主 論 文 の 内 容 の 要 旨

学位申請者 氏　　名	鈴木 耕二	ローマ字 氏　　名	Koji Suzuki

論文題名

Algorithms for approximating the number of smooth integers
滑らかな整数の個数を近似するアルゴリズム

内容の要旨

小さな素因数のみを持つ正の整数を滑らかな整数と呼ぶ。滑らかな整数の研究は Ramanujan の時代から続く深淵な数学的主題であると共に、素因数分解問題を主要な応用として持つことで広く知られる。本論文では滑らかな整数の個数を近似するアルゴリズムについて述べる。本論文の構成は以下の通りである。

まず第 1 章において、近代的な素因数分解アルゴリズムを概観し、滑らかな整数の性質に関する既存研究について述べる。二次ふるい法、数体ふるい法など、最新の素因数分解アルゴリズムの計算効率は滑らかな整数の発生頻度によって決まる。このため、滑らかな整数の個数を近似する手法は素因数分解アルゴリズムの計算量推定、並びに素因数分解の困難さに安全性の根拠を置く RSA 暗号の堅牢性評価において主要な役割を担う。滑らかな整数の個数を近似する手法の研究は、Ramanujan が Hardy に宛てた有名な手紙の中で言及して以来、100 年を優に超える歴史を持つが、第 1 章では既存研究の中でも唯一高精度な推定値を与えることが可能な Hildebrand-Tenenbaum の第一近似式を主に取り上げる。また、この第一近似式を滑らかな関数で近似した第二近似式についても言及する。

次に第 2 章では、上記 Hildebrand-Tenenbaum の第一近似式を改良することにより、従来手法よりも高速に計算可能な滑らかな整数の個数を近似するアルゴリズムを与える。このアルゴリズムの漸近的計算量は従来手法のものと同一ではあるが、数値計算の際に実質的な高速性を与えることが出来る。Hildebrand 等の第一近似式を用いて滑らかな整数の個数の推定値を得るには、小さな素数の全列挙とこれらの素数に関連する複雑な方程式を数値的に解く必要がある。同章ではこの小さな素数の列挙無しに、この方程式の解を効率的かつ高精度に近似する新しい手法を与える。これにより、Hildebrand 等の第一近似式を用いて推定値を算出する際の計算量を大幅に削減することが可能となる。同章では、従来手法と比較して新しいアルゴリズムは約 4 倍高速であることを示す数値実験結果を与える。

更に第 3 章では、Hildebrand-Tenenbaum の第二近似式を改良することにより、多項式時

間計算量を有する近似アルゴリズムを与える。Hildebrand 等の第二近似式を利用して滑らかな整数の個数を推定する場合、数値積分を含む複雑な計算が必要となる。このため、近似精度に関わる顕著な問題が生じることが理由で、滑らかな整数の個数推定に上記第二近似式を利用することはこれまで行われて来なかった。第 3 章では、第 2 章で与えた近似手法の中間結果と、積分自体の計算に中点法を利用することにより、上記第二近似式の精度に関わる問題を解決する。Hildebrand 等の第二近似式を利用することで大幅な計算量の削減が可能となり、第 3 章で与えるアルゴリズムの計算量は多項式時間計算量となる。この計算量評価は発見的な推定によるものではなく、理論的に確定的なものである。Hildebrand 等の第一近似式を利用して推定値を計算する従来アルゴリズムの計算量は指数時間計算量であるため、新しいアルゴリズムの計算量は著しく小さなものと言える。

また、第 4 章では擬似滑らかな整数の性質について述べる。限定された個数の比較的大きな素因数を持ち、それ以外は小さな素因数のみで構成される正の整数を擬似滑らかな整数と呼ぶ。擬似滑らかな整数は数体ふるい法などの高速化テクニックに利用され、その分布に関する研究は最新の素因数分解アルゴリズムの解析に必須なものと言える。ここでは、擬似滑らかな整数と滑らかな整数の比率に関する推定式を与える。この推定式に第 2 章および第 3 章で与えた近似アルゴリズムを併用することにより、高精度かつ高速に擬似滑らかな整数の個数を推定することが可能となる。

最終章である第 5 章において、本論文の成果に関する結論を述べる。第 2 章および第 3 章で与えた滑らかな整数の個数を推定するアルゴリズム、および第 4 章で与えた擬似滑らかな整数と滑らかな整数の比率に関する推定式を利用することにより、二次ふるい法、数体ふるい法など、最新の素因数分解アルゴリズムの計算量、並びにそれらに高速化テクニックを併用した場合の計算量を高精度で推定することが可能となった。このことは現代の情報化社会の根幹を支える RSA 暗号の安全性評価に対して大きな意義を持つ。また、素因数分解問題とは独立に、滑らかな整数の研究は Ramanujan の時代から続く主要な数学的主題であり、本論文の成果はこの研究に対して計算論的な側面から貢献を与えるものと言える。