素数いろいろ

Ｈ１　下尾　知

１、素数

（１）素数の定義

知っているとは思いますが、素数の定義をあらためて確認しましょう。

素数：１およびその数自身の他に約数を有しない正の整数。

「広辞苑　第五版」より

例えば、１３は１と１３と－１と－１３でのみ割り切れますが、約数も正の整数ですので、－１や－１３は１３の約数ではありません。ゆえに１３は素数です。

誤解がないために書いておきますが、

「１、およびその数自身の他に約数を有しない正の整数。」ではなく、

「１およびその数自身、の他に約数を有しない正の整数。」ですので、

１は素数ではありませんよ。

また、１でも素数でもない正整数を合成数と言います。

他には、双子素数と言うものがあります。

双子素数とは

｛３，５｝｛５，７｝｛１１，１３｝｛１７，１９｝｛２９，３１｝

のように差が２である素数の組のことです。

数が大きいものであれば、｛９９９８９，９９９９１｝などがあります。

また、双子素数予想は、

「双子素数は無限に存在する」

というものなのですが、いまだに解決されていません。

（２）エラトステネスの{EQ ¥* jc2 ¥* "Font:ＭＳ 明朝" ¥* hps10 ¥o¥ad(¥s¥up 9(ふるい),篩)}

「エラトステネスの篩」というのは、正整数の集合から、素数だけを篩い出す方法です。

素数を習った人はおそらく聞いたことがあるでしょう。

では実際にこの方法を使って１００までの素数表を作ってみましょう。

まず、２～１００の整数を並べます。

次に、２は素数なので残して、２から先の２の倍数を消します。

次に、残った最初の数３を残して、３から先の３の倍数を消します。

次に、残った最初の数５を残して、５から先の５の倍数を消します。

次に、残った最初の数７を残して、７から先の３の倍数を消します。

次に、残った最初の数１１を残して、１１から先の１１の倍数を消します。
ですが、もう残っている１１の倍数はありません。
　なぜなら、１１×２，１１×３，…，１１×１０はもう消えているので、消すことが出来るのは１１×１１以上の１１の倍数であり、それはすでに範囲外だからです。
結局、２乗が１００を超えないところまで、つまり、１０までの素数を使って消せばいいのです。

以上のような作業をすると下のようになります。

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~~

つまり、１００までの素数は、
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
になります。

　次に、このような作業をした後に何個の素数が残るか、というのを数えるのではなく、計算して求めてみましょう。
（ここで出てくる[ｎ]というのはガウス記号といって、ｎの整数部分を表しています。）

　まず、２，３，５，７の倍数の個数を計算します。
　　２の倍数は[１００÷２]＝５０個、
　　３の倍数は[１００÷３]＝３３個、
　　５の倍数は[１００÷５]＝２０個、
　　７の倍数は[１００÷７]＝１４個
なのですが、２，３，５，７は素数であり、１は素数ではないので、それらを修正すると、結局１１４個になります。
　でも、これを１００から引いてしまうと引きすぎてしまうので、次は、重複部分の個数を計算しましょう。
　　６の倍数は[１００÷６]＝１６個、

１０の倍数は[１００÷１０]＝１０個、
１４の倍数は[１００÷１４]＝７個、
１５の倍数は[１００÷１５]＝６個、
２１の倍数は[１００÷２１]＝４個、
３５の倍数は[１００÷３５]＝２個、
合計すると４５個になります。
でも、これでは戻しすぎるので、今度はさらに重複している部分の個数を計算しましょう。
３０の倍数は[１００÷３０]＝３個、
４２の倍数は[１００÷４２]＝２個、
７０の倍数は[１００÷７０]＝１個、
１０５の倍数は[１００÷１０５]＝０個、
合計６個になります。
最後に、４個重複している部分の個数を計算してみます。
２１０の倍数は[１００÷２１０]＝０個、
これ以上重複している部分はありません。
結局、残った個数は１００－１１４＋４５－６＋０＝２５個になります。
この方法は、素数表の範囲が大きくなるとコンピューターでも計算が大変になってしまいます。しかし考え方は重要であり、このような考え方のことを包除原理といいます。

（３）素数が無限にあることの証明
素数が無限にあることの証明にはいろいろな方法がありますが、ここでは１番簡単な証明法を紹介しておきます。

証明　素数の個数が有限個であったとして、最大の素数をＭとする
Ｎ＝　１×２×……×Ｍ＋１
を作る。これは明らかにＭより大きいので、合成数である。
ところが、すべての素数である１，２，……，Ｍのどれで割っても１余って、割り切れない。ということは、Ｎが素数であることになり、矛盾する。
ゆえに、素数の個数は有限個ではない。

これはあくまで数多くある証明の一つです。他の証明を見てみたいと言う人は、本を買ってみたり、ホームページをみたりして、いろいろと調べてみてください。

２、いろいろな素数
（１）　メルセンヌ素数
昔の数学者はいつも素数を表す式について、いろいろ考えました。その中でメルセンヌという数学者は、a^n-1（ｎは自然数)の形を考えました。

しかし、$a^n-1=(a-1)(a^{n-1}+a^{n-2}+\cdots\cdots+1)$であるから、$a>2$ならば$a^n-1$はいつも合成数です。

だとすると、$a=2$ならばどうなるのでしょうか。2^n-1の形の数はどのような場合に素数になるのでしょうか。いくつか計算してみましょう。

$M_n=2^n-1$と置きます。

ｎ＝１のとき、$M_1=2^1-1=1$　　ｎ＝９のとき、$M_9=2^9-1=551$

ｎ＝２のとき、$M_2=2^2-1=\underline{3}$　　ｎ＝１０のとき、$M_{10}=2^{10}-1=1023$

ｎ＝３のとき、$M_3=2^3-1=\underline{7}$　　ｎ＝１１のとき、$M_{11}=2^{11}-1=2047$

ｎ＝４のとき、$M_4=2^4-1=15$　　ｎ＝１２のとき、$M_{12}=2^{12}-1=4095$

ｎ＝５のとき、$M_5=2^5-1=\underline{31}$　　ｎ＝１３のとき、$M_{13}=2^{13}-1=\underline{8191}$

ｎ＝６のとき、$M_6=2^6-1=63$　　ｎ＝１４のとき、$M_{14}=2^{14}-1=16383$

ｎ＝７のとき、$M_7=2^7-1=\underline{127}$　ｎ＝１５のとき、$M_{15}=2^{15}-1=32767$

ｎ＝８のとき、$M_8=2^8-1=255$

下線を引いているのが素数です。

まず、ｎが合成数のとき、ｎ＝ｓ×ｔ，$2^s=r$と置くと、

$$2^n-1=2^{s\times t}-1=r^t-1=(r-1)(r^{t-1}+\cdots\cdots+1)$$

となり、ｓ＞１だからｒ＞２で、2^n-1が合成数であることがわかります。しかし、ｎ＝１１のときは素数にならないので、ｎが素数の場合に絶対素数になるわけではありません。

そこで、メルセンヌは「ｎが２５７までの中で

ｎ＝２，３，５，７，１３，１７，１９，３１，６７，１２７，２５７（全て素数）

のときにM_nも素数である」と予想しました。（おそらく大変な計算をしたのでしょう）

現在では、M_{67}，M_{257}のときは素数ではなく、M_{61}，M_{89}，M_{107}は予想から抜けていたことがわかっています。

なぜこんなことが断言できるのかというと、リュカという人が１８９１年に、メルセンヌ型の整数に対して、それほど長い時間をかけずに素数かどうかを判定できる、リュカ・テストと呼ばれる方法を発見しました。どんな方法かというと、例えばM_7が素数かどうか確かめたいとき、４から始めて、(mod M_7) で２乗しては２を引くという操作を続けます。

$M_7=127$

$a_1=4$

$a_2\equiv 4^2-2\equiv 14$ （mod M_7）

$a_3\equiv 14^2-2\equiv 67$ （mod M_7）

$a_4\equiv 67^2-2\equiv 42$ （mod M_7）

$a_5\equiv 42^2-2\equiv 111$ （mod M_7）

$a_6\equiv 111^2-2\equiv 0$ （mod M_7）

a_{7-1}まで計算して、

$a_{7-1}\equiv 0$ （mod M_7）ならばM_7は素数であり、

$a_{7-1} \not\equiv 0 \pmod{M_7}$ ならば M_7 は素数ではありません。

（b≡c(mod a)というのは、ｂとｃの差がａで割り切れることを表しており、このことをｂとｃがａに関して合同である、という）

以上のような方法を使えば、とても大きな素数を見つけ出すことが可能になります。ちなみに、２００２年までの最大のメルセンヌ素数は$M_{13466917}$です。

（２） 完全数

数にはいろいろな分類があるが、その中に過剰数、不足数、完全数というものがあります。

まず、過剰数というのはその数自身を除いた約数の総和がその数より大きい数のことを表します。例えば、２４はその数自身を除いた約数の総和が１＋２＋３＋４＋６＋８＋１２＝３６となり、２４より大きいので過剰数です。

次に、不足数というのはその数自身を除いた約数の総和がその数より小さい数のことを表します。例えば、２５はその数自身を除いた約数の総和が１＋５＝６となり、２５より小さいので不足数である。素数はその数自身を除いた約数は１のみなので、明らかに不足数です。

最後に、完全数というのはその数自身を除いた約数の総和がその数と等しくなる数のことを表します。例えば、６はその数自身を除いた約数の総和が１＋２＋３＝６となるので完全数です。次に小さい完全数は２８で、その後は４９６，８１２８，……と続きます。

では、どんな数が完全数になるのでしょうか。驚くべきことに、この答えは完全ではありませんが、かの有名なユークリッドによって２３００年も昔に出されています。

「もし単位から始まり順次に１対２の比をなす任意個の数が定められ、それらの総和が素数になるようになされ、そして全体が最後の数に掛けられてある数をつくるならば、その積は完全数であろう。」

このままだと何を言っているのかわからないので、わかりやすく解説してみたいと思います。

まず、「単位から始まり順次に１対２の比をなす任意個の数が定められ、それらの総和が素数になる」というのは、$1+2+2^2+2^3+2^4+\cdots\cdots+2^{n-1}=2^n-1$が素数である、と言っています。つまり、メルセンヌ素数のことです。これが「最後の数に掛けられる」のだから、$N=2^{n-1}(2^n-1)$が完全数である、とユークリッドは主張しています。

ユークリッドはｎ＝３のときの具体的な場合を証明していますが、その証明は完全に一般的です。しかし、ユークリッドの証明はたいへん長く、また現代式とはだいぶ違うので、ここでは現代風に書き直した証明をのせておきます。

ｎを正整数とする。2^n-1が素数ならば、$N=2^{n-1}(2^n-1)$は完全数である。

証明　2^{n-1}の約数と2^n-1の約数との積はＮの約数で、また2^{n-1}と2^n-1は互いに素だ

から、これでNの約数は尽くされる。

2^{n-1}の約数は１，２，2^2，2^3，2^4，……，2^{n-1}

2^n-1は素数だから、その約数は１，2^n-1

ゆえに、Nの約数は

1×1，$1\times(2^n-1)$，2×1，$2\times(2^n-1)$，……$2^{n-1}\times1$，$2^{n-1}\times(2^n-1)$

である。

結局、Nの約数（N自身も含む）の総和は、

$(1+2+2^2+2^3+2^4+\cdots\cdots+2^{n-1})(1+2^n-1)=(2^n-1)2^n=2N$

であるから、N自身を除いた約数の総和は$2N-N=N$である。

次に気になるのは、この逆はどうなのだろうか、ということです。

つまり、Nが完全数ならば、$2^{n-1}(2^n-1)$の形でなければならないか、ということです。

ユークリッドはこの証明はしなかったが、後のオイラーは、偶数の完全数は$2^{n-1}(2^n-1)$の型に限ることを、次のように証明した。（ここで出てくる$\sigma_1(N)$というのはNの約数の総和を表しており、$a=b\times c$（ｂとｃは互いに素）のとき$\sigma_1(a)=\sigma_1(b)\times\sigma_1(c)$である。ちなみに$\sigma_0(N)$というのはNの約数の個数である。）

偶数の完全数は$N=2^{n-1}(2^n-1)$の型に限る。

証明　Nが偶数の完全数であるとする。Nから因数２をできるだけ出して、

$N=2^{r-1}k$，ｋは奇数

とする。ｒ－１としたのはあとの形と合わせるためである。

$\sigma_1(N)=\sigma_1(2^{r-1}k)=\sigma_1(2^{r-1})\,\sigma_1(k)$

$\sigma_1(2^{r-1})=1+2+2^2+2^3+2^4+\cdots\cdots+2^{r-1}=2^r-1$

だから、

$\sigma_1(N)=(2^r-1)\,\sigma_1(k)$……①

Nは完全数だから、

$\sigma_1(N)=2N=2^rk=(2^r-1)k+k$……②

①，②より$(2^r-1)\,\sigma_1(k)=(2^r-1)k+k$

両辺を(2^r-1)で割ると、

$$\sigma_1(k)=k+\frac{k}{2^r-1}$$

右辺の２項はｋの約数で、その和が約数全体の和$\sigma_1(k)$になるのだから、ｋの約数は２つだけ。よってｋは素数で、もう一つの項は１でなければならない。よって、

$k=2^r-1$（素数）

ゆえに、$N=2^{r-1}(2^r-1)$

いまだに、奇数の完全数は発見されていません。「存在しないであろう」という予想ですが、証明されていません。存在したとしても100^{100}以上だそうです。

（３） フェルマー素数

「素数を表す式はあるか」という問題でかの有名なフェルマーは、

$$F = 2^m + 1$$

という型の数を考えました。

mから２のベキをできるだけ出して、

$$m = 2^t k = uk,\ k \text{は奇数}$$

とします。さらに、$2^u = v$と置くと、

$$F = 2^m + 1 = 2^{uk} + 1 = (2^u)^k + 1 = v^k + 1$$

kは奇数だから、$k > 1$ならば、

$$v^k + 1 = (v + 1)(v^{k-1} - v^{k-2} + \cdots\cdots + 1)$$

のように因数分解されて、素数ではありません。

そこで、Fが素数であるためには、$k = 1$，$m = 2^n$で

$$F_n = 2^{(2^n)} + 1$$

となることが必要です。

この形の整数が素数であるかどうかはこれだけではわかりません。この形の整数のことをフェルマー数、その中で素数であるものをフェルマー素数といいます。

フェルマーは「フェルマー数$F_n = 2^{(2^n)} + 1$はすべて素数である」と予想しました。果たしてこの予想は当たっているのでしょうか。

実は、この予想は間違っています。

ではどのように間違っているのか見てみましょう。

$F_0 = 2^1 + 1 = 3$

$F_1 = 2^2 + 1 = 5$

$F_2 = 2^4 + 1 = 17$

$F_3 = 2^8 + 1 = 257$

$F_4 = 2^{16} + 1 = 65537$

ここまでは苦労して調べれば、全て素数であることが判ります。

でも次が問題で、

$F_5 = 2^{32} + 1 = 4294967297 = 641 \times 6700417$

であるから、F_5は合成数です。このことは、フェルマーの予想が出てから１００年も後にオイラーによって見つけられました。フェルマーの予想に反して、F_5からあとはまだ素数は発見されておらず、いまでは、F_5からF_{30}までは全て合成数である、ということがわかっています。F_5以降は全て合成数であろうという予想もなされています。

３、あとがき

短い文章ですが、素数については書き始めるときりがないのでこれでおしまいです。

いろいろな素数についての話、いかがだったでしょうか。私は素数というものが昔から好きだったのですが、今回は「素数入門　計算しながら理解できる」を読んでみて、素数にもいろいろなものがあることを知りました。この本には素数のことだけでなく、整数全般のこともいろいろ書いてあり、しかも多くの数学者の説明が書いてあるので、なかなか面白い入門書です。興味がある人は、是非読んでみてください。

初めて部誌を書いたので、どんな風にすればいいのか、どのくらい難しくすればいいのか、というのがわかりませんでした。もしかしたら、他の人よりも簡単になったかも知れません。

最後に、ここまで読んで頂きありがとうございます。来年も灘の文化祭に来て数学研究部に寄って頂けるのをお待ちしております。

４、参考文献

ブルーバックス「素数入門　計算しながら理解できる」　著者　芹沢正三