フェルマーテストとカーマイケル数

本題に入る前にフェルマーの小定理とその周辺について復習しておこう．

定理 1 フェルマーの小定理 $(a,p)=1$ のとき $a^{p-1}\equiv 1 \pmod{p}$

［証明略］

定理 2 任意の a について $a^{p}\equiv a \pmod{p}$

［証明］$(a,p)=1$ のときは前定理より明らか．$(a,p)\neq 1$ のときは $a\equiv 0 \pmod{p}$ なので両辺とも 0 となり，当然成り立つ． ［証明おわり］
通常はこのようにするメリットはないと思われる．

定理 3 オイラーの定理 $(a,n)=1$ のとき $a^{\phi(n)}\equiv 1 \pmod{n}$

［証明略］

定義 1 フェルマーテスト $(a,n)=1$ である a について $a^{n-1}\equiv 1 \pmod{n}$ であるような合成数 n を，a **を底とする偽素数**と呼ぶ

定義 2 $(a,n)=1$ である全ての a について $a^{n-1}\equiv 1 \pmod{n}$ である n が素数で無い場合，そのような合成数 n を，**カーマイケル数**と呼ぶ

ここで誤解してはならないのはカーマイケル数は 偽素数の中の偽素数というわけではない．つまり a を底とする偽素数の集合を F_a とすると，カーマイケル数は $F_2\cap F_3\cap, F_5\cap,\cdots$ というわけではない．たとえば最も小さいカーマイケル数は 561 であるが，$561\in F_2$ であるが，$561\notin F_3$ である．つまりフェルマーテストを通る以前に 3 の倍数なのである．次に小さいカーマイケル数 1105 は $1105\in F_2, 1105\in F_3$ であるが，$1105\notin F_5$ である．もちろんカーマイケル数 $\in F_2\cup F_3\cup, F_5\cup,\cdots$ ではある．さらに言えばカーマイケル数 $\in F_2$ である．少し考えてみれば当たり前のことではある．後述するがカーマイケル数は偽素数のなかの偽素数というわけではないが，それに近いものがある．

定理 4 カーマイケル数は奇数である．

［証明］背理法で証明する．もし偶数のカーマイケル数 n があったとする．フェルマーテストを通っているので，この n について $(a,n)=1$ であれば

$$a^{n-1}\equiv 1 \pmod{n}$$
$$\therefore a^{n}\equiv a \pmod{n}$$

明らかに $(n-1,n)=1$ であるから $a=n-1$ を代入して，

$$(n-1)^{n}\equiv n-1 \pmod{n}$$
$$\therefore (-1)^{n}\equiv -1 \pmod{n}$$

この合同式は $n=2$ 以外では成り立たない．また 2 は合成数でない．よって，このような式が成り立つ偶数の合成数は無い．よってカーマイケル数は奇数である． ［証明おわり］

さてコンピュータでカーマイケル数を求めてみよう．次のプログラムは ActiveBacic Version 4.23.00 用に書いたものであるが，色々な BASIC を渡り歩いてたどり着いたものなので，ヘンテコなものになっている．

```
#prompt
DIM CELLS(65536) As Long
dim Mi As Long,n as  Qword,S as long, i as long, Pii as long,PIii as long,Piii as long
dim p as Qword,pii as long ,a as Qword,nn as long
LET CELLS(1) = 2
LET Mi = 0
FOR n = 2 TO 821641
   LET S = Sqr(n)
   For i = 1 To n - 1
      LET p = CELLS(i)
      If p > S Then GoTo 5
      If n MOD p  = 0 Then GoTo 10
   Next i
5    'PRINT n;
     LET Mi = Mi + 1
     LET CELLS(Mi) = n
10 NEXT n
   LET Piii = 1
      FOR n = 399001 TO 821643 STEP 2
30    IF CELLS(PIii) = n THEN GOTO 100'n が素数ならば，カーマイケル数は合成数なのでパスする．
      IF CELLS(PIii) < n THEN
         LET PIii = PIii + 1
         GOTO 30
      END IF
      FOR pii = 1 TO PIii - 1
         LET p = CELLS(pii)
         IF n mod p  = 0 THEN GOTO 40' 素数の倍数ならカーマイケル数かも知れないが，以降のテストは不要．
         LET a = 1
         FOR nn = 1 TO (n - 1)
            LET a = a * p mod n ' 実際はこの部分が時間をとっているものと思われる．
'if nn=(n-1)/2 and (a=1 or a=n-1) then 40 時間短縮を試みたが失敗だった．
         NEXT nn
         IF a <> 1  THEN GOTO 100
40    NEXT pii
50    PRINT n
100 NEXT n
```

最初に 65636 個の素数を小さい順に求めておく．なぜ 65636 個かと言うと，一等最初は VBA を用いたので，Excel の古いバージョンはセルが縦に 653636 個しか取れなかったためである．その最後の素数は 821643 である．n=3 から初めて順に奇数について調べてゆく．素数の倍数でないものについてその素数の $n-1$ 乗を n で割った余りを求め 1 にならなかったらカーマイケル数である．

コンピュータを走らせっぱなしで 3 時間かけても 29 個までしか出なかった．求める速度はだんだん遅くなっていき，100000 を超えるころになるとほとんど止まったようになる．これではさすがに話しにならない．そこでほかのアルゴリズムを考えてみた．

定理 5 自然数 n のカーマイケル関数を $\lambda(n)$ とすると，n がカーマイケル数である必要十分条件は

$$\lambda(n)|n-1$$

である．

［証明］$\lambda(n)|n-1$ ならば n はカーマイケル数であることの証明

$(a,n)=1$ であれば

$$a^{\lambda(n)} \equiv 1 \pmod{n}$$

$n-1=d\lambda(n)$ とすると，

$$a^{n-1} = a^{d\lambda(n)} = \left(a^{\lambda(n)}\right)^d \equiv 1 \pmod{n}$$

n がカーマイケル数ならば $\lambda(n)|n-1$ であることの証明

背理法により証明する．n がカーマイケル数であり $\lambda(n) \not| n-1$ とすると，

$$n-1 = d\lambda(n) + r \quad (r < \lambda(n))$$

とおける．n はカーマイケル数なので，$(a,n)=1$ である任意の a について

$$\begin{aligned} a^{n-1} &\equiv 1 \pmod{n} \\ a^{d\lambda(n)+r} &\equiv 1 \pmod{n} \\ \left(a^{\lambda(n)}\right)^d a^r &\equiv 1 \pmod{n} \\ a^r &\equiv 1 \pmod{n} \end{aligned}$$

しかしこれは $\lambda(n)$ が $a^x \equiv 1 \pmod{n}$ となる最小の x であることと矛盾する．よって逆も証明された．

［証明おわり］

定理 6 コルセルトの判定法自然数 n がカーマイケル数である必要十分条件は n が奇数で，平方数の素因数を持たず，$n-1$ が全ての素因数 -1 の倍数であることである．

n が奇数で，平方数の素因数を持たず，$n-1$ が全ての素因数 -1 の倍数であれば n がカーマイケル数になることはカーマイケル関数の定義から明らかであるのでその逆のみを証明する．

カーマイケル数であれば奇数であることは，定理 4 で証明済みである．また $n-1$ が全ての素因数 -1 の倍数であることもカーマイケル関数の定義から明らかである．問題は n が平方数の素因数をもたないということである．もし n が奇素数 p について因数 $p^m (m \geq 2)$（をもてば，カーマイケル関数の定義より，

$$\lambda(n) = \mathrm{lcm}(p^{m-1}(p-1), q, r, \cdots)$$

つまり $n-1$ は p の倍数である．一方 n も p の倍数であり，

$$n-1 \equiv n \equiv 0 \pmod{p}$$

となりこのようなことはありえない．よって証明された． ［証明おわり］

さて，このコルセルトの判定法を用いてカーマイケル数を求めてみよう．

```
#console
DIM CELLS(100000) As Long
dim Mi As Long,n as  Qword,S as long, i as long, Pii as long,PIii as long,Piii as long
dim p as Qword,pii as long ,a as Qword,nn as long
Open "output.txt" For Output As #1
LET CELLS(1) = 2
LET Mi = 0
FOR n = 2 TO 1000000
   LET S = Sqr(n)
   For i = 1 To n - 1
      LET p = CELLS(i)
      If p > S Then GoTo 5
      If n MOD p  = 0 Then GoTo 10
   Next i
5    'PRINT n;
     LET Mi = Mi + 1
     LET CELLS(Mi) = n
10 NEXT n ' ここまではあらかじめ素数を求めておく部分で，本体ではない．
      FOR n = 3 TO 1000000 STEP 2 ' 奇数のみを調べる．
      PIii=1
30      p=CELLS(PIii)
IF p = n THEN GOTO 100' もし n が素数ならば，カーマイケル数は合成数なので，パスする
if n mod p=0 then
if n mod p^2=0 then goto 100
if (n-1) mod (p-1)<>0 then goto 100
       end if
      IF p < n THEN
      LET PIii = PIii + 1
         GOTO 30
      END IF
50    PRINT n
print #1, n;",";
100 NEXT n
end
```

今度は先ほどのプログラムと違って断然速い．まだ改善の余地はあるが，1000000 以下のカーマイケル数 43 個を求めるのに約 6 分かかった．実行結果は次の通りである．

561 ,1105 ,1729 ,2465 ,2821 ,6601 ,8911 ,10585 ,15841 ,29341 ,41041 ,46657 ,52633 ,62745 ,63973 ,75361 ,101101 ,115921 ,126217 ,162401 ,172081 ,188461 ,252601 ,278545 ,294409 ,314821 ,334153 ,340561 ,399001 ,410041 ,449065 ,488881 ,512461 ,530881 ,552721 ,656601 ,658801 ,670033 ,748657 ,825265 ,838201 ,852841 ,997633

もう少しカーマイケル数について調べてみよう．

定理 7 カーマイケル数は少なくとも 3 個の素因数からなる．

［証明］カーマイケル数はそもそも合成数なので 1 個の素因数からなる，つまり素数であることはない．それでは 2 個の素因数からなることはないことを証明しよう．

カーマイケル数 n が 2 個のみの素因数 p, q からなると仮定する．つまり

$$n = pq \quad (p \geq 3, q \geq 7, p \neq q) \tag{1}$$

と書ける．またコルセルトの判定法より

$$n - 1 = \frac{(p-1)(q-1)a}{2d} \quad (a \geq 1, d \geq 1) \tag{2}$$

ここで $\dfrac{(p-1)(q-1)}{2d}$ というのは $p-1, q-1$ の最小公倍数を表す．つまり $2d$ は最大公約数である．2 がついているのは p, q は必ず奇数だから $p-1, q-1$ は素因数 2 を必ず持つためである．つまり

$$p - 1 = 2dx, q - 1 = 2dy \quad (x \geq 1, y \geq 1, x \neq y) \tag{3}$$

と書くことができる．(1),(2),(3) より

$$(2dx + 1)(2dy + 1) - 1 = 2adxy$$

展開して整理すると，

$$(4d^2 - 2ad)xy + 2dx + 2dy = 0$$

両辺を $2d$ で割って

$$(2d - a)xy + x + y = 0 \tag{4}$$

$2d - a = k \quad (k \in \mathbb{Z})$ とすると

$$\begin{aligned} kxy + x + y &= 0 \\ k^2xy + kx + ky + 1 &= 1 \\ (kx + 1)(ky + 1) &= 1 \\ (kx + 1, ky + 1) &= (\pm 1, \pm 1) \\ (kx, ky) &= (0, 0), (-2, -2) \end{aligned}$$

$(kx, ky) = (0, 0)$ のときは $k = 0$ となり (4) より $x + y = 0$ となるので不適．$(kx, ky) = (-2, -2)$ のときは $x = y$ となりこれも矛盾する．よってカーマイケル数が 2 個のみの素因数でなることはない．　［証明おわり］

さて，カーマイケル数について深入りしてしまった感があるので，戻って偽素数について調べてみよう．

```
#prompt
DIM CELLS(100000) As Long
dim Mi As Long,n as  Qword,S as long, i as long, Pii as long,PIii as long,Piii as long
dim p as Qword,pii as long ,a as Qword,nn as long
Open "output.txt" For Output As #1
LET CELLS(1) = 2
LET Mi = 0
FOR n = 2 TO 100000
   LET S = Sqr(n)
   For i = 1 To n - 1
      LET p = CELLS(i)
      If p > S Then GoTo 5
      If n MOD p  = 0 Then GoTo 10
   Next i
5    'PRINT n,
     LET Mi = Mi + 1
     LET CELLS(Mi) = n
goto 20
10 'print n
    if p<>2 then
a=1
FOR nn = 1 TO (n - 1)
            LET a = a * 2 mod n '実際はこの部分が時間をとっているものと思われる.
        NEXT nn
          IF a =1 then
print n
print #1,n
end if
end if
20 NEXT n
```

2 を底とした偽素数である．100000 以下の偽素数は次の 78 個である．計算するのに約 3 分かかった．

341 ,561 ,645 ,1105 ,1387 ,1729 ,1905 ,2047 ,2465 ,2701 ,2821 ,3277 ,4033 ,4369 ,4371 ,4681 ,5461 ,6601 ,7957 ,8321 ,8481 ,8911 ,10261 ,10585 ,11305 ,12801 ,13741 ,13747 ,13981 ,14491 ,15709 ,15841 ,16705 ,18705 ,18721 ,19951 ,23001 ,23377 ,25761 ,29341 ,30121 ,30889 ,31417 ,31609 ,31621 ,33153 ,34945 ,35333 ,39865 ,41041 ,41665 ,42799 ,46657 ,49141 ,49981 ,52633 ,55245 ,57421 ,60701 ,60787 ,62745,63973 ,65077 ,65281 ,68101 ,72885 ,74665 ,75361 ,80581 ,83333 ,83665 ,85489 ,87249 ,88357 ,88561 ,90751 ,91001 ,93961

赤字がカーマイケル数である．当然ながらカーマイケル数は全て 2 を底とした偽素数である．10000000 以下の偽素数を求めるのには 3 時間程度かかった．全部で 245 個である（参考文献 [1] のデータは誤植である．[4] を参照すべし）．

少しプログラムを変えるだけで他の底についての偽素数を調べることができる．3 を底とした 100000 以下の偽素数は 2 の場合と全く同数の 78 個である．求めるのに約 5 分かかった．

91 ,121 ,286 ,671 ,703 ,949 ,1105 ,1541 ,1729 ,1891 ,2465 ,2665 ,2701 ,2821 ,3281 ,3367 ,3751 ,4961 ,5551 ,6601 ,7381 ,8401 ,8911,10585 ,11011 ,12403 ,14383 ,15203 ,15457 ,15841 ,16471 ,16531 ,18721 ,19345 ,23521 ,24046 ,24661 ,24727 ,28009 ,29161 ,29341 ,30857 ,31621 ,31697 ,32791 ,38503 ,41041 ,44287 ,46657 ,46999 ,47197 ,49051 ,49141 ,50881 ,52633 ,53131 ,55261 ,55969 ,63139 ,63973 ,65485 ,68887 ,72041 ,74593 ,75361 ,76627 ,79003 ,82513 ,83333 ,83665 ,87913 ,88561 ,88573 ,88831 ,90751 ,93961 ,96139 ,97567

561 と 62745 以外のカーマイケル数 14 個がこの中に含まれている（赤字部分）．さて 2 を底とする偽素数と 3 を底とする偽素数の共通部分を調べてみよう．

1105, 1729, 2465, 2701, 2821, 6601, 8911, 10585, 15841, 18721, 29341, 31621, 41041, 46657, 49141, 52633, 63973, 75361, 83333, 83665, 88561, 90751, 93961

23 個中カーマイケル数は 14 個でぐんとその占める割合は増す．

5 を底とした 100000 以下の偽素数は 73 個である．求めるのにこれも約 5 分かかった．

4,124,217,561,781,1541,1729,1891,2821,4123,5461,5611,5662,5731,6601,7449,7813,8029,8911, 9881, 11041,11476,12801,13021,13333,13981,14981,15751,15841,16297,17767,21361,22791,23653, 24211, 25327, 25351, 29341,29539,30673,32021,35371,36661,36991,38081,40501,41041,42127,44173,44801,45141,46657, 47641,48133,50737,50997,52633,53083,53971,56033,58807,59356,63973,67921,68101,68251,75361, 79381, 80476,88831,90241,91636,98173

1105,2465,10585,62745 以外，つまり 5 の倍数以外のカーマイケル数は全て含まれている．また 2,3,5 を底とする偽素数の共通部分は

1729, 2821, 6601, 8911, 15841, 29341, 41041, 46657, 52633, 63973, 75361

となり，全てカーマイケル数になってしまった．7 を底とする偽素数を求めてフェルマーテストは終わりにしよう．どうやら 2 以外は実行時間があまり変わらないようだ．今度も 73 個であった．

6,25,325,561,703,817,1105,1825,2101,2353,2465,3277,4525,4825,6697,8321,10225,10585,10621, 11041, 11521,12025,13665,14089,16725,16806,18721,19345,20197,20417,20425,22945,25829,26419,29234, 29341, 29857,29891,30025,30811,33227,35425,38081,38503,39331,45991,46657,49241,49321,50737,50881, 58825, 59305,59641,62745,64285,64681,65131,67798,75241,75361,76049,76627,78937,79381,84151,87673, 88399, 88831,89961,92929,95821,97921

今度はカーマイケル数は 8 個しかない．さて，ここまで求めてきた偽素数の積集合，100000 以下の偽素数の中の偽素数と呼べるのはたった 3 個の数字である．

$$29341 = 13 \times 37 \times 67,$$
$$46657 = 13 \times 37 \times 97,$$
$$75361 = 11 \times 13 \times 17 \times 31$$

参考文献

[1] 芹沢正三『素数入門』（講談社ブルーバックス，2002 年）

[2] 「integer sequence」<http://oeis.org/classic/A2997>

[3] 「算術算法研究」<http://matsumoto-lab.hp.infoseek.co.jp/index.html>

[4] 「Wolfram Mathworld」<http://mathworld.wolfram.com/>