整数の分解

因数分解は、与えられた文字式を別の文字式の積に直している。文字式は便宜上 x などの文字を使っているが、文字が数の代わりであると考えると、因数分解は、与えられた数を別の数の積に直していると見ることができる。もっとも因数分解の例を出すまでもなく、たとえば 12 は

$$12 = 3 \times 4 = 2 \times 6 = 2 \times 2 \times 3 = 24 \times \frac{1}{2}$$

のように、いろいろな積の形にできることが分かるだろう。もし、分数を含めて整数を分解してよいなら、分解の仕方は無数にある。しかし、正の整数だけの積に分解するなら、分解の仕方は有限個しかない。また、$12 = 3 \times 4$ はさらに $3 \times 2 \times 2$ に分解することもでき、しかもこれ以上の分解はできない。整数を正の整数の積で表し、なおかつそれ以上小さな数の積にできないように分解することを**素因数分解**という。そして、素因数分解に現れる整数は**素数**と呼ばれる。12 の素因数分解であれば、いま見てきたように $2 \times 2 \times 3$ や $3 \times 2 \times 2$ を指すが、この 2 つの表記は積の順番が違うだけで、ふたつの 2 とひとつの 3 の積であることは同じである。つまり、素因数分解の仕方はただ一通りだけに決まる。

素数と素因数分解

素因数分解に現れる数が素数であると言ったが、素数はそれ以上他の整数の積に分解できないことから、**約数**を持たない数と言っても同じことである。もっとも約数とは、ある整数を割り切ることができる整数のことなので、素数が約数を持たない数と定義するのは正確ではない。なぜなら、どんな素数 p であっても必ず 1 と p は約数になっているからである。しかし、1 と p 以外の約数を持たないことは明らかだから

素数とは、1 と自分自身以外の約数を持たない数

と定義するのがよい。また、ここでは負の約数は考えないことにする。

すると今度は、素数という言葉を使って素因数分解を定義できる。

素因数分解とは、整数を素数の積で表すことである

基本的にはこれらの定義でよいのであるが、定義にしたがって 12 を素数の積、すなわち 1 と自分自身以外の約数を持たない数の積にすると、$2 \times 2 \times 3$ の他にも

$$2 \times 2 \times 3 \times 1, \quad 2 \times 2 \times 3 \times 1 \times 1, \quad \ldots$$

なども 12 の素因数分解となって、収拾がつかない事態を招いてしまう。これを避けるためには、素因数分解の定義を「1 以外の素数の積で表す」に改めるか、または素数の定義を「1 と自分自身以外の約数を持たない数（ただし、1 は素数でないとする）」に改める必要がある。言葉を改めるだけならば前者の方が簡単であるが、実際は後者の立場、すなわち素数の定義に

ただし、1 は素数ではない

を加える立場をとっている。

素因数分解をすることにおいてはどちらの立場も同じであるが、後者の立場の方が**素因数分解の一意性**と相性が良い。一意性とは、素因数分解の仕方がただ一通りしかないことを意味する。つまり 12 の素因数分解は、積の順番を考慮しなければ $2\times2\times3$ 以外にないことになる。前者の立場、すなわち 1 を素数に含めると 12 の素因数分解は、積の順番を考慮しなくても $2\times2\times3$, $2\times2\times3\times1$, ... のように一意に決まらず、それを素因数分解の定義で一通りに定めることになってすっきりしないのである。

素因数分解の一意性

さて、ここまで素因数分解は一通りの表し方しかないと述べ、それがごく当たり前のことのように受け入れているが、本当にそうであろうか。たとえば、整数 x の素因数分解が $x=ab$ であるなら、他に a, b と違う値の c, d を用いて $x=cd$ となるようなことは起こらないのだろうか。私たちは長い間の計算の習慣や知識から、x が素数の積 ab で表されるなら、別の素数の積 cd になることはあり得ないと感じているに違いない。日常の生活ではこのような漠然とした理解でも困ることはないであろう。しかし数学においては、漠然とした考えは排除されなくてはならない。そのためには、素数の定義と素因数分解の定義から、$x=ab=cd$ のような素因数分解があり得ないことを示す必要がある。

ここでは、素因数分解の一意性の証明にはなっていないが、$x=ab=cd$ のような素因数分解があり得ないことを示してみよう。まず、a, b, c, d はどの 2 数をとっても等しいものはないとする。また、a, b, c, d は素数であるから、どれも 2 以上の整数であることに注意しよう。このとき、もし $ab=cd$ ならば $ab-cd=0$ であるから、多少無理はあるが a を ( ) の外へくくり出して

$$a\left(b-\frac{cd}{a}\right)=0$$

とすることができる。これは a と $b-\dfrac{cd}{a}$ の積が 0 であることを意味するが、$a \neq 0$ なのだから

$$b-\frac{cd}{a}=0$$

でなくてはならない。また、b は整数なので $\dfrac{cd}{a}$ も整数でなくてはならない。ところが、a, c, d は素数であったのだから、c と d には $1, c, d$ 以外の約数はない。このことは $\dfrac{cd}{a}$ が a で約分されないことを意味する。しかし、$\dfrac{cd}{a}$ は整数でなくてはならないとしたら、それは $a=c$ か $a=d$ のときに限るだろう。$a=c$ とすると

$$b-\frac{cd}{a}=0 \text{ は } c,\ a \text{ が約分されて } b-d=0$$

となるから $b=d$ である。$a=d$ としても同様に $b=c$ である。いずれにしても $ab=cd$ ならば、$a=c$ かつ $b=d$ であるか、$a=d$ かつ $b=c$ なのである。

以上で、整数が ab に素因数分解されるならば、別の 2 数による素因数分解はないことが分かった。ただし、別の 3 数による素因数分解があるかもしれないので、これだけで素因数分解の一意性を証明したことにはならない。

素数は無限にある

素数について調べることは、現代数学においてもっとも重要なことのひとつである。なぜなら、素数について分からないことがまだたくさんあるからだ。しかし、素数が無限に存在していることは紀元前から知られていたことである。このことはユークリッド[1]が証明したと伝えられている。証明は以下のとおりである。

まず、素数が有限個しかないと仮定し、有限個の素数を小さい順に $p_1, p_2, p_3, \ldots, p_N$ とする。ここで

$$P=(p_1 \cdot p_2 \cdot p_3 \cdots p_N)+1$$

という数を考える。素数は有限個しかなく、P は $p_1, p_2, p_3, \ldots, p_N$ のどれとも違うので素数ではない。すなわち**合成数**—素因数分解できる数—である。合成数は素数で割り切れるはずだが、P は $p_1, p_2, p_3, \ldots, p_N$ のいずれで割っても 1 余るから、P を割り切る別の素数 p_X がなければならない。これは素数が $p_1, p_2, p_3, \ldots, p_N$ しかないことに反する。この矛盾は、素数が有限個であると仮定したために生じたので、仮定は間違っている。よって、素数は無限個ある。(証明終)

[1]ユークリッドまたはエウクレイデス（365?B.C.–275?B.C.）：古代ギリシアの数学者、天文学者。

4

証明の前提になっているのは

1 より大きい数は素数か合成数のどちらかであり、合成数は素数で割り切れる

という事実である。素数に関する事実は他にもあって、

N が 2 から $(N-1)$ までの素数で割り切れなければ、N は素数である

も正しい。この事実をもとにすれば証明は、P は $p_1, p_2, p_3, \ldots, p_N$ のいずれで割っても割り切れないから素数であり、素数が $p_1, p_2, p_3, \ldots, p_N$ しかないことに反する、と述べてもよいことになる。ただ、この証明と

$(p_1 \cdot p_2 \cdot p_3 \cdots p_N) + 1$ の形の数が素数である

ということは別の話であることに注意されたい。実際、$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 + 1 = 510511$ とした場合、2 から 17 までの素数で割れないからといって 510511 が素数であるとは言えない。なぜなら素数は有限個ではないからである。510511 は 17 より大きな素数 19, 97, 277 で割れる。