

ある数が素数かを判定するアルゴリズムは、計算科学の理論上も暗号などの実用上も重要な問題だ。有史以来、より速く解くための探求が続き、有名なアルゴリズムだけでも10以上は存在する。

一番シンプルなものは、試し割法だ。与えられた数 n に対して、 n より小さい数で割り切れるかどうかを順番に確かめる。 $\sqrt{n}$ まで試す必要があるので、 n が増えれば計算時間も増えていく。

次に歴史的に古く、学校でも習うエラトステネスのふるいがある。

n が素数でなくても「probably prime」となる確率が 4^{-k} ある。ここでパラメータ k を増やすことで、誤る確率は減らせるが、計算量は増えてしまう。確率（精度）と時間がトレードオフになっている。

確率的でなく決定的アルゴリズムのMillerテストは、“拡張されたリーマン予想が正しい”という前提の下では、多項式時間で判定できる²⁾。この多項式時間は最速を意味する。アルゴリズムを発見し・正しさを証明するのは難しいが、一旦証明されてしまえば、リーマン予想のような“大定理”に困難さが吸収されて、トレードオ

数 | 理 | の | 窓

アルゴリズムの トレードオフ



Step1: 2から n までの整数をテーブルに並べる。

Step2: 残っている中の最小数を p とおき、 p 以外の p の倍数をすべて消していく。

Step3: Step2の操作を繰り返して、最終的にテーブルに残ったものが素数。

計算時間¹⁾は、2から n までを一気に扱うため、試し割法に比べて圧倒的に速い。その反面、数を並べるテーブルが必要で、使用メモリ（空間）は大きくなる。つまり、時間と空間のトレードオフが発生している。

さらに、速く解くために、精度を犠牲にした確率的に判定するアルゴリズムも存在する。ミラー-ラビン素数判定法は、その1つで、入力 n が、素数であれば出力は常に正しく「probably prime」である。しかし、入力

なく高速化できる。そして、巡回セールスマンなど、多くの組合せ最適化問題にも精度と時間のトレードオフがあるが、これらの解消に向けて量子アルゴリズムなどのチャレンジは続いている。

世界には、環境と経済成長などトレードオフが多く存在し、政治的な決着では解決にはほど遠い。次世代が困らないためにも、技術革新・イノベーションを手段として、我々世代は、どの程度、宿題をやり終えられるだろうか。（外園 康智）

- 1) やや計算が必要だが、計算量オーダーは $O(n \log(\log n))$ となり、入力サイズを考慮すると指数時間オーダーになる。これは、多項式時間よりはるかに遅い。
- 2) リーマン予想を仮定しなくても、2002年にAKS素数判定法が発明されて、決定的多項式時間で判定できる。