

# 初等・中等教育における「素数」の指導の考察

榎本 里志

## 1 はじめに

2022年（令和4年）、平成30年告示の高等学校の新学習指導要領での指導が、1年生から始まった。この学年の生徒は、平成29年告示の小学校、中学校の学習指導要領に基づいて学習してきた生徒であり、高等学校の数学では、数学Cの復活や、科目間での指導内容の移行があるなど、平成21年告示の学習指導要領で学んでいる高等学校2年生、3年生とは異なるカリキュラムで学習することになる。

今回の学習指導要領の中で、小学校の算数、中学校、高等学校の数学の指導内容に関連した項目の中で、とくに目についた点の一つに「素数」がある。

従前（平成20年告示）の学習指導要領では、素数は、小学校5年生で、約数・倍数、最大公約数・最小公倍数を扱う中で取り上げられており、その数の定義とその神秘性について学ぶ機会を得ている。さらに、中学校3年生になって、素因数分解の仕組みとその方法を学んでいた。

これに対し、新学習指導要領では、素数は、中学校1年生で初めてその定義を学び、素因数分解も含めて、ここで学ぶこととなった。

したがって、小学校5年生では、約数・倍数や、最大公約数・最小公倍数は学ぶものの、とくに素数という用語は姿を消した（各学校の指導にもよる）。さらに、高等学校では、特別な扱いはなく、数学Aの「場合の数」の問題として、素因数分解を利用した約数の個数を求めたり、「数学と人間の活動」の中で、整数の性質を学ぶ上で、「互いに素」であることや「素数」の再確認をする程度である。

このような、小学校、中学校、高等学校での素数についての指導の流れの中で、数学が現代社会の中で果たす役割の中でも、とくに存在感ある素数について、現実の学校教育にその影響が大きい入学試験問題なども引用しながら、素数の指導について考察した。

## 2 初等教育から中等教育での素数の指導を考える

小学校で学ぶ算数は、実生活に必要な最小限度の数的な処理について扱っているが、その中で、小学校5年で学ぶ分数の加法、減法の計算において、約分や通分を説明するためには、自然数の倍数や約数、最大公約数や最小公倍数の原理を習得する必要がある。

学習指導要領では、[内容の取り扱い]として、「最大公約数や最小公倍数を形式的に求

めることに偏ることなく、具体的な場面に即して取り扱うものとする」とし、学習指導要領解説では、「二つの整数の公約数や公倍数の集合は、それぞれの整数の約数や倍数からなる集合の共通な要素からなるものである。例えば、8の約数は  $\{1, 2, 4, 8\}$  であり、12の約数は  $\{1, 2, 4, 6, 12\}$  である。これらから、8と12の公約数は  $\{1, 2, 4\}$  となる。最大公約数は、公約数の中で最大の数であるから、4であることがわかる。また、8の倍数は  $\{8, 16, 24, 32, \dots\}$  であり、12の倍数は、 $\{12, 24, 36, 48, \dots\}$  である。これらから8と12の公倍数は  $\{24, 48, 72, \dots\}$  となる。最小公倍数は公倍数の中で最小の数であるから、24であることがわかる。…」としているが、例えば、7と11では、それぞれの約数は  $\{1, 7\}$ 、 $\{1, 11\}$  であるから、最大公約数が1に対し、最小公倍数は77という大きな数になってしまう。このことから、二つの数についての最大公約数や最小公倍数の性質に興味をもつ生徒は少なからずいるのではないかと考えられる。従前の学習指導要領では、このことも意識して、小学校5年生で素数の定義を導入していたと推察される。

算数・数学の指導において、「思考力、判断力、表現力」の育成は最も重要な目標であるが、さらに、「数学的活動と数学を学ぶ意義や楽しさ」を教室で如何に伝えるかが重要である。そのような観点にたつて、とくに、初等教育での素数の指導について考えてみよう。

### ・素数を探す

ある数が素数かどうかを調べる（考えさせる）ことは、小学校段階でも可能である。素数の定義「1と自分自身以外に約数を持たない数、ただし、1は素数でない」という定義は「それ自身の約数が2個である数」に置き換えられるが、この定義にしたがって素数をあらいだす方法について考えさせてみよう。

生徒は、1は素数でない定義に基づいて2は1と2しか約数がないから素数、3も同様に、1と3しか約数がないから素数、4は、1と2と4が約数になるから素数でない……と1つずつそれぞれの数の約数がどうなっているか愚直に調べていくことが想定できる。そこで、素数に関する性質の存在を指導する場面になる。

◆1「正の整数  $n$  が素数かどうかを判定するには、 $\sqrt{n}$  以下の素数で割り算すればよい」

【証明】ここで、 $\sqrt{n}$  に着眼したのは、 $n$  が合成数なら必ず  $\sqrt{n}$  より小さい素因数を持つからである。つまり、整数  $n$  が合成数とすると、少なくとも素因数  $p, q$  を用いて、

$$n = pq \quad (0 \leq p \leq q < n) \text{ で表される。ここで、} n = pq \geq p^2 \text{ であるから、} p \text{ は } \sqrt{n} \text{ 以下}$$

の素因数であるから、上のことがいえる。

[証明終]

2桁までなら素数か合成数であるかを判断することは、小学生でもそれほど難しいことではないが、3桁や4桁以上になると容易なものでないが、上のことを使えば多少計算が節約できることを知るのも新鮮味を与えるのではないか。

たとえば2017ならば、 $44 < \sqrt{2017} < 45$  であるから、43までの素数

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43の14個の数字で割り切れなければ素数ということになる。実際、1171は、これらの素数で割り切れず素数である

この考えにより、ここ数年の西暦が、素数か合成数かを考えさせるのも面白い。

2017素数,  $2018 = 2 \times 1009$ ,  $2019 = 3 \times 673$ ,  $2020 = 2 \times 2 \times 5 \times 101$ ,  $2021 = 43 \times 47$   
 $2022 = 2 \times 2 \times 3 \times 101$ ,  $2023 = 7 \times 17 \times 17$ , …

## ◆2 「エラトステネスの篩」

まず、2以外の偶数は素数でないから、これらを除く。さらに、3は素数であるから3の倍数で偶数でない「9, 15, …」も素数でない。4はすでに除かれているから、次に5が素数であるから、5の倍数で、2と3の倍数でない「25, 35, …」を除く。

このようにして、順に素数である数と素数でない数(合成数)を見つけていくことが「エラトステネスの篩(ふるい)」であるが、この「篩」という言葉も現代生活では死語に近い。

この生活用具の説明することも、農業の歴史を見る側面からも授業中の話題として、生徒の興味を引き起こすこともできる。

### ・規則性を考える

さて、文字式が伴うので、中学校以上になるが、次に考えるのが規則性である。

整数の中で、偶数や奇数はそれぞれ、 $n = 1, 2, 3, \dots$ として、 $2n$ ,  $2n+1$ とおけるが、素数を一般的に表現する方法はないだろうか。

2や3の倍数は素数でないから、 $6n$ で表される数は素数でない。さらに、

$6n-2 = 2(3n-1)$  は2の倍数,  $6n-3 = 3(2n-1)$  は3の倍数

$6n-4 = 2(3n-2)$  は2の倍数であるから、素数は、少なくとも6の倍数でない数のうち、 $6n-1$ ,  $6n-5$  すなわち、6で割って1か5余る数だけが、素数となる候補になることが、中学生なら理解可能である。

これにより、 $6 \times 1 - 1 = 5$ や、 $6 \times 2 - 5 = 7$ ,  $6 \times 2 - 1 = 11$ ,  $6 \times 3 - 5 = 13$  …は素数であるが、 $n = 20$ とすると、 $6 \times 20 - 1 = 119 = 7 \times 17$ ,  $6 \times 20 - 5 = 115 = 5 \times 23$ となり、ともに素数ではない。

すなわち、ある数が素数ならば、 $6n-5$  もしくは、 $6n-1$ の形で表されるが、その逆は成り立たない。ここで、必要性、十分性の数学の論理を学ぶ機会になる。

そこで、素数をどう表現したら良いかの疑問を投げかけることも思考力の育成にもつながるが、これは、数学上の永遠の課題であり、それが現代社会の基盤になっていることが、生徒の興味関心を喚起することに繋がるのではないか。

### ・素数の無限性

素数が無数に存在することは、紀元前300年頃にユークリッドが証明している。ただ、2020年4月時点で知られている最大の素数は、大型のコンピュータを駆使して2486万2048桁の数があることが発見されているが、素数には限りがあることの証明は背理法の簡単な例題になる。

## ◆3 「素数の数は無限である。」

【証明】[背理法による]

素数が有限であると仮定して、それらすべてを小さい順に、 $p_1, p_2, p_3, \dots, p_n$ とおくと、 $N = p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1$ という整数をつくると、あきらかに、 $N > p_n$ である。

$N$ は、 $p_1, p_2, p_3, \dots, p_n$ のどれでも割り切れないから素数である。

$N > p_n$  より、 $N$  は、 $p_1, p_2, p_3, \dots, p_n$  とは異なる素数である。これは、素数が有限であると仮定したことに矛盾する。よって、素数は無限に存在する。 [証明終]

紀元前300年頃にユークリッドが証明したとする方法も示しておきたい。

#### 【ユークリッドによる証明】

任意の異なる  $n$  個の素数を、小さい順に、 $p_1, p_2, p_3, \dots, p_n$  とおく。

ここで、 $N = p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1$  という数を考えると、あきらかに、 $N > p_n$  である。

$N$  が素数ならば、 $N > p_n$  より、 $N$  は  $p_1, p_2, p_3, \dots, p_n$  とは異なる素数となる。

$N$  が合成数ならば、 $N$  を割り切る素数が存在する筈であるが、 $N$  は  $p_1, p_2, p_3, \dots, p_n$  で割り切れないから、 $N$  を割り切るような、 $p_1, p_2, p_3, \dots, p_n$  とは異なる素数が存在する。

いずれにしても、 $p_1, p_2, p_3, \dots, p_n$  とは異なる素数が存在するから、素数は無限に多く存在する。 [証明終]

ここで、2つの証明についてみると、 $N = p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1$  とおいたときに、 $N$  が素数であるとしてはいけない。実際、 $N = 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$  は素数であるが、 $N = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031 = 59 \times 509$  となり、合成数となる。

すなわち、 $N = p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1$  の形の数は、素数の場合もあるし合成数となる場合もある。ユークリッドの証明はそこをクリアーしたものであり、背理法による証明は、素数が有限個と仮定したことの矛盾を利用したものであることを注意しておきたい。

#### ・素因数分解の可能性と一意性

新たに中学校1年生で学ぶことになった素因数分解であるが、これについて疑問を持つ生徒もいる。それは、どんな整数でも素数の積で表すことができるのかということと、素因数分解可能できたとしても、それが、一通りであるかである。これについても、きちんと説明しておく必要がある。

たとえば、12345 という5桁の整数の素因数分解では、最初、末尾が5であるから、素因数5に着目して、 $12345 = 5 \times 2469$  とした生徒と、偶数でないから次の素数である3で割ってみた、 $12345 = 3 \times 4115$  となって、最初に気がついた素因数によっては、素因数分解が、1通りではないのではという疑問である。この場合は、 $12345 = 3 \times 5 \times 823$  となるから(823は、小さいほうから数えて143番目の素数である)、この素因数分解は、先に5に着目しても3に着目しても結果は1通りに決まることを示せるが、もっと大きな数の場合には、必ず1通りになるかは、きちんとした説明が必要である。

◆4 「(1) 任意の正の整数  $n$  ( $n \geq 2$ ) は有限個の素数の積として表すことができる。

(これを素因数分解という)

(2) 素因数分解は、素因数の積の順序を無視すれば、その表し方は1通りである。

【証明】(1) (数学的帰納法を用いる) (i)  $n = 2$  のとき、 $n$  は素数だから成り立つ。

(ii)  $2 \leq k \leq n-1$  のとき、すべての  $k$  に対して有限個の素数の積で表されると仮定する。

$n$  が素数のときは成り立つことが明らかである。

$n$  が素数でないときは、ある正の整数  $a, b$  が存在して、 $n = ab$  ( $1 < a < n, 1 < b < n$ ) が成り立つ。仮定より、 $a, b$  はともに素数の積で表される。したがって、 $n$  も素数の積で表すことができる。

以上のことより、任意の正の整数  $n$  ( $n \geq 2$ ) は有限個の素数の積として表すことができる。

(2)  $n$  が2通りに素因数分解されたとすると、

$n = p_1 p_2 \cdots p_h = q_1 q_2 \cdots q_k$  ( $h \geq k$ ) と表される。このとき、 $p$  同士、 $q$  同士には同じ素数があってもよい。 $h \geq k$  により、素数  $p_1$  は  $q_1 q_2 \cdots q_k$  を割り切ることができる。このとき、 $q_1, q_2, \dots, q_k$  もすべて素数だから、 $p_1$  は、 $q_1, q_2, \dots, q_k$  のどれかを割り切る。 $q$  のどれを割り切るかは番号の付け替えにすぎないので、それを  $q_1$  とすると素数同士の割り算なので、 $p_1 = q_1$  といえることができる。したがって、これらを約すると、 $p_2 \cdots p_h = q_2 \cdots q_k$  となる。

$p_2$  に対しても同様なことがいえるから、 $p_3 \cdots p_h = q_3 \cdots q_k$  となり、これを繰り返すと、 $h > k$  とすると、 $p_{k+1} \cdots p_h = 1$  となる矛盾。したがって、 $h = k$  となり、素因数の順序を無視すれば素因数分解は一通りである。 [証明終]

これまでの、素数の基本的性質の証明に用いた、背理法や、数学的帰納法はそれぞれ、高等学校の数学1や数学Bで扱う内容であるため、中学生にはハードルが高いものの、高校生にとって難解なものではない。すなわち、素数の扱いには、学修者それぞれの学習の進捗状況に応じた対応ができるのではないかと。

### ・素数の表れ方の不思議

素数の出方には、興味ある性質がある。2桁の素数を見てみると、

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97

の25個あるが、2以外の偶数は素数でないから、3, 5, 7や11, 13, 17, 19, 41, 43などのように間の偶数を経て連続する素数の分布が見られる部分がある。このうち、3, 5, 7のような間に偶数1つだけがあって3個連続する素数を三つ子素数、2つだけ連続する素数を双子素数と呼ばれているが、このような性質を持つ素数の分布の不思議さに着目する生徒もいる。これまでに、38万桁を超える双子素数が確認されているが、このような双子素数が無限に存在することについて一般的な証明に取り組んだ小学生がいたことに驚かされる。三つ子素数には、次のことが言える。

#### ◆5 「三つ子素数は、3, 5, 7しかない」

【証明】三つ子素数の最小のものを、 $n$  とすると、他の2つは、 $n+2$ 、 $n+4$  とおける。このとき  $n$ 、 $n+2$ 、 $n+4$  のいずれかは3の倍数である。(なぜなら、連続する3つの数  $n$ 、 $n+1$ 、 $n+2$  には必ず3の倍数があり、 $n+4 = (n+1)+3$  であるから、 $n+1$  と  $n+4$  は3で割った余りは等しい)

3の倍数で素数となるのは3のみであるから、 $n$ 、 $n+2$ 、 $n+4$  のいずれかが3の場合で、かつすべて素数であるのは、3, 5, 7 しかない。 [証明終]

#### ◆6 「双子素数」

三つ子素数の存在は、素数全体からみてもただ1通りしかないことが証明されたが、双子素数の数は無限に存在するとの予想であり、いまだ証明されていない所謂、数学の未解決問題の1つであるが、この双子素数の存在証明に取り組み、今一步のところまでの論文を書いた小学4年生がいる。

この小学生 梶田光君は完全数（自分以外のある数の約数の和がそれ自身に等しい。たとえば、 $6=1+2+3$ 、 $28=1+2+4+7+14$  など）などについても取り組み、彼自身が発見した定理が4つもあるという。

梶田君が、小学4年生のときに書いた論文「双子素数予想の証明」について掲載させていただこう。

「 $x$ までの素数の個数を求める素数計数関数を $\pi(x)$ とすると、 $x$ と $x+2$ が素数であるか

どうかを求める関数は、 $(\pi(x)-\pi(x-1))(\pi(x+2)-\pi(x+1))=\begin{cases} 1 & (x, x+2 \text{ がともに素数}) \\ 0 & (\text{それ以外}) \end{cases}$  である。

よって、 $x$ 以下の双子素数のペアのうち小さいほうの素数の個数は、

$$\sum_{n=3}^x (\pi(n)-\pi(n-1))(\pi(n+2)-\pi(n+1)) \text{ となる。}$$

双子素数の組が無数にあることは、この式が発散することと同値である。」

この論文は残念ながら発散の証明が不完全だったため解けていなかったとのことであるが、双子素数という整数論の難解なテーマに対し、解析的な手法により、計算できる独自の式に書き直すという斬新な発想をする小学生の存在と、その豊かな才能に期待は膨らむ。

双子素数や三つ子素数など、素数の分布について考えると、素数が頻繁に現れる自然数の部分が存在に対して、連続する奇数の中で、長い区間素数が存在しない部分がある。これを素数砂漠というが、そのような箇所があるかも知能なところである。

実際、1桁の素数は4個あり、2桁の素数を10毎に区切ると、10～19では4個あるが、90～99では1個しかない。3桁になると、114～126では間の13個には1つもなく、4桁では、1130～1150までの21個には素数はない。

#### ◆7「いくらでも広い素数砂漠は存在する」

【証明】連続する $n-1$ 個の数を、 $n!+2$ 、 $n!+3$ 、 $\dots$ 、 $n!+n$ とすると、 $2 \leq k \leq n$ に対して、 $n!+k$ は $k$ の倍数なので、これら $n-1$ 個の数はすべて合成数（素数でない）。

したがって、これは長さの $n-1$ 以上の素数砂漠の一部であり、これは任意の $n$ について成立するのでいくらでも長い素数砂漠が構成存在する。 [証明終]

たとえば、 $7!=5040$ だから、5042、5043、5044、5045、5046、5047の連続する6個の数はすべて合成数であり、この区間には素数は存在しない。

ここまで、中学生や高校生にも理解できる程度の、素数の基本的とみられるいくつかの性質について述べてきたが、ある整数までにいったいどのくらいの数の素数があるかを近似的に述べた「素数定理」について触れておこう。

◆「(素数定理) 整数 $x$ までの素数の個数を $\pi(x)$ とすると、

$$\pi(x) \sim \frac{x}{\log x} \quad \text{すなわち、} \lim_{x \rightarrow \infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1$$

$x$ が非常に大きい数の場合は、素数の個数は、対数を用いた関数に近似されるというこの定理は、18世紀末、15歳のガウス（ドイツ）他によって予想されていたもので、1896年

フランスのアダマールとベルギーのプーサンによって別々に証明された。この定理の証明は、複素関数論を用いたもので難解なものである。さらに、1948年にハンガリー出身のエルデーシュとノルウェー出身のセルバーグ（2人とも後にアメリカへ）により、初等的な方法により証明した。

さて、実際の素数の数は、10以下では4個、100以下では25個、1000以下では168個、10000以下では、1229個 存在するが、この定理についてみてみよう。

$$\pi(10)=4, \pi(100)=25, \pi(1000)=168, \pi(10000)=1229 \quad \text{である。}$$

ここで、 $f(x)=\frac{x}{\log x}$  とおき、対数を常用対数に変換すると、

$$f(x)=\frac{x}{\log_{10} x}=\frac{x}{\log_{10} x} \times \log_{10} e \approx \frac{x}{\log_{10} x} \times \log_{10} 2.718 \approx \frac{x}{\log_{10} x} \times 0.4342$$

$$\text{となるから, } f(10^n) \approx \frac{10^n}{\log_{10} 10^n} \times 0.4342 = \frac{10^n}{n} \times 0.4342$$

$$n=1 \text{ のとき, } f(10) \approx \frac{10^1}{1} \times 0.4342 = 4.342, \quad n=2 \text{ のとき, } f(10^2) \approx \frac{10^2}{2} \times 0.4342 = 21.71$$

$$n=3 \text{ のとき, } f(10^3) \approx \frac{10^3}{3} \times 0.4342 = 144.73, \quad n=4 \text{ のとき, } f(10^4) \approx \frac{10^4}{4} \times 0.4342 = 1085.5$$

のように、確かめることができるが、小さな数ではこの定理が正しいことを実感することは難しいが、 $x=10^{10}$  として、コンピュータで計算した結果、その誤差は約4.8%、 $x=10^{20}$  とすると、その誤差は約2.3%となり、 $x \rightarrow \infty$  とすることで、定理を実感できる。

### 3 学ぶ楽しさ

昨年、本研究論集で「アクティブ・ラーニング」について拙稿を記述したが、その中で「なんで数学を学ぶの」という項目を立てた。その中では、算数・数学を学ぶ意義について述べたものの、やや抽象的な記述になった感もある。その反省を踏まえて、素数の指導を通して「数学を学ぶ楽しさや意義」について考えてみよう。

気候変動による温暖化の影響からか、私が子どもの頃は、めったに聞くこともなかった南方系の蝉「クマゼミ」の北限が北上し、その「蝉時雨」を、ここ神奈川でも聞くようになった。その蝉時雨に関して、半世紀以上の夏を経験してきた者にとって、特に賑やかな夏と、比較的穏やかな夏とがあることに、うすうすは感ずることもあったが、このことについて、蝉の特筆すべき性質があることを生徒に紹介しておきたい。

#### ◆「素数ゼミ」

セミは通常、数年の間、地中で少しずつ成長を続け、羽化（成虫になること）して、太陽の光をみてからは、せいぜい2週間程で息絶えてしまう。地上に出てからのわずかな期間、雄のセミは精一杯鳴くことで、雌のセミと仲良くなり、子孫を残していく。

この繰り返しは、氷河時代からずっと続いているようだが、アメリカの東部・南部に、13年、17年の間、地中で羽化することを待っているセミがいるようだ。この、セミは素数

ゼミと呼ばれ、その特異な習性に研究がなされてきた。

セミはその進化の過程において、羽化する周期の異なるセミ同士が交配すると、親の羽化する周期とは異なる幼虫ができ、それらはやがて次の世代を残すときに交配する相手がいなくなり、結果、子孫を残せないという現象がおきるようだ。

さらに、セミの天敵（主に鳥たち）も、周期的に大発生し、短い間しか地上にいることができないセミの羽化する周期とが一致してしまうと、大量に捕食されてしまい絶滅する恐れもある。

そこで、セミが成長に要するために地中に住む期間12年から18年程度の中で、異なる周期のセミ同士が羽化するタイミングをできるだけズラしたり、天敵の鳥たちが大量発生するタイミングを避ける必要があり、結果、最大公約数ができるだけ大きくなる素数である13年周期、17年周期の素数ゼミが誕生してきたようだ。

このように、素数ゼミたちは、厳しい氷河時代からずっと進化を遂げながら生き延びているが、何十万年もかかった氷河時代と比べ、現代の気候変動の速さは、セミの進化のスピードをはるかに越えるものであり、この貴重なセミの存在が続くのか危惧される。

#### ◆「RSA暗号」

前項で示したとおり、2021は、素因数分解をすると、 $2021 = 43 \times 47$  となるが、このように4桁の小さい数ですら、その素因数分解は容易ではない。まして、それが大きな桁数の数になれば、その計算は不可能に近いことは理解できる。

それに対し、 $43 \times 47 = 2021$  を求めることは、小学4年生でも十分求めることができるが、大きな数字を素因数分解するのは、これまで述べたように多少の計算の工夫はできても、結局、総当たりする以外に素因数を見つけ出す方法はない。したがって、コンピュータで素因数分解しようとしても、大きな数であれば膨大な時間がかかることになる。

この素因数分解の難しさに着目したのがRSA暗号である。ここで、暗号とは「特定のルールにしたがって変換されたデータ」であり、第3者がみても理解できないようにしたものであり、暗号を作成することを暗号化、暗号されたデータを元に戻すことを復号化というが、スマホやパソコンなど、セキュリティ対策を考える中で、暗号化の仕組みが気になっている人は多いと思う。

暗号には、いろいろなものがあり、その中でRSA暗号とは、「自分だけがもっている秘密キー（キーAとする）」と「皆に知らせている公開キー（キーBとする）」の2つのキーをつかって暗号化、復号化する暗号方式である。

ここで、キーAで作成したものはキーBだけしか戻せず（実際は、一部の例外を除いてはできない）が、キーBで作成したものはキーAだけしか戻せないような仕組みの暗号である。この仕組みを利用した暗号がRSA暗号で、これを1977年に発明したアメリカの3人の名前「R. L. Rivest, A. Shamir, L. Adleman」に由来している。

・RSA暗号は、具体的には、次のような手順になる。

Step 1 受信者が公開キーと秘密キーを生成する

i) 異なる大きな2つの素数  $p, q$  を任意にとる。

ii)  $n = pq$  とする。

iii)  $(p-1)(q-1)$  と互いに素な自然数  $e$  を任意にとる。（「互いに素」とは、最大公約数が 1 となるような数のこと）

iv)  $ed$  を  $(p-1)(q-1)$  で割った余りが 1 となる自然数  $d$  を任意にとる。

ここで、 $p$ ,  $q$ ,  $d$  は秘密キーであり、 $n$ ,  $e$  が公開キーとなる。

**Step 2** 送信者がメッセージを暗号化

i) 送りたいメッセージを自然数  $x$  ( $x < n$ ) とする。

ii)  $x$  を  $e$  乗し、これを  $n$  で割った余りを  $y$  とする。（この  $y$  が暗号文）

**Step 3** 受信者がメッセージを復号化

i)  $y$  を  $d$  乗する。

ii) これを、 $n$  で割った余りが、もとの  $x$  となる。

[具体的な例]

**Step 1** i) 計算が大変なので、ここでは、 $p=11$ ,  $q=3$ （秘密）とする。

ii)  $n=11 \times 3=33$ （公開）。

iii)  $(p-1)(q-1)=10 \times 2=20$  と互いに素な自然数 3（公開）をとる。

iv)  $d=7$ （秘密）として、 $(p-1)(q-1)=20$  で割った余りが 1 となる。

**Step 2** i)  $x=29$ （送りたい値）( $29 < 33$ ) とする。

ii)  $x=29$  を 3 乗 (=24389) し、これを 33 で割った余りは 2（暗号値）

**Step 3** i) 2 を 7 乗する (=128)。

ii) これを、33 で割った余りは、もとの 29 となる。

このように、公開鍵暗号方式は、暗号キーと復号キーが別々の暗号方式で、使用されたデータを解読するために使うのは復号キーであり、暗号キーでない。すなわち、暗号キーは公開されても問題ないが、復号キーは、絶対に秘密にしておかなくてはならない。

つまり、復号キーが解読されなければ、安全性は守られるということになる。

公開キー暗号方式で使われる暗号アルゴリズムには、様々な種類のものがあるが、RSA 暗号もその一種であり、公開キーで作成し暗号化、秘密キーを持つ者のみが復号化できる方法である。この仕組みは、逆の方向に使うことでデジタル署名にも応用できる。

すなわち、秘密キーを持つ側が、秘密キーによって自身の署名を暗号化し、この署名を受け取った側が公開キーによって署名を復号できれば、その署名が公開キーと対になる秘密鍵キー暗号化されたものだとは判明することになる。

このように、暗号とデジタル署名を両方とも達成できるアルゴリズムとして、世界で初めて登場し、現在まで 30 年以上の間、安全性を守る上での強力な暗号基盤として中心的な役割を担ってきており、2048 ビット (617 桁) の RSA 暗号は、スーパーコンピュータでも解読が困難とされている。

このように、素因数分解の難しさを安全性の根拠にするということは、逆も立場からみれば、時間を掛けてコンピュータで計算すれば素因数分解されてしまう危険性がある。

将来、現在のスーパーコンピュータを凌ぐとされている、量子コンピュータ（スーパーコンピュータでも 1 万年かかる計算を、わずか 3 分 20 秒で処理できるといわれており、従

来のコンピュータとは全く発想が異なる「量子力学」特有の理論を用いてつくられるコンピュータのこと)が実用化されると、RSA暗号の安全性が確保されていくのかは不明である。

#### 4 入学試験問題にみる素数

方程式や関数、図形などと比べ、教科書での扱いは少なく教室で学ぶ機会は多くはないが、高等学校や大学の入学試験では素数に関する出題例も少なくない。

中学校や高等学校の指導において、少なからず影響の多い入学試験から、これまで述べた基本的な素数の性質を基にしたいくつかの出題例をあげ、初等・中等教育での素数指導のあり方を考えてみよう。

##### 【素因数分解の例として】

[例題1] 999975 を素因数分解せよ。(2017 慶応義塾高校)

【略解答】 $1000000 - 25 = (1000 - 2)(1000 + 5) = 995 \times 1005 = 3 \cdot 5^2 \cdot 67 \cdot 199$

[例題2]  $\sqrt{\frac{2520n}{11}}$  の値が自然数になる最小の自然数  $n$  の値を求めなさい。

(2017 函館ラサール高)

【略解答】 $2520 = 2^3 \cdot 3^2 \cdot 5 \cdot 7$  より  $n = 11 \cdot 2 \cdot 5 \cdot 7 = 770$

##### 【双子素数と三つ子素数や、素数の規則性に着眼させる例として】

##### [例題3]

次は、先生、Aさん、Bさんの会話です。これを読んで、下の①、②に答えなさい。

先生「右の図のように、11から50までの自然数を並べます。この中で、11と13のように「差が2である2つの素数」の値は全部で4個あります。残りの3個をすべて教えてください。」

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

Aさん「です。」

先生「そのとおりです。では『差が2である2つの素数』の間にある自然数は、何の倍数ですか。」

Aさん「2の倍数だと思います。理由は、『差が2である2つの素数』ともに奇数だから、その間の数は必ず偶数になるからです。」

先生「そうですね。その説明は、51以上の自然数でも成り立ちますね。」

Bさん「先生、私は3の倍数でもあると思います。」

Aさん「どうして、3の倍数なのですか。」

Bさん「11以上の自然数について、次のように説明できます。」

(説明)  イ

先生「二人ともよく考えましたね。11以上の自然数について、『差が2である2つの素数』の間にある自然数は、2の倍数でもあり、3の倍数でもあるので、6の倍数でもあります。」

- ① ア にあてはまる、『差が2である2つの素数』の値をすべて書きなさい。
- ② イ にあてはまる、『差が2である2つの素数』の間にある自然数は3の倍数である理由を説明しなさい。 (2016 埼玉県公立高校)

【略解答】

- ① 17と19, 26と31, 41と43
- ② 連続する3つの自然数の中には必ず3の倍数が1つあり、差が2である「2つの素数」は、ともに3の倍数ではないので、その間の数が3の倍数である。

【素数の定義を確認させる例として】

【例題4】  $n^2 - 18n + 72$  が素数となる自然数  $n$  をすべて求めなさい。(2021 明治大中野高)

【略解答】  $(n-12)(n-6)$  より,  $n-12 = \pm 1$  or  $n-6 = \pm 1$  より  $n = 5, 13$

【数学A程度の数的処理能力を要する例として】

【例題5】 次の2つの条件を同時に満たす自然数  $n$  の値を求めなさい。

・  $2020 - n$  の値は93の倍数である      ・  $n - 780$  の値は素数である (2020 大阪府立高)

【略解答】  $2020 - n = 93k$  より,  $n - 780 = 1240 - 93k = 31(40 - 3k)$  より  $k = 13$   $\therefore n = 811$

【定義をもとに、限られた時間の中で思考力・数的処理能力を問う例として】

【例題6】 AとBを整数として、A以上B未満の素数の個数をA★Bで表すとします。

(1)  $10 \star 50 = [ \quad ]$

(2)  $(200 \star A) \times (A \star B) \times (B \star 50) = 9$  となるA, Bの組のうち、AとBの和が最も大きくなるのは  $A = [ \quad ]$ ,  $B = [ \quad ]$  のときです。 (2020 女子学院中)

【略解答】 (1) 11 (2)  $9 = 1 \times 1 \times 9$  or  $1 \times 3 \times 3$  より,  $A = 37$ ,  $B = 47$

他に、教科書にはない定義をもとに、思考力・判断力・計算力を問うものとして、2021年の栄光学園中では、「素積数」の定義を与えて考えさせる出題も注目される。

一方、大学入試では、基本的な素数の知識を確認する出題から、かなり高い思考力が必要なもので多彩であり、高等学校では殆ど学習する機会がないことを踏まえると、素数指導の難しさがある。いくつかの例をみてみよう。

【素数の基本を確認させる例として】

【例題7】 素数についての以下の問いに答えよ。

- (1) 2以外の2つの素数の和は素数にならないことを示せ。
- (2) 素数を小さいものから順番に10個書き上げよ。(答えのみでよい)
- (3) 2を含めた3つの素数の2乗の和は素数でないことを示せ。
- (4) 2以外の3つの素数の2乗の和で表される最小の素数を求めよ。(2022 北星学園大)

【略解答】 (1) 2以外の素数は、すべて奇数、奇数 + 奇数は偶数となるから素数にならない

(2) 略

(3) 2でない素数を  $p, q$  とする ( $p, q$  はともに3以上の奇数) と、 $(\text{奇数})^2 = \text{奇数}$  であるから、 $2^2 + p^2 + q^2$  は2より大きい偶数となって、素数にならない

[注]本問では $p$ ,  $q$ が異なることを前提にした。でない $と$ ,  $2^2+2^2+3^2=17$ は素数となる。

$$(4) 3^2+5^2+7^2=83$$

[例題8] 以下の問いに答えよ。 $f(n)=n^4-2n^2-3$

(1)  $f(n)$ を $n$ の2次式の積で表せ。

(2)  $n$ が自然数のとき、 $f(n)$ が素数になる $n$ は1つだけ存在する。このときの $n$ と素数 $f(n)$ を求めよ。(2021 北星学園大)

【略解答】(1)  $f(n)=n^4-2n^2-3=(n^2-3)(n^2+1)$

(2)  $n$ が自然数のとき、 $n^2+1 \geq 2$  したがって、 $n^2-3=1$ より、 $n=2$ ,  $f(n)=5$

[例題9] 次の問いに答えよ。

(1) 5以上の素数は、ある自然数 $n$ を用いて $6n+1$ または $6n-1$ の形で表されることを示せ。

(2)  $N$ を自然数とする。 $6N-1$ は、 $6n-1$  ( $n$ は自然数)の形で表される素数を約数にもつことを示せ。

(3)  $6n-1$  ( $n$ は自然数)の形で表される素数は無限に多く存在することを示せ。

(2009 千葉大)

【略解答】(1) 5以上の素数は、2の倍数でも3の倍数でもない $ので$ , 6で割った余りは1か5であり、 $6n+1$ ,  $6n-1$  ( $n$ は自然数)と表される。

(2)  $6N-1$  ( $N$ は自然数)は2でも3でも割り切れず、5以上であるから、素因数分解したときに表れる素数は、奇数であるから、 $6n+1$ あるいは $6n-1$  ( $n$ は自然数)と表される。ここで、 $6N-1$ がすべて $6n+1$ の形の素数しか約数にもたない $とすると$ ,  
 $6N-1=(6n_1+1)(6n_2+1)\cdots(6n_k+1)$  ( $n_1, n_2, \dots, n_k$ は整数)となり、左辺は6で割ると余り5、右辺は6で割ると余り1となり矛盾

(3)  $6n-1$  ( $n$ は自然数)の形で表される素数が有限であると仮定し、それらを $6n_1-1, 6n_2-1, \dots, 6n_k-1$  ( $n_1, n_2, \dots, n_k$ は整数)とする。このとき、(2)より、整数 $A=(6n_1-1)(6n_2-1)\cdots(6n_k-1)-1$ は、 $6n-1$ の形の素数で割り切れる筈だから $6n_1-1, 6n_2-1, \dots, 6n_k-1$ 以外に割り切れることになり矛盾。

【素数となる数、素数となる条件などを確認させる例として】

[例題10]  $P$ は3よりも大きい素数であり、 $p+4$ も素数であるとする。次の問いに答えよ。

(1)  $p$ を6で割った余りは1であることを示せ。

(2)  $p+2$ は3の倍数であることを示せ。

(3)  $(p+1)(p+2)(p+3)$ は120の倍数であることを示せ。(2021 富山大)

【略解答】(1) 例題9で触れたように、 $p$ は、 $6n \pm 1$ の形。 $p=6n-1$ のとき、

$$p+4=6n+3=3(2n+1) \text{ となり素数でない。}$$

(2)  $p+2=6n+3=3(2n+1)$  より

(3)  $(p+1)(p+2)(p+3)=12(3n+1)(3n+2)(2n+1)$  で  $3n+1, 3n+2$ は連続する整数なのでどちらかは2の倍数 さらに、 $p, p+1, p+2, p+3, p+4$ は連続する整数なので、どれかは5の倍数であるが、 $p, p+4$ は5ではない素数だから、 $p+1, p+2, p+3$ のいずれかは5の倍数である。

〔例題11〕  $n$  を2以上の自然数とする。 $n$  と  $n^2 - 2n + 3 = 3$  がどちらも素数となるときのすべての  $n$  を和を  $S$  とする。 $\frac{S}{2}$  の値を求めよ。〔選択肢省略〕 (2021 自治医大)

【略解答】  $n = 2$  のとき、 $n^2 - 2n + 3 = 3$  となり適する、 $n \geq 3$  のとき、 $n$  は奇数なので、 $n^2 - 2n + 3$  は偶数であり、 $n^2 - 2n + 3 = (n-1)^2 + 2 > 2$  であるから不適したがって、 $S = 2$  より、 $\frac{S}{2} = 1$

〔例題12〕  $n^3 - 7n + 9$  が素数となるような整数  $n$  をすべて求めよ。 (2018 京都大)

【略解答】  $n^3 - 7n + 9 = (n^3 - n) - 6n + 9 = (n-1)n(n+1) - 3(2n-3)$   
 $(n-1)n(n+1)$  は連続する3整数の積、 $3(2n-3)$  は3の倍数となり、 $n^3 - 7n + 9$  は常に3の倍数、したがって、 $n^3 - 7n + 9 = 3$ 、 $(n-1)(n-2)(n+3) = 0$  より、 $n = 1, 2, -3$

〔例題13〕 素数  $p, q$  を用いて  $p^q + q^p$  と表される素数をすべて求めよ。 (2016 京都大)

【略解答】  $p, q$  は2以上だから、 $p^q + q^p > 2^2 + 2^2 \geq 8$ 、 $p, q$  がともに奇数とすると、 $p^q, q^p$  はともに奇数だから、 $p^q + q^p$  が偶数となって矛盾。したがって、 $p, q$  のどちらかは偶数だから、 $q = 2$  として、 $p^2 + 2^p = f(p)$  とおくと、 $f(3) = 3^2 + 2^3 = 17$  は素数  
 $p \geq 5$  のとき、 $p$  は3の倍数でないから、 $p \equiv \pm 1 \pmod{3}$  であり、 $p^2 \equiv 1 \pmod{3}$

また、 $p$  は奇数であるから、 $2^p \equiv (-1)^p = -1 \pmod{3}$   
 $f(1) = 1^2 + 2^1 = 3 \equiv 0 \pmod{3}$        $f(-1) = (-1)^2 + (-1)^p \equiv 0 \pmod{3}$   
 となり、 $f(p)$  は17より大きい3の倍数だから素数にならない。

ゆえに、求める素数は17

【素数の個数に関する例として】

〔例題14〕 1000以下の素数は250個以下であることを示せ。 (2021 一橋大)

【略解答】 集合  $X$  の要素の個数を  $n(X)$  で表す。1から1000までの自然数全体の集合  $U$  の部分集合で、2の倍数全体の集合を  $A$ 、3の倍数全体の集合を  $B$ 、5の倍数全体の集合を  $C$  とすると、

$$n(A) = 500, \quad n(B) = 333, \quad n(C) = 200, \quad n(A \cap B) = 166, \quad n(B \cap C) = 66, \quad n(C \cap A) = 100, \\ n(A \cap B \cap C) = 33$$

したがって、2, 3, 5のいずれかの倍数であるものの個数は、  
 $n(A \cup B \cup C) = 500 + 333 + 200 - 166 - 66 - 100 + 33 = 734$  であり、この中の素数は、2, 3, 5の3個であるから、集合  $A \cup B \cup C$  の要素で合成数は  $734 - 3 = 731$  (個) である。さらに、集合  $A \cup B \cup C$  に含まれない合成数を探すと、6個の素数 7, 11, 13, 17, 19, 23 から平方数をつくると、これら6個は、すべて1000以下の合成数、さらに、異なる2つの積は、 ${}_6C_2 = 15$  (個) あり、これらも1000以下の合成数。すなわち、集合  $U$  の合成数であるから、すくなくとも  $731 + 21 = 752$  (個) は集合  $U$  の合成数。したがって、集合  $U$  に含まれる素数は少なくとも、 $1000 - 752 = 248$  (個) 以下である。

〔注〕「オイラー関数」あるいは「オイラーの  $\varphi$  関数」といえる考え方をを用いて、

$N = 2 \cdot 3 \cdot 5^2 \cdot 7 = 1050$  とする。1から $N$ までの自然数の中で、 $N$ と互いに素であるものの個数は

$$N - \left( \frac{N}{2} + \frac{N}{3} + \frac{N}{5} + \frac{N}{7} \right) + \left( \frac{N}{2 \cdot 3} + \frac{N}{2 \cdot 5} + \frac{N}{2 \cdot 7} + \frac{N}{3 \cdot 5} + \frac{N}{3 \cdot 7} + \frac{N}{5 \cdot 7} \right) - \left( \frac{N}{2 \cdot 3 \cdot 5} + \frac{N}{2 \cdot 3 \cdot 7} + \frac{N}{2 \cdot 5 \cdot 7} + \frac{N}{3 \cdot 5 \cdot 7} \right) + \left( \frac{N}{2 \cdot 3 \cdot 5 \cdot 7} \right) = N \left( 1 - \frac{1}{2} \right) \left( 1 - \frac{1}{3} \right) \left( 1 - \frac{1}{5} \right) \left( 1 - \frac{1}{7} \right) = 240$$

したがって、 $N$ 以下の素数は、2, 3, 5, 7の4個を加えて244(個)である。よって、1000以下の素数も244(個)以下である。

【メルセンヌ数、メルセンヌ素数に関する例として】

【例題15】 正の整数 $n$ に対して $M_n = 2^n - 1$ とする。このとき、次の問いに答えよ。

(1)  $M_1, M_2, M_3, M_4, M_5, M_6$ を求めよ。

(2) 正の整数 $k, l$ に対して、 $n = kl$ のとき、 $M_n = (2^k - 1) \sum_{j=1}^l (2^k)^{j-1}$  が成り立つことを示せ。

(3) 次の命題が真であることを示せ。  $n$ は合成数である  $\Rightarrow M_n$ は合成数である

(4) (3)の命題の裏を述べよ。また、 $n = 11$ とすることにより、(3)の命題の裏が偽であることを示せ。(2020 富山県立大)

【略解答】(1)  $M_1 = 1, M_2 = 3, M_3 = 7, M_4 = 15, M_5 = 31, M_6 = 63$

(2)  $\sum_{j=1}^l (2^k)^{j-1} = \frac{(2^k)^l - 1}{2^k - 1}$  であるから、 $n = kl$ のとき、 $\frac{(2^k)^l - 1}{2^k - 1} = \frac{2^n - 1}{2^k - 1}$  より

$$(2^k - 1) \sum_{j=1}^l (2^k)^{j-1} = 2^n - 1 = M_n$$

(3)  $n$ が合成数であるとき、 $k, l$ を2以上の自然数として、 $n = kl$ と表されるから、

(2)より、 $M_n = (2^k - 1) \sum_{j=1}^l (2^k)^{j-1}$  この右辺について、

$$2^k - 1 \geq 2^2 - 1 = 3, \sum_{j=1}^l (2^k)^{j-1} \geq \sum_{j=1}^2 (2^2)^{j-1} = 5 \quad \text{であるから、} M_n \text{は合成数である。}$$

(4) (3)の命題の裏は「 $n$ が1または素数  $\Rightarrow M_n$ は1または素数」

11は素数であり、 $M_{11} = 2^{11} - 1 = 2047 = 23 \times 89$ より、 $M_{11}$ が合成数であるから。

【ピタゴラス数と関連した例として】

【例題16】 正の整数の組 $(a, b, c)$ が次の式を満たすとする。

$$a^2 + b^2 = c^2$$

(1)  $a, b, c$ のうち少なくとも1つは偶数であることを示せ。

(2)  $a, b, c$ のうち素数でないものがあることを示せ。(2018 北海道大)

【略解答】(1) すべて奇数とすると、左辺は偶数、右辺は奇数となり矛盾。

(2) すべてが素数であるとする。(1)より、少なくとも1つは偶数であるが、偶数の素数は2しかない。したがって、 $a, b, c$ のうち1つは2、残りは奇素数となる。 $a, b, c$ は、正の整数なので、 $c \neq 2$  そこで、 $a = 2$ とすると、 $4 + b^2 = c^2 \Leftrightarrow 4 = (b - c)(b + c)$

これより、 $b-c=1$ 、 $b+c=4$  これを解いて、 $b=1.5$ 、 $c=2.5$ となり、 $b, c$  が奇素数に反する。

### 【 $n!$ と関連した例として】

【例題17】  $n$  を2以上の自然数とする。

- (1)  $n$  が素数または4のとき、 $(n-1)!$  は  $n$  で割り切れないことを示せ。
- (2)  $n$  が素数でなくかつ4でもないとき、 $(n-1)!$  は  $n$  で割り切れることを示せ。

(2016 東工大)

【略解答】 (1)  $n$  が素数のとき、 $(n-1)! = 1 \cdot 2 \cdots (n-1)$  が  $n$  で割り切れるためには、  
 $1, 2, 3, \dots, n-1$  のいずれかが  $n$  の倍数でなければならないが、  
 $0 < 1 < 2 < 3 < \cdots < n-1 < n$  より  $1, 2, 3, \dots, n-1$  のどれも  $n$  の倍数でない。  
 $n=4$  のとき、 $(4-1)! = 6$  は4の倍数でない。

(2)  $n$  が素数でないから  $n=pq$  ( $p \geq q \geq 2$ ) となる整数  $p, q$  が存在する。

(i)  $p \neq q$  のとき  $(n-1)-p = (p-1)(q-1) + (q-2) > 0$  より、 $n-1 > p$  だから

$(n-1)! = 1 \cdot 2 \cdots q \cdots p \cdots (n-1)$  は  $pq = n$  で割り切れる。

(ii)  $p = q$  のとき  $n \neq 4$  より、 $p \geq 3$  だから

$(n-1)-2p = (p-1)^2 - 2 > 0$  より、 $n-1 > 2p$  だから

$(n-1)! = 1 \cdot 2 \cdots p \cdots (2p) \cdots (n-1)$  は  $p^2 = n$  で割り切れる。

【参考】 東工大では、2011年のAO入試で、「 $n!$  が  $n^2$  の倍数となる自然数  $n$  を求めよ」という出題例がある。

この略解は、 $n=1$  のときは成立。 $n \geq 2$  のとき、 $n! = n(n-1)!$  より、 $(n-1)!$  が  $n$  の倍数になればよい。上記の問いの結果から、 $n$  が素数でなくかつ4でもないとき、 $(n-1)!$  は  $n$  で割り切れるから、 $n \geq 6$  の合成数も適することになる。

以上のように、大学入試問題における素数の扱いは多彩であり、高等学校の学習指導要領に記載された学習内容では、正解にたどり着くには高いハードルがあると感ずる。

本稿で示したもの以外に、カタラン数と関連した2021年の東工大での例など、素数が取り上げられた例は多数あったが、本稿の主旨とページ数を考えて割愛した。

## 5 あとがき

高等学校までの学習指導要領上では、素数に関して、その定義と素因数分解程度の扱いであるが、素数には不思議な性質が数多くあり、それが現代社会への影響が大きい分野であることは周知のことである。

ところが、それら多くのことを教室で学ぶための物理的な時間を確保することは難しい現実がある。そのような中で、素数の様々な性質やその神秘性に興味・関心を抱く生徒も

少なからず存在していることも現実である。

本拙稿では、素数について、最小限教室で扱っておきたい内容や、現実には、高等学校、大学の入学試験で取り上げられている例をあげ、素数指導のあり方について再考したいという思いを述べたかった。

しかし、調べれば調べるほどに、素数の奥深さ、難解さに直面し、複素関数論との関係、ゴールドバッハ予想 リーマン予想など素数研究上、避けて通れない内容も自身の浅学の知識では、十分なものが書けなかった。本稿が、素数の指導をあらためて検討しようと考えている中学校、高等学校の先生方の1つの問題提起となってもらえれば幸いである。

---

### 【参考文献】

- ・ 高等学校学習指導要領（平成30年告示）
- ・ 高等学校学習指導要領解説（平成30年告示）
- ・ 中学校学習指導要領解説（平成29年告示）
- ・ 小学校学習指導要領解説（平成29年告示）
- ・ 旺文社 全国大学／高等学校 入試問題正解 数学
- ・ 2022. 3. 11付 朝日新聞
- ・ 岩波書店 松坂和夫 代数学入門
- ・ 文藝春秋 吉村 仁 素数ゼミの謎
- ・ 講談社ブルーバックス 神永正博 現代暗号入門
- ・ Newton 他