$a^2 + mb^2 = c$の自然数解の研究

林　幸昌　　森谷 智明

平成 18 年 2 月 16 日

目 次

1 目的

$a^2 + mb^2 = c$ の研究は昨年度（2005 年度）に中平健さんと服部真宏さんが係数 $m = 3, 5$ の場合を研究している。今回は、特 $m = 6, 7$ の場合を考え、方程式 $a^2 + 6b^2 = c$, $a^2 + 7b^2 = c$ において、解がある場合の c の性質を調べ、またあたえられた c に対して解 (a, b) がいくつあるか、などを研究する。（$m = 6$ を林、$m = 7$ を森谷が担当）

2 方法

2.1 Prolog

プログラミング言語 Prolog を用いて、方程式の自然数解を求め、その結果から解の性質を予想する。

2.2 素イデアル分解の一意性

$\mathbb{Z}[\sqrt{-m}]$ において、$c = a^2 + mb^2 = (a + b\sqrt{-m})(a - b\sqrt{-m})$ と因数分解できるので、素イデアル分解の一意性を利用して予想したことを証明する。 ($m = 6$ のとき、類数が 2 であることを使う。)

3 プログラム

3.1 $a^2 + 6b^2 = c$ を担当した林が作成したプログラム

```
/** a^2+mb^2=c の解と c mod 6,24 **/
/** (X:c の開始位置、Y:c の終了位置、Z:係数 m の値) **/
/** (T=0 ⇒ c:全て、T=1 ⇒ c:素数のみ、T=2 ⇒ c:合成数のみ) **/

abc(X,Y,Z,T):-
    nl,write('c'),put(9),write('(a,b)'),
    put(9),write('c no soinsuubunkai'),
    put(9),write('c mod 6'),
    put(9),write('c mod 24'),nl,nl,abc_1(X,Y,Z,T).
    abc_1(X,Y,Z,T):- X>Y.
    abc_1(X,Y,Z,T):- T == 0 ,
        abc_2(X,Z,T),X1 is X+1,abc_1(X1,Y,Z,T).
    abc_1(X,Y,Z,T):- T == 1 ,
        prime_1(X,P),(P == 0 ->
           (X1 is X+1);
       (abc_2(X,Z,T),X1 is X+1)),abc_1(X1,Y,Z,T).
    abc_1(X,Y,Z,T):- T == 2 ,
        prime_1(X,P),(P == 1 ->
```

```
          (X1 is X+1);
      (abc_2(X,Z,T),X1 is X+1)),abc_1(X1,Y,Z,T).

abc_2(C,N,T):-
  D is 1,Q is 0,abc_2_1(A,B,C,D,N,Q,T).
    abc_2_1(A,B,C,D,N,Q,T):- D>C,(Q == 0 ->
        (write(''));(put(9),prime_dec1(C),
         res_q(C = 6*U1 + V1),put(9),res_q(C = 24*U2 + V2),
                           write(V1),put(9),write(V2))).
    abc_2_1(A,B,C,D,N,Q,T):- A1 is D*D,B1 is (C - A1)/N,
    (B1>0 ->
    (B2 is sqrt(B1) ->
    (integer(B2) -> gcd(U =(D,B2)),

      ( U == 1 ->
      ( Q == 0 ->

        (nl,Q1 is Q+1,write(C),put(9),write('('),write(D),
                  write(','),write(B2),write(')'),tab(2),D1 is D+1);
        (Q1 is Q,write('('),write(D),write(','),write(B2),
                                       write(')'),tab(2),D1 is D+1));
        (Q1 is Q,D1 is D+1));(Q1 is Q,D1 is D+1));
                                (Q1 is Q,D1 is D+1));(Q1 is Q,D1 is D+1)),
    abc_2_1(A,B2,C,D1,N,Q1,T).



/** ルジャンドル記号計算 **/
leg(A/P):- Y is A,Z is P,X is 1,prime_1(P,U),leg_00(A/P,Y/Z,X,U).

leg_00(A/P,Y/Z,X,0):- nl,write('Warning : P is not Prime number.[A/P]').
leg_00(A/P,Y/Z,X,1):- leg_0(A/P,Y/Z,X).

/** (1)-(7) **/

leg_0(-1/P,Y/Z,X):- Q is (P-1)/2,integer(Q),X1 is (-1)^Q*X,leg_Write(Y/Z,X1).
leg_0(A/P,Y/Z,X):- A<(-1) -> (A1 is A+P,leg_0(A1/P,Y/Z,X));leg_1(A/P,Y/Z,X).

leg_1(1/P,Y/Z,X):- X1 is 1*X,leg_Write(Y/Z,X1).
leg_1(A/P,Y/Z,X):- Q is A/P,integer(Q),X1 is 0*X,leg_Write(Y/Z,X1).
leg_1(2/P,Y/Z,X):-  Q is ((P^2)-1)/8,integer(Q),X1 is (-1)^Q*X,leg_Write(Y/Z,X1).
leg_1(A/P,Y/Z,X):- A>P,res_q4(A,P,R,Q),leg_1(R/P,Y/Z,X).
leg_1(A/P,Y/Z,X):- prime_2(A,Pr1),prime_2(P,Pr2),
```

```
      Pr1==1 ->
      (Pr2==1 ->
      Q is (P-1)*(A-1)/4,integer(Q),X1 is (-1)^Q*X,leg_0(P/A,Y/Z,X1);
      leg_2(A/P,Y/Z,X));leg_2(A/P,Y/Z,X).

leg_2(A/P,Y/Z,X):- pdp_once(A,S,T),leg_2_1(S/P,T/P,Y/Z,X).
leg_2_1(S/P,T/P0,Y/Z,X):-
      S == 1 -> leg_Write(Y/Z,X);leg_2_2(S/P,T/P0,Y/Z,X).
leg_2_2(1/P,T/P0,Y/Z,X):- X1 is 1*X,leg_2(T/P0,Y/Z,X).
leg_2_2(2/P,T/P0,Y/Z,X):- Q is ((P^2)-1)/8,integer(Q),X1 is (-1)^Q*X,leg_2(T/P0,Y/Z,X1).
leg_2_2(A/P,T/P0,Y/Z,X):- prime_2(A,Pr1),prime_2(P,Pr2),
      Pr1==1 ->
      (Pr2==1 ->
      Q is (P-1)*(A-1)/4,integer(Q),X1 is (-1)^Q*X,res_q4(P,A,R,Q9),
                                                    leg_2_2(R/A,T/P0,Y/Z,X1);
      leg_3(A/P,T/P0,Y/Z,X));leg_3(A/P,T/P0,Y/Z,X).

leg_3(A/P,T/P0,Y/Z,X):- pdp_once(A,S,T1),leg_3_1(S/P,T1/P,T/P0,Y/Z,X).
leg_3_1(S/P,T1/P1,T/P0,Y/Z,X):-
      S == 1 -> leg_2(T/P0,Y/Z,X);leg_3_2(S/P,T1/P1,T/P0,Y/Z,X).
leg_3_2(1/P,T1/P1,T/P0,Y/Z,X):- X1 is 1*X,leg_3(T1/P1,T/P0,Y/Z,X).
leg_3_2(2/P,T1/P1,T/P0,Y/Z,X):- Q is ((P^2)-1)/8,integer(Q),
                                          X1 is (-1)^Q*X,leg_3(T1/P1,T/P0,Y/Z,X1).
leg_3_2(A/P,T1/P1,T/P0,Y/Z,X):- prime_2(A,Pr1),prime_2(P,Pr2),
      Pr1==1 ->
      (Pr2==1 ->
      Q is (P-1)*(A-1)/4,integer(Q),X1 is (-1)^Q*X,res_q4(P,A,R,Q9),
                                          leg_3_2(R/A,T1/P1,T/P0,Y/Z,X1);
      leg_4(A/P,T1/P1,T/P0,Y/Z,X));leg_4(A/P,T1/P1,T/P0,Y/Z,X).

leg_4(A/P,T1/P1,T/P0,Y/Z,X):- nl,write('muri desu!').


leg_Write(Y/Z,X):- nl,write('('),write(Y),write('/'),write(Z),write(') = '),write(X).




/** 商と余り **/
res_q4(A,B,R,Q):- Q is floor(A/B), R is A - B*Q.
res_q(A = B*Q + R):- Q is floor(A/B),R is A - B*Q.
```

```
/** X=(A を割り切れる最小素数),Y=（A/X の商） **/
pdp_once(A,X,Y):- Y1 is A,pdp_once1(A,2,X,Y,Y1).
pdp_once1(1,B,X,Y,Y1):- X is 1,Y is 1,!.
pdp_once1(A,B,X,Y,Y1):- Y1<B.
pdp_once1(A,B,X,Y,Y1):- Q is Y1/B,
     integer(Q) -> (X is B,Y is Q);
                   (B1 is B+1,pdp_once1(A,B1,X,Y,Y1)).



/** 最大公約数 **/
gcd(A,B):-
     ((A>B) -> (A1 is A,B1 is B); (A1 is B,B1 is A)),E is 0,
     gcd1(D,A,B,A1,B1,E).
   gcd1(D,A,B,A1,B1,E):- E>0.
   gcd1(D,A,B,A1,B1,E):-
   res_q(A1=B1*Q+R),
   ((R == 0) ->
      (D is B1,write('gcd'),write('('),write(A),write(','),
                                write(B),write(') = '),write(D),E1 is E+1);
      (B2 is floor(B1/2),E1 is E)),
   gcd1(D,A,B,A1,B2,E1).


gcd(D = (A,B)):-
     ((A>B) -> (A1 is A,B1 is B); (A1 is B,B1 is A)),E is 0,C is B1,
     gcd1(D,A,B,A1,B1,C,E).
   gcd1(D,A,B,A1,B1,C,E):- E>0.
   gcd1(D,A,B,A1,B1,C,E):-
   res_q(A1=C*Q1+R1),res_q(B1=C*Q2+R2),
   ((R1 == 0) ->
      ((R2 == 0) ->
      (D is C,E1 is E+1);
      (E1 is E,C1 is C-1));(E1 is E,C1 is C-1)),
   gcd1(D,A,B,A1,B1,C1,E1).



/** 素数判定 **/
prime(1):- P is 0,write('Sosuu Deha Nai').
prime(X):- N is X,P is 0,prime1(X,N,M,K,P).
    prime1(X,1,M,K,P):- .
```

```
    prime1(X,N,M,K,P):- N==1.
    prime1(X,N,M,K,P):- N1 is N-1,M1 is X/N1,
      (N1 == 1 ->
              (P1 is P,write('Sosuu De Aru'),prime1(X,N1,M1,K,P1));
       (integer(M1) ->
            (P1 is P+1,write('Sosuu Deha Nai'),N2 is N1-N1+1,prime1(X,N2,M1,K,P1));
   (P1 is P,prime1(X,N1,M1,K,P1)))).

prime_1(1,P):- P is 0.
prime_1(X,P):- K is 0,N is X,prime_11(X,N,M,K,P).
    prime_11(X,N,M,K,P):- N==1.
    prime_11(X,N,M,K,P):- N1 is N-1,M1 is X/N1,
      (N1 == 1 ->
              (P is K+1,prime_11(X,N1,M1,K,P));
       (integer(M1) ->
           (P is K,N2 is N1-N1+1,prime_11(X,N2,M1,K,P));
   (prime_11(X,N1,M1,K,P)))).


/** 奇素数判定 **/
prime_2(1,P):- P is 0.
prime_2(2,P):- P is 0.
prime_2(X,P):- K is 0,N is X,prime_21(X,N,M,K,P).
    prime_21(X,N,M,K,P):- N==1.
    prime_21(X,N,M,K,P):- N1 is N-1,N1>0,M1 is X/N1,
      (N1 == 1 ->
              (P is K+1,prime_21(X,N1,M1,K,P));
       (integer(M1) ->
           (P is K,N2 is N1-N1+1,prime_21(X,N2,M1,K,P));
   (prime_21(X,N1,M1,K,P)))).



/** 素数表 **/
prime(A,B):- B<A.
prime(A,B):- prime_1(A,P),
     (P == 1 -> (write(A),nl,A1 is A+1,prime(A1,B));(A1 is A+1,prime(A1,B))).


/** 素因数分解 **/

prime_dec1(1):- write('1').
prime_dec1(A):- Y is 2,B is A,X is 0,Z is 0,prime_dec1_1(A,B,X,Y,Z).
```

```
prime_dec1_1(A,B,X,Y,Z):- B = Y,(X == 0 ->
    (Z == 0 -> (write('prime'));
       write(Y));(X1 is X+1,write('^'),write(X1))).
prime_dec1_1(A,B,X,Y,Z):- res_q(B=Y*J+K),
    K == 0 ->
       (X == 0 ->
         (write(Y),X1 is X+1,Z1 is Z+1,prime_dec1_1(A,J,X1,Y,Z1));
         (X1 is X+1,Z1 is Z+1,prime_dec1_1(A,J,X1,Y,Z1)));
     (X == 0 ->
        (Y1 is Y+1,X0 is X*0,prime_dec1_1(A,B,X0,Y1,Z));
       (X == 1 ->
          (write('*'),X0 is X*0,Z1 is Z+1,prime_dec1_1(A,B,X0,Y,Z1));
          (write('^'),write(X),write('*'),X0 is X*0,Z1 is Z+1,
                                          prime_dec1_1(A,B,X0,Y,Z1)))).
```

3.2 $a^2 + 7b^2 = c$ を担当した森谷が作成したプログラム

/** $A^2 + 7B^2 = C$ について,A と C の値から B を探す。 **/

```
tomoaki(A,B,C):- X is A*A,
                 X1 is C -X,
                 X1 >  0,
                 B1 is sqrt(X1/7),
                 B is floor(B1+0.1),
                 B * B =:= X1/7.
```

/** 不等号に数字、右側の I には変数を入力。その範囲内で繰り返し。使うときは for と fail で繰り返す部分を挟む。制御述語 fail を使ってループする。**/

```
for(I =< J,I):- I=< J.
for(I =< J,K):- I=< J,
              I1 is I+1,for(I1 =< J,K).
```

/** $A^2 + 7B^2 = C$ について,C から (A,B) を探す。 **/

```
tototo(A,B,C):- C0 is floor(sqrt(C)),
                for(1=< C0,A),
                tomoaki(A,B,C).
```

/** C = $<N$ となる C で解 (A,B,C) を探す。変数 3 つ, 数字 1 つを入力。**/

```
daen(A,B,C,N):- for(3= <  N,C),tototo(A,B,C).
```

/** C = $<N$ となる C で解 (A,B,C) を探す。変数 1 つ, 数字 1 つを入力。**/

```
daen0([A,B,C],N):- daen(A,B,C,N).
```

/** C = $<N$ となる C で解 (A,B,C) を出力。変数 1 つを入力。yes を出力させる為に 2 行目がある。**/

```
daen00(N):- daen0(F,N),write(F),nl,fail.
daen00(N).
```

/** C = $<N$ となる素数 C で解 (A,B,C) を出力。**/

```
daenp(N):- daen(A,B,C,N),judgeprime(C),write(A),tab(1),write(B),tab(1),write(C),nl,fail.
daenp(N).
```

/** 上の述語に,C を 7 で割った余りの出力を追加 **/

```
daenpmod(N):- daen(A,B,C,N),judgeprime(C),res_q(C = 7*Q2 + R7),
              write(A),tab(1),write(B),tab(1),write(C),tab(1),write(R7),nl,fail.
daenpmod(N).
```

/** C = $<N$ となる合成数 C での解 (A,B,C) と C の素因数分解を出力, 但し A と B は互いに素でありCは7の倍数でない。変数１つを入力。**/

```
daennotp(N):- daen(A,B,C,N),not(judgeprime(C)),
              gcd(D=A*X1+B*Y1),
              D = 1,
              res_q(C = 7*Q2 + R),
              R =\= 0,
              write(A),tab(1),write(B),tab(1),write(C),tab(1),soinsubunkai2(C),nl,fail.
daennotp(N).
```

/** 上の述語を C=N に限定した **/

```
daennotpjust(C):- tototo(A,B,C),not(judgeprime(C)),
                  gcd(D=A*X1+B*Y1),D=1,
                  res_q(C = 7*Q2 + R),R =  \ = 0,
                  write(A),tab(1),write(B),tab(1),write(C),tab(1),soinsubunkai2(C),nl,fail.
daennotpjust(C).
```

/** $p \equiv 1, 2, 4 \bmod 7$ となる素数 p を小さい順に並べる **/

```
prime124(N):- for(2 =<  N,L),judgeprime(L),res_q(L = 7*Q+R),(R=1;R=2;R=4),
              write(L),tab(1),write(R),nl,fail.
prime124(N).
```

/**入力した数を素因数分解。指数を使わないプログラムで Prolog がシンプル。**/

```
soinsubunkai(C9):- I=2,write(C9),write(=),!,soinsubunkaihajime(C9,I,Q2,R2).
```

/** 小さい数から割っていく **/

```
soinsubunkaihajime(C9,I,Q,R):- I =<  sqrt(C9) ->  res_q(C9 = I*Q+R4),
                                                  (R4 = 0 ->  write(I),write(*),
                                                              soinsubunkaihajime(Q,I,Q1,R1);
   I2 is I+1,soinsubunkaihajime(C9,I2,Q2,R2));
                                                  write(C9),!.
```

/** A,B を入力。最大公約数 D を出力。X,Y は変数。**/

```
gcd(D=A3*X+B*Y):-  ((A3*B) =:= 0)  ->
                   (D=1);
                   ((res_q(A3=B*Q1+R),
                   (A1,B1)=(B, R),
                                   (B1=0 ->  D is A1;
                  gcd(D=A1*X1+B1*Y1),
                                    X1 is 1,!))).
```

/** program4.4(テキストの 4.1 を 使う) **/

/** A を B で割る。 **/

```
res_q(A = B*Q2 + R):- Q2 is floor(A/B), R is A - B*Q2.
```

/** P85 4.1 **/

/** 入力した数が素数なら Yes, それ以外は No。**/

```
judgeprime(0):- !,fail.
judgeprime(1):- !,fail.
judgeprime(N):- I8 is 2,hanbetu(I8,N).
```

/** 処理速度を速める。大きな数になると処理速度が大分違う。パソコンに優しい。単独では使わない。 **/

```
hanbetu(I8,C):- (C9 is sqrt(C),I8 >  C9 ->  !;
                     hayashinohurui2(I8,C),!).
```

/** 林君に教わった。素数なら残るふるい。単独では使わない。**/

```
hayashinohurui2(B8,C) :-  I3 is C/B8,
                      (integer(I3) -> !,fail;
                                   B1 is B8 + 1,hanbetu(B1,C),!).
```

/** N(入力) の中に I(入力) が J(変数) 個ある。**/

```
count_soinsu(I,N,J):- count_soinsu3(I,N,0,J).
```

/** 述語に組み込み易く上を改良。**/

```
count_soinsu3(I,N,C,C2):- res_q(N=I*Q+R),(R=0 ->  C1 is C+1,count_soinsu3(I,Q,C1,C2);
         C2 is C).
```

/** 素因数分解の改良版。複雑な Prolog だけど、指数表記となり TeX での出力は綺麗。4 未満と以上で場合分け。 **/

```
soinsubunkai2(S):- S =< 3,write(S).
soinsubunkai2(S):- soinsubunkai3(S).
soinsubunkai3(S):- soinsubunkai4(S,2).
```

/** D は割った後の出涸らし。**/

```
soinsubunkai4(S,W):- W=< sqrt(S),count_soinsu(W,S,C),  /** S の中に W がいくつあるか **/
    (C=0 ->  D is S;
                        (C=1 ->  write(W),D is S/W;
                                write(W),write(^),write(C),D is S/(W^C)),
```

```
(D=\=1 ->  write(*);!)),
  (D=1 ->  !;
 W1 is W+1,(W1=< sqrt(D)->  soinsubunkai4(D,W1);
 write(D))).
```

4　結果

4.1　m = 6 のときの自然数解（ただし、gcd(a, b) = 1 のときに限る）

c	(a, b)	c の素因数分解	c mod 24
7	(1, 1)	7	7
10	(2, 1)	2×5	10
15	(3, 1)	3×5	15
22	(4, 1)	2×11	22
25	(1, 2)	5^2	1
31	(5, 1)	31	7
33	(3, 2)	3×11	9
42	(6, 1)	$2 \times 3 \times 7$	22
49	(5, 2)	7^2	1
55	(1, 3) (7, 1)	5×11	7
58	(2, 3)	2×29	10
70	(4, 3) (8, 1)	$2 \times 5 \times 7$	22
73	(7, 2)	73	1
79	(5, 3)	79	7
87	(9, 1)	3×29	15
97	(1, 4)	97	1
103	(7, 3)	103	1
105	(3, 4) (9, 2)	$3 \times 5 \times 7$	9
106	(10, 1)	2×53	10
118	(8, 3)	2×59	22
121	(5, 4)	11^2	1
127	(11, 1)	127	7
145	(7, 4) (11, 2)	5×29	1
150	(12, 1)	$2 \times 3 \times 5^2$	6
151	(1, 5)	151	7
154	(2, 5) (10, 3)	$2 \times 7 \times 11$	10
159	(3, 5)	3×53	15
166	(4, 5)	2×83	22
175	(11, 3) (13, 1)	$5^2 \times 7$	7
177	(9, 4)	3×59	9
186	(6, 5)	$2 \times 3 \times 31$	18
193	(13, 2)	193	1
199	(7, 5)	199	7
202	(14, 1)	2×101	10
214	(8, 5)	2×107	22
217	(1, 6) (11, 4)	7×31	1
223	(13, 3)	223	7

c	(a, b)	c の素因数分解	$c \mod 24$
231	$(9, 5)$ $(15, 1)$	$3 \times 7 \times 11$	15
241	$(5, 6)$	241	1
249	$(15, 2)$	3×83	9
250	$(14, 3)$	2×5^3	10
262	$(16, 1)$	2×131	22
265	$(7, 6)$ $(13, 4)$	5×53	1
271	$(11, 5)$	271	7
294	$(12, 5)$	$2 \times 3 \times 7^2$	6
295	$(1, 7)$ $(17, 1)$	5×59	7
298	$(2, 7)$	2×149	10
303	$(3, 7)$	3×101	15
310	$(4, 7)$ $(16, 3)$	$2 \times 5 \times 31$	22
313	$(17, 2)$	313	1
319	$(5, 7)$ $(13, 5)$	11×29	7
321	$(15, 4)$	3×107	9
330	$(6, 7)$ $(18, 1)$	$2 \times 3 \times 5 \times 11$	18
337	$(11, 6)$	337	1
343	$(17, 3)$	7^3	7
346	$(14, 5)$	2×173	10
358	$(8, 7)$	2×179	22
367	$(19, 1)$	367	7
375	$(9, 7)$	3×5^3	15
385	$(1, 8)$ $(13, 6)$ $(17, 4)$ $(19, 2)$	$5 \times 7 \times 11$	1
393	$(3, 8)$	3×131	9
394	$(10, 7)$	2×197	10
406	$(16, 5)$ $(20, 1)$	$2 \times 7 \times 29$	22
409	$(5, 8)$	409	1
415	$(11, 7)$ $(19, 3)$	5×83	7
433	$(7, 8)$	433	1
438	$(12, 7)$	$2 \times 3 \times 73$	6
439	$(17, 5)$	439	7
447	$(21, 1)$	3×149	15
454	$(20, 3)$	2×227	22
457	$(19, 4)$	457	1
463	$(13, 7)$	463	7
465	$(9, 8)$ $(21, 2)$	$3 \times 5 \times 31$	9
474	$(18, 5)$	$2 \times 3 \times 79$	18
487	$(1, 9)$	487	7
490	$(2, 9)$ $(22, 1)$	$2 \times 5 \times 7^2$	10

c	(a, b)	c の素因数分解	$c \mod 24$
511	$(5, 9)$ $(19, 5)$	7×73	7
519	$(15, 7)$	3×173	15
535	$(7, 9)$ $(23, 1)$	5×107	7
537	$(21, 4)$	3×179	9
538	$(22, 3)$	2×269	10
550	$(8, 9)$ $(16, 7)$	$2 \times 5^2 \times 11$	22
553	$(13, 8)$ $(23, 2)$	7×79	1
577	$(19, 6)$	577	1
582	$(24, 1)$	$2 \times 3 \times 97$	6
583	$(17, 7)$ $(23, 3)$	11×53	7
586	$(10, 9)$	2×293	10
591	$(21, 5)$	3×197	15
601	$(1, 10)$	601	1
502	$(4, 9)$	2×251	22
505	$(11, 8)$ $(17, 6)$	5×101	1

4.2 m = 7 のときの自然数解（ただし、gcd(a, b) = 1 のときに限る）

表 1: $A^2 + 7B^2 = C$ の整数解。C は合成数。

A	B	C	C の素因数分解	A	B	C	C の素因数分解
1	1	8	2^3	1	9	568	$2^3 \times 71$
3	1	16	2^4	15	7	568	$2^3 \times 71$
5	1	32	2^5	4	9	583	11×53
1	3	64	2^6	24	1	583	11×53
5	3	88	$2^3 \times 11$	5	9	592	$2^4 \times 37$
9	1	88	$2^3 \times 11$	23	3	592	$2^4 \times 37$
3	4	121	11^2	17	7	632	$2^3 \times 79$
11	1	128	2^7	25	1	632	$2^3 \times 79$
1	5	176	$2^4 \times 11$	10	9	667	23×29
13	1	176	$2^4 \times 11$	18	7	667	23×29
3	5	184	$2^3 \times 23$	11	9	688	$2^4 \times 43$
11	3	184	$2^3 \times 23$	25	3	688	$2^4 \times 43$
13	3	232	$2^3 \times 29$	19	7	704	$2^6 \times 11$
15	1	232	$2^3 \times 29$	23	5	704	$2^6 \times 11$
1	6	253	11×23	13	9	736	$2^5 \times 23$
15	2	253	11×23	27	1	736	$2^5 \times 23$
9	5	256	2^8	17	8	737	11×67
11	5	296	$2^3 \times 37$	25	4	737	11×67
17	1	296	$2^3 \times 37$	9	10	781	11×71
12	5	319	11×29	23	6	781	11×71
16	3	319	11×29	27	4	841	29^2
1	7	344	$2^3 \times 43$	1	11	848	$2^4 \times 53$
13	5	344	$2^3 \times 43$	29	1	848	$2^4 \times 53$
3	7	352	$2^5 \times 11$	2	11	851	23×37
17	3	352	$2^5 \times 11$	26	5	851	23×37
5	7	368	$2^4 \times 23$	3	11	856	$2^3 \times 107$
19	1	368	$2^4 \times 23$	17	9	856	$2^3 \times 107$
8	7	407	11×37	13	10	869	11×79
20	1	407	11×37	29	2	869	11×79
9	7	424	$2^3 \times 53$	5	11	872	$2^3 \times 109$
19	3	424	$2^3 \times 53$	23	7	872	$2^3 \times 109$
11	7	464	$2^4 \times 29$	27	5	904	$2^3 \times 113$
17	5	464	$2^4 \times 29$	29	3	904	$2^3 \times 113$
5	8	473	11×43	9	11	928	$2^5 \times 29$
19	4	473	11×43	19	9	928	$2^5 \times 29$
13	7	512	2^9	25	7	968	$2^3 \times 11^2$
9	8	529	23^2	31	1	968	$2^3 \times 11^2$
19	5	536	$2^3 \times 67$	17	10	989	23×43
23	1	536	$2^3 \times 67$	31	2	989	23×43

表 2: 解を複数持つC

A	B	C	C の素因数分解	A	B	C	C の素因数分解
1	17	2024	$2^3 \times 11 \times 23$	27	91	58696	$2^3 \times 11 \times 23 \times 29$
29	13	2024	$2^3 \times 11 \times 23$	57	89	58696	$2^3 \times 11 \times 23 \times 29$
41	7	2024	$2^3 \times 11 \times 23$	113	81	58696	$2^3 \times 11 \times 23 \times 29$
43	5	2024	$2^3 \times 11 \times 23$	139	75	58696	$2^3 \times 11 \times 23 \times 29$
				153	71	58696	$2^3 \times 11 \times 23 \times 29$
5	19	2552	$2^3 \times 11 \times 29$	211	45	58696	$2^3 \times 11 \times 23 \times 29$
23	17	2552	$2^3 \times 11 \times 29$	237	19	58696	$2^3 \times 11 \times 23 \times 29$
37	13	2552	$2^3 \times 11 \times 29$	239	15	58696	$2^3 \times 11 \times 23 \times 29$
47	7	2552	$2^3 \times 11 \times 29$				
				137	190	271469	$11 \times 23 \times 29 \times 37$
31	21	4048	$2^4 \times 11 \times 23$	199	182	271469	$11 \times 23 \times 29 \times 37$
39	19	4048	$2^4 \times 11 \times 23$	263	170	271469	$11 \times 23 \times 29 \times 37$
45	17	4048	$2^4 \times 11 \times 23$	311	158	271469	$11 \times 23 \times 29 \times 37$
59	9	4048	$2^4 \times 11 \times 23$	361	142	271469	$11 \times 23 \times 29 \times 37$
				409	122	271469	$11 \times 23 \times 29 \times 37$
1	27	5104	$2^4 \times 11 \times 29$	487	70	271469	$11 \times 23 \times 29 \times 37$
27	25	5104	$2^4 \times 11 \times 29$	521	2	271469	$11 \times 23 \times 29 \times 37$
69	7	5104	$2^4 \times 11 \times 29$				
71	3	5104	$2^4 \times 11 \times 29$	80	1291	11673167	$11 \times 23 \times 29 \times 37 \times 43$
				388	1283	11673167	$11 \times 23 \times 29 \times 37 \times 43$
31	25	5336	$2^3 \times 23 \times 29$	508	1277	11673167	$11 \times 23 \times 29 \times 37 \times 43$
53	19	5336	$2^3 \times 23 \times 29$	760	1259	11673167	$11 \times 23 \times 29 \times 37 \times 43$
67	11	5336	$2^3 \times 23 \times 29$	1172	1213	11673167	$11 \times 23 \times 29 \times 37 \times 43$
73	1	5336	$2^3 \times 23 \times 29$	1600	1141	11673167	$11 \times 23 \times 29 \times 37 \times 43$
				2152	1003	11673167	$11 \times 23 \times 29 \times 37 \times 43$
13	32	7337	$11 \times 23 \times 29$	2432	907	11673167	$11 \times 23 \times 29 \times 37 \times 43$
43	28	7337	$11 \times 23 \times 29$	2468	893	11673167	$11 \times 23 \times 29 \times 37 \times 43$
83	8	7337	$11 \times 23 \times 29$	2768	757	11673167	$11 \times 23 \times 29 \times 37 \times 43$
85	4	7337	$11 \times 23 \times 29$	2972	637	11673167	$11 \times 23 \times 29 \times 37 \times 43$
				3112	533	11673167	$11 \times 23 \times 29 \times 37 \times 43$
5	39	10672	$2^4 \times 23 \times 29$	3140	509	11673167	$11 \times 23 \times 29 \times 37 \times 43$
33	37	10672	$2^4 \times 23 \times 29$	3160	491	11673167	$11 \times 23 \times 29 \times 37 \times 43$
93	17	10672	$2^4 \times 23 \times 29$	3308	323	11673167	$11 \times 23 \times 29 \times 37 \times 43$
103	3	10672	$2^4 \times 23 \times 29$	3412	67	11673167	$11 \times 23 \times 29 \times 37 \times 43$

5　考察 1　m = 6 の場合 ($a^2 + 6b^2 = c$)

5.1　プログラム実行結果からの予想

定義 5.1 方程式の解 (a, b, c) の c について、単独で解 c に出てくる素数を強い素数（hard prime）、単独では出ず解 c の素因子で出てくる素数を弱い素数（soft prime）と呼ぶことにする。m の値を決めると素数を

- 強い素数（hard prime）
- 弱い素数（soft prime）
- 解 c の素因子に全く登場しない素数

の 3 通りに分類することができる。

4.1 節の結果をもとに、c が素数の場合と合成数の場合とでそれぞれ予想する。

c が素数の場合

c が素数 p の場合は、$p = 7, 31, 73, 79, 97, 103, 127, 151, \cdots$ となっているので、$p \equiv 1 \mod 6$ が成り立っていると予想できる。ちなみに、mod 24 で考えると $p \equiv 1, 7 \mod 24$ となる。

また、解の個数に注目すると 1 個しか存在しないことも予想できる。

c が合成数の場合

c が合成数 t の場合は、t を素因数分解して hard prime と soft prime に分けることができる。hard prime に関しては、上記の素数の場合と事情は同じである。素因数分解で出てくる素数のうち、c に出てこない素数を soft prime と呼ぶが、soft prime を p' とすると、$p' \equiv 5, 11 \mod 24$ の関係があると予想できる。(ただし、$p' = 2, 3$ は除く)

解の個数の関係においては、t を素因数分解して（互いに異なる）素因子の数を r とする（2, 3 は素因子として勘定しない）と、（解の個数）$= 2^{r-1}$ と予想できる。

5.2　4.1 節の考察

定義 5.2 p は奇素数であるとし、a, b は整数を表すとする。

(1) $a \not\equiv 0 \pmod p$ とする。方程式

$$x^2 \equiv a \pmod p$$

をみたす整数 x が存在するとき a は（法 p に関する）**平方剰余**であるという。また、平方剰余でないとき平方非剰余という。

(2) 次の式で記号 $\left(\frac{a}{p}\right)$ を定める。

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & a \equiv 0 \pmod p \\ 1 & a \not\equiv 0 \pmod p \text{ で } a \text{ が平方剰余のとき} \\ -1 & a \not\equiv 0 \pmod p \text{ で } a \text{ が平方非剰余のとき} \end{cases}$$

この $\left(\frac{a}{p}\right)$ を**ルジャンドルの平方剰余記号**という。（**ルジャンドル記号**ともいう。）

命題 5.3　p, q を相異なる奇素数、a, b を p と互いに素な整数とすると、次が成り立つ。

(1) $\left(\frac{1}{p}\right) = 1$

(2) $\left(\frac{ap + b}{p}\right) = \left(\frac{b}{p}\right)$

(3) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

(4) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$（第 1 補充法則）

(5) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$（第 2 補充法則）

(6) $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$（平方剰余の相互法則）

命題 5.4　方程式 $a^2 + pb^2 = c^2$ の解 (a, b, c)　$(\gcd(a, b, c) = 1)$ に対して、c の素因数 q(2 を除く) は

$$\left(\frac{-p}{q}\right) = 1$$

を満たさなければならない。

5.2.1　解の存在の証明

証明すべきこと（$a^2 + 6b^2 = c$, $\gcd(a, b, c) = 1$ において）

①　c が素数 p で、$p = 1, 7 \mod 24$ のとき解が存在して、その他の素数のとき、解は存在しない
②　c の素因子 p について $\left(\frac{-6}{p}\right) = 1$ が成り立つ
③　$\left(\frac{-6}{p}\right) = 1$ なら $a^2 + 6b^2 = p$ となる a, b が存在するか、$a^2 + 6b^2 = pp'$ となる a, b, p' が存在する

証明①

(1)$p = (24m + 1)$ 型 $(m \in \mathbb{N})$ の素数の場合

ルジャンドル記号の定義より、$\left(\frac{-6}{p}\right)$, $p = (24m + 1)$ を調べる
$\left(\frac{-6}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right)$
ここで、$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{12m} = 1$

$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{576m^2+48m}{8}} = (-1)^{6(12m^2+m)} = 1$
$\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}\times\frac{3-1}{2}}\left(\frac{p}{3}\right) = (-1)^{12m}\left(\frac{24m+1}{3}\right) = 1\times\left(\frac{1}{3}\right) = 1\times 1 = 1$
より、$\left(\frac{-6}{p}\right) = 1\times 1\times 1 = 1$ となり、$p = (24m+1)$ 型 (つまり、$p = 1 \mod 24$) のとき解が存在する。

(2)$p = (24m+7)$ 型 ($m \in \mathrm{N}$) の素数の場合

(1) と同様にして、
$\left(\frac{-6}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right)$
ここで、$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{12m+3} = -1$
$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{576m^2+336m+48}{8}} = (-1)^{6(12m^2+7m+1)} = 1$
$\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}\times\frac{3-1}{2}}\left(\frac{p}{3}\right) = (-1)^{12m+3}\left(\frac{24m+7}{3}\right) = (-1)\left(\frac{1}{3}\right) = (-1)\times 1 = -1$
より、$\left(\frac{-6}{p}\right) = (-1)\times 1\times(-1) = 1$ となり、$p = (24m+7)$ 型 (つまり、$p = 7 \mod 24$) のとき解が存在する。

(3)$p = (24m+5)$ 型 ($m \in \mathrm{N}$) の素数の場合

(1)(2) と同様にして、
$\left(\frac{-6}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{2}{p}\right)\left(\frac{3}{p}\right)$
ここで、$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = (-1)^{12m+4} = 1$
$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (-1)^{\frac{576m^2+192m+15}{8}} = (-1)^{2(36m^2+12m+1)} = 1$
$\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}\times\frac{3-1}{2}}\left(\frac{p}{3}\right) = (-1)^{12m+2}\left(\frac{24m+5}{3}\right) = 1\times\left(\frac{2}{3}\right) = 1\times(-1)^{\frac{9-1}{8}} = -1$
より、$\left(\frac{-6}{p}\right) = 1\times 1\times(-1) = -1$ となり、$p = (24m+5)$ 型 (つまり、$p = 5 \mod 24$) のとき解は存在しない。
(この証明では $p = (24m+5)$ 型が単独で解 c に登場しないということが示された。$p = (24m+5)$ 型は c の素因子としては登場する)

以上のように同様の計算をすると、$p = (24m+1)$ 型 , $(24m+7)$ 型では $\left(\frac{-6}{p}\right) = 1$ となるので、p が解 c として現れるが、その他の p においては、単独で解 c に現れることはない。 (Q.E.D.)

証明②

$a^2 + 6b^2 = c$ より $a^2 + 6b^2 \equiv 0 \pmod{p} \iff a^2 \equiv -6b^2 \pmod{p}$ $\cdots$ (a) となる。
ここで、$gcd(b,p) = 1$ であるので、$1 = bb_1 + pp_1$ をみたす整数 b_1, p_1 が存在する。

よって、$1 \equiv bb_1$ (mod p)　$\cdots$ (b)　となる。
(a) の両辺に b_1^2 をかけて、$a^2b_1^2 \equiv -6b^2b_1^2$ (mod p)　となり、(b) より $a^2b_1^2 \equiv -6$ (mod p)　となる。
これは、$x^2 \equiv -6$ (mod p) をみたす整数 x が存在することを表している。
つまり、$\left(\frac{-6}{p}\right) = 1$　　(Q.E.D.)

証明③

$\mathbb{Z}[\sqrt{-6}] = \{a + b\sqrt{-6} | a, b \in \mathbb{Z}\}$　と　$\mathbb{Z}[\sqrt{-6}]$　の元 p で生成される単項イデアル (p) からなる剰余環 $\mathbb{Z}\left[\sqrt{-6}\right]/(p)$ について考える。

$$\begin{aligned} \mathbb{Z}[\sqrt{-6}]/(p) &\cong \mathbb{Z}[X]/(X^2 + 6, p) \\ &\cong \mathbb{F}_p[X]/(X^2 + 6) \end{aligned}$$

より、$\mathbb{F}_p[X]/(X^2 + 6)$ について考える。
$\mathbb{F}_p[X]/(X^2 + 6)$ は整域ではないので $\mathbb{Z}[\sqrt{-6}]/(p)$ も整域ではない。
つまり、(p) は素イデアルではない。よって、(p) は $\mathbb{Z}[\sqrt{-6}]$ 上で必ず分解する。
その分解を、$(p) = J_{\mathfrak{p}_1}J_{\mathfrak{p}_2}$ ($J_{\mathfrak{p}_1}J_{\mathfrak{p}_2}$ は素イデアル)　とすると $J_{\mathfrak{p}_2} = \overline{J_{\mathfrak{p}_1}}$ となる。
ここで、$J_{\mathfrak{p}_1}$ が単項イデアルの場合と、非単項イデアルの場合とで場合分けをする。
簡単のため、これからは $J_{\mathfrak{p}_1}$ を $J_{\mathfrak{p}}$ と書くことにする。

(1) $J_{\mathfrak{p}}$ が単項イデアルの場合
$J_{\mathfrak{p}} = (\alpha)$, $\alpha = a + b\sqrt{-6}$ と書けるので、
$(p) = (\alpha)(\overline{\alpha}) = (N(\alpha))$　($N(\alpha)$ は α のノルム)　となる。
つまり、$p = N(\alpha) = a^2 + 6b^2$ となり、p に対して a と b が定まる。

(2) $J_{\mathfrak{p}}$ が非単項イデアルの場合
$(p) = J_{\mathfrak{p}}\overline{J_{\mathfrak{p}}}$, $(p') = J'_{\mathfrak{p}}\overline{J'_{\mathfrak{p}}}$　(p' に対する素イデアルを $J'_{\mathfrak{p}}$ とかくことにする)
となるような、(p') を用意する。　($J'_{\mathfrak{p}}$ も非単項イデアル)
$(pp') = J_{\mathfrak{p}}\overline{J_{\mathfrak{p}}}J'_{\mathfrak{p}}\overline{J'_{\mathfrak{p}}}$
このとき、$J_{\mathfrak{p}}J'_{\mathfrak{p}}$ は単項イデアルであるので、$J_{\mathfrak{p}}J'_{\mathfrak{p}} = (\beta)$, $(\beta = a' + b'\sqrt{-6})$ と書ける。
したがって、$(pp') = (N(\beta))$ となるので、
$pp' = a'^2 + 6b'^2$ となり、pp' に対して a' と b' が定まる。

以上より、$\left(\frac{-6}{p}\right) = 1$ なら $a^2 + 6b^2 = p$ となる解が存在するか、$a^2 + 6b^2 = pp'$ となる p' が存在する　　(Q.E.D.)

ここで、(1) と (2) にあたる例を紹介する。

(1) の例

$$
\begin{aligned}
J_{151} &= (1 + 5\sqrt{-6}) \\
\overline{J_{151}} &= (1 - 5\sqrt{-6}) \\
(151) &= (1 + 5\sqrt{-6})(1 - 5\sqrt{-6}) = (N(1 + 5\sqrt{-6})) \\
151 &= N(1 + 5\sqrt{-6}) = 1^2 + 6 \cdot 5^2
\end{aligned}
$$

(2) の例

$$
\begin{aligned}
J_5 &= (2 + \sqrt{-6}, 1 - 2\sqrt{-6}) \\
J_{11} &= (3 + 2\sqrt{-6}, 5 - 4\sqrt{-6}) \\
J_5\overline{J_5} &= (5) \\
J_{11}\overline{J_{11}} &= (11) \\
(55) &= (5)(11) = J_5\overline{J_5}J_{11}\overline{J_{11}} = J_5J_{11}\overline{J_5J_{11}} = J_5\overline{J_{11}J_5}J_{11} \\
J_5J_{11}\overline{J_5J_{11}} &= (J_5J_{11})(\overline{J_5J_{11}}) = (1^2 + 6 \cdot 3^2) \\
J_5\overline{J_{11}J_5}J_{11} &= (J_5\overline{J_{11}})(\overline{J_5}J_{11}) = (7^2 + 6 \cdot 1^2) \\
55 &= 1^2 + 6 \cdot 3^2 \\
&= 7^2 + 6 \cdot 1^2
\end{aligned}
$$

5.2.2 解の個数の関係

5.2.1 節を踏まえて、c の素因子と解 a, b の個数の関係を考える。
このとき、$\mathbb{Z}[\sqrt{-6}]$ において、

- 単項イデアル $\times$ 非単項イデアル = 非単項イデアル
- 非単項イデアル $\times$ 非単項イデアル = 単項イデアル
- 素イデアル分解の一意性が成り立つ (ただし、積の順序は除く)

は、事実として扱う。

まず、$a^2 + 6b^2 = c$ ($\gcd(a, b) = 1$) が成り立つ一番小さな素数 $p = 7$ について考える。
$J_7 = (1 + \sqrt{-6})$, $\alpha = 1 + \sqrt{-6}$ とすると、$(7) = J_7\overline{J_7} = (N(\alpha))$ から
$7 = N(\alpha) = 1^2 + 6 \cdot 1^2$ となり、一つの解が出てくる。
同様に、$J_{31} = (5 + \sqrt{-6})$, $\beta = 5 + \sqrt{-6}$ とすると、$(31) = J_{31}\overline{J_{31}} = (N(\beta))$ から
$31 = N(\beta) = 5^2 + 6 \cdot 1^2$ となり、やはり一つの解が出てくる。

このことから、$(p) = J_\mathfrak{p}\overline{J_\mathfrak{p}}$ と素イデアル分解した $J_\mathfrak{p}$ が単項イデアルの場合には $c = p$ の解が一つ出てくることが分かる。

次に、イデアル (7) と (31) をかけて (217) を考える。
$(J_7, \overline{J_7}, J_{31}, \overline{J_{31}}$ はすべて単項イデアル)
このときは、$(217) = (7)(31) = (J_7\overline{J_7})(J_{31}\overline{J_{31}}) = J_7\overline{J_7}J_{31}\overline{J_{31}}$ となるが、
$J_7\overline{J_7}J_{31}\overline{J_{31}} = J_7J_{31}\overline{J_7J_{31}} = (J_7J_{31})(\overline{J_7J_{31}})$
$= J_7\overline{J_{31}J_7}J_{31} = (J_7\overline{J_{31}})(\overline{J_7}J_{31})$
の 2 通りを考えることができ、それぞれ
$(J_7J_{31})(\overline{J_7J_{31}}) = (-1 + 6\sqrt{-6})(-1 - 6\sqrt{-6}) = (1^2 + 6 \cdot 6^2)$
$(J_7\overline{J_{31}})(\overline{J_7}J_{31}) = (11 + 4\sqrt{-6})(11 - 4\sqrt{-6}) = (11^2 + 6 \cdot 4^2)$
と変形できる。すなわち、
$217 = 1^2 + 6 \cdot 6^2 = 11^2 + 6 \cdot 4^2$ の 2 通りの解が出てくることが分かった。

さらに、イデアル (7) と (31) と (73) をかけて (15841) を考える。
$(J_7, \overline{J_7}, J_{31}, \overline{J_{31}}, J_{73}, \overline{J_{73}}$ はすべて単項イデアル)
$J_{73} = (7 + 2\sqrt{-6})$ とすると、
$(15841) = (7)(31)(73) = (J_7\overline{J_7})(J_{31}\overline{J_{31}})(J_{73}\overline{J_{73}}) = J_7\overline{J_7}J_{31}\overline{J_{31}}J_{73}\overline{J_{73}}$ より
$J_7\overline{J_7}J_{31}\overline{J_{31}}J_{73}\overline{J_{73}} = (J_7J_{31}J_{73})(\overline{J_7J_{31}J_{73}}) = (-79 + 40\sqrt{-6})(-79 - 40\sqrt{-6}) = (79^2 + 6 \cdot 40^2)$
$= (J_7J_{31}\overline{J_{73}})(\overline{J_7J_{31}}J_{73}) = (65 + 44\sqrt{-6})(65 - 44\sqrt{-6}) = (65^2 + 6 \cdot 44^2)$
$= (J_7\overline{J_{31}J_{73}})(\overline{J_7}J_{31}J_{73}) = (125 + 6\sqrt{-6})(125 - 6\sqrt{-6}) = (125^2 + 6 \cdot 6^2)$
$= (J_7\overline{J_{31}J_{73}})(\overline{J_7}J_{31}\overline{J_{73}}) = (29 + 50\sqrt{-6})(29 - 50\sqrt{-6}) = (29^2 + 6 \cdot 50^2)$
となり、$c = 15841$ のときは 4 通りの解が存在する。

以上より、単項イデアル $J_\mathfrak{p}, \overline{J_\mathfrak{p}}$ から生成されるイデアル (p) どうしをかけた場合は、かけた回数を r として (解の個数) $= 2^{r-1}$ が成り立つ。

次は、$a^2 + 6b^2 = c$ $(gcd(a, b) = 1)$ が成り立つ合成数 $c = 55$ について考える。
$(55 = 5 \times 11$ で、$J_5 = (2 + \sqrt{-6}, 1 - 2\sqrt{-6})$, $J_{11} = (3 + 2\sqrt{-6}, 5 - 4\sqrt{-6})$ は非単項イデアル)
$(55) = (5)(11) = J_5\overline{J_5}J_{11}\overline{J_{11}}$ が成り立つ。これの積の順序を変えて、
$= (J_5J_{11})(\overline{J_5J_{11}}) = (J_5\overline{J_{11}})(\overline{J_5}J_{11})$ について、それぞれ考える。
$(J_5J_{11})(\overline{J_5J_{11}})$ について
$J_5J_{11} = (2 + \sqrt{-6}, 1 - 2\sqrt{-6})(3 + 2\sqrt{-6}, 5 - 4\sqrt{-6})$
$= (-6 + 7\sqrt{-6}, 34 - 3\sqrt{-6}, 27 - 4\sqrt{-6}, -43 - 14\sqrt{-6})$
$= (7 + \sqrt{-6})(-\sqrt{-6}, 4 - \sqrt{-6}, 3 - \sqrt{-6}, -7 - \sqrt{-6})$
ここで、$1 \in (-\sqrt{-6}, 4 - \sqrt{-6}, 3 - \sqrt{-6}, -7 - \sqrt{-6})$ なので、
$J_5J_{11} = (7 + \sqrt{-6})$ となる。よって、$\overline{J_5J_{11}} = (7 - \sqrt{-6})$ となるので、
$(J_5J_{11})(\overline{J_5J_{11}}) = (7 + \sqrt{-6})(7 - \sqrt{-6}) = (7^2 + 6 \cdot 1^2)$ から、$55 = 7^2 + 6 \cdot 1^2$ がいえる。
$(J_5\overline{J_{11}})(\overline{J_5}J_{11})$ においても同様にして、
$J_5\overline{J_{11}} = (1 + 3\sqrt{-6})$, $\overline{J_5}J_{11} = (1 - 3\sqrt{-6})$ がいえるので、
$(J_5\overline{J_{11}})(\overline{J_5}J_{11}) = (1 + 3\sqrt{-6})(1 + 3\sqrt{-6}) = (1^2 + 6 \cdot 3^2)$ となり、$55 = 1^2 + 6 \cdot 3^2$ がいえる。

同様にして、合成数 $c = 1537$ についても考えることができる。

つまり、1537 = 29 × 53 より、(29) = $J_{29}\overline{J_{29}}$, (53) = $J_{53}\overline{J_{53}}$ なる非単項イデアル J_{29} , J_{53} が存在して、
(1537) = (29)(53) = $J_{29}\overline{J_{29}}J_{53}\overline{J_{53}}$
= $(J_{29}J_{53})(\overline{J_{29}J_{53}})$ = $(J_{29}\overline{J_{53}})(\overline{J_{29}}J_{53})$
のそれぞれの積を考えることができる。
したがって、(1537) = $(1^2 + 6\cdot 16^2)$ = $(19^2 + 6\cdot 14^2)$ より、
1537 = $1^2 + 6\cdot 16^=19^2 + 6\cdot 14^2$ の 2 通りの解を得ることができる。

c = 55, 1537 の結果より、2 つの soft prime の積で 2 つの解がでることがわかる。
（偶数個 (r 個) の soft prime の積の場合、(解の個数) = 2^{r-1} 個となる。soft prime が奇数個の場合、解は存在しない。）

その次に、$a^2 + 6b^2 = c$ ($gcd(a,b) = 1$) が成り立つ一番小さな合成数 c = 10 について考える。
$J_2 = (2, \sqrt{-6})$, $J_5 = (2 + \sqrt{-6}, 1 - 2\sqrt{-6})$ とすると、(2) = $J_2\overline{J_2}$, (5) = $J_5\overline{J_5}$ となるので
(10) = (2)(5) = $J_2\overline{J_2}J_5\overline{J_5}$ が成り立つ。これの積の順序を変えて、
= $(J_2J_5)(\overline{J_2J_5})$ = $(J_2\overline{J_5})(\overline{J_2}J_5)$ について、それぞれ考える。
$(J_2J_5)(\overline{J_2J_5})$ について
$J_2J_5 = (2, \sqrt{-6})(2 + \sqrt{-6}, 1 - 2\sqrt{-6}) = (4 + 2\sqrt{-6}, 2 - 4\sqrt{-6}, -6 + 2\sqrt{-6}, 12 + \sqrt{-6})$
$= (2 + \sqrt{-6})(2, -2 - \sqrt{-6}, \sqrt{-6}, 3 - \sqrt{-6})$
ここで、$1 \in (2, -2 - \sqrt{-6}, \sqrt{-6}, 3 - \sqrt{-6})$ なので、
$J_2J_5 = (2 + \sqrt{-6})$ となる。よって、$\overline{J_2J_5} = (2 - \sqrt{-6})$ となるので、
$(J_2J_5)(\overline{J_2J_5}) = (2 + \sqrt{-6})(2 - \sqrt{-6}) = (2^2 + 6\cdot 1^2)$ から、$10 = 2^2 + 6\cdot 1^2$ がいえる。
$(J_2\overline{J_5})(\overline{J_2}J_5)$ においても同様にして、
$J_2\overline{J_5} = (2 - \sqrt{-6})$, $\overline{J_2}J_5 = (2 + \sqrt{-6})$ がいえるので、
$(J_2\overline{J_5})(\overline{J_2}J_5) = (2 - \sqrt{-6})(2 + \sqrt{-6}) = (2^2 + 6\cdot 1^2)$ となり、$10 = 2^2 + 6\cdot 1^2$ がいえる。
この結果をみると、違うイデアルの積の組み合わせで同じ式が導かれている。
これは、$J_2 = (2, \sqrt{-6})$ つまり $\overline{J_2} = (2, \sqrt{-6})$ であり、$J_2 = \overline{J_2}$ が成り立っているからである。

c = 10 のときをふまえて、c = 15 のときも同様に考えることができる。
つまり、$J_3 = (3, \sqrt{-6})$ より $J_3 = \overline{J_3}$ がいえるので、解は $15 = 3^2 + 6\cdot 1^2$ の 1 通りである。

これらの結果をふまえると、soft prime のうち p = 2, 3 のときはその他の soft prime のときとは事情が違っていそうである。もう少し、p = 2, 3 について調べてみる。

それでは、15 = (3 × 5) にさらに 2 と 11 をかけて c = 330 を考えてみる。
(330) = (2)(3)(5)(11) = $(J_2J_2)(J_3J_3)(J_5\overline{J_5})(J_{11}\overline{J_{11}})$ より、
$(J_2J_3J_5J_{11})(J_2J_3\overline{J_5J_{11}})$ と $(J_2J_3J_5\overline{J_{11}})(J_2J_3\overline{J_5}J_{11})$ について調べる。
$(J_2J_3J_5J_{11})(J_2J_3\overline{J_5J_{11}})$ については $(J_2J_3J_5J_{11}) = (6 + 7\sqrt{-6})$ より $330 = 6^2 + 6\cdot 7^2$ となり、
$(J_2J_3J_5\overline{J_{11}})(J_2J_3\overline{J_5}J_{11})$ については $(J_2J_3J_5\overline{J_{11}}) = (18 - \sqrt{-6})$ より $330 = 18^2 + 6\cdot 1^2$ となる。
c = 330 = (2 × 3 × 5 × 11) のときの解は 2 つである。

次に、c = 70 = (2 × 5 × 7) を考える。
(70) = (2)(5)(7) = $J_2\overline{J_2}J_5\overline{J_5}J_7\overline{J_7}$ より、

$(J_2J_5J_7)(J_2\overline{J_5J_7})$ と $(J_2J_5\overline{J_7})(J_2\overline{J_5}J_7)$ について調べる。
$(J_2J_5J_7)(J_2\overline{J_5J_7})$ については $(J_2J_5J_7) = (-4 + 3\sqrt{-6})$ より $70 = 4^2 + 6 \cdot 3^2$ となり、
$(J_2J_5\overline{J_7})(J_2\overline{J_5}J_7)$ については $(J_2J_5\overline{J_7}) = (8 - \sqrt{-6})$ より $70 = 8^2 + 6 \cdot 1^2$ となる。
$c = 70 = (2 \times 5 \times 7)$ のときの解は 2 つである。

以上より、c の素因子中の 2,3 においては、解の個数に影響がないことがわかる。

これらのことをまとめると、c の値を素因数分解して $c = p_1^{e_1}p_2^{e_2}\cdots p_r^{e_r}$ としたとき、$p_t^{e_t}$ $(1 \leqq t \leqq r)$ の個数 (つまり r) が解の個数に関係あり、その関係は (解の個数) $= 2^{r-1}$ となる。また、soft prime は常に偶数個存在する。ただし、2,3 は $p_t^{e_t}$ の個数として勘定しない。(つまり、解の個数に影響しない。)

今までの考察をふまえて、例えば $c = 66990 = 2 \times 3 \times 5 \times 7 \times 11 \times 29$ は解の個数に影響をあたえる素因子の数が 4 つで、そのうち soft prime の数が 3 つなので解は存在しないが、これに 53 をかけて $c = 3550470$ とすると解の個数に影響をあたえる素因子の数が 5 つで、そのうち soft prime の数が 4 つとなるので解が $2^{5-1} = 16$ 個出現する。

参考） $c = 3550470$ のときのプログラムの実行結果

```
 ?- abc(3550470,3550470,6,0).

c       (a,b)   c の素因数分解    |    c mod 6 c mod 24


3550470
       (48,769)  (144,767)  (408,751)  (828,691)  (972,659)  (996,653)
       (1212,589)  (1284,563)  (1368,529)  (1608,401)  (1656,367)  (1776,257)
       (1812,211)  (1824,193)  (1836,173)  (1884,13)
                                        2*3*5*7*11*29*53    |    0       6

Yes
```

6　考察 2　m = 7 の場合 ($a^2 + 7b^2 = c$)

6.1　C の分類

6.1.1　① C が素数 P のとき

表 3: $A^2 + 7B^2 = C$ の自然数解。C が素数のとき。

A	B	C	C mod 7	A	B	C	C mod 7	A	B	C	C mod 7
2	1	11	4	17	2	317	2	23	4	641	4
4	1	23	2	18	1	331	2	25	2	653	2
1	2	29	1	15	4	337	1	22	5	659	1
3	2	37	2	2	7	347	4	15	8	673	1
6	1	43	1	4	7	359	2	26	1	683	4
5	2	53	4	11	6	373	2	1	10	701	1
2	3	67	4	6	7	379	1	3	10	709	2
8	1	71	1	19	2	389	4	26	3	739	4
4	3	79	2	17	4	401	2	20	7	743	1
10	1	107	2	13	6	421	1	24	5	751	2
9	2	109	4	16	5	431	4	27	2	757	1
1	4	113	1	10	7	443	2	19	8	809	4
8	3	127	1	1	8	449	1	11	10	821	2
5	4	137	4	3	8	457	2	16	9	823	4
11	2	149	2	20	3	463	1	22	7	827	1
12	1	151	4	12	7	487	4	4	11	863	2
10	3	163	2	22	1	491	1	25	6	877	2
2	5	179	4	18	5	499	2	6	11	883	1
4	5	191	2	17	6	541	2	30	1	907	4
9	4	193	4	22	3	547	1	8	11	911	1
13	2	197	1	23	2	557	4	24	7	919	2
6	5	211	1	11	8	569	2	10	11	947	2
11	4	233	2	2	9	571	4	29	4	953	1
8	5	239	1	16	7	599	4	20	9	967	1
16	1	263	4	19	6	613	4	23	8	977	4
5	6	277	4	13	8	617	1	12	11	991	4
13	4	281	1	8	9	631	1				

表 4: 7 を法として 1,2,4 と合同な素数 P 。

P	P mod 7	P	P mod 7	P	P mod 7
2	2	281	1	631	1
11	4	317	2	641	4
23	2	331	2	653	2
29	1	337	1	659	1
37	2	347	4	673	1
43	1	359	2	683	4
53	4	373	2	701	1
67	4	379	1	709	2
71	1	389	4	739	4
79	2	401	2	743	1
107	2	421	1	751	2
109	4	431	4	757	1
113	1	443	2	809	4
127	1	449	1	821	2
137	4	457	2	823	4
149	2	463	1	827	1
151	4	487	4	863	2
163	2	491	1	877	2
179	4	499	2	883	1
191	2	541	2	907	4
193	4	547	1	911	1
197	1	557	4	919	2
211	1	569	2	947	2
233	2	571	4	953	1
239	1	599	4	967	1
263	4	613	4	977	4
277	4	617	1	991	4

上記２つの表の C と P が同じになる。
このことから，
$P \equiv 1, 2, 4 \bmod 7$
のとき，必ず一つだけの解をもつことが推測できる。
この P を hard prime と呼ぶ。

6.1.2 $X^2 + 7Y^2 = Z$ を満たす素数 Z は必ず $Z \equiv 1, 2, 4 \bmod 7$ となることの証明

ルジャンドル記号で考える。
$X^2 + 7Y^2 = Z$ で Z の素因数を P とする。$\gcd(X, Y, Z) = 1$ だから $X^2 + 7Y^2 \equiv 0 \pmod{p}$ … ①
Y と P は互いに素だから，$1 = Y \cdot K + P \cdot N$ となる $K, N \in$ 整数 がある。
① $\times K^2$は $(XK)^2 + 7(YK)^2 \equiv 0$
$1 \equiv YK$ より．これを代入し $(X_1)^2 + 7 \equiv 0 \Leftrightarrow (X_1)^2 \equiv -7$
従って，$\left(\frac{-7}{p}\right) = 1$
次に，$\left(\frac{-7}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{7}{p}\right)$
$= (-1)^{\frac{p-1}{2}} \cdot (-1)^{3\frac{p-1}{2}} \left(\frac{p}{7}\right) = (-1)^{\frac{p-1}{2}\cdot 4} \left(\frac{p}{7}\right) = \left(\frac{p}{7}\right) = 1$

$$\left(\begin{array}{l} \text{なぜなら} \\ \cdot \left(\frac{7}{p}\right) = \left(\frac{p}{7}\right)(-1)^{\frac{7-1}{2}\cdot\frac{p-1}{2}} \\ \cdot p \neq 7 \\ \cdot \left(\frac{p}{7}\right) = 1 \Leftrightarrow x^2 \equiv p \pmod{7} \text{が解を持つ} \Leftrightarrow x \equiv 1, 2, 3 \Leftrightarrow x^2 \equiv 1, 4, 2 \end{array}\right)$$

従って，$p \equiv 1, 2, 4$
$(Q.E.D)$

6.1.3 $Z \equiv 1, 2, 4 \bmod 7$ を満たす 2 と 7 とは異なる素数 P は C = P として解が 1 つあることの証明。

証明)

$R_0 = \mathrm{Z}\left[\sqrt{-7}\right] \subset R = \mathrm{Z}[\omega]$
ここで，$\omega = \frac{-1+\sqrt{-7}}{2} \Leftrightarrow 2\omega = -1 + \sqrt{-7} \Leftrightarrow 2\omega + 1 = \sqrt{-7} \Leftrightarrow 4\omega^2 + 4\omega + 1 = -7$
$\Leftrightarrow 4\omega^2 + 4\omega + 8 = 0 \Leftrightarrow \omega^2 + \omega + 2 = 0$　解と係数の関係から $\omega + \bar{\omega} = -1,\ \omega\bar{\omega} = 2$
また, 定理より,R では素因数分解の一意性が成り立ち,R_0 では素因数分解の一意性が成り立たない。また, 次が成り立つ。
1.R では既約元は素元になる。
2.P を奇素数とすると，$PR_0 = PR \cap R_0$
◯$PR_0 = PR \cap R_0$ の証明
・$R_0 \subset R$ から $PR_0 \subset PR$
$PR_0 \cap R_0 \subset PR \cap R_0$
$PR_0 \subset PR \cap R_0$
・$PR \cap R_0 \ni X = P(A + B\omega) = C + D\sqrt{-7} \cdots *$
$P\left(A + B\frac{-1+\sqrt{-7}}{2}\right) = C + D\sqrt{-7}$

$$2PA - PB + PB\sqrt{-7} = 2C + 2D\sqrt{-7}$$
$$2PA - PB - 2C + (PB - 2D)\sqrt{-7} = 0$$
$$\begin{pmatrix} 2PA - 2C - PB = 0 \\ PB - 2D = 0 \ \cdots \star \end{pmatrix} \star \Leftrightarrow PB = 2D$$
P:odd より B は even

$R_0 \subset R$
$R_0/(R_0 \cap PR) \subset R/PR$
$R_0/PR_0 \subset R/PR$
$PR_0 = (P)$
$PR = (P)$
$R_0/PR_0 = (Z)[\sqrt{-7}]/(P) \subset (Z)[\omega]/(P)$
$$\begin{pmatrix} \text{なぜなら } A \subset B \supset J \\ (A/(A \cap J) \subseteq B/J)) \\ A \ni \alpha \text{かつ} \alpha \ni J \text{ なら} \alpha \ni A \cap J \\ \text{ここで } (P) \text{ は } P \text{ から生成されるイデアル} \end{pmatrix}$$
$Z[\sqrt{-7}]/(P) \cong F_P[X]/\left(X^2 + 7\right)$
$X^2 + 7$ に解があるから整域ではない。つまり $\alpha\beta = 0\,(\alpha, \beta \neq 0)$ となる α, β がある。
$Z[\omega]/(P)$ は整域ではない。$*$ より P は可約元。
だから $P = (x + y\omega)(x + y\bar{\omega})$
$$= x^2 + \left(\omega + \bar{\omega}xy + \omega\bar{\omega}y^2\right)$$
$$= x^2 - xy + 2y^2$$
$$P = x^2 - xy + 2y^2$$
$y : even$ を証明。$y : odd$ を仮定すると
$$P \equiv 1 \equiv x^2 - xy \mod 2$$
$$xy \equiv x^2 - xy \text{ P:odd}$$
$$x \equiv x^2 - 1 \text{ 矛盾}$$
$y : even$ である。

$$P = N(x + 2y'\omega)$$
$$= N\left(x + \left(-1 + \sqrt{-7}y'\right)\right)$$
$$= N\left(x - y' + y'\sqrt{-7}\right)$$
$$= \left(x - y' + y'\sqrt{-7}\right)\left(x - y' - y'\sqrt{-7}\right)$$
$$= (x - y')^2 + 7(y')^2$$
$(Q.E.D)$

6.2 ② C が合成数 t のとき

t を素因数分解してその素因数のうち hard prime にならない素因数を soft prime と呼ぶ。soft prime を P' とするとこの場合，$P' = 2$ である。

6.3 hard prime の例

$2^2 + 7 \cdot 1^2 = 11$
$4^2 + 7 \cdot 1^2 = 23$
$1^2 + 7 \cdot 2^2 = 29$

6.4 C が合成数の例

$1^2 + 7 \cdot 1^2 = 8 = 2^3$
$3^2 + 7 \cdot 1^2 = 16 = 2^4$
$5^2 + 7 \cdot 1^2 = 32 = 2^5$
2^r は $r \geq 3$ となる

$\cdot C$ の素因数に hard prime があるとき。
$5^2 + 7 \cdot 3^2 = 88 = 2^3 \cdot 11$
$9^2 + 7 \cdot 1^2 = 88 = 2^3 \cdot 11$
$3^2 + 7 \cdot 4^2 = 121 = 11^2$
$\vdots$
$1^2 + 7 \cdot 5^2 = 176 = 2^4 \cdot 11$
$13^2 + 7 \cdot 1^2 = 176 = 2^4 \cdot 11$
$1^2 + 7 \cdot 6^2 = 253 = 11 \cdot 23$
$15^2 + 7 \cdot 2^2 = 253 = 11 \cdot 23$
この結果から $2^r (r \geq 3)$ は hard prime もどき、といえそうである。

6.5 hard prime 11 と 23 を考える。

$11 = 2^2 + 7 \cdot 1^2 = (2 + \sqrt{-7})(2 - \sqrt{-7})$
$23 = 4^2 + 7 \cdot 1^2 = (4 + \sqrt{-7})(4 - \sqrt{-7})$
従って
$11 \cdot 23 = (2 + \sqrt{-7})(2 - \sqrt{-7})(4 + \sqrt{-7})(4 - \sqrt{-7})$
$= (1 + 6\sqrt{-7})(1 - 6\sqrt{-7})$
$= 1 + 7 \cdot 6^2$
$11 \cdot 23 = (2 + \sqrt{-7})(4 - \sqrt{-7})(2 - \sqrt{-7})(4 + \sqrt{-7})$
$= (15 + 2\sqrt{-7})(15 - 2\sqrt{-7})$
$= 15^2 + 7 \cdot 2^2$

6.6　2^3 と 11 を考える。

$2^3 = 8 = 1^2 + 7 \cdot 1^2$
$= (1 + \sqrt{-7})(1 - \sqrt{-7})$
$11 = (2 + \sqrt{-7})(2 - \sqrt{-7})$
⋮
同様

6.7　表から考えられる一つの結論

$A^2 + 7B^2 = C$(gcd(A,B)=1,C は 7 の倍数でない) を満たす自然数解で、1 つの C に対し解が複数あるときがある。C の素因数に素数が L 個含まれるとき (但し 2 は個数から除いて、hard prime もどきである $2^r (r \geq 3)$ は 1 つとして数える。)、解は 2^{L-1} 個ある。

7　感想

卒業研究はいくつか予想で終わってしまったものもあり、また森谷君との連携がほとんどなく $m = 6$ と $m = 7$ がそれぞれ別々なものとなってしまったことが心残りです。ただ、Prolog を使いプログラムを 1 から作り上げ、そのプログラムの計算結果から予想し証明した一連の過程はこれからの人生で必ず役に立つと確信しています。飯高先生には理解の遅い私に対して丁寧に指導してくださり、感謝の念であふれています。本当にありがとうございました。（林　幸昌）

林さんの証明を読んで，その緻密さと比較してしまい，私は数式で人を納得させるよりもプログラムを書いて作品を作ったり，プログラムで答えを出したりする方が向いていると感じた。数学の証明より、問題を解く方が向いているのかなと。今までの人生の結果がこうなのだから仕方がないが、これからは証明で人を納得させることを磨いていきたい。少しずつだけれど一生かけて磨いていこうと思う。私の Prolog プログラムは頭悪いと後悔し続けています。Pascal の癖が抜けないで if 文を多様してしまいます。もっと数学的に考えられてシンプルなプログラムを作れるようにしたいです。その為にも、一度にプログラムを書こうとするのではなく、一つ変更したらコンパイル、という癖を付けなければ、と思います。プログラムを思いつくままに付け足すのではなく、よりシンプルで洗練されるようプログラムを煮詰める作業が必要かと思いました。やっぱり数学科なのだからシンプルで綺麗なものを作りあげたいです。Prolog は if 文をあまり使わないでいいことが一昨昨日になって理解出来ました。述語を 2 個定義して、条件文を適当に付ければ if と同じ分岐が出来るのですね。

パートナーは林君で本当に良かったと思う。私の数学の説明のてきとうさにイライラせず、私のゼミでの親睦会企画に一言も文句を言わないその心の広さに改めてお礼を言いたい。林君のおかげで一年間自由に楽しく過ごせました。本当にありがとうございます。林君以外のパートナーは考えられないです。一緒に組んでいると安心感があります。

だらだらと書きましたが，改めて。数学科の皆様，ゼミのみんな，林君，そして飯高先生，本当に今までありがとうございました。みんながいるから自分がいる，と思います。卒業してもゼミでの思い出を胸に秘め，頑張って生きていこうと思います。皆様お元気で。(森谷　智明)

参考文献

[1] 山田奈央『ある双曲線と楕円の整数点の存在について』（2001 年度 飯高ゼミ 卒論）

[2] 中平健 服部真宏『$a^2 + pb^2 = c$ の自然数解の研究』（2004 年度 飯高ゼミ 卒論）

[3] 中島匠一 共立講座 21 世紀の数学『代数と数論の基礎』（共立出版 2000 年）

[4] 飯高茂『コンピュータを用いた数学的活動』（数学教育の会 数学教育研究 番外編 2002 年）

[5] 飯高茂 共立講座 21 世紀の数学『平面曲線の幾何』（共立出版 2001 年）

8 付録

表 5: $a^2 + 6b^2 = c$ のときの素数の分類

素数	c の値として存在するか	c の素因子として存在するか	素数の分類	c mod 24
2	no	yes	soft prime	2
3	no	yes	soft prime	3
5	no	yes	soft prime	5
7	yes	yes	hard prime	7
11	no	yes	soft prime	11
13	no	no		13
17	no	no		17
19	no	no		19
23	no	no		23
29	no	yes	soft prime	5
31	yes	yes	hard prime	7
37	no	no		13
41	no	no		17
43	no	no		19
47	no	no		23
53	no	yes	soft prime	5
59	no	yes	soft prime	11
61	no	no		13
67	no	no		19
71	no	no		23
73	yes	yes	hard prime	1
79	yes	yes	hard prime	7
83	no	yes	soft prime	11
89	no	no		17
97	yes	yes	hard prime	1
101	no	yes	soft prime	5
103	yes	yes	hard prime	7
107	no	yes	soft prime	11
109	no	no		13
113	no	no		17
127	yes	yes	hard prime	7
131	no	yes	soft prime	11
137	no	no		17
139	no	no		19
149	no	yes	soft prime	5

素数	c の値として存在するか	c の素因子として存在するか	素数の分類	c mod 24
151	yes	yes	hard prime	7
157	no	no		13
163	no	no		19
167	no	no		23
173	no	yes	soft prime	5
179	no	yes	soft prime	11
181	no	no		13
191	no	no		23
193	yes	yes	hard prime	1
197	no	yes	soft prime	5
199	yes	yes	hard prime	7