A2　整数の計算

【最大公約数 GCD・最小公倍数 LCM】

整数m, ｎ（m＞ｎ）の最大公約数ｇを計算する。

（ユークリッド Euclid の互除法・人類が最初に発見したアルゴリズム）

変数wを用いて次ぎの３ステップをｎ＝０となるまで繰り返す

新 wを　m mod ｎ とし、新 m を ｎ、新 ｎ を ｗ で置き換える

最後のmが最大公約数ｇである

ディオパントス Diophantos 方程式

ｇ＝ｘm＋ｙｎ　となる整数ｘ、ｙが存在する。

BASIC によるプログラム

m mod n は、m を n で割ったときの余りを表す。　15 mod 7 = 1　である。

m を n で割ったときの商が m¥n で得られる。

```
100 DEFINT A-Z
110 INPUT "a= ";A: INPUT "b= ";B
120 J=0
130 R(0)=A: R(1)=B
140 J=J+1
150    Q(J)=R(J-1)¥R(J): R(J+1)=R(J-1) MOD R(J)
160    IF R(J+1)<>0 THEN 140
170 X(0)=0: Y(0)=1: X(1)=1: Y(1)=-Q(1)
180 FOR K=2 TO J-1
190    X(K)=X(K-2)-Q(K)*X(K-1): Y(K)=Y(K-2)-Q(K)*Y(K-1)
200 NEXT K
210 PRINT: PRINT
220 PRINT "G.C.M. = "; R(J); TAB(20); "L.C.M. = "; (A/R(J))*B: PRINT
230 PRINT A; "*"; X(J-1);" + "; B; "*"; Y(J-1); " = "; R(J)
240 PRINT: PRINT
250 END
```

Mathematica での計算例

```
GCD[12345,54321]
3
ExtendedGCD[12345,54321]
{3,{3617,-822}}
3617*12345+(-822)*54321
3
```

Mathematica の簡単なプログラム

```
m=12345
n=54321
While[n!=0,  w=Mod[m,n];  m=n;  n=w]
m
```

上の w=Mod[m,n]　を　w=m-Floor[m/n]*n　としてもよい。

ExtendedGCD をプログラムすること。

【エラトステネスの篩（ふるい）】

自然数 n(>2) を与えて、n までの素数をすべて列挙する方法。
2 から n までの整数のテーブルを用意し、順に 2 の倍数、３の倍数、…を除く。

Mathematica での計算例

```
eratosthenes[n_]:=Module[{i,j,t},
      t=Table[i,{i,2,n}];
      For[i=2,i<n,i++,
      While[!MemberQ[t,i] && i<=n,i++];
      j=i+i;
      While[j<=n,t=Complement[t,{j}];j=j+i];
      ];t]
```

eratosthenes[100] を実行すると、
{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}
erastosthenes[1000] は少し時間がかかる。

1000 個の素数のリストを作成するには、ｋ番目の素数 Prime[k] を使って
Table[Prime[k],{k,1,1000}] でよいが、極めて早い。

1000 までの素数リストを作成するには、次の実行でよい。

```
n=1000; t={}; k=1;
While[Prime[k]<n, t=Append[t,Prime[k]]; k++];  t
```

【１９９９　センター試験　数学Ｂの問題　ＢＡＳＩＣプログラムから】

整数 15 は次のように連続した２つ以上の正の整数の和として表わすことができる。

15 = 1 + 2 + 3 + 4 + 5 = 4 + 5 + 6 = 7 + 8

１より大きい整数ｎについて、これを連続した二つ以上の整数の和で表わすことができるかどうかを調べる次のプログラムと同じような結果が得られる Mathematica の関数 contQ[n] を作れ。

```
110  INPUT “n=”;N
120  FOR J=1 to N-1
130     W=0
140     FOR K=J to N
150        PRINT K;
160        W=W+K
170        IF W>N THEN PRINT “No” : GOTO 200
180        IF W=N THEN PRINT “Yes” : GOTO 200
190      NEXT K
200  NEXT J
210  END
```

このプログラムでは、 n=? に対して 10 を入力すると、新たに表示される最初の２行は

```
 1   2   3   4   Yes
 2   3   4   5   No
```

である。
このプログラムで Yes のときだけ表示させるにはどうしたらよいか。

2～100 までの範囲で、Yes が１回も表示されないような n を調べること。また、
Yes が表示されるｎについては、そのすべての方法のリストを表示させよ。

【n^2-n+41 は素数か】

n を 1～100 の範囲で調べること。

```
f[n_]:=n^2-n+41;
Do[Print[n,"   ",f[n],"   ",PrimeQ[f[n]]],{n,1,100}]
```

$n^2-79n+1601$ではどうなるか調べること。

【Ｃｏｌｌａｔｚ問題（角谷の予想)】

２以上の自然数ｎに対して、ｎが奇数ならばｎを３倍して１を足し、その値を２で割る。ｎが偶数ならば、ｎを２でわる。この操作を繰り返すとｎは１に収束する。

例　3->5->8->4->2->1
7->11->17->26->13->20->10->5
9->14->7
15->23->35->53->80->80->40->20
31->47->...->3644->...->53

内容は単純であるが、未解決の問題である。

ｎを入力し、n から始まり、4->2->1 で終わるリスト {n,..., 4, 2, 1} を作成する。
ｎが２から１００００までの整数のとき、リスト {n,..., 4, 2, 1}　の長さが最大となるｎを調べること。

【カプレカ数６１７４】

４桁の数を１つとる。例えば 1998 とする。この数を構成する４桁の数を並べかえて、一番大きい数と、一番小さい数を求め、この２数の差を求める。ここでは

9981 - 1899 = 8082

この操作をカプレカ操作という。新しくできた数にこの操作を行う。４桁にならないときは左に０を埋めて４桁とする。

8820 - 0288 = 8532

これを繰り返して

8532 - 2358 = 6174
7641 - 1467 = 6174

６１７４に到達すると、この数字が繰り返される。この場合は 3 回の操作で到達した。

0000, 1111, ..., 9999 を除く 9990 個の４桁の数は、このカプレカ操作を何回か行うことでで 6174 に至るという事実を、カプレカ操作の回数で分類して示すこと。

0 回　　1 個　（6174）
1 回　383 個
2 回　576 個
…

カプレカは１９４０年代に活躍したインドの数学者

このような操作で得られる数 6174 を核と呼ぼう。４桁以外の場合について核の存在だけを探した結果は、次のようである。（西山　豊　１９９０）

２桁　　なし
３桁　　４９５

４桁　　６１７４
５桁　　なし
６桁　５４９９４５　　６３１７６４
７桁　　なし
８桁　６３３１７６６４　　９７５０８４２１

【数字根・田村の問題】

ある数の各桁の各桁の数字の和を求めることを繰り返すと、遂に１桁の数が得られる。これを元の数の数字根という。

1999 ➔28➔10➔1

一方、ある数の各桁の数字の積を求めることを繰り返すと、遂に１桁の数が得られる。これを元の数の積の数字根という。

1999➔729➔126➔12➔2

さて、１９９９年は平成１１年である。

１９９９の和の数字根は１１の積の数字根に等しく、

１９９９の積の数字根は１１の和の数字根に等しい。

このようなことは、よくあることだろうか？

Ｇａｒｄｎｅｒ（１９７９）により、積の数字根に関連して、ステップ数を持続数と呼ぶ。x の持続数を p(x) と書く。p(1999)=4 である。
与えられた正の整数 n に対して p(x) = n となる最小の x を求めるプログラムを作れ。

【循環素数】

素数 11939 は各桁の数を左に回転させた 19391，93911，39119，91193 のいずれも素数である。このような５桁の循環素数をすべて求めよ。

【部分分数への分解】

有理数 $\frac{n}{m}$ を、例えば　$\frac{1}{20}=\frac{1}{4}-\frac{1}{5}$，　$\frac{1}{120}=\frac{1}{3}+\frac{4}{5}-\frac{9}{8}$　のように、簡単な有理数の和に分解すること。

$\frac{4}{5}=\frac{1}{a}+\frac{1}{b}+\frac{1}{c}$ となる整数 a,b,c が古代エジプトの本に載っている。

まず、分母を素因数分解する。FactorInteger[m] により、m を異なる素数冪の積に分解する。m=a*b*c*… のとき拡張最大公約数 ExtendedGCD[a,b] により、ディオパンソス方程式が解け、最大公約数 g が {g, {s, t}} と表わされ、 g = s*a + t*b が成り立つ。

【連分数への分解】

Nest[1/(1-#)&,x,3] を実行して、連分数　$\cfrac{1}{1-\cfrac{1}{1-\cfrac{1}{1-x}}}$　を表示せよ。

どの分子も１の連分数 $a_0+\cfrac{1}{a_1+\cfrac{1}{a_2+\cfrac{1}{a_3}}}$ を $[a_0;a_1,a_2,a_3]$ と略記し正則連分数という。

パッケージ　<<NumberTheory`Master` をロードし、ContinuedFraction[x,n] を用いる。
連分数表示を通常の分数に変換するには、関数 Normal を用いる。

$\sqrt{3}$, π の近似連分数を求め（n=5,10)、真値と比較せよ。

【ルース＝アーロン・ペア】

連続する整数で,双方の素因子の和が等しい数のペア　無数に存在する（エルディシュ）
７１４＝ベーブルースの通算ホームラン数（１９３５）　２　３　７　１７
７１５＝ハンク・アーロンの新記録（１９７４）　５　１１　１３
（２＋３＋７＋１７＝２９＝５＋１１＋１３）
放浪の天才数学者エルディシュ　ポール・ホフマン　平石律子訳　草思社　より
このようなペアを１００００までの連続する数から探すこと

【中国の剰余定理】

複数の合同式 $\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \cdots \\ x \equiv a_n \pmod{m_n} \end{cases}$ は $GCD[m_1, m_2, \cdots, m_n] = 1$ のとき解 x がある。

これを、求めるには
```
<<NumberTheory`Master`
ChineseRemainderTheorem[{a1,a2,...,an},{m1,m2,...,mn}]
```
とする。

次の合同式を求めよ。$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{5} \end{cases}$

【オイラー予想１７６９】

予想では、n≧3 のとき $x_1^{\,n} + x_2^{\,n} + \cdots + x_{n-1}^{\,n} = x_n^{\,n}$ は正整数解を持たない。
次の反例をチェックすること。

１９６６　27^5 + 84^5 + 110^5 + 133^5 = 144^5
１９８８　95800^4 + 217519^4 + 414560^4 = 422481^4　（楕円曲線論による）

【完全数】

自身を除く約数の和が元の数になる整数を<u>完全数</u>という。
6 = 2*3 = 1 + 2 + 3,　28 = 2^2 * 7 = 1 + 2 + 4 + 7 + 14
だから、６や２８は完全数である。

等比数列の和の公式を使えば
$p = 2^n - 1$ が素数ならば $N = p * 2^{n-1} = (2^n - 1)2^{n-1}$ は完全数
が分かる。逆に偶数の完全数はこのような数に限る（オイラーの定理）
これを用いて、

6 = (2^2-1) * 2^1　　28 = (2^3-1) * 2^2
496 = (2^5-1) * 2^4　　8196 = (2^7-1) * 2^6

は完全数である。ここまでは紀元１００年ごろまでにギリシャ人が発見した。
実は、１００万までの完全数はこの４つだけである。その続きは

(2^13-1) * 2^12
(2^17-1) * 2^16
(2^19-1) * 2^18

が完全数である。

(2^756839 -1)* 2^756838　455633 桁の数
32 個目に発見されたもの　Gage & Slowinski 1992/3

現在知られている完全数は３８個である。完全数が無数にあるか否かは未解決。
奇数の完全数が存在するか否かも未解決であるが，10^{50} 以下には存在しないことが分かっている.

【メルセネンス数】

$n>1, a^n-1$ が素数ならば、a = 2 で n は素数でなければならない。
この形の数をメルセンヌ数という。pが素数でも $Mp=2^p-1$ が素数になるわけではない。
メルセンヌ素数 Mp は次のものが知られている。(1979 まで 25 個)

p＝ 2，3，5，7，13，17，19，31，61，89,107,127，521，607，1279，2203，
2281，3217，4253，4423，9689，9941，11213，19937，21701

p= 31 のときＯＫ　　オイラー（スイス）　1772
p= 67 のときＮｏ　　リュカ（フランス）　1876 間接的に示した
M67 = 193707721*761838257287　コール（アメリカ）　1903
p=127 のときＯＫ　　リュカ（フランス）　1876
p=257 のとき　Ｎｏ　　1922 間接的に示した
p=216091 のときＯＫ　1985　Mp は 65050 桁
p=6972593 のとき OK　1999
このときの Mp は現在知られている最大の素数である。何桁であるか。

メルセンヌは p=257 まで調べて、p=257 のとき OK としたが誤っていた。しかしいま、Mathematica で素因子を見つけるのは困難であろう。
メルセンヌ素数に関するホームページ　http://mersenne.org/prime.htm

【フェルマー数】

$F(n)=2^{2^n}+1$ は素数とフェルマーは予想した。
このような素数はフェルマー数と呼ばれる。 n=5 はフェルマー数でない。

F(1) = 2^2 + 1 = 5
F(2) = 2^4 + 1 = 17
F(3) = 2^8 + 1 = 257
F(4) = 2^16 + 1 = 65537
ここまでは素数
F(5) = 2^32 + 1 = 641*6700417 (オイラー)
・・・・
F(20)=2^10458576 + 1 は素数ではない。まだ素因数は知られていない。

【ウィルソンの定理】

任意の素数 p について (p-1)! + 1 は p で割り切れる。次を確認すること。

(2-1)! + 1 = 2
(3-1)! + 1 = 3
(5-1)! + 1 = 25 = 5*5
(7-1)! + 1 = 721 = 7*103
(11-1)! + 1 = 3628801 = 11*329891
(13-1)! + 1 = 479001601 = 13*2834329
(17-1)! + 1 = 2092278988001 = 17*61*137*139*1059511
(19-1)! + 1 = 64023705728001 = 19*23*29*61*67*123610951

最初に証明したのは　Lagrange(1773)

【ライプニッツの定理】
自然数 p > 2 について
p が素数 <===> (p-2)! -1 が p の倍数

【双子素数】
n - 1 と n + 1 が共に素数である組を双子素数という。例えば
(3,5,7), (11,13), (17,19)
・・・
1993/07　(1691232×1001×10^4020 - 1, 1691232×1001×10^4020 + 1)
である。双子素数が無限組あるか否かは未解決問題である。

１００００までの３子と双子の組をすべて求めること。

【$a^2+b^3=c^4$】
a,b,c が自然数のとき、
$a^2+b^3=c^4$　や　$a^2+b^4=c^3$　や　$a^3+b^4=c^2$
を満たすものを発見せよ。（例えば１～100 の範囲で）

【フェルマー予想とその証明の歴史】
フェルマーは１６４０年頃、「ディオファントスの数論」という本の中に
$x^n+y^n=z^n(n\geq 3)$ は自明でない整数解をもたない
ことを証明したが、余白が狭くて書けないという書き込みをした。 パリの科学アカデミーが賞金 3000 フランで解答を募集した。
1908　ゲッチンゲン王立協会が賞金１０万マルクで解答を募集
ウォルフスケール賞（設立当時１０万マルク２００７年９月１３日まで有効）
1659　n=4 フェルマ　1753　n=3 オイラー　1828　n=5 ディリクレ・ルジャンドル
1839　n=7 メレ　1847　n≦36 クンマー　1857　n≦100 クンマー
1930　n≦ 616　1954　n≦ 2,500　1964　6,000
1975　29,000　1976　125,000　1987　150,000
1992　100 万　1993　400 万
1983　ファルティングス　n≧4 に対し互いに素な整数解は有限個しかない
1993　アンドリュー・ワイルズ　谷山ーベイユの予想を解くことで完全証明
ケンブリッジ大・アイザック・ニュートン数理科学研究所で発表（1993/６/23）
ハイデルク大・フラッハの業績等を土台にしている。
Annals of Math 1995/05 に論文掲載し、最終決着した。

【リュカテスト】

p を素数とし $Mp = 2^p - 1$ とおく。Mp が素数か否かを判定する能率的なアルゴリズム。

S(1) = 4, S(i+1) = S(i)^2 - 2 として S(i) を定める。

p≧3 ならば、 Mp が素数 <===> S(p-1) は Mp で割り切れる

【素因数分解】

与えられた自然数 n を素因数分解するのは一般的な方法が見つかっていない。n より小さい素数で割ってみるという素朴な方法しか考えられない。その計算手順は n の桁数が k のとき、およそ 10^k に比例する手間がかかる。従って大きい桁の素因数分解はコンピュータでも大変困難である。

ＲＳＡ暗号方式の発見者リベストは

N = 11438 16257 57888 86766 92357 79976 14661 20102 182
96721 24236 25625 61842 93570 69352 45733 89783 059
71235 63958 70505 89890 75147 59929 00268 79543 541

という１２９桁の数を素因数分解すれば解ける暗号の解読を懸賞問題として、Scientific American 誌上に提出し、５０年はかかると予測していた。

1994/4/27 この素因数分解は解けてしまった。その方法は正攻法であったが、世界中のボランティア６００人を動員して、スーパーコンピュータ数百台を使い、実に８ヶ月の計算をした結果だったという。

（情報セキュリティの科学・ブルーバックス１９９５・２　p.141）

【素数判定法】

フェルマーの小定理

m^(p-1) mod p = 1 for all prime p and m such that 1<m<p

により、n が素数ならば

2^(n-1) mod n = 1　(***)

一方、n が素数でなくて (***)　が成り立つのは極めて稀である。例えば５０桁の数のときは１００万に１つ位しかない。従って (***) が成り立てば素数、そうでなければ非素数と判定しても、殆ど正しい。

ラビン(Rabin)テスト

n は奇数とする。

n - 1 = 2^e * m, (m,2) = 1

となる e, m　に対して l = 2^e -1 とおく。

ランダムな a (1 < a < n) に対して

a^m mod n = 1　　(0)
a^m mod n = n - 1　　(1)
a^(2m) mod n = n - 1　　(2)
a^(4m) mod n = n - 1　　(3)
a^(8m) mod n = n - 1　　(4)
・・・
a^(lm) mod n = n - 1　　(e)

のどれもが成り立てば「一応ＯＫ」とし、そうでなければ直ちに「非素数」とする。

非素数でも「一応ＯＫ」となる確率は 1/4 未満であることが分かっているので「一応ＯＫ」のときは、改めて a を選び直してテストをし、２度目も「一応ＯＫ」となる確率は、(1/4)^2 = 0.0625 未満である。これを１０回繰り返して、非素数」とならなければ n を素数と

考えても、その危険率は 1/1000 万未満となる。
　このテストで組み込まれた PrimeQ[n] は ｎ ＜2.5 ×10^10 では正しい答えを保証している。

２００桁を超える（ほぼ確実な）素数を求める方法
　For[p=10^200, !PrimeQ[p],p++]; p　　（数秒で求められる）

１００桁を超える確実な素数の求め方（参考文献・山田修司による）
　フェルマーの小定理を用いると、次のことが分かる。
　　ｐを素数、ｋを 0＜ｋ＜ｐであるような偶数とする。ｎ＝ｐｋ＋１とおく。

$$a^{pk} \equiv 1 \pmod{n}, \quad (a^k - 1, n) = 1$$

　　を満たすような整数ａ（１＜ａ＜ｎ）が存在すればｎは素数である。
　そこで、適当な素数ｐをえらび、ｋ＝ｐ－１，ｐ－３，ｐ－５ と試しながら
　また、ａ＝２,３,… について
　　{Mod[a^(p k), p k + 1], GCD[a^k –1, p k+1]}
　が {1, 1} になるものを探す。この見つかった素数について、同じ操作を繰り返すと、大きな桁の素数が得られる。

【素数分布・ガウスの予想】
自然数 n までの素数の数を　π(n) で表す。
　　π(2)=1, π(10)=4 π(100)=25

n が大きくなると　$\pi(n) \approx \dfrac{n}{\log n}$　と１７歳のガウスが予想(1792)し、プーサンとアダマールが同時にゼータ関数の性質を用いて正しいことを証明した(1896)。

```
Do[Print[PrimePi[10^n],"    ",N[10^n/Log[10^n]]],{n,1,9}]
  4    4.34294
  25    21.7147
  168    144.765
  1229    1085.74
  78498    72382.4
  664579    620421.6
  5761455    5.42868 10^6
        50847534    4.82549 10^7
```

n を 10^10 としても、両者の比はなかなか１に近くはない。
ｎが小さい間は、もっと良い近似式をルジャンドルが得ている。

$$\pi(n) \approx \frac{n}{\log n - 1.08366}$$

【整数論に関連した関数】
メービウスの関数
　整数 n が k 個の異なる素数の積のとき、k が偶数なら 1, k が奇数なら –1, １でない２乗因子を含むときは 0 とする。この関数 μ(n) を作ること。
　　例　μ(15)=1, μ(30)=-1, μ(60)=0
　MoebiusMu

乗法的関数

自然数に対して定義された複素数値をとる関数を数論的関数といい、
f(1)=1,　(m,n)=1 ならば f(mn)=f(m)f(n) となるとき、乗法的という。

メービウスの反転公式

乗法的関数 f, g について、
g(n)=Σ{f(d) such that d | n} ⇔ f(n)=Σ{μ(d)g(n/d) such that d | n}

オイラーの関数

整数 n より小さく、n と互いに素となる整数の個数を求める関数を作ること。
例　φ(7)=6, φ(15)=8, φ(30)=8, φ(60)=16
EulerPhi

平方剰余

合同式 $x^2 \equiv a \pmod{m}$ が整数解をもつとき、a を m を法とする平方剰余といい、整数解を持たぬときは、a を m を法とする平方非剰余という。

a が m を法とする平方剰余であるための必要十分条件は、
1) a が m のすべての素因子 p(≠2)を法として平方剰余であり、
2) 4|m または 8|m のときは a≡1(mod 4) または a≡1(mod 8)
となることである。
m = 11 のとき、1, 3, 4, 5, 9 は平方剰余である。

ルジャンドルの記号・ヤコビの記号

p は奇数で素数とする。

ルジャンドルの記号$\left(\frac{a}{p}\right)$は、(a, p)=1 のとき、a が p を法とする平方剰余ならば 1, 平方非剰余ならば -1 の値をとり、p | a のとき 0 をとる記号である。

$$\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right),\ \left(\frac{a}{p}\right)\equiv a^{\frac{p+1}{2}} \pmod{p}$$

ヤコビの記号$\left(\frac{n}{m}\right)$は、m が奇数でかつ素数のとき、ルジャンドルの記号に帰着する。m | n のときは 0 である。そうでないとき、$m=\Pi_i\ p_i$（各 p_i は素数)と表し $\left(\frac{n}{m}\right)=\Pi_i\left(\frac{n}{p_i}\right)$ で定義する。

$$n\equiv n' \pmod{m} \Rightarrow \left(\frac{n}{m}\right)=\left(\frac{n'}{m}\right)$$

$$\left(\frac{nn'}{m}\right)=\left(\frac{n}{m}\right)\left(\frac{n'}{m}\right)$$

例 $\left(\frac{17}{23}\right)=-1,\ \left(\frac{365}{1847}\right)=1$
JacobiSymbol[n,m]

参考書

田島一郎　整数（数学ワンポイント双書）　共立出版　１９７７
高木貞治　初等整数論講義　共立出版　１９５１（初版）
山田修司　Mathematica で楽しむ数理科学　牧野書店　１９９９