The Diophantine Equation $x^2-1=(y^2-1)(z^2-1)$

by
Kenji Kashihara

Key Words: 整数解, イデヤル, 根原解

Abstract

I. When we fix z to a constant n, we can show the way to solve it and the results for n≦131071 by using "UBASIC."

II. We consider the first equation on the basis of the results of I. We will give the algorism which reduces all integral solutions to the obious one (1, n, 1) or (1, 1, n).

1. 不定方程式 $x^2-1=(n^2-1)(y^2-1)$

1. 1 考え方

z を n に固定して x と y に関する不定方程式

$$x^2-1=(n^2-1)(y^2-1) \tag{1}$$

の整数解について考える.

$n=0$のときは $x^2+y^2=2$ より,

$(x, y)=(\pm1, \pm1)$ であり,

$n=\pm1$ のときは $x=\pm1$, y は任意の整数である.

また方程式の対称性も考えるならば $x, y>0$,

$n\geqq2$ の場合を求めれば十分である.

$$x^2-(n^2-1)y^2=2-n^2 \tag{2}$$

$$(x+y\sqrt{n^2-1})(x-y\sqrt{n^2-1})=2-n^2 \tag{3}$$

(1)は(2)または(3)の形に変形できるから

$n^2-1=k^2m$, mは平方因子を含まない

とし, 2次体 $Q(\sqrt{m})$ におけるイデヤル分解を考える.

$$A=(x+y\sqrt{n^2-1}) \tag{4}$$

とおくと, (3)より

$$A\overline{A}=(n^2-2) \tag{5}$$

が成り立つ.

逆に(5)を満たすAが単項イデヤルでしかも(4)の形で表せると仮定すると, (5)より

$(x+y\sqrt{n^2-1})(x-y\sqrt{n^2-1})$

$=\pm(n^2-2)$

+の方は $x^2+1=(n^2-1)(y^2-1)$

となり, 8 を法として成立しない. よって(3)が成り立つ.

したがって, 次のようなアルゴリズムで(2)の整数解が求められる.

I n^2-2 を素因数分解し, さらに各素数を素イデヤルの積に分解する.

II 共役なイデヤルを $A\overline{A}=(n^2-2)$ となるように A と $\overline{A}$ に振り分ける.

III IIで得られた A が単項イデヤルか否か, また $\sqrt{m}$ の係数が k で割り切れるか否かを調べる.

1. 2 同伴解

<u>定義1</u> (x_1, y_1), (x_2, y_2) が共に(2)の整数解で,

$x_2+y_2\sqrt{n^2-1}=(x_1+y_1\sqrt{n^2-1})\varepsilon$

ε は $Q(\sqrt{m})$ の単数

なる関係があるとき, (x_1, y_1) と (x_2, y_2) は(2)の<u>同伴解</u>であるという.

<u>補題1</u> (2)の整数解 (x_1, y_1) の同伴解 (x_2, y_2) は次の式で表すことができる.

$$x_2+y_2\sqrt{n^2-1}=(x_1+y_1\sqrt{n^2-1})\,\varepsilon \qquad (6)$$

$$\varepsilon=(n+\sqrt{n^2-1})^e,\ e\in Z \qquad (7)$$

証明

$(n+\sqrt{n^2-1})(n-\sqrt{n^2-1})=1$ より

$\varepsilon\overline{\varepsilon}=1$

したがって，(x_1, y_1) が(2)の整数解ならば(6)，(7)により定まる (x_2, y_2) も(2)の整数解となる．

逆に (x_1, y_1) と (x_2, y_2) が同伴解であるとすると，(6)を満たす単数 ε が存在し，

$$\varepsilon=(x_2+y_2\sqrt{n^2-1})/(x_1+y_1\sqrt{n^2-1})$$
$$=(x_2+y_2\sqrt{n^2-1})(x_1-y_1\sqrt{n^2-1})/(2-n^2)$$

i) $m\equiv 2,3$ (4) の場合

$n^2-1=k^2m, 2-n^2\equiv 1$ より

$\varepsilon\equiv integer(mod\ k)$

ii) $m\equiv 1$ (4) の場合

$n^2-1=k^2m\equiv k^2$ (4) より n は奇数，

k は偶数である．したがって

$$2-n^2=1-(n^2-1)$$
$$=1-mk^2$$
$$\equiv 1 \qquad (2k)$$

$\varepsilon\equiv integer\ (mod\ 2k)$

i) ii) より

$\varepsilon=(n+\sqrt{n^2-1})^e,\ e\in Z$　　*Q. E. D.*

注意1　(7)の ε を自明な単数と呼ぶことにする．自明な単数の存在することが不定方程式(2)の特徴の1つである．

補題2　(2)の2つの整数解 (x_1, y_1) と (x_2, y_2) が同伴解である条件は次の合同式が成立することである．

$x_1y_2-x_2y_1\equiv 0\ (mod\ \ n^2-2)$

証明

$$x_2+y_2\sqrt{n^2-1}$$
$$=(x_1+y_1\sqrt{n^2-1})(n+\sqrt{n^2-1})$$

とすると，

$$x_1y_2-x_2y_1$$
$$=x_1(x_1+ny_1)-\{nx_1+y_1(n^2-1)\}\ y_1$$
$$=x_1^2-(n^2-1)\ y_1^2$$
$$\equiv 2-n^2$$
$$\equiv 0 \quad (n^2-2)$$

逆に

$$x_1y_2-x_2y_1\equiv 0 \quad (n^2-2) \qquad (8)$$

とすると

$$\varepsilon'=(x_2+y_2\sqrt{n^2-1})/(x_1+y_1\sqrt{n^2-1})$$
$$=\{x_1x_2-y_1y_2(n^2-1)+(x_1y_2-x_2y_1)\times\sqrt{n^2-1}\}/(2-n^2) \qquad (9)$$

$$N\varepsilon'=1 \qquad (10)$$

(8)，(9)，(10)より

$x_1x_2-y_1y_2(n^2-1)\equiv 0 \quad (n^2-2)$

よって ε' は $Q(\sqrt{m})$ の整数であり，単数である．故に (x_1, y_1) と (x_2, y_2) は同伴解である．　　*Q. E. D.*

注意2　$(x, y)=(\pm 1, 1)$ は明らかに(2)の整数解である．これらとその同伴解を(2)の自明解と呼ぶ．自明解の存在することが不定方程式(2)のもう1つの特徴である．

補題3　$A\overline{A}=(n^2-2)$ を満たすAが(2)の自明解を与える条件は $\pm 1+\sqrt{n^2-1}\in$ Aである．

証明　十分条件であることを示す．

$(\pm 1+\sqrt{n^2-1})\subset$ A

両辺のノルムは等しいから

A$=(\pm 1+\sqrt{n^2-1})$　　*Q. E. D.*

1．3　素数の$Q(\sqrt{m})$での分解[1)]

補題4．1　$m=2,3$　(4) のとき

(1)　(2) $=P^2, P=[2, \sqrt{m}]$　　$(m\equiv 2)$

$P=[2, 1+\sqrt{m}]$　　$(m\equiv 3)$

(2)　$p\nmid d(=4m$ 判別式) なる素数 p について

$(p)=P\overline{P}$　($\lambda_p(m)=1$　のとき)

$P=[p, r+\sqrt{m}], r^2\equiv m \quad (p)$

$(p)=P$　($\lambda_p(m)=-1$　のとき)　　※

(3)　$p\neq 2, p|d$　なる素数 p について

$(p)=P^2,\ P=[p, \sqrt{m}]$　　※

注意3　(イ)　$\lambda_p(m)$ はルジャンドルの記号

(ロ)　(2)の r について

$k=1$　のとき　$r=1$

$\because n^2-1\equiv 1 \quad \therefore m\equiv 1 \quad (p)$

$k\neq 1$　のとき　$r=modinv[3)](k, p)$

$\because n^2-1\equiv 1 \quad (p)$

$k^2m\equiv 1 \quad (p)$

$\therefore m\equiv \{modinv(k, p)\}^2$

(ハ)　$\lambda_p(d)=\lambda_p(4m)=\lambda_p(m)$

$=\lambda_p(n^2-1)=1$

より(2)の※は起こらない．

(ニ)(3)の※も同様

$n^2-2\equiv 0 \quad (p)\Rightarrow n^2-1\not\equiv 0 \quad (p)$

$\Rightarrow m\not\equiv 0 \quad (p)$

補題4　2　$m\equiv 1$　(4) のとき

(1)　(2) $=P\overline{P}$　($m\equiv 1$　(8))　　※

$P=[2, \omega], \omega=(1+\sqrt{m})/2$

(2) $=P$　　($m\equiv 5$　(8))　　※

(2) $p\neq 2, p\nmid d(=m)$ なる素数 p について

$(p)=P\overline{P}$ $(\lambda_p(m)=1$ のとき)

$P=[p, r+w]$

$(2r+1)^2\equiv m\ (p)$

$(p)=P$ $(\lambda_p(m)=-1$ のとき) ※

(3) $p\mid d$ なる素数 p について

$(p)=P^2$, $P=[p, q+\omega]$

$p=2q+1$ ※

注意4 (イ) (2)の r について補題3．1と同様簡単に求められる．r が偶数のときは $p-r$ で置きかえその後 r を $2r+1$ と見れば良い．

(ロ) ※はすべて今の問題では起こらない．

(1) $2\mid n^2-2\Rightarrow 2\mid n\Rightarrow n^2-1\equiv 3$ (4)

$\Rightarrow k^2m\equiv 3\Rightarrow m\equiv 3$ (4)

(2) $\lambda_p(m)=\lambda_p(k^2m)=\lambda_p(n^2-1)=1$

(3) 補題4．1(3)と同じ

1．4 イデヤルの積の標準底[1)]

補題5 原始イデヤル $J=[a, b+\omega]$ と素イデヤル $P=[p, r+\omega]$ の積は以下のようになる．

(1) $p\nmid a$ のとき

$JP=[ap, t+\omega]$

$t\equiv b\ (a), t\equiv r\ (p)$

(2) $p\mid a$, $b+r+\omega+\overline{\omega}\not\equiv 0\ (p)$ のとき

$JP=[ap, t+\omega]$

i) $m\equiv 2,3$ (4) のとき $\omega=\sqrt{m}$

$t\equiv (br+m)x+bpy\ \ (ap)$

$(b+r)x+py=1$

ii) $m\equiv 1$ (4) のとき $\omega=(1+\sqrt{m})/2$

$t\equiv \{br+(m-1)/4\}\ x+bpy\ \ (ap)$

$(b+r+1)x+py=1$

(3) $p\mid a$, $b+r+\omega+\overline{\omega}\equiv 0\ (p)$ のとき

$JP=p\,[a/p, b+\omega]$

証明 (1) $(a, p)=1$ より

$au+pv=1$, $^\exists u, v\in Z$

$t\equiv rau+bpv\ \ (ap)$ とすれば

$t\equiv b\ (a), t\equiv r\ (p)$

$JP=[a, b+\omega][p, r+\omega]$

$=[a, t+\omega][p, t+\omega]$

$JP\supset[ap, t+\omega]$ (11)

$a\mid N(t+\omega), p\mid N(t+\omega)$ より

$ap\mid N(t+\omega)$ よって $[ap, t+\omega]$ は標準底である．

(11)の両辺のノルムは共に ap で等しいから，

$JP=[ap, t+\omega]$ である．

(2) i) $JP=[a, b+\omega][p, r+\omega]$

$=(ap, a(r+\omega), p(b+\omega),$

$br+m+(b+r)\sqrt{m})$

$(b+r, p)=1$ より

$(b+r)u+pv=1$, $^\exists u, v\in Z$

$t\equiv (br+m)u+pbv\ \ (ap)$ とする

$JP\supset(ap, t+\sqrt{m})$ (12)

$ap=N(JP)\mid N(t+\omega)$

よって $[ap, t+\sqrt{m}]$ は標準底であり，(12)の両辺のノルムは等しいから

$JP=[ap, t+\omega]$ である．

ii) $JP=[a, b+\omega][p, r+\omega]$

$=(ap, a(r+\omega), p(b+\omega),$

$br+(m-1)/4+(b+r+1)\omega)$

$(b+r+1, p)=1$ より

$(b+r+1)u+pv=1$, $^\exists u, v\in Z$

$t\equiv \{br+(m-1)/4\}\ u+pbv\ \ (ap)$

とすると

$JP\supset[ap, t+\omega]$

両辺のノルムは等しいから

$JP=[ap, t+\omega]$ である．

(3) $JP=[a, b+\omega][p, r+\omega]$

$=[a/p, b+\omega][p, b+\omega]$

$\cdot[p, r+\omega]$

$=p\ [a/p, b+\omega]$

$\because\ [p, b+\omega]=[p, -r-\overline{\omega}]$

1．5 単項イデヤルの判定

補題6 $[a, b+\omega]$ が単項イデヤルである条件[1)2)]

(1) $m\equiv 2,3$ (4) の場合

$(b+\sqrt{m})/a$ を連分数展開するとき，

$r+\sqrt{m}$ が終項に現れるか否かで定まる．

$(r=[\sqrt{m}])$ このとき

$[a, b+\sqrt{m}]=(Q_n(r-\sqrt{m})+Q_{n-1})$

である．Q_n, Q_{n-1} は近似分数の分母とする．

(2) $m\equiv 1$ (4) の場合

$(b+\omega)/a$ を連分数展開するとき，

$(r+\sqrt{m})/2$ が終項に現れるか否かで定まる．

r は $\sqrt{m}$ を越えない最大の奇数とする．

このとき

$[a, b+\omega]=(Q_n(r-\sqrt{m})/2+Q_{n-1})$

である．

証明 (1) $[a, b+\sqrt{m}]$ が単項イデヤルとすると

$[a, b+\sqrt{m}]=\rho\ [1, \sqrt{m}]$

$b+\sqrt{m}=u\rho+v\rho\sqrt{m}$

$a=s\rho+t\rho\sqrt{m}, ut-sv=\pm1$

$\therefore (b+\sqrt{m})/a$

$=(u+v\sqrt{m})/(s+t\sqrt{m})$

よって $(b+\sqrt{m})/a$ は $\sqrt{m}$ と対等となり，前者を連分数展開すると終項に $r+\sqrt{m}$ が現れる．r は $\sqrt{m}$ を越えない最大の整数である．

逆に結論を仮定すると，

$$(b+\sqrt{m})/a=\frac{P_n(r+\sqrt{m})+P_{n-1}}{Q_n(r+\sqrt{m})+Q_{n-1}}$$

$$=\frac{\{P_n(r+\sqrt{m})+P_{n-1}\}\{Q_n(r-\sqrt{m})+Q_{n-1}\}}{N\{Q_n(r+\sqrt{m})+Q_{n-1}\}}$$

$=\{\cdots+(P_nQ_{n-1}-P_{n-1}Q_n)\sqrt{m}\}/N$

ここで $P_nQ_{n-1}-P_{n-1}Q_n=\pm1$

$\therefore a=\pm N, N=N\{Q_n(r+\sqrt{m})+Q_{n-1}\}$

$\therefore [a, b+\sqrt{m}]\supset(Q_n(r-\sqrt{m})+Q_{n-1})$

両辺のノルムは共に a で等しいから

$[a, b+\sqrt{m}]=(Q_n(r-\sqrt{m})+Q_{n-1})$

(2)　(1)とほぼ同様にして証明できるのでここでは省略する．

注意5　$(b+\omega)/a$ を連分数展開するとき終項の分母が(1)の場合1，(2)の場合2となれば単項イデヤルといえる．

1．6　基本単数の求め方[1)]

(5)を満たす A が単項イデヤルであり，かつ(4)の形で表せるならば不定方程式(2)の整数解を得る．そうでないときでも適当な単数を掛けて(4)の形（$\sqrt{m}$ の係数が k で割り切れる）にできるかも知れない．そこで基本単数が必要となる．

補題7　θ を判別式 $d>0$ に属する簡約された二次無理数，$\theta=[k_1, k_2, \cdots\cdots, k_n, \theta]$ をその連分数展開の循環の一節，P_n/Q_n，P_{n-1}/Q_{n-1} を近似分数とすると

$E=Q_n\theta+Q_{n-1}$

は $Q(\sqrt{m})$ の基本単数を与える．

1．7　例 $n=11$ の場合

$$x^2-120y^2=-119 \qquad (13)$$

(1)　119, 120を素因数分解する．

$119=7\cdot17$，$120=2^2\cdot30$

$\therefore k=2, m=30, m\equiv2$　(4)

(2)　(7)，(17) を $Q(\sqrt{30})$ で素イデヤルの積に分解する．[補題4．1を用いる．]

(7) $=\overline{P}\overline{P}, P=[7, 3+\sqrt{30}]$

$3^2\equiv30$　(7)

(17) $=Q\overline{Q}$，$Q=[17, 8+\sqrt{30}]$

$8^2\equiv30$　(17)

$\therefore (x+y\sqrt{120})(x-y\sqrt{120})=PPQQ$

$\therefore (x+y\sqrt{120})=PQ, \overline{P}\overline{Q}, \overline{P}Q, P\overline{Q}$

この内2つずつは共役の関係にある．

(3)　標準底を求める．[補題5を用いる．]

$PQ=[7, 3+\sqrt{30}][17, 8+\sqrt{30}]$

$=[7, 59+\sqrt{30}][17, 59+\sqrt{30}]$

$59\equiv3$　(7)，$59\equiv8$　(17)

$=[119, 59+\sqrt{30}]$

$P\overline{Q}=[7, 3+\sqrt{30}][17, -8+\sqrt{30}]$

$=[119, 94\sqrt{30}]$

$94\equiv3$　(7)，$94\equiv-8$　(17)

(4)　自明解はいずれか．[補題3を用いる．]

$2(59+\sqrt{30})-119=-1+\sqrt{120}$

$\therefore -1+\sqrt{120}\in PQ$

$PQ, \overline{P}\overline{Q}$ より生ずる解は自明解およびその同伴解である．

(5)　$P\overline{Q}$ は単項イデヤルか．[補題6を用いる．]

$(94+\sqrt{30})/119$

$=[0, 1, 2, 1, 4+\sqrt{30}]$

λ_j：連分数展開の第 j 項

$P_{j+2}=P_{j+1}\lambda_{j+2}+P_j, P_0=1, P_1=\lambda_1$

$Q_{j+2}=Q_{j+1}\lambda_{j+2}+Q_j, Q_0=0, Q_1=1$

$\therefore (94+\sqrt{30})/119$

$$=\frac{3(4+\sqrt{30})+2}{4(4+\sqrt{30})+3}$$

$=(14+3\sqrt{30})/(19+4\sqrt{30})$

$\therefore P\overline{Q}=(-19+4\sqrt{30})$

$\overline{P}Q=(19+4\sqrt{30})$

2|4 より，これらは(13)の整数解を与える．

(13)の整数解 (x, y) は

$x+y\sqrt{120}$

$=(\pm1+\sqrt{120})(11+\sqrt{120})^e$

または $(\pm19+2\sqrt{120})(11+\sqrt{120})^e$

＋のとき $e\geqq0$，－のとき $e>0$

1．8　プログラムとその出力の例

以上の方法で n が与えられると不定方程式(2)のすべての整数解を求めることができる．「*UBASIC*」[3)]という言語を用いて，(2)の整数解を求めるプログラムを作成し，$n\leqq131071$ の範囲で実行し，結果を得ている．ここにそのプログラム（表2）とその出力の例（表1）を示す．

```
 33539  から  33539  までの  自明でない整数解の代表
N= 33539 K= 2 M= 281216130  23 * 73 * 463 * 1447
[ 23 , 12 +√ 281216130 ] [ 73 , 37 +√ 281216130 ]
[ 463 , 232 +√ 281216130 ] [ 1447 , 724 +√ 281216130 ]
[ 1124864519 , 562432260 +√ 281216130 ] 自明解
[ 1124864519 , 1071614195 +√ 281216130 ]
[ 1124864519 , 81388686 +√ 281216130 ]
[ 1124864519 , 590570621 +√ 281216130 ]
単項( 28139201 + 1678 √ 281216130 )
n= 33539          28139201          839      669941          20

[ 1124864519 , 485386745 +√ 281216130 ]
[ 1124864519 , 994568680 +√ 281216130 ]
[ 1124864519 , 4343171 +√ 281216130 ]
単項( 290210686219 + 17305864 √ 281216130 )
n= 33539          4326401           129      4359941          130

[ 1124864519 , 513525106 +√ 281216130 ]
```

表—1　$n=33539$の場合（計算機の出力）

```
 10 '                                                    ed2
 20 ' X ^ 2 - ( N ^ 2 - 1 ) Y ^ 2 = - ( N ^ 2 - 2 )  の整数解
 30 '          N 1  から  N 2  までの  自明でない整数解の代表
 40 '                                  ,89.1.3.  9.24
 50 '
 60 dim P(30),R(30),S%(30)
 70 input N1,N2
 80 lprint N1;" から ";N2;"  までの  自明でない整数解の代表"
 90 for N=N1 to N2
100 ' N ^ 2 - 1 の分解
110 W=N^2-1
120 Z=W
130 K=1
140 M=1
150 SD=prmdiv(W)
160 W=W¥SD
170 if W@SD then M=M*SD:goto 190
180 W=W¥SD:K=K*SD
190 if W>1 goto 150
200 print "N=";N;"K=";K;"M=";M;
210 ' N^2-2の分解
220 dec Z
230 W=Z
240 L%=1
250 SD=prmdiv(W)
260 P(L%)=SD
270 W=W¥SD
280 if W>1 then inc L%:goto 250
290 for I%=1 to L%
300 print P(I%);
310 if I%<L% print "*";
320 next I%
```

```
330 ' N^2 は素数か?
340 if L%=1 print "自明解":goto 1220
350 if M@4=1 goto 1240
360 if N@2=1 goto 410
370 if L%=2 print "自明解":goto 1220
380 R(1)=0
390 if M@4=3 then R(1)=1
400 goto 430
410 if K=1 then R(1)=1:goto 430
420 R(1)=modinv(K,P(1))
430 for I%=2 to L%
440 if K=1 then R(I%)=1:goto 460
450 R(I%)=modinv(K,P(I%))
460 next I%
465 print
470 for I%=1 to L%
480 S%(I%)=1
485 print " [";P(I%);",";R(I%);"+√";M;"] ";
490 next I%
495 print
500 ' 標準底を求める。
510 A=P(1):B=R(1)
520 C=1:I%=2
530 if gcd(A,P(I%))=1 then B1=A*R(I%)*S%(I%):C1=A:goto 570
540 C1=B+R(I%)*S%(I%)
550 if gcd(C1,P(I%))>1 then A=A¥P(I%):C=C*P(I%):goto 620
560 B1=B*R(I%)*S%(I%)+M
570 X=modinv(C1,P(I%))
580 Y=(1-X*C1)¥P(I%)
590 B=B*P(I%)*Y+B1*X
600 A=A*P(I%)
610 B=B@A
620 inc I%
630 if I%<=L% goto 530
640 if C>1 print C;
650 print " [";A;",";B;"+√";M;"] ";
660 ' 単項か? 単項の底, 単数
670 if C>1 goto 700
680 if B*K@A=1 print "自明解";:goto 1140
690 if B*K@A=A-1 print "自明解";:goto 1140
700 QM=isqr(M)
710 Q0=0:Q1=1
720 S%=0:SS%=1
730 if A>0 then Q=(B+QM)¥A
740 if A<0 then Q=(-B-QM-1)¥(-A)
750 B=A*Q-B
760 A=(M-B^2)¥A
770 inc S%
780 if S%=1 goto 730
790 W=Q1:Q1=Q*Q1+Q0:Q0=W
800 E=(B-sqr(M))/A
810 if E>0 goto 730
820 if E+1<0 goto 730
830 if SS%=1 then SS%=0:A0=A:B0=B:goto 850
840 if (A=A0)*(B=B0) goto 1140
850 if (A=1)*(B=QM)=0 goto 730
860 print "単項";
870 ' Ⅳ Kを法として integer? 単数をかけて integer にできるか?
```

```
 880 Q0=C*(Q1*QM+Q0)
 890 Q1=C*Q1
 895 print "(";Q0;"+";Q1;"√";M;")";
 900 if Q1@K=0 goto 1130
 910 Q2=0:Q3=1
 920 B=QM:A=1
 930 S%=0
 940 if A>0 then Q=(B+QM)¥A
 950 if A<0 then Q=(-B-QM-1)¥(-A)
 960 B=A*Q-B
 970 A=(M-B^2)¥A
 980 inc S%
 990 if S%>1 goto 1020
1000 if (A=1)*(B=QM) goto 1040
1010  goto 940
1020 W=Q3:Q3=Q*Q3+Q2:Q2=W
1030 if (A=1)*(B=QM)=0 goto 940
1040 Q2=Q3*B+Q2
1050 D=gcd(Q3,K)
1060 if Q1@D goto 1140
1070 print " 通過";
1080 W1=Q0@K:W2=Q1@K
1090 W=Q0:Q0=Q2*Q0+Q3*Q1*M:Q1=W*Q3+Q2*Q1
1100 if Q1@K=0 goto 1130
1110 if (Q0@K=W1)*(Q1@K=W2)=0 goto 1090
1120 goto 1140
1130 Y=Q1¥K:X=Q0
1131 Y1=N*Y-X:X1=X*N-Y*(N*N-1)
1132 if X1<0 then goto 1139
1133 X=X1:Y=Y1:goto 1131
1139 lprint:lprint "n=";N,X,Y,-X1,Y1
1140 I%=L%
1150 S%(I%)=-S%(I%)
1160 if S%(I%)=-1 lprint:goto 510
1170 dec I%
1180 if I%>2 goto 1150
1190 if P(1)=2 goto 1210
1200 if I%=2 goto 1150
1210 print
1220 next N
1230 end
1240 if N@2=0 then R(1)=0:I%=2:goto 1260
1250 for I%=1 to L%
1260 if K=1 then G=1:goto 1290
1270 G=modinv(K,P(I%))
1280 if G@2=0 then G=P(I%)-G
1290 dec G
1300 R(I%)=G¥2
1310 next I%
1315 print
1320 for I%=1 to L%
1330 S%(I%)=1
1335 print " [";P(I%);",";R(I%);"+(1+√";M;")/2] ";
1340 next I%
1345 print
1350 ' 標準底を求める。
1360 A=P(1):B=R(1):C=1:I%=2
1370 P=P(I%):R=R(I%)
```

```
1380 if S%(I%)=-1 then R=-R-1
1390 if A@P then B1=A*R:C1=A:goto 1420
1400 if (B-R)@P then A=A¥P:C=C*P:goto 1470
1410 B1=B*R+(M-1)¥4:C1=B+R+1
1420 X=modinv(C1,P)
1430 Y=(1-C1*X)¥P
1440 B=B*P*Y+B1*X
1450 A=A*P
1460 B=B@A
1470 inc I%
1480 if I%<=L% goto 1370
1490 if C>1 print C;
1500 print " [";A;",";B;"+(1+√ ";M;")/2] ";
1510 if (2*B*K+K)@A=A-1 print "自明解";:goto 1920
1520 if (2*B*K+K)@A=1 print "自明解";:goto 1920
1530 QM=isqr(M)
1540 Q0=0:Q1=1:BB=QM
1550 S%=0:SS%=1
1560 if BB@2=0 then dec BB
1570 A=A*2:B=B*2+1
1580 if A>0 then Q=(B+QM)¥A
1590 if A<0 then Q=(-B-QM-1)¥(-A)
1600 B=A*Q-B
1610 A=(M-B^2)¥A
1620 inc S%
1630 if S%=1 goto 1580
1640 W=Q1:Q1=Q*Q1+Q0:Q0=W
1650 E=(B-sqr(M))/A
1660 if E>0 goto 1580
1670 if E+1<0 goto 1580
1680 if SS%=1 then SS%=0:A0=A:B0=B:goto 1700
1690 if (A=A0)*(B=B0) goto 1920
1700 if (A=2)*(B=BB)=0 goto 1580
1710 print "単項";
1720  Q0=C*Q0+C*Q1*(BB-1)¥2:Q1=C*Q1
1725 print "(";Q0;"+";Q1;"(1+√ ";M;")/2)";
1730 if Q1@(2*K)=0 goto 1910
1740 Q2=0:Q3=1:B=BB:A=2:S%=0
1750 if A>0 then Q=(B+QM)¥A
1760 if A<0 then Q=(-B-QM-1)¥(-A)
1770 B=A*Q-B
1780 A=(M-B^2)¥A
1790 inc S%
1800 if S%=1 goto 1750
1810 W=Q3:Q3=Q*Q3+Q2:Q2=W
1820 if (A=2)*(B=BB)=0 goto 1750
1830 D=gcd(Q3,K*2)
1840 if Q1@D goto 1920
1850 Q2=Q3*(BB-1)¥2+Q2
1860 W1=Q0@(2*K):W2=Q1@(2*K)
1870 W=Q0:Q0=Q2*Q0+Q3*Q1*(M-1)¥4:Q1=W*Q3+Q2*Q1+Q1*Q3
1880 if Q1@(2*K)=0 goto 1910
1890 if (Q0@(2*K)=W1)*(Q1@(2*K)=W2)=0 goto 1870
1900 goto 1920
1910 X=Q0+Q1¥2:Y=Q1¥K¥2
1911 Y1=N*Y-X:X1=X*N-Y*(N*N-1)
1912 if X1<0 then goto 1919
1913 X=X1:Y=Y1:goto 1911
```

```
1919 lprint:lprint "n=";N,X,Y,-X1,Y1
1920 I%=L%
1930 S%(I%)=-S%(I%)
1940 if S%(I%)=-1 lprint:goto 1350
1950 dec I%
1960 if I%>1 goto 1930
1970 goto 1210
1980 end
```

表—2 $x^2-1=(n^2-1)(y^2-1)$ の整数解を求めるプログラム

$|n|\leqq 10000$, $|y|\leqq 10000$ における $x^2-1=(n^2-1)(y^2-1)$ の非自明解

n	y					
11	2	* 41	* 900	3	* 64	* 1405
23	3	* 134	* 6161	4	* 181	* 8322
39	4	* 307		5	* 386	
41	2	* 153		* 11	* 900	
59	5	* 584		6	* 703	
64	3	* 373		* 11	* 1405	
83	6	* 989		7	* 1156	
111	7	* 1546		8	* 1769	
134	3	* 781		* 23	* 8322	
143	8	* 2279		9	* 2566	
153	2	* 571		* 41		
179	9	* 3212		10	* 3571	
181	4	* 1425		* 23	* 8322	
219	10	* 4369		11	* 4808	
263	11	* 5774		12	* 6301	
307	4	* 2417		* 39		
311	12	* 7451		13	* 8074	
363	13	* 9424		14		
373	3	* 2174		* 64		
386	5	* 3821		* 39		
419	14			15		
476	15			16		
543	16			17		
571	2	* 2131		* 153		
584	5	* 5781		* 59		
611	17			18		
683	18			19		
703	6	* 8377		* 59		
759	19			20		
781	3	* 4552		* 134		
839	20			21		
900	* 11			* 41		
923	21			22		
989	6			* 83		
1011	22			23		
1103	23			24		
1156	7			* 83		
1199	24			25		
1299	25			26		
1403	26			27		
1405	* 11			* 64		
1425	4			* 181		
1511	27			28		
1546	7			* 111		

n	y	
2519	35	36
2566	9	* 143
2663	36	37
2811	37	38
2963	38	39
3119	39	40
3212	9	* 179
3279	40	41
3443	41	42
3571	10	* 179
3611	42	43
3783	43	44
3821	5	* 386
3959	44	45
4139	45	46
4323	46	47
4369	10	* 219
4511	47	48
4552	3	* 781
4703	48	49
4808	11	* 219
4899	49	50
5099	50	51
5303	51	52
5511	52	53
5723	53	54
5774	11	* 263
5781	5	* 584
5939	54	55
6159	55	56
6161	* 23	* 134
6301	12	* 263
6383	56	57
6611	57	58
6843	58	59
7079	59	60
7319	60	61
7451	12	* 311
7563	61	62
7811	62	63
7953	2	* 2131
8063	63	64
8074	13	* 311
8319	64	65

1623	28		29		8322	*	23	* 181
1739	29		30		8377		6	* 703
1769	8		* 111		8579		65	66
1859	30		31		8843		66	67
1983	31		32		9111		67	68
2111	32		33		9383		68	69
2131	2	* 7953	* 571		9424		13	* 363
2174	3		* 373		9659		69	70
2243	33		34		9939		70	71
2279	8		* 143					
2379	34		35		33539		20	* 839
2417	4		* 307				129	130

表－3　$x^2-1=(n^2-1)(y^2-1)$ の非自明解

2．不定方程式　$x^2-1=(y^2-1)(z^2-1)$

2．1　計算の結果

表2に示したプログラムの実行結果を紙面の都合上 $n\leqq 10000$, $y\leqq 10000$ の範囲でまとめたものを表3に示した．これだけで十分全体の考察ができる．表の最後に $n=33539$ の場合をつけ加えておいた．計算した範囲ではこの場合に限って非自明解が2組存在するので特にあげておいた．n の欄は非自明解をもつ n の値であり，y の欄はその非自明解の y の値である．x の値は省いてある．同じ枠内の y の値は同伴解である．点線をはさんで反対側の y の値は対称なものと同伴解である．

$n=11$ の場合 $(x,y)=(19,2)$ が解で，対称な $(-19,2)$ も解である．

$(-19+2\sqrt{120})(11+\sqrt{120})$

$=31+3\sqrt{120}$

この計算により $(31,3)$ が $(19,2)$ と対称ものと同伴解である．

次に無印と＊印の意味を説明する．

$n=11$ のとき $y=2$ が非自明解である．

$x^2-(11^2-1)y^2=2-11^2$

$y=2$ はこの方程式の非自明解である．しかし，同じ解を

$x^2-(2^2-1)z^2=2-2^2$

の解と見ると自明解である．

このような場合表中の y の値を無印としてある．

$n=11$ のとき $y=41$ については y を固定して

$x^2-(41^2-1)z^2=2-41^2$

の解と見てもやはり非自明解である．

このような場合表中の y の値に＊印をつけてある．

2．2　根原解について[1)]

$$x^2-(n^2-1)y^2=2-n^2 \qquad (2)$$

のグラフは双曲線であり，したがって(2)の整数解を求めることは(2)の双曲線上の格子点を求めることになる．対称性から第1象限で求めれば十分である．

定義2　$f:(x,y)\longrightarrow(X,Y)$

$$\Longleftrightarrow \quad X+Y\sqrt{n^2-1}=(x+y\sqrt{n^2-1})(n+\sqrt{n^2-1})$$

補題8　双曲線(2)の $y>0$ の分枝上の点は f により同じ分枝上を右へ移動し，f^{-1} により左へ移動する．

証明　$(n+\sqrt{n^2-1})(n-\sqrt{n^2-1})=1$

より(2)の上の点は f により(2)の上で移動することは明らかである．(x,y) が(2)の $y>0$ の分枝上，

$f:(x,y)\longrightarrow(X,Y)$ とすると

$X=nx+y(n^2-1)$, $Y=x+ny$

(x,y) が第1象限または y 軸との交点のとき，$X>x$, $Y>0$ である．

(x,y) が第2象限にあるとき，

$X-x=(n-1)x+y(n^2-1)$

$=(n-1)\{x+y(n+1)\}$

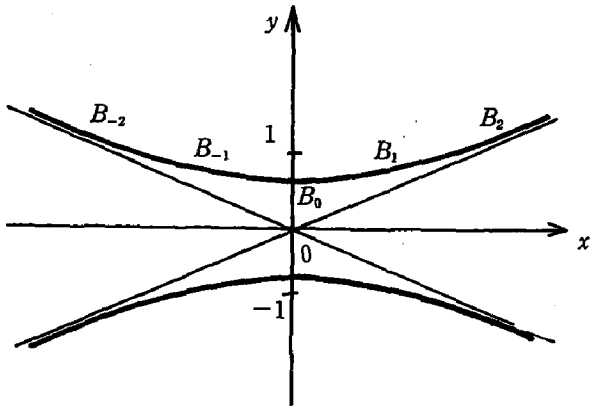
$y^2(n+1)^2-x^2$

$=2(n+1)y^2-2+n^2>0$

$\therefore X>x$

$(ny)^2-x^2=y^2-2+n^2>0$

$\therefore Y>0$　　*Q. E. D.*



図－1　根原解

双曲線(2)とy軸との交点をB_0，B_0をfで移した点をB_1，B_1をfで移した点をB_2，次々とfで移して得られる点を$B_3, B_4\cdots\cdots$，B_0をf^{-1}で次々と移して得られる点を$B_{-1}, B_{-2}\cdots\cdots$とすると孤$B_nB_{n+1}$上の点は孤$B_{n+1}B_{n+2}$上の点に移る．しかも格子点は格子点に移るから．(2)が整数解をもてば孤B_0B_1(B_0を含みB_1は含まない)上に同伴解が唯1つ存在する．これを根原解という．

補題9　$x^2-(n^2-1)y^2=2-n^2$　(2)

の解が根原解である条件は$y<n$，$x>0$である．

証明　$B_0(0, y_0)$を(2)とy軸との交点とすると，

$y_0=\sqrt{(n^2-2)/(n^2-1)}$

$y_0\sqrt{n^2-1}(n+\sqrt{n^2-1})$

$=y_0(n^2-1)+ny_0\sqrt{n^2-1}$

$f: B_0\longrightarrow B_1$とすると，

$B_1(y_0(n^2-1), ny_0)$

$ny_0<n$

$(ny_0)^2-(n-1)^2$

$=\dfrac{n^2(n^2-2)-(n-1)^2(n^2-1)}{n^2-1}$

分子$=2n(n^2-n-1)+1>0$

$\therefore ny_0>n-1$

$\therefore n-1<ny_0<n$

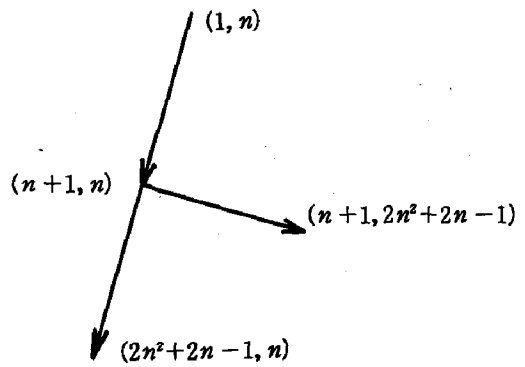
よって(2)の整数解がB_0B_1上にある条件は

$x>0, y<n$である．

注意6　1つの整数解から根原解を求めるにはfまたはf^{-1}で移すことを繰り返しxの符号が変わる前後を見て$x>0, y>0$の方をとれば良い．他方をy軸に関して対称に移すと共役なものの根原解が得られる．

2．3　結果の考察

2．3．1　表3のyの欄に2, 3, 3, 4……のように連続する自然数が現れている．



図—2　解の派生

以下(y, z)により解のy，zの値を示し，xの値は省略して表す．

$(1+\sqrt{n^2-1})(n+\sqrt{n^2-1})$

$=(n^2+n-1)+(n+1)\sqrt{n^2-1}$

$(1+\sqrt{n^2-1})(n+\sqrt{n^2-1})^2$

$=\cdots+(2n^2+2n-1)\sqrt{n^2-1}$

よってzをnに固定すると自明解の系列

$(1, n)\longrightarrow(n+1, n)$

$\longrightarrow(2n^2+2n-1, n)\cdots$

が得られる．

$(n+1, n)$に着目し，yを$n+1$に固定すると

$(n^2+n-1+n\sqrt{(n+1)^2-1})$

$\times(n+1+\sqrt{(n+1)^2-1})$

$=\cdots+(2n^2+2n-1)\sqrt{(n+1)^2-1}$

$\therefore(n+1, n)\longrightarrow(n+1, 2n^2+2n-1)$

$N=2n^2+2n-1$とおく．

(N, n)はzをnに固定した方程式で見れば自明解の系列に属するが，yをNに固定した方程式で見ると$n<N$より，これは根原解であり，$n\neq1$，$N-1$より非自明解である．対称性から(n, N)も解でzをNに固定するとき$y=n$は非自明解である．$(n+1, N)$も同様にしてzをNに固定するとき$y=n+1$は非自明解といえる．

補題10　$N=2n^2+2n-1$のとき

$x^2-(N^2-1)y^2=2-N^2$

は$y=n, y=n+1$なる非自明解をもつ．

すなわち，次の恒等式が成り立つ．

$(2n^3+2n^2-2n-1)^2-1$

$=\{(2n^2+2n-1)^2-1\}(n^2-1)$

$(2n^3+4n^2-1)^2-1$

$=\{(n+1)^2-1\}\{(2n^2+2n-1)^2-1\}$

2．3．2

その他の非自明解についても自明解から派生することが確かめられる．$n=41$および$n=900$のときの非自明解が自明解からどのように派生するかを図3に示す．左下への派生はzを固定した方程式の同伴解であり，右下への派生はyを固定した方程式の同伴解である．表1の最後にあげておいた$n=33539$の場合も図4より明らかである．

2．4　結論

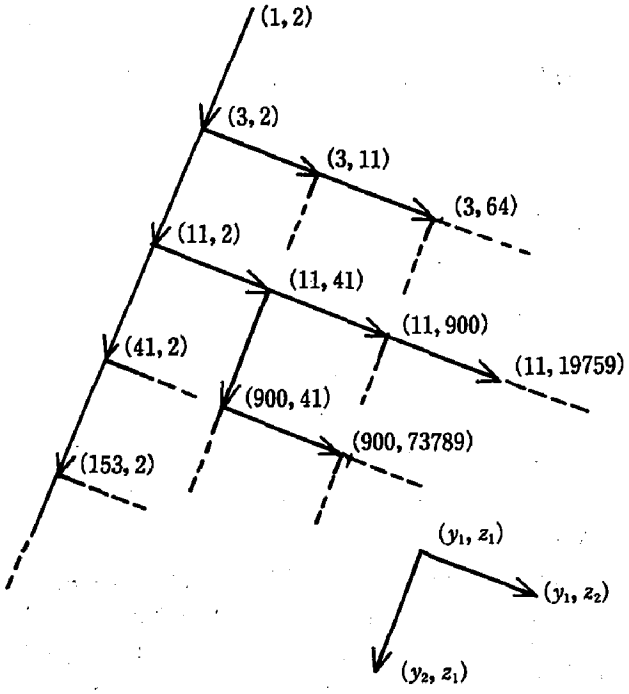
定理　不定方程式

$x^2-1=(y^2-1)(z^2-1)$

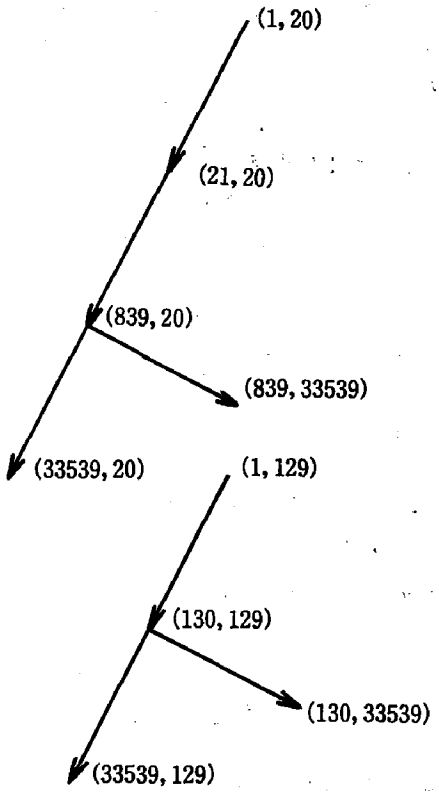
の整数解はすべて自明解

$(x, y, z)=(1, 1, n), (1, n, 1)$

$n=2, 3, 4, \cdots\cdots$



図－3 解の派生



図－4 解の派生

より派生する.

注意7 $(\pm1, 0, \pm1), (\pm1, \pm1, 0)$
$(\pm1, \pm1, \pm1)$ は除いて考える.
方程式の対称性から $x, y, z > 0$ とする.

証明 自明解$(1, 1, n), (1, n, 1), n \geqq 2$ より出発し, y または z のいずれかを固定してできる方程式の同伴解として, 1つの解より2つの方向に解が派生する. 逆に, 任意の整数解があると y または z を固定した方程式の根原解を逆上ると補題9により $min(y, z)$ が減少し, ついに y または z が1になる. すなわち自明解より派生する解である. 派生する方向は2つあるがその内一方においては根原解であるから元へ戻る道は一本であり, これらの解の網が交差することはない.

2．5 終わりに

$3\times8=24$のような数は他にあるのかどうかという疑問を最初に抱いたのは徳島大学工学部学生の節見隆宏君である. また同大学教養学部の片山真二先生には多大のご教示をいただいた. ここに感謝の意を表します. なお, 同じような2次不定方程式

$(x^2\pm1)=(y^2\pm1)(z^2\pm1)$

が考えられる. 大半は解を持たないことが確かめられ, 解をもつ場合はこの問題と同じ方法で解けると考えている.

3．文献

(1) 高木貞治；初等整数論講義, 共立出版, p. 208—240, p. 288—292, p. 321—348
(2) 小野 孝；数論序説, 裳華房, p. 12—20, p. 177—186
(3) 木田祐司；*UBASIC*86, 日本評論社