約数

整数は数の基本である。整数を使いこなすだけでも、日常の用途はほぼすべて賄（まかな）えるだろう。生活する上ではそれで十分なのだろうが、整数の仕組みを知っておくことも重要なのかもしれない。たとえば、12 個の卵をパッケージに収めるとき、縦 × 横 に並べるなら 3×4 や 2×6 のように詰め方はいく通りかある。そのようにできるのは、12 が 3 や 4 で割り切れるからである。

ある整数 n を割り切ることができる整数を、n の**約数**という。12 の約数であれば $\{1, 2, 3, 4, 6, 12\}$ の 6 個が該当するが、整数を基本に考えるのであれば 12 の約数は

$$\pm 1,\ \pm 2,\ \pm 3,\ \pm 4,\ \pm 6,\ \pm 12$$

の 12 個になる。負の約数は日常で使うことはないので、多少違和感があるかもしれない。しかし、数学で約数というと負の値まで含めて考えるのが一般的である。約数は、とくに述べなければ整数全体で考えるものとし、もし負の約数が不要なら**正の約数**と明記すればよい。

整数 n を割り切る整数が約数なのだから、n の約数は有限個である。12 の約数の個数は 12 個で、そのうち正の約数の個数は 6 個である。小さい数の約数の個数は、約数を書き並べて数えれば分かることである。また、$12 \div \underline{2} = \underline{6}$ から分かるように、12 の約数に $\underline{2}$ が含まれるなら $\underline{6}$ も約数である。約数は原則 2 個同時に見つけられるものだ。しかし、大きな数になると、すべての約数を探すことに苦労するだろう。

約数を探すにはプログラムを組むとよいのだが、Microsoft Excel のワークシート上でも、ほどほどの大きさの数なら比較的簡単に見つけられる。ちょっと無理をしているが関数だけでも何とかなるものである。

◇	A	B	C	D	E	F
1	正の整数を入力	の約数（	（※ C1）	行目まで）	（※ E1）	（※ F1）
2					↓下へコピーする	↓下へコピーする
3		約数は	（※ C3）	個	↓	↓
4					↓	↓
5					↓	↓
6					↓	↓

※ セルの式

（C1） =INT(SQRT(A1))

（E1） =IF(AND(ROW()<=$C$1,MOD($A$1,ROW())=0),$A$1/ROW(),"")

（F1） =IF(E1="","",$A$1/E1)

（C3） =COUNTIF(E:F,">0")-IF(C1^2=A1,1,0)

A1 セルに適当な正の整数を入力してみよう。入力した値に応じて、約数表示に必要な最大行数が C1 セルに示されるので、E、F 列は必要なだけ “↓下へコピーする” とよい。もちろん、あらかじめ 100 行先までコピーしておけば、10000 までの整数の約数はすべて 100 行目までに表示される。

10000 までの約数を表示するのに必要な行数が 100 行でよい理由は、約数は 2 個同時に見つけられるからである。n の約数 a の相方は $b = \frac{n}{a}$ であるから、a を 1 から順に大きくして n で割ると、b は n から順に小さな値になっていく。つまり、大きくなる a と小さくなる b が等しくなるところまで割り算をすればよいことになる。そこは $\sqrt{n}$ だ。したがって、10000 までの約数は $\sqrt{10000} = 100$ までにすべて出揃うのだ。

ただし、A1 セルに入力した数が平方数の場合は、最後のところで a と b の値が本当に等しくなるので、同じ約数が 2 個同時に見つかることになる。したがって重複して数えないために、個数を 1 減らさなくてはならない。それが C3 セルの式に “-IF(C1^2=A1,1,0)” が追加されている理由だ。もっとも、調べている整数が平方数かどうかは、一番下で見つかった約数のペアを見れば一目瞭然であるが。

ちなみに、A1 セルに負の値を入力するとエラーになるのは、C1 セルの SQRT 関数のせいである。エラーを起こさないためには C1 セルの式を “=INT(SQRT(ABS(A1)))” にするとよいのだが、それだけでは不十分である。表示された数と符号が逆の約数が漏れてしまうからだ。しかし、苦労して負の数の約数を表示させるようにすることもあるまい。

合成数・素数

もし Microsoft Excel で、整数の約数を表示させて遊んだなら容易にわかるように、整数にはたくさんの約数を持つものとそうでないものがあることに気づくだろう。少ない約数しか持たない整数のうち、1 と自身以外に約数のない数は、眺めていて拍子抜けするものである。たとえば、570 なら賑（にぎ）やかに約数が表示されるのに、571 ならあっさりしたものだ。繁華街で整数の約数を見せびらかすなら賑やかな方が良さそうだが、数学的に重要なのは 1 と自身以外に約数を持たない整数である。この定義から、対象とするのは正の整数に限ることになる。負の整数まで含めると、± 1 が約数となり条件に合わなくなってしまう。このような整数を**素数**と呼び、素数以外の数は**合成数**と呼ぶ。素数を小さい順に並べると、

$$2,\ 3,\ 5,\ 7,\ 11,\ 13,\ 17,\ 19,\ 23,\ 29,\ 31,\ 37,\ 41,\ 43,\ 47,\ \ldots$$

である。571 はこれらの中に含まれる。

ここに現れない数が合成数であるが、1 つ例外がある。それは 1 だ。1 は自身の 1 以外に約数を持たないという点で素数の条件を満たすが、この後で述べる素因数分解に関わる理由から素数に含

めない。では合成数かというと、そうでもない。合成数は、たとえば $12 = 2 \times 6$ のように自身以外の約数の積にできるが、1 は自身以外の約数の積で表せない。

素因数分解

合成数を素数の積で表すことを**素因数分解**という。たとえば 12 は単に 2×6 とするのではなく、$2 \times 2 \times 3$ と表すことが素因数分解である。ちなみに、$12 = 2 \times 6$ と見て、2 や 6 を 12 の**因数**ということもある。因数と約数は同じものを指すが、因数と言うと何となく 1 と自身の数を除く真の約数という雰囲気が漂う。要するに因数の積にしたとき、因数がすべて素数であるものが素因数分解ということなのだ。

ある整数が与えられたとき、その整数を素因数の積に分解するには、小さい素数から順に割ってみればよい。たとえば 570 は、

$$570 = 2 \times 285 = 2 \times 3 \times 95 = 2 \times 3 \times 5 \times 19$$

と素因数分解ができる。一方 571 は、2, 3, 5, ... と割り算をしても一向に割り切れないので、素数ではないかと思い始めるだろう。では、どの時点で素数である確信が持てるかというと、$571 \div 23 = 24.8\cdots$ までの割り算をしたときである。前述の理由から $\sqrt{571} \approx 23.6\cdots$ まで調べれば十分だからだ。割り算を試す素数は 2 から 23 までの 9 個だが、571 は一の位を見れば 2 でも 5 でも割り切れないのは明らかだから、2 と 5 を除く 7 個の素数を試すだけで十分である。

素因数分解には重要な性質がある。それは

積の順番を無視すれば、素因数分解は一意に決まる

ことである。どういうことかというと、$570 = 2 \times 3 \times 5 \times 19$ も $570 = 3 \times 2 \times 19 \times 5$ も同じことであるから、570 の素因数は 2, 3, 5, 19 が各 1 個ずつ以外にないことを意味している。実際は、性質というより定理であるのだが、ここではほぼ自明のこととして性質と呼ばせてもらうことにする。

実はここに 1 を素数の仲間に入れなかった理由がある。もし 1 を素数の仲間にしたら、$570 = 2 \times 3 \times 5 \times 19 = 2 \times 3 \times 5 \times 19 \times 1 \times 1$ など、1 の個数違いで一通りに分解できると言えなくなってしまうからだ。

* * *

1 を素数の仲間に入れないのは、素因数分解が一意に決まるようにするためだが、1 と自身以外に約数がない数を素数と呼ぶなら、1 こそ素数中の素数ではないかと考える向きもあろう。確かにその部分に目を向ければ 1 は究極の素数かもしれない。しかし、そうすると素因数分解の定義を「1 以外の素数の積で表す」とする必要があるが、素因数分解ができなくなるわけではない。仮に 1 を素数に含めたら、

1. 素因数分解とは、整数を 1 以外の素数の積で表すことである。
2. 素数とは、1 と自身以外に約数がない整数である。

といった定義になるだろう。この場合は、素因数分解の定義に「1 以外の」という注釈は付くが、素数の定義は簡素である。一方、現在採用されているものは

1. 素因数分解とは、整数を素数の積で表すことである。
2. 素数とは、1 と自身以外に約数がない整数である。ただし、1 は素数ではない。

である。この場合は、素因数分解の定義は簡素だが、素数の定義には注釈が付く。

いずれの場合でも、素数の区別や素因数分解は正しく行われるだろうから、問題は起こらないはずである。現状の定義が好まれるのは、「素因数分解」を「素数の積」と簡便に言い換えられることが影響しているかもしれない。もし 1 が素数なら、「素因数分解」を「1 以外の素数の積」と言うことになり、簡便に言い換えていることにならない。一方、いずれの定義でも「素数」は「1 と自身以外に約数のない整数（。ただし、1 は素数ではない）」と言うしかないので、どのみち簡便には程遠い。素数という言葉から 1 を除くことで、その後の使い勝手が良くなると思われるのだ。

1 を素数の仲間に入れないことで、よい副作用も生じる。それは「素数とは、約数をちょうど 2 個持つ整数である」と言い換えてもよいことだ。こう言えば、約数を 1 個しか持たない 1 は、自動的に弾かれる。▌

最大公約数・最小公倍数

ここでは正の約数に限って話を進める。2 個以上の整数があり、それぞれの約数に共通している約数を**公約数**といい、そのうち最大の公約数を**最大公約数（gcd := greatest common divisor）**という[1]。どんな整数も約数 1 を持っているので、最小公約数を定義する意味はない。

また、ある整数 n を整数倍した整数が n の**倍数**であるが、ここでも正の倍数に限ることにする。2 個以上の整数があり、それぞれの倍数に共通している倍数を**公倍数**といい、そのうち最小の公倍数を**最小公倍数（lcm := least common multiple）**という。倍数はいくらでも大きい数が存在するので、最大公倍数は存在しない。

正の整数を対象に具体例を挙げよう。たとえば 36 と 60 については

$$\begin{aligned} 36 \text{ の約数} &:= \{1,\ 2,\ 3,\ 4,\ 6,\ 9,\ 12,\ 18,\ 36\} \\ 60 \text{ の約数} &:= \{1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 10,\ 12,\ 15,\ 20,\ 30,\ 60\} \end{aligned}$$

なので、公約数は $\{1,\ 2,\ 3,\ 4,\ 6,\ 12\}$ で、最大公約数は $\gcd(36,\ 60) = 12$ である。ここで $\gcd(a,\ b)$ は、a と b の最大公約数の意味で用いた。また、

$$36 \text{ の倍数} := \{36,\ 72,\ 108,\ 144,\ 180,\ 216,\ \ldots\}$$

[1] gcm := greatest common measure と言うこともある。

$$60\text{の倍数} \quad := \quad \{60,\ 120,\ 180,\ 240,\ 300,\ \ldots\}$$

なので、最小公倍数は、$\mathrm{lcm}(36,\ 60) = 180$ であることはすぐ分かるが、いま公倍数は $\{180,\ \ldots\}$ の先が見えていない。しかし公倍数は、最小公倍数の倍数の集合 $\{180,\ 360,\ 540,\ \ldots\}$ である。当然のように、最大公約数が 12 であったときの公約数は、最大公約数 12 の約数の集合になっているはずである。

なぜだろう。それは、素因数分解をして $36 = 2^2 \cdot 3^2$、$60 = 2^3 \cdot 3 \cdot 5$ と見れば分かる。ちなみに $\times$ の省略記号として、一部 $\cdot$ を用いた。

まず公倍数だが、$36 = (2^2 \cdot 3^2)$ と $60 = (2^2 \cdot 3 \cdot 5)$ の倍数は、見辛いことは承知の上で

$$\begin{aligned} 36 \quad &:= \quad \{(2^2 \cdot 3^2) \times 1,\ (2^2 \cdot 3^2) \times 2,\ (2^2 \cdot 3^2) \times 3,\ (2^2 \cdot 3^2) \times 4,\ \ldots\} \\ 60 \quad &:= \quad \{(2^2 \cdot 3 \cdot 5) \times 1,\ (2^2 \cdot 3 \cdot 5) \times 2,\ (2^2 \cdot 3 \cdot 5) \times 3,\ (2^2 \cdot 3 \cdot 5) \times 4,\ \ldots\} \end{aligned}$$

と書ける。この中から共通の倍数を見つけるのだが、最初に見つかる公倍数 180 は $2^2 \cdot 3^2 \cdot 5$ である。これは、36 の倍数の集合に含まれる $(2^2 \cdot 3^2) \times 5$、および 60 の倍数の集合に含まれる $(2^2 \cdot 3 \cdot 5) \times 3$ のことである。36 の倍数は $(2^2 \cdot 3^2) \times n$、60 の倍数は $(2^2 \cdot 3 \cdot 5) \times n$ の形なので、36 と 60 の公倍数は少なくとも $(2^2 \cdot 3^2 \cdot 5) \times n$ の形でなければならない。したがって、公倍数の集合は最小公倍数の倍数の集合なのである。

公約数も同じ理屈である。$36 = 2^2 \cdot 3^2$ の約数が $\{1,\ 2,\ 3,\ 4,\ 6,\ 9,\ 12,\ 18,\ 36\}$ であるのは、2 個の 2（2^2）と 2 個の 3（3^2）のうち、何を何個掛けたかによる。2 を 2 個掛ければ $2^2 = 4$ が、2 と 3 を 1 個ずつ掛ければ $2 \cdot 3 = 6$ という具合だ。何も掛けなければ約数 1 である。

このことは、36 と 60 の約数を

$$\begin{aligned} 36 \quad &:= \quad \{\ (2^0 \cdot 3^0),\ (2^0 \cdot 3^1),\ (2^0 \cdot 3^2),\ (2^1 \cdot 3^0),\ (2^1 \cdot 3^1), \\ &\qquad (2^1 \cdot 3^2),\ (2^2 \cdot 3^0),\ (2^2 \cdot 3^1),\ (2^2 \cdot 3^2)\ \} \\ 60 \quad &:= \quad \{\ (2^0 \cdot 3^0 \cdot 5^0),\ (2^0 \cdot 3^0 \cdot 5^1),\ (2^0 \cdot 3^1 \cdot 5^0),\ (2^0 \cdot 3^1 \cdot 5^1), \\ &\qquad (2^1 \cdot 3^0 \cdot 5^0),\ (2^1 \cdot 3^0 \cdot 5^1),\ (2^1 \cdot 3^1 \cdot 5^0),\ (2^1 \cdot 3^1 \cdot 5^1), \\ &\qquad (2^1 \cdot 3^0 \cdot 5^0),\ (2^1 \cdot 3^0 \cdot 5^1),\ (2^1 \cdot 3^1 \cdot 5^0),\ (2^1 \cdot 3^1 \cdot 5^1)\ \} \end{aligned}$$

と書くとよい。この中の共通の約数は 2 と 3 と 5 を同じ個数だけ掛けたものだが、36 の約数には 5 が含まれておらず、60 の約数には 3 が最大 1 個あるだけだ。したがって、同じ個数だけ掛けることができるのは 2 が 2 個と 3 が 1 個までということになる。よって、36 と 60 の公約数は

$$\{(2^0 \cdot 3^0),\ (2^0 \cdot 3^1),\ (2^1 \cdot 3^0),\ (2^1 \cdot 3^1),\ (2^2 \cdot 3^0),\ (2^2 \cdot 3^1)\} = \{1,\ 3,\ 2,\ 6,\ 4,\ 12\}$$

である。ちなみに、2 や 3 を掛ける個数が 0 個であるとは、1 に何も掛けていないことであるから、$2^0 = 3^0 = 1$ と見ている。余談ながら、数学の世界では一般に $n^0 = 1$ と定義されるので、$2^0 = 1$ はここだけの特別な表記ということではない。