}\cdots p_k^{e_k}$ （ $p_1,\cdots,p_k$ は相異なる素数）と素因数分解すると、

$$\sigma(N)=\frac{p_1^{e_1+1}-1}{p_1-1}\cdots\frac{p_k^{e_k+1}-1}{p_k-1} \tag{1}$$

と表せるから、$\sigma(N)$ の性質を研究するうえでは

$$\sigma(p^e)=\frac{p^{e+1}-1}{p-1} \tag{2}$$

あるいは多項式

$$x^e+\cdots+x+1=\frac{x^{e+1}-1}{x-1} \tag{3}$$

のとる値の数論的性質の研究が重要であると考えられる。ここでは、筆者がこの性質について考え、気になったけれども解決の難しいと思われる問題について記したい。

もっとも基本的な問題は

$$\frac{x^m-1}{x-1}=y^n \tag{4}$$

となる (x,m,y,n) （自明な例を除くため、 $x,y,n\geq 2, m\geq 3$ とする）を求める問題である。これには $(3,5,11,2),(7,4,20,2),(18,3,7,3)$ が知られており、それ以外には存在しないと予想されているが、未だ解決されていない。(4) ははじめ、Nagell と Ljunggren によって研究されたことから、Nagell-Ljunggren 方程式と呼ばれている。4 つの変数 x,m,y,n のうち x,m,y のいずれか 1 つを固定すれば、解を全て求めることが原理的に可能であることは知られている（[8]）。

m が合成数のとき、p を m の素因数とすると、

$$\frac{x^p-1}{x-1}=p^l y^q (l\in\{0,1\}) \tag{5}$$

となることが知られている。Bugeaud, Hanrot, Mignotte, Mihailescu はもしこの式が満足されるなら、 $p\geq 29$ であることを示した ([1] および [6])。[1] の方法は、2 変数の対数一次形式に関する Laurent, Nesterenko, Mignotte の結果 [4] を使い q に対する上界（[1] の定理 5）を得た後、やや特殊な方法で (x,y) に関する上界（[1] の定理 6）を得、続いて lattice reduction の方法を使うものである（lattice reduction についての詳細は原論文である [3] を、その不定方程式への応用についての詳細は [7] を参照）。残る状況については [6] が類数条件を用いて解決した。

---

*2000 Mathematics Subject Classification: 11A05(Primary) 11A25, 11D61(Secondary).

筆者が気になった問題は (4) の一般化として、k を与えられた整数としたときに

$$\frac{x^m-1}{x-1}=y_1^{e_1}y_2^{e_2}\cdots y_k^{e_k} \tag{6}$$

を満たす $(x, m, y_1, \cdots, y_k, e_1, \cdots, e_k)$ の非自明なものを全て求めるという問題である。

m および $y_1, \cdots, y_k$ の全てを固定した時にこれを満たす非自明解が有限個しかなく、しかもそれらを全て求めることが原理的には可能であることは知られている（[8] を参照）。しかし、 $k \geq 2$ のときには、 m を固定しただけでは解の有限性を示すことは今のところ出来ていない。

対数一次形式に関する Matveev の結果 [5] を使えば、 $y_1, \cdots, y_k$ のうちの $k-1$ 個と m とを固定すれば、(6) の非自明解は有限個であり、全て求める事が原理的に可能であることを示す事ができるが、実際には $e_1, \cdots, e_k$ の上界が非常に大きいため、全ての非自明解を求める事は現在の計算機では不可能と思われる。

$k=2$ でかつ、$m \equiv 3 \pmod 4$ のときは、問題は 2 変数の対数一次形式に帰着することができ、したがって Laurent, Nesterenko, Mignotte の結果を用いてより強い評価を得ることができる。しかし、最も簡単な事例である $(m, y_1)=(3, 7)$ 、すなわち方程式 $x^2+x+1=7^{e_1}y^{e_2}$ の場合でさえも、この方法は e_1, e_2 に対しては良い評価（ 10^4 以下）を与えるが、(x, y) に対しては lattice reduction を用いても得られる評価は非常に大きく、 $e_1 \leq e_2 = 11$ の場合でさえ、その上界は 10^{1000} を超えてしまう。これは $k=1$ のときに [1] で用いられた独自の方法が使えないためである。

したがって、 $k=2$ で m および y_1 が固定されているときでさえ、(6) の非自明な解を全て求めることは非常に難しいといえる。さしあたってはこの場合に [1] の定理 6 に相当するような (x, y) の上からの評価を与えることのできる還元法を考えていきたい。

References

[1] Y. Bugeaud, G. Hanrot and M. Mignotte, Sur l'équation diophantienne $\frac{x^n-1}{x-1}=y^m$, III, *Proc London Math. Soc.***84** (2002), 59–78.

[2] Y. Bugeaud and P. Mihailescu, On the Nagell–Ljunggren equation $(x^n-1)/(x-1)=y^q$, *Math. Scand.*, to appear.

[3] A. K. Lenstra, H. W. Lenstra, Jr. and L. Lovász, Factoring polynomials with rational coefficients, *Math. Ann.* **261**(1982), 515–534.

[4] M. Laurent, Y. Nesterenko and M. Mignotte, Formes linéaires en deux logarithmes et déterminants d'interpolation, *J. Number Theory* **55**(1995), 285–321.

[5] E. M. Matveev, An explicit lower bound for a homogeneous rational linear form in the logarithms of algebraic numbers II, *Izv. Math.* **64**(2000), 1217–1269.

[6] P. Mihailescu, Class number conditions for the diagonal case of the equation of Nagell-Ljunggren, preprint.

[7] B. M. M. de Weger, Algorithms for diophantine equations, CWI tract 65, Centrum voor Wiskunde en Informatica, Amsterdam, 1989.

[8] T. N. Shorey and R. Tijdeman, Exponential Diophantine equations, Cambridge Tracts in Mathematics 87, Cambridge University Press, 1986.

Tomohiro Yamada
Department of Mathematics,
Graduate School of Science,
Kyoto University, Kyoto, 606-8502, Japan
e-mail: `tyamada@math.kyoto-u.ac.jp`