

Carmichael 数の計算

岡山大学 理 頼永 正春

Fermat の小定理の逆が成り立たないような整数, 即ち,
 $(a, n) = 1$ となるすべての正整数 a に対して,
 $a^{n-1} \equiv 1 \pmod{n}$ が成り立つような合成数 n を絶対擬
素数または Carmichael 数という.

Carmichael 数を数値的に求めるには, 現在のところ,
次の Chernick の定理が唯一の拠所である.

定理 1. (J. Chernick [2]) 正整数 n が
Carmichael 数であるための必要十分条件は n が相異なる
3 個以上の奇素数 $p_1, p_2, \dots, p_k$ の積であって, 各素因
数 p_i ($i = 1, 2, \dots, k$) に対して, $n \equiv 1 \pmod{p_i - 1}$
を満たすことである.

L. E. Dickson [3] によれば, 1910 年頃に, Carmichael
自身がすでにこの定理に気付いていたらしく, 数個の
Carmichael 数を見つけているようである. しかし,

Carmichael の論文が手に入らないので、詳しい事は分らない。

この定理により、Carmichael 数を計算機上で求めることが原理的に可能となる。しかしながら、Chernick の定理を単に用いるだけではあまりよい効率を得られない。計算の効率を高めるために、種々の方法が提案されている。要するに計算に好都合な必要条件を導き出し、それを 'ふるい' として用い、得られた候補に対して Chernick の定理を適用する。特に次の定理は極めて有用である。

定理 2. 整数 n が Carmichael 数で、 p が n の 1 つの素因数ならば、 n は $px+1$ の形の素因数を含まない。

以下、Carmichael 数を計算するいくつかの方法と最近までの結果を紹介する。

1°. Beeger の方法. N. G. W. H. Beeger [1] は $n = pqr$ (p, q, r は素数) の形の Carmichael 数を求める方法を提案した。

先づ、Chernick の定理により、ある正整数 x, y に対して、

$$pq = 1 + (r-1)x, \quad pr = 1 + (q-1)y \quad (1)$$

であるから、これより、 r を消去して

$$q = 1 + (p-1)(p+x)/(xy-p^2) \quad (2)$$

を導く。また、 p に対して、 g, r の取り得る値の範囲を調べ、結局、(2)式において、与えられた素数 p に対して、 $x = 2, 3, \dots, p-2$ に対して、 g を求め、(1)式から r を決定する。

Beeger はこの方法により、 $p = 3, 5, 7, \dots, 43$ に対して 54個の Carmichael 数を求めた。Beeger の方法で、 p を与えられた時、 pg^r が Carmichael 数となるような g, r ($p < g < r$) が存在しない事がある。 $p \leq 1000$ の範囲には $p = 11, 197$ の 2例がある。

Beeger の方法は N を平方因子を含まない奇数として、 Ngr (g, r は素数、 $g, r > N$ の素因数) の形の Carmichael 数を求める方法に拡張できる。しかし、この時、 g, r の取り得る値の大きさは、一般に、 g は N^2 のオーダーに、 r は N^3 のオーダーになるので、 N が大きくなると g, r の素数性の判定に時間がかかり、次第に効率が悪くなる。

筆者は g, r がオーバーフローしないという制限 ($< 2^{34}$) の下で $N \leq 6000$ について計算を実行した。(岡山大学計算機センタ, ACOS 700 を使用)

2°. 普遍形式による方法。 M を非負の整数値をとるパラメーターとし、 α_n を n 個 ($n \geq 3$) の相異なる $a_i M + b_i$ の形の奇数の積とする。すべての M の値に対して、合同式

$U_n \equiv 1 \pmod{a_i M + b_i - 1} \quad (i=1, 2, \dots, n)$ が成り立つとき, U_n を普遍形式 (universal form) という.

ある M に対して, すべての因数 $a_i M + b_i$ が素数ならば, Chernick の定理から, U_n は Carmichael 数である.

Chernick はこの普遍形式を用いて, かなりの個数の Carmichael 数を求めた.

最近, S.S. Wagstaff [7] は次の普遍形式

$$U_3(M) = (6M+1)(12M+1)(18M+1)$$

を用いて 321 桁の Carmichael 数を見つけた. 以下に, その M の値と, $U_3(M)$ の値を紹介する.

$M =$ 73 28517132 62373770 42833051 15698260 79825001 98696237
 26846779 39558839 14228225 25876339 63462201 59279282 85851850
 $U =$ 5 10097651 43959249 35442924 80932774 56279161 66422617
 58239613 10579841 88849784 22849780 91128590 55248262 18356898
 74002783 53571488 38474305 31105418 73196218 42459950 73938057
 88336374 85286596 13137137 81439007 23170631 02191638 94923024
 77317009 21197794 18509950 24840245 83806981 77310433 20215974
 89437261 95369370 82075885 79386408 51976601

この Carmichael 数は現在, 知られているものの中で最大であると思われる. 因みに, それまでの記録は J.R. Hill [5] の 77 桁の Carmichael 数であった.

3° 2 進数に対応させる方法. 整数 $N = 3^{e_1} 5^{e_2} \dots p_t^{e_t}$

($e_i = 0$ または 1) に 2 進数 $b = e_t e_{t-1} \dots e_2 e_1$ を対応させ、平方因子を含まない奇数を組織的に発生させる方法である。この方法は結局、最大の素因数 p を与えたとき、 N は平方因子を含まない奇数で、 N の素因数が p より小で、 Np が Carmichael 数となるような N を求めることである。この方法は比較的小さい素因数を数多く含むような Carmichael 数を求めるのに好都合である。筆者の実験で得た最大のものは次の 15 個の素因数からなる 27 桁の Carmichael 数である。

$$11 \cdot 29 \cdot 31 \cdot 37 \cdot 41 \cdot 43 \cdot 61 \cdot 71 \cdot 73 \cdot 79 \cdot 97 \cdot 113 \cdot 127 \cdot 131 \cdot 151 \\ = 433\ 65633789\ 34455936\ 09056001$$

4° 最大素因数を求める方法。上の 3° とは逆に、先ず、整数 N を与えて、 Np が Carmichael 数となるような p を求める方法である。Chernick の定理から、 $p-1$ は $N-1$ の約数であるから、 $N-1$ を素因数分解して、 $N-1$ の約数を組織的につくり出し、その中から、1 を加えたものが素数となるようなものを探すと、 Np が Carmichael 数の候補となる。あとは、Chernick の定理により検証すればよい。

5° ある区間内の Carmichael 数の個数。Carmichael 数の分布を調べる上で、ある区間内の Carmichael 数の個数を知ることは重要である。

さて、方法3° $\in N \leq \bar{N}$ まで実行し、方法4° $\in p \leq \bar{p}$ まで実行したとする。今、 Np $\in$ Carmichael 数とする。

もし、 $N \leq \bar{N}$ ならば、 Np は方法3° で求められている。
また、もし、 $p \leq \bar{p}$ ならば、 Np は方法4° で求められている。従って、 $\bar{N}\bar{p}$ を越えない Carmichael 数は方法3° か方法4° のどちらかで求められている。

実際に、筆者は 方法3° $\in \bar{p} = 151$ 、方法4° $\in \bar{N} = 50251257$ まで実行した。従って、 $\bar{N}\bar{p} = 7587939807$ 以下のすべての Carmichael 数が求まったことになる。

方法3° で限界 $\bar{p} = 151$ をふやすことはやや困難である。
そこで、 $N \leq 2^{31}$ の制限の下で $\bar{p} = 199$ まで実行した。

ところが、 $2^{31} \cdot 151 = 3.24 \times 10^{10}$ であるから、もし、探索の範囲 10^{10} 内では、この制限下の計算は方法3° と同値である。従って、

$$\bar{N}\bar{p} = 50251257 \times 199 = 10000000143 \geq 10^{10}$$

となり、結局 10^{10} 以下のすべての Carmichael 数が求まったことになる。

副産物として、 10^{10} 以上の Carmichael 数がかたりの個数得られたが、現在、筆者の手にある Carmichael 数の分布については以下の表の通りである。（実際には、20,000 個以上の Carmichael 数を得たが、まだ、整理中であるので、

この表は中間報告である)

Bound	Number of C. N.	Logarithmic Ratio
N	C(N)	$\log C(N)/\log N$
10^3	1	-----
10^4	7	0.2113
10^5	16	0.2408
10^6	43	0.2722
10^7	105	0.2887
10^8	255	0.3008
10^9	646	0.3122
10^{10}	1547	0.3189
10^{11}	3360	0.3205
10^{12}	5584	0.3122
10^{13}	7017	0.2954
10^{14}	8201	0.2789
10^{15}	9113	0.2633

なお, P. Erdős [4] は Carmichael 数の分布について,
次のような予想をしている. $C(N) \leq N$ 以下の Carmichael
数の個数とするとき,

$$\log C(N) / \log N \rightarrow 1 \quad (N \rightarrow \infty)$$

しかし, 筆者の実験はこの予想とは一致しない. また,
Wagstaff も $C(N)$ についてのある予想を述べているが, 現在
検討中である.

参考文献

- [1] N. G. W. H. Beeger : On composite number n for which $a^{n-1} \equiv 1 \pmod{n}$ for every a prime to n . Script Math., 16(1956), 133-135.
- [2] J. Chernik : On Fermat's simple theorem. Bull. Amer. Math. Soc. 45(1939), 269-294
- [3] L. E. Dickson : History of the theory of numbers. vol. I. Chelsea Publ. Co. (1952)
- [4] P. Erdos : On pseudoprimes and Carmichael numbers, Publ. Math. Debrecen. 4(1956), 201-206.
- [5] J. R. Hill : Large Carmichael numbers with three prime factors, Not. Amer. Math. Soc. 26(1979), A-374.
- [6] M. Yoninaga : Numerical computation of Carmichael numbers, Math. J. Okayama Univ. 20(1978), 151-163 and 21(1979).
- [7] S. S. Wagstaff : Large Carmichael numbers, Math. J. Okayama Univ. 22(1979).