埼 玉 新 聞

（第３種郵便物認可）

サイ・テクこらむ

知と技の発信

【576】

埼玉大学・理工学研究の現場

素数判定の難しさ

山田 敏規 准教授

突然ですが、正の整数1380471373は素数でしょうか？それとも合成数でしょうか？これを調べるために最初に思い付く方法は、1380471373を割り切る2以上の整数が存在するかどうかを調べることかと思います。1380471373が合成数であるときには2以上$\sqrt{1380471373}$（1380471373の正の平方根）＝37154・…以下の約数が存在するので、2以上37154以下の各整数で1380471373を割って、割り切れる数がひとつでも存在すれば1380471373は合成数、存在しなければ素数と判定できます。これを人間の手で行うと時間がかかりますが、コンピューターならば大した時間がかかりません。実際、1秒かからずに1380471373が素数であると判定できます。

では、同じ方法を100桁（10の99乗以上100乗未満）の正の整数Nで試すとどうでしょう。2以上$\sqrt{N}$以下の各整数でNを割ることで原理的にはNが素数であるか合成数であるかを判定できますが、仮にコンピューターが1秒間に1垓（がい、10の20乗）回の割り算を行うことができると仮定しても、最悪の場合に$\sqrt{N}\div 1垓 \fallingdotseq 3\cdot 16\times 10^{29}$秒≒約$1\times 10^{22}$年かかるので、実際には判定は不可能です。

素数はオンラインショッピングの際に使われている暗号の中で鍵と呼ばれる重要な役割を果たしており、暗号の安全性を確保するためには300～1000桁の巨大な素数を用いることが推奨されています。巨大な素数を生成するには、必要な桁数の奇数をランダムに生成し、その奇数が素数であるかどうかを判定することを繰り返すため、高速な素数判定手法が必要とされます。

現在、素数判定にはミラー・ラビン素数判定法が用いられています。この手法は、正の奇数Nが与えられたときにN未満の正の整数aをランダムに選び、$b(0)=a^u \bmod N$, $b(k)=b(k-1)^2 \bmod N$ $(=a^{u\times 2^k} \bmod N)$とおく$(k=1,\cdots,L-1)$と$b(0)=1$または$b(k)=N-1$であるkが存在するときにNを素数と、さもなければ合成数と判定します。ここでuとLはそれぞれ$N-1=u\times 2^L$を満たす奇数と正の整数とします。また、x^yはxのy乗を、$x \bmod N$はxをNで割った余りを表します。ミラー・ラビン素数判定法は、四則演算の総回数がNの桁数nに比例するので、最初の手法と比べて格段に速いですが、判定に誤りを含むので注意が必要です。素数を誤って合成数と判定することはありませんが、合成数を4分の1以下の確率で誤って素数と判定します。このため、整数aを独立に何回か選んでミラー・ラビン素数判定法を適用し、全てのaでNを素数と判定したときのみ最終的にNを素数と、1回でもNを合成数と判定したときは最終的にNを合成数と判定することで誤り確率を0に近づけます。

四則演算の回数がnの多項式で抑えられる、誤りのない素数判定法も現在知られていますが、実用上はまだまだ計算時間がかかるために高速化が大きな課題です。

やまだ・としのり　1969年生まれ。98年東京工業大学大学院修了。博士（工学）。東京工業大学大学院助手、埼玉大学工学部講師を経て、2005年4月から現職。専門は離散アルゴリズム、特に、グラフ・アルゴリズム。