素数

TOP『時間と空間の物理学』へ戻る

素数はユークリッドやエラトステネスの昔から、多くの優れた数学者によって研究されてきましたが、与えられた任意の数が素数であるか否かを判定する効率的方法（数学的理論と言っても良い）については、未だにはっきりした解答は得られていないようです。

確かに、素数を小さい方から順に並べてみると、その現れ方はランダム（不規則）で、はっきりとした規則性を見いだすのは中々困難です。したがって、ある素数の、次の素数を予測することも、不可能に思われます。

ですが、数の世界に不規則が堂々と居座っているのも、なんとなく癪（しゃく）ではあります。そこで、ある数が素数であるかどうかを判別する方法について、どの程度有効かはともかくとして、私なりに気づいた事柄を少し述べてみたいと思います。

1　素数に見られる規則性

一見ランダムに現れて来るように見える素数ですが、やはりその存在には一定の規則性が認められます。

以下に述べる文中には素数でない数も登場しますが、それらの数（1 を除く）は、分かり易く赤字にしておきます。

或る数を［6n］（ n は自然数＝ 1, 2, 3, 4, ････ n ）とすると、素数のすべては、［6n+1］もしくは［6n-1］のいずれかで表すことができます。別の言い方をすれば、素数のすべては、［6n+1］もしくは［6n-1］のいずれかの数列に属するということです。（念のために言っておくと、［6n+1］及び［6n-1］で表される数というの

は、6 で割ると必ず 1 もしくは 5 という剰余が出るという意味ですから、当然 2 及び 3 も因数として含んでいない数です。）

さて二つの数列には、もちろん素数でないもの（＝合成数*＝赤字表示）も混じっていますが、取りあえず話を進めます。

*1 を除く二つ以上の自然数の積の形で表すことが出来る数が**合成数**です。

素数列を、このように［6n+1］と［6n-1］の二つのグループに分けてみると、実に簡単な規則性が姿を現します。［6n+1］を A グループ、［6n-1］を B グループとしますと、素数 P は、$P = 6n + 1$　もしくは $P = 6n - 1$　のいずれかの数列に属します。すなわち A グループ、B グループそれぞれのグループにおいて、素数は、最初の素数を基準に 6 つ目ごとの位置にだけ出現する、ということなのです。

これは、少なくとも［90］以内の“小さい素数”の範囲では成り立っています。

A グループ（［6n+1］）　（n=0 の場合すなわち［1］を、素数ではありませんが例外的に配置し、以下 n=1 から n=14 までを適用した結果です。

1, 7, 13, 19, 25, 31, 37, 43, 49, 55, 61, 67, 73, 79, 85　（初項“1”、等差“6”の等差数列）

B グループ（［6n-1］）　（n=1 から n=15 までを適用した結果です。

5, 11, 17, 23, 29, 35, 41, 47, 53, 59, 65, 71, 77, 83, 89　（初項“5”、等差“6”の等差数列）

よく見ると分かると思いますが、A グループの各数字に［10］をプラスした数が 5 を除く B グループを形成しています。そして A、B のグループを合わせると、1 を除く黒字はすべて素数であると同時に、［90］以内に存在する素数のすべてを含んでいることもわかると思います。

また、それぞれのグループに属している数字は、“1 と 89”、“7 と 83”、“13 と 77”のように（素数かどうかはともかく）、加えると［90］になる数だけで構成されています。

以上が、素数（とその親戚数）のあいだに見られる性質というか、一種の規則性です。

2　素数判定

2.1　数列と函数（方程式）

あまり難しい話をするつもりはありませんし、そもそも出来ませんが簡単に言うと、私は数列とは函数 $y = f_{(x)}$ の x が、自然数 n を含む数式に限定されたものだと理解しています。

したがって、$P = 6n + 1$ も $P = 6n - 1$ は勿論数列です。しかしこれらの数列は“素数の数列”ではありません。何故ならこの式の P は素数ではないからです。強いて言うなら“素数候補の数列”でしょうか。

もし“素数数列”と呼べる式（n に順番に 1、2、3、‥‥ n と代入していくとき、P が順番に素数だけを与えてくれる様な方程式）を立てることができたら、素数は容易に確定できるのですが、それは原理的に不可能でしょう。素数数列の一般項を自然数 n を使って定義することができないからです。

したがって与えられた数 P が素数であることを証明するためには、P が素因数分解出来ないことを示すほかないことになります。

この素因数分解、すなわち検証作業（テスト）は具体的には、対象の数 P を必要なすべての素数で割って見ることになりますが、P が大きな数になればなるほど、大変な時間と労力とが必要になってきます。

そこで浮かんだのが $P = 6n \pm 1$ という“素数候補の数列”と、それを二つのグループに分けて扱うというアイデアです。

2.2　合成数の特定—1

二つにグループに分けした“素数候補の数列”から、まず合成数を特定し、それを自然数列から除外することで二次的に素数を特定するという方法を用いれば、、素因数分解に依るよりはかなり楽です。

まず、$P = 6n \pm 1$ の式中に存在する合成数の特定について説明します。

n に注目するのですが、形としてもシンプルですし、運用も（後に紹介しますが）容易です。　　※ 特に式中の加減記号（ ＋　－) の関係には注意が必要

［A］　**或る数 P が**　$P = 6n + 1$　**で表される場合**

$n = (P - 1) \div 6$

（以下の式中、m 及び a は、共に自然数）

（1）$n = (6m + 1)a + m$　**の時**　**P は $(6m + 1)$ の倍数、すなわち合成数です。**

（2）$n = (6m - 1)a - m$　**の時**　**P は $(6m - 1)$ の倍数、すなわち合成数です。**

［B］　**或る数 P が**　$P = 6n - 1$　**で表される場合**

$n = (P + 1) \div 6$

（1）$n = (6m + 1)a - m$　**の時**　**P は $(6m + 1)$ の倍数、すなわち合成数です。**

（2）$n = (6m - 1)a + m$　**の時**　**P は $(6m - 1)$ の倍数、すなわち合成数です。**

以上は一般公式です。

2.3　合成数の特定―2

まず前項で示した公式を、もう少し利用し易い式に書き直した具体的な例を紹介します。

今仮にわかっている素数が 19 までだとしたら、5 以上 19 までのすべての素数について

［A］	［B］
$n = 5a - 1$	$n = 5a + 1$
$n = 7a + 1$	$n = 7a - 1$
$n = 11a - 2$	$n = 11a + 2$
$n = 13a + 2$	$n = 13a - 2$
$n = 17a - 3$	$n = 17a + 3$
$n = 19a + 3$	$n = 19a - 1$

というように式を作ります。［2 と 3 は素数ですが、初めから P ($P = 6n \pm 1$）の式中に含まれませんので、考慮する必要がありません。］

n は勿論求める素数 P ($P = 6n \pm 1$）の式中の n のことです。

この 12 個の式を使って、19×19 つまり数値 $19^2 = 361$ 近辺までにある素数の全てを拾い出すことができます。

この式で見つけ出せる素数より更に大きな素数を見つけるには、まず 19 以上の素数を特定してからということになります。（7 から続く素数列のうち、一つで

も欠落があると、この“素数予測”“素数判定”は成り立ちません。）

では続けましょう。混乱を避けるために A グループと B グループに分けて作業を進めます。

（1）A グループに分類した 6 つの式で、それぞれ $6n+1$ の数値が 361 以内に収まるような n をもとめます。ちなみに、この場合の n の最大値は 60 ですね。それぞれの式で 60 **未満**の n を列挙します。（60 は入れません）

$n = 5a - 1$　　4　9　14　19　24　29　34　39　44　49　54　59

最初の数に 5 を加えていくだけです。乗法を使っても結構。以下も同様に

$n = 7a + 1$　　8　15　22　29　36　43　50　57

$n = 11a - 2$　　9　20　31　42　53

$n = 13a + 2$　　15　28　41　54

$n = 17a - 3$　　14　31　48

上記の**数表の中に無い数**を拾い出してみると、次のようになります。

5　6　7　10　11　12　13　16　17　18　21　23　25　26　27　30　32　33　35　37　38　40　45　46　47　51　52　55　56　58

30 個‥‥以外にたくさんある印象ですが、これらの数を n に持つ $6n+1$ は、すべて素数です。

（2）次に A グループに施したと同じ操作を B グループに対しても行います。

$n = 5a + 1$　　6　11　16　21　26　31　36　41　46　51　56

$n = 7a - 1$　　6　13　20　27　34　41　48　55

$n = 11a + 2$　　13　24　35　46　57

$n = 13a - 2$　　11　24　37　50

$n = 17a + 3$　　20　37　54

数表の中に無い数を拾い出してみると、次のようになります。

4　5　7　8　9　10　12　14　15　17　18　19　22　23　25
28　29　30　32　33　38　39　40　42　43　44　45　47
49　52　53　58　59

以上の 33 個です。これらの数を n に持つ $6n-1$ も、すべて素数です。

見つかる素数の中で最も小さい素数は、今回の場合 $n=4$ が適用される $6n-1$ ですから、23 ということになります。これが素数 19 の次の素数です。見つかった最も大きい素数は、$6n-1$　$n=59$ の 353 です。

値 19 まである 5 個の素数を使って、値 353 の素数まで、新たな素数 63 個を発見できました。漏れはありません。

2.4　その後の展開

当然のことですが、見つけた素数の数が増えて行くにつれ、上記の作業も増えていきます。大きなケタ数になれば、現実的にはコンピューターの力を借りなければ処理不可能だと思います。

しかし、計算そのものは加減乗除を使うだけの、しかも実に単純な計算なので、紙と鉛筆だけでかなりの所までやれます。根気と注意力が必要ですが。

それでは素数 353 以後に挑戦します。本当は見つけた素数全部を使いたいのですが、たくさんだと記述が長くなるので、ここでは少しだけ、やり方を見て頂く程度にします。好きな量だけ進めていけるのも長所ですかね。

今回は前の項で使った数表に素数 $n=19a\pm3$ を一つだけ追加してみます。それで、数値 $23^2=529$ 近辺までに潜む素数を確定できます。

使用済みの数 $n<60$ は分かり易く青字にしておきましょう。(不要なのです)

$n=5a-1$	4　9　14　19　24　29　34　39　44 49　54　59　64　69　74　79　84
$n=7a+1$	8　15　22　29　36　43　50　57　64 71　78　85
$n=11a-2$	9　20　31　42　53　64　75　86
$n=13a+2$	15　28　41　54　67　80
$n=17a-3$	14　31　48　65　82

$n = 19a + 3$　　22　41　60　79

数表の中に無い 88 未満の数を拾い出してみると、次のようになります。

61　62　63　66　68　70　72　73　76　77　81　83　87

これらの数が n である $6n + 1$ は素数です。

もう 1 つのグループも同様に

$n = 5a + 1$　　6　11　16　21　26　31　36　41　46　51　56　61　66　71　76　81　86

$n = 7a - 1$　　6　13　20　27　34　41　48　55　62　69　76　83

$n = 11a + 2$　　13　24　35　46　57　68　79

$n = 13a - 2$　　11　24　37　50　63　76

$n = 17a + 3$　　20　37　54　71

$n = 19a - 3$　　16　35　54　73

数表の中に無い 88 未満の数は

60　64　65　67　70　72　74　75　77　78　80　82　84　85　87

これらの数が n である $6n - 1$ は素数です。

新たに確定できた素数は最小が $6 \times 60 - 1 = 359$ で、最大は $6 \times 87 + 1 = 523$ の 28 個です。359 は前項で見つけ出した最大の素数 353 の次に位置する素数です。

2.5　蛇足

未知の新しい素数の発見といえば、有名な“メルセンヌ数”に触れないわけにはいきませんが‥。

メルセンヌ数は 2 のベキ乗数から 1 を引いた数で、数式で書けば　$M_n = 2^n - 1$ です。

もちろんメルセンヌ数の中には素数も合成数も含まれています。にもかかわらず新しい素数発見にメルセンヌ数が重宝される一番の理由は、効率の良い検算（テスト）法が研究されたからだろうと思います。

さらに、“新しい素数の発見”が、既知の素数を超える大きなケタ数の素数

を特定することだと考える場合には、より一層メルセンヌ数には価値があるでしょう。

しかし、メルセンヌ数に対する私の関心はそれ程高くありません。理由は、あまりに特殊な素数であり過ぎるからです。素数は、既に検証済みのものだけでも膨大な数ありますが、その中でいわゆるメルセンヌ素数と呼ばれるものは、僅か数 10 個です。ほとんどの素数はメルセンヌ数と関係ないのです。

はっきり言って、素数とメルセンヌ数のあいだには、直接的な関連性はありませんから、“素数そのものの研究”には、メルセンヌ数を扱う必要はないと思っています。

ここに紹介した方法を利用すれば、一つのメルセンヌ素数と次のメルセンヌ素数との間に放置されたすべての素数を漏れなく拾い上げることが出来ます。

TOP『時間と空間の物理学』へ戻る