様　式　Ｃ－１９、Ｆ－１９、Ｚ－１９　（共通）

科学研究費助成事業　　研究成果報告書

平成　２８　年　　６　月　２９　日現在

機関番号：　１５３０１
研究種目：　挑戦的萌芽研究
研究期間：　2012～2015
課題番号：　２４６５０００７

研究課題名（和文）疑似平方数に基づいた高速な確定的素数判定アルゴリズムの開発

研究課題名（英文）Development of Fast Deterministic Primarity Testing Algorithms Based on Pseudosquares

研究代表者

神保　秀司（JIMBO, Shuji）

岡山大学・自然科学研究科・講師

研究者番号：００２２６３９１

交付決定額（研究期間全体）：（直接経費）　　1,800,000円

研究成果の概要（和文）：疑似平方数は、平方数の条件を拡張した形の条件を満たす数である。巨大な疑似平方数に基づいた高速な確定的素数判定アルゴリズムの中の特定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した。カーマイケル数は、フェルマ・テストと呼ばれる素数判定法で判定が極めて困難な数である。提案した予想の解決は、直接確定的素数判定アルゴリズムの高速化には繋がらないが、疑似平方数に関連した理論研究の進展が期待される。

研究成果の概要（英文）：Pseudosquares are integers that satisfy conditions obtained by extending the ones that square numbers satisfy. A conjecture that asserts relations between a condition used in a fast deterministic primarity testing algorithm based on huge pseudosquares and Carmichael numbers has been proposed. It is hard to determine that a Carmichael number is not a prime number by the Fermat test. The conjecture proposed does not directly accelerate deterministic primarity testing algorithms. However, development of theoretical research on pseudosquares is expected.

研究分野：　理論計算機科学

キーワード：　疑似平方数　素数判定　アルゴリズム理論

１．研究開始当初の背景

(1) 今世紀の初頭に決定性多項式時間確定的素数判定アルゴリズムである AKS アルゴリズムが開発された。しかしながら、AKS アルゴリズムを実装したときの実行時間は、従来の主流アルゴリズムである Adleman-Pomerance-Rumely 素数判定法 (APR 法) などに遠く及ばないことが知られている。APR 法は、理論的には多項式時間アルゴリズムではないが、実用的な範囲の大きさの入力に対しては、その桁数の 4.5 乗程度の実行時間の増加であるとされている。

(2) 近年暗号系の実装などで数千ビットの大きさの整数の素数判定をする要求が増大することが予想されている。従って、現在一般的に利用できる計算機環境 (例えばノートパソコン) で確定的素数判定をする際、APR 法の実行速度でも不十分な程巨大な整数が与えられることを想定する必要があり、より高速な確定的素数判定アルゴリズムの開発が望まれていた。

(3) 疑似平方数を素数判定に利用する方法は、古くから提案されていた。素数 p に対する疑似平方数 L_p とは、次の 3 条件を満たす最小の正整数である。 a. $L_p \equiv 1 \pmod 8$ 。 b. $2 < q \le p$ を満たす各素数 q について L_p は q を法としたときの平方剰余である。 c. L_p は平方数でない、すなわち $L_p = n^2$ を満たす正整数 n は、存在しない。

２．研究の目的

(1) 本研究の目的は、入力を 1 万ビット以下の長さの正整数 N に制限した高速な確定的素数判定アルゴリズムの開発であり、理論研究に重点をおく。入力 N の制限範囲は、暗号で実際に素数判定の対象にしている数を考慮したものであり、判定が確定的であるとは、確率的な動作による誤りが生じないことをいう。

(2) 研究に用いる確定的素数判定の基本原理は、疑似平方数 (pseudosquare) に基づいたものである。大規模計算機環境を利用して得られた従来の結果から、この原理を用いたアルゴリズムの時間計算量が入力の正整数 N の桁数の 3 乗に比例する程度であることが予想され、これは、数学上の未解決予想である拡張リーマン予想を仮定して確率的素数判定アルゴリズムであるミラー・ラビン法から得られる確定的アルゴリズムの時間計算量よりも優れている。

３．研究の方法

(1) 本研究では、 確定的素数判定への入力を 1 万ビット以下の長さの正整数に限定する。目標とするアルゴリズムは、基本的には次の定理に基づいて作成する。この定理は、Lukes らにより提案されたものである。

定理 1　p は任意の素数とし、B は任意の正整数とする。正整数 N が次の条件をすべて満たすならば、N は素数かまたは素数の累乗である。

1. N は、B 以下の約数をもたない。
2. $N < BL_p$ が成り立つ。
3. $q \le p$ を満たす各素数 q について $q^{(N-1)/2} \equiv \pm 1 \pmod N$ が成り立つ。

4a. $N \equiv 5 \pmod 8$ ならば、$2^{(N-1)/2} \equiv -1 \pmod N$ が成り立つ。

4b. $N \equiv 1 \pmod 8$ ならば、 $r^{(N-1)/2} \equiv -1 \pmod N$ および $2 < r \le p$ を満たす素数 r が存在する。

本研究では、十分大きい素数 p に対して疑似平方数 L_p の正確な値を求めず、十分大きい下界を評価することを試みる。

(2) Schinzel により次の疑似平方数 L_p の下界が得られている。

定理 2　拡張リーマン予想 (ERH) を仮定すれば、任意の $\varepsilon > 0$ について、$p_0(\varepsilon)$ が存在して、$p > p_0(\varepsilon)$ ならば $(1-\varepsilon)\sqrt{p} < \log L_p$ が成り立つ。

この証明には、Bach による複素領域上の解析関数 $L(s,\chi)$ についての補題 (E. Bach, Explicit bounds for primality testing and related problems, Math. Comp. 55 (1990), 355-380.) が使われている。本研究では、Bach の議論を離散構造上で展開し直し、拡張リーマン予想 (ERH) を仮定しない疑似平方数 L_p の下界の導出を目指す。

(3) 素数判定アルゴリズムの高速化に直接関わるのは、L_p の下界であるが、上界を精密に評価するこも下界の評価を理論的に解明する上での手掛かりとなることが期待される。上界は、背景の (3) で述べた疑似平方数の条件 b. を満たす正整数を無作為抽出し、それが条件 a. と c. を満たすことを調べることにより得られる。試行回数を増やすことにより精度を上げることができる。

４．研究成果

(1) $n < L_p(k)$ を満たす最小の正整数 k を $k(n)$ で表し、k 番目の素数を $p(k)$ で表す。従って、 $p(1) = 2$ が成り立つ。さらに、条件 A を次のように定義する。

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。

論文③及び学会発表⑤において次の予想を提案した。

予想　条件 A を満たす正整数は、すべてカーマイケル数である。

この予想が成り立てば、定理１の条件 4a., 4b. をカーマイケル数であるか否かの判定に置き換えることができる。

(2) 目的に沿った研究成果ではないが、本研究で試みた探索アルゴリズムを一部流用することにより論文 ①、及び、学会発表 ①、②、③ の成果が得られた。この成果は、グラフ理論の分野に属している。以下に成果の概要述べる。

与えられたオイラーグラフのオイラー回路で最短部分閉路の長さが最大であるものの最短部分閉路の長さをそのグラフのオイラー回帰長と呼ぶ。 3 以上の奇数 n に対して $e(n)$ で n 点からなる完全グラフ K_n のオイラー回帰長を表す。従来、15 以上の奇数 n について $n-4 \leqq e(n) \leqq n-2$ が成り立つことが知られていた。今回の研究により、 15 以上の任意の奇数 n について $e(n) \leqq n-3$ が成り立つことが示された。

現時点で $e(n)$ の値は、完全には決定されていない。研究代表者は、15 以上の奇数 n について $e(n) = n-4$ が成り立つこと予想している。関数 $e(n)$ の値を厳密に決定することは、興味深い課題である。この成果の特長として、証明の一部に計算機による探索結果が使われている点が挙げられる。特に独自プログラムを使って探索問題を解くことをせず、探索問題を整数計画問題に変換し一般的な整数計画ソルバに解かせることにより、解の信頼性を著しく向上させることができた。論文 ②、及び、学会発表 ④ においても、整数計画ソルバを信頼性の高い探索手段として活用している。

(3) 目的に沿った形の成果は得られなかったが、上に述べた (1) の成果については、これが素数判定アルゴリズム作成についての理論研究の為の手掛かりの一つになることを期待している。(2) の成果については、現在、集中的に研究を継続している。

(4) Bach の議論を離散構造上で展開し直し、疑似平方数 L_p の良好な下界を拡張リーマン予想 (ERH) を仮定せずに導出することを最重要課題としていたが、成果はまったく得られなかった。第一の原因は、研究代表者が解析学についての理解と洞察に極めて乏しかったことである。また、現時点では、その方向が不適切ではないかという予想が強まっている。疑似平方数を素数判定の効率化に活用するという基本的な方針を変えずに、より見通しの良いアプローチで高速な確定的素数判定アルゴリズムが開発できることを予想している。

５．主な発表論文等
（研究代表者、研究分担者及び連携研究者には下線）

〔雑誌論文〕（計　3　件）

① Shuji JIMBO and Akira MARUOKA, Improvement of the Upper Bound on the Eulerian Recurrent Lengths of Complete Graphs, Proceedings of the 9th Hungarian-Japanese Symposium on Discrete Mathematics and Its Applications, 査読有, 2015, 407-416

② Shuji JIMBO, Improvement on Searching Minimum Dominating Vertex Sets of Complete Grid Graphs using an IP Solver, 京都大学数理解析研究所講究録 (RIMS Kokyuroku, ISSN 1880-2818), 査読無, Vol. 1873, 2014, 135-140

③ 桑木 康佑・神保 秀司 (Kosuke KUWAGI and Shuji JIMBO)、疑似平方数に基づいた素数判定アルゴリズム (Algorithms for Primality Testing Based on Pseudosquares)、京都大学数理解析研究所講究録 (RIMS Kokyuroku, ISSN 1880-2818)、査読無、1809 巻、2012、65-72

〔学会発表〕（計　6　件）

① 神保 秀司・丸岡 章 (Shuji Jimbo and Akira Maruoka)、完全グラフのオイラー回帰長の上界と下界の改良 (An Improvement of Upper and Lower Bounds on the Eulerian Recurrent Lengths of Complete Graphs)、第 146 回アルゴリズム研究会 (情報処理学会)、2014 年 01 月 30 日～2014 年 01 月 31 日、函館市民会館大会議室 (北海道・函館市)

② 神保 秀司 (Shuji Jimbo)、完全グラフのオイラー回帰長の上界と下界 (Upper and Lower Bounds on the Eulerian Recurrent Lengths of Complete Graphs)、平成 25 年度 (第 64 回) 電気・情報関連学会中国支部連合大会、2013 年 10 月 19 日、岡山大学・津島キャンパス (岡山県・岡山市)

③ 神保 秀司 (Shuji Jimbo)、完全グラフのオイラー回帰長についての予想の進展 (Progress on the Conjecture on the Eulerian Recurrent Lengths of Complete Graphs)、第 12 回情報科学技術フォーラム (FIT 2013)、2013 年 09 月 04 日～2013 年 09 月 06 日、鳥取大学・鳥取キャンパス (鳥取県・鳥取市)

④ 神保秀司・香西成人 (Shuji, Jimbo and Kouzai, Naruhito)、整数計画ソルバーを用いた囲碁における連数最大値探索の効率化

(Improvement on searching the maximum ren count in Go using an IP solver)、第 75 回情報処理学会全国大会、2013 年 03 月 06 日～2013 年 03 月 08 日、東北大学・川内キャンパス（宮城県・仙台市）

⑤ 神保 秀司（Shuji Jimbo)、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)、第 11 回情報科学技術フォーラム（FIT 2012)、2012 年 09 月 04 日～2012 年 09 月 06 日、法政大学・小金井キャンパス（東京都・小金井市）

６．研究組織

(1)研究代表者

神保 秀司（JIMBO, Shuji）

岡山大学・大学院自然科学研究科・講師

研究者番号：00226391