

## 「素数の見つけ方」

1 から始まり, 1 ずつ増える数列  $\{1, 2, 3, \dots\}$  に含まれる数を自然数という. 自然数とそのマイナスの数および 0 のなす集合を  $\mathbb{Z}$  と書き,  $\mathbb{Z}$  に属する数を整数という:

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$$

状況をより明確にしたい場合には整数のことを有理整数という.

次の定理は整除性の基本となる.

定理 0.1  $a$  を自然数,  $b$  を整数とするとき

$$b = qa + r, \quad 0 \leq r < a$$

となるような整数  $q, r$  がただ一組存在する.

整数  $a, b \in \mathbb{Z}$  に対し, ある整数  $q$  が存在して

$$b = aq$$

となるとき,  $a$  は  $b$  を割り切る, あるいは  $b$  は  $a$  で割り切れる, あるいは  $a$  は  $b$  の約数である, あるいは  $b$  は  $a$  の倍数であるという.  $a$  が  $b$  を割り切ることを  $a|b$  と表す.  $b$  が  $a$  で割り切れない時,  $a \nmid b$  と書く.  $a$  が  $b$  を割り切る時,  $-a$  も  $b$  を割り切るから, 約数といった場合には正の約数を意味するものとする. 2 で割り切れる整数を偶数, 2 で割り切れない整数を奇数という. 1 と自分自身以外では割り切れない自然数を素数という.

素数を見つけるためのもっとも原始的な方法としては, 次のエラトステネスの篩 (ふるい) がある. 2 以上の自然数  $2, 3, 4, \dots$ , を書き出しておく. まず, 2 に丸を付けて, 2 より大きい 2 の倍数をすべてけす. (紙に書いて行う時には, 斜線で消すのがよいだろう.) 次に 2 より大きな数で消されなかった数 (3 が残っているはずである.) に丸をつけて残し, そのそれ (つまり 3) より大きいそれ (つまり 3) の倍数をすべて消す. 次にそれ (つまり 3) より大きくて, 消されずに残った数 (つまり 5) に丸をつけてのこし, こいつ (つまり 5) より大きいこいつ (つまり 5) の倍数をすべて消す. 以下同様に繰り返したとき, すべての自然数は丸を付けられるか斜線で消えることがわかる. 丸をつけられたものは素数, 斜線で消されたものは合成数である.

演習 0.2 下の表を利用して、100以下の素数をすべて求めよ。

素数が無限個あることは古代ギリシャから知られていた。証明は背理法で行う。素数が有限個しかないとして、それらのすべてを  $p_1, p_2, \dots, p_m$  とする。自然数  $n = p_1 p_2 \cdots p_m + 1$  を考える。どんな自然数も素数の積に分解するから、 $n$  はある素数で割り切れるはずである。しかし、 $n$  は  $p_1, \dots, p_m$  のいずれでも割り切れないから矛盾である。よって素数は無限個なければならない。

後に述べるように大きな素数は暗号に応用することができるため、大きな素数を見つけることは重要な問題である。先に示したように素数は無限に存在するから、いくらでも大きな素数が存在するはずである。しかし、具体的に大きな素数を見つけることは大変難しい問題である。現在知られている最大の素数は2008年8月23日に発見された  $2^{43112609} - 1$  で、その桁数は12,978,189桁。コンピュータを用いた計算によって、素数であることが示された。この素数のように、 $2^n - 1$  の形の素数をメルセンヌ (M. Mersenne) 素数という。この形の整数は素数になるものを多く含んでおり、現在、知られている最大の素数は上にのべたメルセンヌ素数で47番目のものである。

素数の世界には不思議な現象が数多くあり、多くの研究者の興味を惹いている。ここでは、未解決の問題を2つご紹介しておこう。

3と5, 5と7, 11と13, 17と19のように、偶数をはさむ2つの素数を双子素数という。双子素数は無限個存在すると予想されているが証明されていない。

4以上の偶数は2つの素数の和として表されると予想されている。  $4 = 2 + 2$ ,  $6 = 3 + 3$ ,  $8 = 5 + 3$ ,  $10 = 7 + 3$ ,  $12 = 7 + 5$  など。この予想はゴールドバッハ (Goldbach) の予想と呼ばれている。

整数  $a, b$  に対し、 $a$  と  $b$  の共通の約数を公約数という。  $a$  と  $b$  の公約数のうちで最大のものを、 $a$  と  $b$  の最大公約数といい、 $\gcd(a, b)$  と書く。  $a$  と  $b$  の最大公約数が1に

|    |    |    |    |    |    |    |    |    |     |
|----|----|----|----|----|----|----|----|----|-----|
| 2  | 3  | 4  | 5  | 6  | 7  | 8  | 9  | 10 |     |
| 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20  |
| 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30  |
| 31 | 32 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40  |
| 41 | 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50  |
| 51 | 52 | 53 | 54 | 55 | 56 | 57 | 58 | 59 | 60  |
| 61 | 62 | 63 | 64 | 65 | 66 | 67 | 68 | 69 | 70  |
| 71 | 72 | 73 | 74 | 75 | 76 | 77 | 78 | 79 | 80  |
| 81 | 82 | 83 | 84 | 85 | 86 | 87 | 88 | 89 | 90  |
| 91 | 92 | 93 | 94 | 95 | 96 | 97 | 98 | 99 | 100 |

なるとき,  $a$  と  $b$  は互いに素であるという.

任意の自然数は一意的に素因数分解される. すなわち, 任意の自然数  $n$  に対し相異なる有限個の素数  $p_1, p_2, \dots, p_k$  と自然数  $e_1, e_2, \dots, e_k$  が存在して

$$n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$$

と, 積の順序を除いて一意的に表示される.