合成数はどこまで素数に近づけるか

山田智宏 (Tomohiro Yamada) @tyamada1093

いうまでもなく素数とは「1 と自分自身以外の約数をもたない数」である。しかし、与えられた数が素数かどうか確かめるために、その数の約数を実際に探し求めるのは非常に時間がかかる。150 桁程度の数でも、たとえば 75 桁の素数同士の積であれば、そのことを確かめるには 1 台の PC では数か月を要することになる。100 桁の素数 2 つの積となると、1 台の PC では非現実的な時間を要する。最近、125 桁の素数 2 つの積を、もとの素数に分解する問題が解かれたが、のべ 2000 年以上を要した（`https://lists.gforge.inria.fr/pipermail/cado-nfs-discuss/2020-February/001166.html`）。

一方、現在、コンピューターと数式処理システムを使えば、もっと大きい、300 桁程度の数でも素数か合成数かは 1 分以内に判定することができる。もちろん、この判定は与えられた数の約数を探し求める素朴な方法ではなく、高度な素数判定法を用いている。すなわち、すべての素数に共通しており、かつ合成数は決してもたないような性質は、素数の定義である「1 と自分自身以外の約数をもたないこと」以外にも存在するのである。

たとえば Wilson の定理（p が素数 $\Leftrightarrow (p-1)! \equiv 1 \pmod{p}$）は素数であることの必要十分条件を与えているが、階乗の計算に非常に時間がかかるため、現実的ではない。

Fermat の小定理は p が素数で $\gcd(a,p)=1$ ならば $a^{p-1} \equiv 1 \pmod{p}$ であることを主張しているが、逆は一般には成り立たない。たとえば $2^{340} \equiv 1 \pmod{341}$ が成り立つが $341 = 11 \times 31$ は合成数である。さらに悪いことに、$\gcd(a,n)=1$ のとき必ず $a^{n-1} \equiv 1 \pmod{n}$ となる合成数 n が無数に多く存在することが知られている（Adleman, Pomerance, and Granville, *Ann. Math.* **140** (1994), 703–722）。そのような数は Carmichael 数と呼ばれるが、その場合には $a^{n-1} \not\equiv 1 \pmod{n}$ となる a を見つけるのは n の約数を探すのと同じくらいに困難となる。

しかし与えられた a について $a^{n-1} \equiv 1 \pmod{n}$ となる合成数 n が非常に少ないことも知られている（たとえば Pomerance, *Math. Comp.* **37** (1981), 587–593）。

このように、素数しかもたないように思えるが、実際には合成数の中にも同じ性質をもつものが稀ではあるが存在するというような性質が存在するし、一方で素数

しかもたない性質でなおかつ、素早く検証できる性質が存在する。そこで、合成数がどこまで素数と共通の性質をもつことができるかを考察していきたい。

たとえば Miller-Rabin の確率的判定法は、Fermat の小定理を少し変形した合同式を使う。$n = 2^s t$ で t を奇数とすると、n が素数で $\gcd(a, n) = 1$ ならば $a^t \equiv 1 \pmod{n}$ となるか、 $a^{2^k t} \equiv -1 \pmod{n}$ となる k が存在することが Fermat の小定理からわかる。不幸なことに、与えられた a に対して、この 2 条件のどちらかが成り立つような合成数はやはり存在する。しかし、n が合成数ならば、上記の 2 条件のどちらも成り立たないような a で比較的小さいものが存在すると予想されている（これは Riemann 予想のある拡張を仮定すれば正しいことが知られている）。

また、実用的な判定法ではないが、Euler の totient 関数 $\varphi(n)$ （$1 \leq a \leq n-1, \gcd(a, n) = 1$ となる a の個数）を考えると、n が素数であることの必要十分条件は $\varphi(n) = n-1$ となることがすぐにわかる。一方、n が合成数の場合 $\varphi(n) < n-1$ となるが、 $\varphi(n)$ が $n-1$ を割り切ることすらないと予想されているが、これも未だ解決されていない（なおこの性質が成り立つとき n は Carmichael 数となる）。

予備知識としては、過去の講演同様、初等整数論の知識だけでも概ね理解できる内容としたい。また、計算量理論や Riemann 予想の知識があればより深く理解できる内容になると思われる。