A-006

疑似平方数に基づいた素数判定とカーマイケル数との関係

Relationship between Primality Testing Based on Pseudosquares and Carmichael Numbers

神保 秀司†
Shuji JIMBO

1 はじめに

素数 p に対する疑似平方数 L_p とは，次の 2 条件を満たす平方数でない最小の正整数である．(1) L_p-1 は 8 の倍数であり，(2) $2<q\leqq p$ を満たす各素数 q について整数 m が存在して L_p-m^2 は q の倍数である．上の (2) は平方剰余についての Legendre の記号を使って次のように表すことができる．(2′) p 以下のすべての奇素数 q について $\left(\frac{L_p}{q}\right)=1$ が成り立つ．定義より，L_p は平方数ではないが，p 以下のどの素数を法としたときも平方数として振る舞う．これ以降，最初の素数を $p(1)=2$ で表し，k 番目の素数を $p(k)$ で表す．

奇素数 p に対する関数値 L_p について，計算機実験の結果に基づいて L_p が p に対して指数関数的に増加することが予想されていて，Lukes らにより，この予想を前提とした高速な確定的素数判定アルゴリズムが提案されている [2]．その中で使われている判定条件のうちの 1 つの必要性について考察し，この判定条件とカーマイケル数の間の関係についての予想を提案する．

2 疑似平方数に基づいた素数判定条件とカーマイケル数

Lukes らは，与えられた奇数 n が素数か，または，素数の累乗であるための次の必要十分条件を与えた [2]．

定理 1 n は 1 より大きい奇数であるとし，B は正整数であるとし，p は素数であるする．このとき，次の条件がすべて成り立てば，n は素数か，または，素数の累乗である．

(1) n の素因数は，すべて B より大きい．

(2) $n<BL_p$ が成り立つ．

(3) $q\leqq p$ を満たすすべての素数 q について $q^{(n-1)/2}\equiv\pm1 \pmod n$ が成り立つ．

(4) $n\equiv5 \pmod 8$ のとき $2^{(n-1)/2}\equiv-1 \pmod n$ が成り立ち，$n\equiv1 \pmod 8$ のとき $r^{(n-1)/2}\equiv-1 \pmod n$ および $r\leqq p$ を満たす奇素数 r が存在する．

以下，$f(n)=O(g(n)(\log g(n))^m)$ を満たす正整数 m が存在することを $f(n)=\tilde{O}(g(n))$ で表す．また，非負整数 n のサイズを n の 2 進桁数とし，$l(n)$ で表す．定理 1 に現れる定数 B の値は，実質的にアルゴリズム全体の計算時間のオーダに影響しないと考えられるため，以下 $B=1$ と仮定する．さらに，与えられた正整数 n に対して，$n<L_{p(k)}$ を満たす最小の正整数 k を $k(n)$ で表す．入力 n に対する定理 1 に基づいたアルゴリズムの計算時間を $T(n)$ で表したとき，$T(n)=\tilde{O}(k(n)(l(n))^2)$ が成り立つことが知られている [2]．現在 $L_{p(k)}$ の値が正確に求まっている k の最大値は，$k=74$ であり，$L_{p(74)}=L_{373}=42350252230805975035193 29$ である [3]．

以下，4 の倍数足す 1 の形で素数の累乗でない合成数 n を定理 1 によって合成数であると判定する場合の条件 (4) の必要性について検討するために次の条件 A を満たす正整数 n の存在を計算機実験により調査した．実験で使ったプログラムの作成には，プログラミング言語として C を採用し，Gnu MP (GMP) ライブラリを利用した．

条件 A n は，異なる素因数をもつ (単一の素数の累乗でない) 奇数の合成数であり，かつ，$p=p(k(n))$ とおいたとき定理 1 の条件 (3) を満たす．

この実験の結果，$n<10^7$ の範囲で条件 A を満たす整数 n は，次の 5 つであることが判明した．$488881=37\cdot73\cdot181$, $3057601=43\cdot211\cdot337$, $3828001=101\cdot151\cdot251$, $6189121=61\cdot241\cdot421$, $9439201=61\cdot271\cdot571$. 上に挙げた素因数分解と下に挙げた定理 2 より，これら 5 つの整数は，すべてカーマイケル数 (Carmichael number) である．

† 岡山大学大学院自然科学研究科
Graduate School of Natural Science and Technology, Okayama University

正整数 n がカーマイケル数であるとは，$1 < a < n$ および $\gcd(a, n) = 1$ を満たすすべての整数 a について $a^{n-1} \equiv 1 \pmod{n}$ が成り立つことである．カーマイケル数について次の定理が知られている．

定理 2 次の条件は，合成数 n がカーマイケル数であるための必要十分条件である．

> n のすべての素因数 p に対して，$p-1 \mid n-1$ ($n-1$ は $p-1$ の倍数である) および $p^2 \nmid n$ (n は p^2 の倍数でない) が成り立つ．

さらに n を 10^{12} 未満の 8241 個のカーマイケル数について条件 A の成立を調べたところ，条件 A を満たすものが 517 個存在することが判明した．興味深いのは，これら 517 個のうち 8 を法として 5 と合同であるものが 6236982181, 43025053501, 613976914981 の 3 つのみであることである．

n をカーマイケル数とし，その素因数分解を $n = p_1 p_2 \cdots p_m$，$p_1 < p_2 < \cdots < p_m$，で表す．$p = p(k(n))$ とおいて次の 2 条件が成り立てば，n は条件 A を満たす．これは，定理 2 と中国剰余定理から容易に導くことができる．

条件 B1 $p < p_1$,

条件 B2 すべての $q \in \{p(1), p(2), \ldots, p(k(n))\}$ とすべての $i \in \{1, 2, \ldots, m\}$ について $q^{(p_i-1)/2} \equiv 1 \pmod{p_i}$ が成り立つ．

条件 B1 および B2 を満たすカーマイケル数を見付けるために，カーマイケル数を導く次の多項式 $U_3(m)$ に着目する [1].

定理 3 任意の正整数 m に対して，$6m+1$，$12m+1$，および $18m+1$ がすべて素数であるなら，

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

はカーマイケル数である．

なお，$U_3(m)$ の形のカーマイケル数が無限に多く存在することが予想されているが，未解決である．

$6m+1$，$12m+1$，および $18m+1$ がすべて素数であり，$L_{p(73)} \leqq U_3(m) < L_{p(74)}$ および $p(74) < 6m+1$ を満たし，かつ，$n = U_3(m)$ が条件 B2 を満たす正整数 m を計算機実験により次のように探索した．$m_0 = 14128869$ とおき，$m_1 = 14839422$ とおいたとき，$U_3(m_0 - 1) < L_{p(73)} = L_{367} < U_3(m_0)$ および $U_3(m_1) < L_{p(74)} = L_{373} < U_3(m_1 + 1)$ が成り立ち，さらに，$p(74) = 373 < 84773215 = 6m_0 + 1$ が成り立つので，$m_0 \leqq m \leqq m_1$ を満たす整数 m で，$6m+1$，$12m+1$，$18m+1$ がすべて素数であり，かつ，$U_3(m)$ が条件 B2 を満たすものを探せばよい．その結果，そのような整数 m は，1815 個存在することが判明した．そのうちの最小のものと最大のものを，それらに対応する $U_3(m)$ の値とともに下に挙げる．

$$\begin{aligned} m_{\min} &= 14128946, \\ U_3(m_{\min}) &= 365539494380103287828349, \\ m_{\max} &= 14839376, \\ U_3(m_{\max}) &= 423498550128100744968172 9. \end{aligned}$$

一方，$m_0 \leqq m \leqq m_1$ を満たす整数 m で $6m+1$，$12m+1$，$18m+1$ がすべて素数でありながら $U_3(m)$ が条件 B2 を満たさないものは，全く存在しないことが判明した．従って，$6m+1$，$12m+1$，および $18m+1$ がすべて素数であり，かつ，$L_{p(73)} \leqq U_3(m) < L_{p(74)}$ を満たす整数 m と $1 \leqq k \leqq 74$ を満たす整数 k の組 (m, k) すべてについて，

$$(p(k))^{(U_3(m)-1)/2} \equiv 1 \pmod{U_3(m)}$$

が成り立つ．

以上の議論に基づいて次の 2 つの予想を提案する．

予想 1 $m \geqq m_0$，かつ，$6m+1$，$12m+1$，および $18m+1$ がすべて素数である任意の整数 m について，$n = U_3(m)$ は条件 B1 および B2 を満たす．

予想 2 条件 A を満たす正整数は，すべてカーマイケル数である．

謝辞

本研究は科研費 JSPS 24650007 の助成を受けたものである．

参考文献

[1] J. Chernick. On Fermat's simple theorem. *Bull. Amer. Math. Soc*, Vol. 45, No. 269–274, p. 5, 1939.

[2] R. F. Lukes, C. D. Patterson, and H. C. Williams. Some results on pseudosquares. *Mathematics of computation*, Vol. 65, No. 213, pp. 361–372, 1996.

[3] J. Sorenson. Sieving for pseudosquares and pseudocubes in parallel using doubly-focused enumeration and wheel datastructures. *Algorithmic number theory*, pp. 331–339, 2010.