方程式 $Z = X^2 + pY^2$ の解について

田中 誉久
学習院大学理学部数学科

平成 25 年 2 月 1 日

目 次

1 目的 **2**

2 方法 **3**
2.1 方法 3
2.2 プログラム 3

3 結果 **8**
3.1 わかったこと 8
3.2 $X^2 + 2Y^2$ の表 9
3.3 $X^2 + 3Y^2$ の表 15
3.4 $X^2 + 5Y^2$ の表 21
3.5 $X^2 + 6Y^2$ の表 26
3.6 $X^2 + 7Y^2$ の表 31
3.7 Z の異なる素因数の個数と方程式 $Z = X^2 + pY^2$ の解の個数の関係 36
3.7.1 $Z = X^2 + 2Y^2$ の場合 36
3.7.2 $Z = X^2 + 3Y^2$ の場合 38
3.7.3 $Z = X^2 + 7Y^2$ の場合 40
3.7.4 $Z = X^2 + 5Y^2$ の場合 41
3.7.5 $Z = X^2 + 6Y^2$ の場合 42

4 考察 **45**
4.1 平方剰余を用いた証明 45
4.2 剰余環とイデアル分解 47
4.2.1 (α) による剰余環が体になる場合 47
4.2.2 (α) による剰余環が環の直和または体の無限小拡大環になる場合 52

1　目的

自然数 X, Y が互いに素であり、X は p で割りきれない時、方程式 $Z = X^2 + pY^2$ の解について研究した。既約元や剰余環、平方剰余から Z の数の規則性について研究することを目的とする。

以下、方程式 $Z = X^2 + 3Y^2$ となる例をいくつか挙げる。

$4 = 1^2 + 3 \cdot 1^2$
$7 = 2^2 + 3 \cdot 1^2$
$19 = 4^2 + 3 \cdot 1^2$
$28 = 1^2 + 3 \cdot 3^2$
$28 = 5^2 + 3 \cdot 1^2$
$31 = 2^2 + 3 \cdot 3^2$
$37 = 5^2 + 3 \cdot 2^2$

この研究では一般に $p = 2, 3, 5, 6, 7$ の場合を調べた。

2　方法

2.1　方法

prolog を使って、自然数 X,Y が互いに素であるとき X^2+pY^2 と素因数分解の値を表示するプログラムを作った。

2.2　プログラム

繰り返し

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

一般互除法

```
gcd(A=(A,0)):-!.
gcd(D=(A,B)):-
B1 is A mod B,A1=B,
gcd(D=(A1,B1)).

/** gcd(D=A*X+B*Y) A,B given; D,X,Y not given **/
gcd(A=A*1+0*0).
gcd(D=A*X+B*Y):-
res_q(A=B*Q+R),
(A1,B1)=(B,R),
gcd(D=A1*X1+B1*Y1),
T is X1-Y1*Q,(X,Y)=(Y1,T).
```

47 と 149 の最大公約数を一般互除法を用いて計算する例

```
1 ?-gcd(D=47*X+149*Y).
D=1,
X=-19,
Y=6
```

素因数分解

```
factor(P/2):-Q is P//2,P =:= 2*Q,!.
factor(P/I):-P1 is floor(sqrt(P)),
for(1=<P1,J),
J1 is 2*J+1,
```

```
Q is P//J1,
P =:= J1*Q,I=J1,!.
factor(P/P):-!.

factorize(P,[P]):-factor(P/I),P==I,!.
factorize(P,List):-factor(P/I),
P1 is P//I,
List=[I|List1],
factorize(P1,List1),!.
```

10 の素因数分解をリストで計算する例

```
1 ?-factorize(10,P).
P=[2,5]
```

$X^2 + 2Y^2$ の表示

```
f2:-for(1=<100,X),for(1=<100,Y),gcd(D=(X,Y)),X mod 2\==0,
        Z is X^2+2*Y^2,Z<2000,Z mod 2=\=0,D==1,factorize(Z,L),write(Z),
write(;),tab(9),
write(L),tab(9),tab(9),write(|),write(X*X+2*Y*Y),nl,fail.
f2.
```

$X^2 + 2Y^2$ の 1000 までの値とその素因数分解の値を計算する例

```
1 ?-f2.
3;        [3]          |1*1+2*1*1
9;        [3,3]          |1*1+2*2*2
11;        [11]          |3*3+2*1*1
17;        [17]          |3*3+2*2*2
19;        [19]          |1*1+2*3*3
27;        [3,3,3]          |5*5+2*1*1
33;        [3,11]          |1*1+2*4*4
33;        [3,11]          |5*5+2*2*2
41;        [41]          |3*3+2*4*4
```

と 1000 までの数が出力されるが以下省略する。実際には、 $X^2 + 2Y^2$ の値は順不同に表示されるので、Excel で $X^2 + 2Y^2$ の値を昇順に直した。後に Excel で $X^2 + 2Y^2$ の値を昇順に直したものを添付する。

X^2+3Y^2 の表示

```
f3:-for(1=<100,X),for(1=<100,Y),gcd(D=(X,Y)),X mod 3\==0,
        Z is X^2+3*Y^2,Z<2000,Z mod 3=\=0,D==1,factorize(Z,L),write(Z),
write(;),tab(9),
write(L),tab(9),tab(9),write(|),write(X*X+3*Y*Y),nl,fail.
f3.
```

X^2+3Y^2 の 1000 までの値とその素因数分解の値を計算する例

```
1 ?-f3.
4;        [2,2]          |1*1+3*1*1
7;        [7]          |2*2+3*1*1
13;        [13]          |1*1+3*2*2
19;        [19]          |4*4+3*1*1
28;        [2,2,7]          |1*1+3*3*3
28;        [2,2,7]          |5*5+3*1*1
31;        [31]          |2*2+3*3*3
37;        [37]          |5*5+3*2*2
43;        [43]          |4*4+3*3*3
```

と 1000 までの数が出力されるが以下省略する。実際には、 X^2+3Y^2 の値は順不同に表示されるので、Excel で X^2+3Y^2 の値を昇順に直した。後に Excel で X^2+3Y^2 の値を昇順に直したものを添付する。

X^2+5Y^2 の表示

```
f5:-for(1=<100,X),for(1=<100,Y),gcd(D=(X,Y)),X mod 5\==0,
        Z is X^2+5*Y^2,Z<2000,Z mod 5=\=0,D==1,factorize(Z,L),write(Z),
write(;),tab(9),
write(L),tab(9),tab(9),write(|),write(X*X+5*Y*Y),nl,fail.
f5.
```

X^2+5Y^2 の 1000 までの値とその素因数分解の値を計算する例

```
1 ?-f5.
6;        [2,3]          |1*1+5*1*1
9;        [3,3]          |2*2+5*1*1
14;        [14]          |3*3+5*1*1
21;        [3,7]          |1*1+5*2*2
```

```
21;        [3,7]          |4*4+5*1*1
29;        [29]          |3*3+5*2*2
41;        [41]          |6*6+5*1*1
46;        [2,23]          |1*1+5*3*3
49;        [7,7]          |2*2+5*3*3
```

と 1000 までの数が出力されるが以下省略する。実際には、 X^2+5Y^2 の値は順不同に表示されるので、Excel で X^2+5Y^2 の値を昇順に直した。後に Excel で X^2+5Y^2 の値を昇順に直したものを添付する。

X^2+6Y^2 の表示

```
f6:-for(1=<100,X),for(1=<100,Y),gcd(D=(X,Y)),X mod 6\==0,
        Z is X^2+6*Y^2,Z<2000,Z mod 6=\=0,D==1,factorize(Z,L),write(Z),
write(;),tab(9),
write(L),tab(9),tab(9),write(|),write(X*X+6*Y*Y),nl,fail.
f6.
```

X^2+6Y^2 の 1000 までの値とその素因数分解の値を計算する例

```
1 ?-f6.
7;        [7]          |1*1+6*1*1
10;        [2,5]          |2*2+6*1*1
15;        [3,5]          |3*3+6*1*1
22;        [2,11]          |4*4+6*1*1
25;        [5,5]          |1*1+6*2*2
31;        [31]          |5*5+6*1*1
33;        [3,11]          |3*3+6*2*2
49;        [7,7]          |5*5+6*2*2
55;        [5,11]          |1*1+6*3*3
55;        [5,11]          |7*7+6*1*1
```

と 1000 までの数が出力されるが以下省略する。実際には、 X^2+6Y^2 の値は順不同に表示されるので、Excel で X^2+6Y^2 の値を昇順に直した。後に Excel で X^2+6Y^2 の値を昇順に直したものを添付する。

X^2+7Y^2 の表示

```
f7:-for(1=<100,X),for(1=<100,Y),gcd(D=(X,Y)),X mod 7\==0,
        Z is X^2+7*Y^2,Z<2000,Z mod 7=\=0,D==1,factorize(Z,L),write(Z),
write(;),tab(9),
```

```
write(L),tab(9),tab(9),write(|),write(X*X+7*Y*Y),nl,fail.
f7.
```

$X^2 + 7Y^2$ の 1000 までの値とその素因数分解の値を計算する例

```
1 ?-f7.
8;        [2,2,2]          |1*1+7*1*1
11;        [11]           |2*2+7*1*1
16;        [4,4]           |3*3+7*1*1
23;        [23]           |4*4+7*1*1
29;        [29]           |1*1+7*2*2
32;        [2,2,2,2,2]           |5*5+7*1*1
37;        [37]           |3*3+7*2*2
43;        [43]           |6*6+7*1*1
53;        [53]           |5*5+7*2*2
```

と 1000 までの数が出力されるが以下省略する。実際には、 $X^2 + 7Y^2$ の値は順不同に表示されるので、Excel で $X^2 + 7Y^2$ の値を昇順に直した。後に Excel で $X^2 + 7Y^2$ の値を昇順に直したものを添付する。

3　結果

3.1　わかったこと

・$p = 2, 3, 7$ のとき、 Z の異なる素因数が n 個なら 2^{n-1} 個の異なる解がある。
しかし、$p = 5, 6$ の時、一部上記の規則性を満たさない時がある。
・$p = 5$ の場合、Z が 2 の倍数のときは全て上記の規則を満たさない。
・$p = 6$ の場合、Z が 2 の倍数または 3 の倍数のときは全て上記の規則を満たさないことがわかった。

・$\mathbf{Z}[\sqrt{-5}]$ において、$Z = X^2+5Y^2$ の解があり、 Z が素数になるものは、$29, 41, 61, 89, 101, 109, \cdots$ であり、$1 \mod 4$ を満たし、$\mathbf{Z}[\sqrt{-5}]$ において既約元になるものは、2 を除いて、$3, 7, 23, 43, 47, 67, \cdots$ となり、$3 \mod 4$ を満たす。
・ $\mathbf{Z}[\sqrt{-6}]$ において、$Z = X^2+6Y^2$ の解があり、 Z が素数になるものは、$7, 31, 73, 79, 97, 103, \cdots$ であり、$1 \mod 6$ を満たし、$Z = X^2+6Y^2$ の解がないが、 $\mathbf{Z}[\sqrt{-6}]$ において既約元になるものは、2 と 3 を除いて、$5, 11, 29, 53, 59, 83, \cdots$ であり、$5 \mod 6$ を満たす。
3.7 でそれぞれの場合についての例を出す。

次に Z から奇素数を取り出し、規則性を考えた結果、以下のことがわかった。
・$p = 2$ のとき 3, 11, 17, 19, 41, 43, 59, 67, 73、... となり、$Z \equiv 1, 3 \mod 8$ を満たす。
・$p = 3$ のとき 7, 13, 19, 31, 37, 43, 61, 67, 73、... となり、$Z \equiv 1, 7 \mod 12$ を満たす。
・$p = 5$ のとき 29, 41, 61, 101, 109, 149, 181, 229, 241、... となり、$Z \equiv 1, 9 \mod 20$ を満たす。
・$p = 6$ のとき 7, 31, 73, 79, 97, 103, 127, 151, 193、... となり、$Z \equiv 1, 7 \mod 24$ を満たす。
・$p = 7$ のとき 11, 23, 29, 37, 43, 53, 67, 71, 79、... となり、$Z \equiv 1, 9, 11, 15, 23, 25 \mod 28$ を満たす。

平方剰余を用いてこれを証明できるので、考察 4.1 で証明する。

$Z = X^2 + 5Y^2$ と $Z = X^2 + 6Y^2$ については規則性が一部乱れるので、 剰余環を使って調べた。
$\mathbf{Z}[\sqrt{-6}] = \left\{a + b\sqrt{-6} : a, b \in \mathbf{Z}\right\}$ において、既約元 α について (α) による剰余環を調べると、剰余環が体になるか、環の直和または無限小拡大環になることがわかった。
考察 4.2 で例を出して確認する。

3.2 $X^2 + 2Y^2$ の表

表 1: $X^2 + 2Y^2$ の値を昇順に直した表

$X^2 + 2Y^2$ の値	因数分解	$X^2 + 2Y^2$ の形で表記
3	[3]	1·1+2·1·1
9	[3, 3]	1·1+2·2·2
11	[11]	3·3+2·1·1
17	[17]	3·3+2·2·2
19	[19]	1·1+2·3·3
27	[3, 3, 3]	5·5+2·1·1
33	[3, 11]	1·1+2·4·4
33	[3, 11]	5·5+2·2·2
41	[41]	3·3+2·4·4
43	[43]	5·5+2·3·3
51	[3, 17]	1·1+2·5·5
51	[3, 17]	7·7+2·1·1
57	[3, 19]	5·5+2·4·4
57	[3, 19]	7·7+2·2·2
59	[59]	3·3+2·5·5
67	[67]	7·7+2·3·3
73	[73]	1·1+2·6·6
81	[3, 3, 3, 3]	7·7+2·4·4
83	[83]	9·9+2·1·1
89	[89]	9·9+2·2·2
97	[97]	5·5+2·6·6
99	[3, 3, 11]	1·1+2·7·7
99	[3, 3, 11]	7·7+2·5·5
107	[107]	3·3+2·7·7
113	[113]	9·9+2·4·4
121	[11, 11]	7·7+2·6·6
123	[3, 41]	5·5+2·7·7
123	[3, 41]	11·11+2·1·1
129	[3, 43]	1·1+2·8·8
129	[3, 43]	11·11+2·2·2
131	[131]	9·9+2·5·5
137	[137]	3·3+2·8·8
139	[139]	11·11+2·3·3
153	[3, 3, 17]	5·5+2·8·8
153	[3, 3, 17]	11·11+2·4·4
163	[163]	1·1+2·9·9
171	[3, 3, 19]	11·11+2·5·5
171	[3, 3, 19]	13·13+2·1·1

表 1: $X^2 + 2Y^2$ の値を昇順に直した表

$X^2 + 2Y^2$ の値	因数分解	$X^2 + 2Y^2$ の形で表記
177	[3, 59]	7·7+2·8·8
177	[3, 59]	13·13+2·2·2
179	[179]	9·9+2·7·7
187	[11, 17]	5·5+2·9·9
187	[11, 17]	13·13+2·3·3
193	[193]	11·11+2·6·6
201	[3, 67]	1·1+2·10·10
201	[3, 67]	13·13+2·4·4
209	[11, 19]	3·3+2·10·10
209	[11, 19]	9·9+2·8·8
211	[211]	7·7+2·9·9
219	[3, 73]	11·11+2·7·7
219	[3, 73]	13·13+2·5·5
227	[227]	15·15+2·1·1
233	[233]	15·15+2·2·2
241	[241]	13·13+2·6·6
243	[3, 3, 3, 3, 3]	1·1+2·11·11
249	[3, 83]	7·7+2·10·10
249	[3, 83]	11·11+2·8·8
251	[251]	3·3+2·11·11
257	[257]	15·15+2·4·4
267	[3, 89]	5·5+2·11·11
267	[3, 89]	13·13+2·7·7
281	[281]	9·9+2·10·10
283	[283]	11·11+2·9·9
289	[17, 17]	1·1+2·12·12
291	[3, 97]	7·7+2·11·11
291	[3, 97]	17·17+2·1·1
297	[3, 3, 3, 11]	13·13+2·8·8
297	[3, 3, 3, 11]	17·17+2·2·2
307	[307]	17·17+2·3·3
313	[313]	5·5+2·12·12
321	[3, 107]	11·11+2·10·10
321	[3, 107]	17·17+2·4·4
323	[17, 19]	9·9+2·11·11
323	[17, 19]	15·15+2·7·7
331	[331]	13·13+2·9·9
337	[337]	7·7+2·12·12
339	[3, 113]	1·1+2·13·13

表 1: X^2+2Y^2 の値を昇順に直した表

X^2+2Y^2 の値	因数分解	X^2+2Y^2 の形で表記
339	[3, 113]	17·17+2·5·5
347	[347]	3·3+2·13·13
353	[353]	15·15+2·8·8
361	[19, 19]	17·17+2·6·6
363	[3, 11, 11]	5·5+2·13·13
363	[3, 11, 11]	19·19+2·1·1
369	[3, 3, 41]	13·13+2·10·10
369	[3, 3, 41]	19·19+2·2·2
379	[379]	19·19+2·3·3
387	[3, 3, 43]	7·7+2·13·13
387	[3, 3, 43]	17·17+2·7·7
393	[3, 131]	1·1+2·14·14
393	[3, 131]	19·19+2·4·4
401	[401]	3·3+2·14·14
409	[409]	11·11+2·12·12
411	[3, 137]	13·13+2·11·11
411	[3, 137]	19·19+2·5·5
417	[3, 139]	5·5+2·14·14
417	[3, 139]	17·17+2·8·8
419	[419]	9·9+2·13·13
433	[433]	19·19+2·6·6
443	[443]	21·21+2·1·1
449	[449]	21·21+2·2·2
451	[11, 41]	1·1+2·15·15
451	[11, 41]	17·17+2·9·9
457	[457]	13·13+2·12·12
459	[3, 3, 3, 17]	11·11+2·13·13
459	[3, 3, 3, 17]	19·19+2·7·7
467	[467]	15·15+2·11·11
473	[11, 43]	9·9+2·14·14
473	[11, 43]	21·21+2·4·4
489	[3, 163]	17·17+2·10·10
489	[3, 163]	19·19+2·8·8
491	[491]	21·21+2·5·5
499	[499]	7·7+2·15·15
513	[3, 3, 3, 19]	1·1+2·16·16
513	[3, 3, 3, 19]	11·11+2·14·14
521	[521]	3·3+2·16·16
523	[523]	19·19+2·9·9

表 1: X^2+2Y^2 の値を昇順に直した表

X^2+2Y^2 の値	因数分解	X^2+2Y^2 の形で表記
531	[3, 3, 59]	17·17+2·11·11
531	[3, 3, 59]	23·23+2·1·1
537	[3, 179]	5·5+2·16·16
537	[3, 179]	23·23+2·2·2
547	[547]	23·23+2·3·3
561	[3, 11, 17]	7·7+2·16·16
561	[3, 11, 17]	13·13+2·14·14
561	[3, 11, 17]	19·19+2·10·10
561	[3, 11, 17]	23·23+2·4·4
563	[563]	15·15+2·13·13
569	[569]	21·21+2·8·8
571	[571]	11·11+2·15·15
577	[577]	17·17+2·12·12
579	[3, 193]	1·1+2·17·17
579	[3, 193]	23·23+2·5·5
587	[587]	3·3+2·17·17
593	[593]	9·9+2·16·16
601	[601]	23·23+2·6·6
603	[3, 3, 67]	5·5+2·17·17
603	[3, 3, 67]	19·19+2·11·11
617	[617]	15·15+2·14·14
619	[619]	13·13+2·15·15
627	[3, 11, 19]	7·7+2·17·17
627	[3, 11, 19]	17·17+2·13·13
627	[3, 11, 19]	23·23+2·7·7
627	[3, 11, 19]	25·25+2·1·1
633	[3, 211]	11·11+2·16·16
633	[3, 211]	25·25+2·2·2
641	[641]	21·21+2·10·10
643	[643]	25·25+2·3·3
649	[11, 59]	1·1+2·18·18
649	[11, 59]	19·19+2·12·12
657	[3, 3, 73]	23·23+2·8·8
657	[3, 3, 73]	25·25+2·4·4
659	[659]	9·9+2·17·17
673	[673]	5·5+2·18·18
681	[3, 227]	13·13+2·16·16
681	[3, 227]	17·17+2·14·14
683	[683]	21·21+2·11·11

表 1: X^2+2Y^2 の値を昇順に直した表

X^2+2Y^2 の値	因数分解	X^2+2Y^2 の形で表記
691	[691]	23·23+2·9·9
697	[17, 41]	7·7+2·18·18
697	[17, 41]	25·25+2·6·6
699	[3, 233]	11·11+2·17·17
699	[3, 233]	19·19+2·13·13
723	[3, 241]	1·1+2·19·19
723	[3, 241]	25·25+2·7·7
729	[3, 3, 3, 3, 3, 3]	23·23+2·10·10
731	[17, 43]	3·3+2·19·19
731	[17, 43]	27·27+2·1·1
737	[11, 67]	15·15+2·16·16
737	[11, 67]	27·27+2·2·2
739	[739]	17·17+2·15·15
747	[3, 3, 83]	5·5+2·19·19
747	[3, 3, 83]	13·13+2·17·17
753	[3, 251]	19·19+2·14·14
753	[3, 251]	25·25+2·8·8
761	[761]	27·27+2·4·4
769	[769]	11·11+2·18·18
771	[3, 257]	7·7+2·19·19
771	[3, 257]	23·23+2·11·11
779	[19, 41]	21·21+2·13·13
779	[19, 41]	27·27+2·5·5
787	[787]	25·25+2·9·9
801	[3, 3, 89]	1·1+2·20·20
801	[3, 3, 89]	17·17+2·16·16
803	[11, 73]	9·9+2·19·19
803	[11, 73]	15·15+2·17·17
809	[809]	3·3+2·20·20
811	[811]	19·19+2·15·15
817	[19, 43]	13·13+2·18·18
817	[19, 43]	23·23+2·12·12
827	[827]	27·27+2·7·7
843	[3, 281]	11·11+2·19·19
843	[3, 281]	29·29+2·1·1
849	[3, 283]	7·7+2·20·20
849	[3, 283]	29·29+2·2·2
857	[857]	27·27+2·8·8
859	[859]	29·29+2·3·3

表 1: X^2+2Y^2 の値を昇順に直した表

X^2+2Y^2 の値	因数分解	X^2+2Y^2 の形で表記
867	[3, 17, 17]	23·23+2·13·13
867	[3, 17, 17]	25·25+2·11·11
873	[3, 3, 97]	19·19+2·16·16
873	[3, 3, 97]	29·29+2·4·4
881	[881]	9·9+2·20·20
883	[883]	1·1+2·21·21
891	[3, 3, 3, 3, 11]	13·13+2·19·19
891	[3, 3, 3, 3, 11]	29·29+2·5·5
907	[907]	5·5+2·21·21
913	[11, 83]	25·25+2·12·12
913	[11, 83]	29·29+2·6·6
921	[3, 307]	11·11+2·20·20
921	[3, 307]	23·23+2·14·14
929	[929]	27·27+2·10·10
937	[937]	17·17+2·18·18
939	[3, 313]	19·19+2·17·17
939	[3, 313]	29·29+2·7·7
947	[947]	15·15+2·19·19
953	[953]	21·21+2·16·16
963	[3, 3, 107]	25·25+2·13·13
963	[3, 3, 107]	31·31+2·1·1
969	[3, 17, 19]	1·1+2·22·22
969	[3, 17, 19]	13·13+2·20·20
969	[3, 17, 19]	29·29+2·8·8
969	[3, 17, 19]	31·31+2·2·2
971	[971]	27·27+2·11·11
977	[977]	3·3+2·22·22
979	[11, 89]	23·23+2·15·15
979	[11, 89]	31·31+2·3·3
993	[3, 331]	5·5+2·22·22
993	[3, 331]	31·31+2·4·4

3.3 X^2+3Y^2 の表

表 2: X^2+3Y^2 の値を昇順に直した表

X^2+3Y^2 の値	因数分解	X^2+3Y^2 の形で表記
4	[2, 2]	1·1+3·1·1
7	[7]	2·2+3·1·1
13	[13]	1·1+3·2·2
19	[19]	4·4+3·1·1
28	[2, 2, 7]	1·1+3·3·3
28	[2, 2, 7]	5·5+3·1·1
31	[31]	2·2+3·3·3
37	[37]	5·5+3·2·2
43	[43]	4·4+3·3·3
49	[7, 7]	1·1+3·4·4
52	[2, 2, 13]	5·5+3·3·3
52	[2, 2, 13]	7·7+3·1·1
61	[61]	7·7+3·2·2
67	[67]	8·8+3·1·1
73	[73]	5·5+3·4·4
76	[2, 2, 19]	1·1+3·5·5
76	[2, 2, 19]	7·7+3·3·3
79	[79]	2·2+3·5·5
91	[7, 13]	4·4+3·5·5
91	[7, 13]	8·8+3·3·3
97	[97]	7·7+3·4·4
103	[103]	10·10+3·1·1
109	[109]	1·1+3·6·6
124	[2, 2, 31]	7·7+3·5·5
124	[2, 2, 31]	11·11+3·1·1
127	[127]	10·10+3·3·3
133	[7, 19]	5·5+3·6·6
133	[7, 19]	11·11+3·2·2
139	[139]	8·8+3·5·5
148	[2, 2, 37]	1·1+3·7·7
148	[2, 2, 37]	11·11+3·3·3
151	[151]	2·2+3·7·7
157	[157]	7·7+3·6·6
163	[163]	4·4+3·7·7
169	[13, 13]	11·11+3·4·4
172	[2, 2, 43]	5·5+3·7·7
172	[2, 2, 43]	13·13+3·1·1
181	[181]	13·13+3·2·2

表 2: X^2+3Y^2 の値を昇順に直した表

X^2+3Y^2 の値	因数分解	X^2+3Y^2 の形で表記
193	[193]	1·1+3·8·8
196	[2, 2, 7, 7]	11·11+3·5·5
196	[2, 2, 7, 7]	13·13+3·3·3
199	[199]	14·14+3·1·1
211	[211]	8·8+3·7·7
217	[7, 31]	5·5+3·8·8
217	[7, 31]	13·13+3·4·4
223	[223]	14·14+3·3·3
229	[229]	11·11+3·6·6
241	[241]	7·7+3·8·8
244	[2, 2, 61]	1·1+3·9·9
244	[2, 2, 61]	13·13+3·5·5
247	[13, 19]	2·2+3·9·9
247	[13, 19]	10·10+3·7·7
259	[7, 37]	4·4+3·9·9
259	[7, 37]	16·16+3·1·1
268	[2, 2, 67]	5·5+3·9·9
268	[2, 2, 67]	11·11+3·7·7
271	[271]	14·14+3·5·5
277	[277]	13·13+3·6·6
283	[283]	16·16+3·3·3
292	[2, 2, 73]	7·7+3·9·9
292	[2, 2, 73]	17·17+3·1·1
301	[7, 43]	1·1+3·10·10
301	[7, 43]	17·17+3·2·2
307	[307]	8·8+3·9·9
313	[313]	11·11+3·8·8
316	[2, 2, 79]	13·13+3·7·7
316	[2, 2, 79]	17·17+3·3·3
331	[331]	16·16+3·5·5
337	[337]	17·17+3·4·4
343	[7, 7, 7]	10·10+3·9·9
349	[349]	7·7+3·10·10
361	[19, 19]	13·13+3·8·8
364	[2, 2, 7, 13]	1·1+3·11·11
364	[2, 2, 7, 13]	11·11+3·9·9
364	[2, 2, 7, 13]	17·17+3·5·5
364	[2, 2, 7, 13]	19·19+3·1·1
367	[367]	2·2+3·11·11

表 2: X^2+3Y^2 の値を昇順に直した表

X^2+3Y^2 の値	因数分解	X^2+3Y^2 の形で表記
373	[373]	19·19+3·2·2
379	[379]	4·4+3·11·11
388	[2, 2, 97]	5·5+3·11·11
388	[2, 2, 97]	19·19+3·3·3
397	[397]	17·17+3·6·6
403	[13, 31]	16·16+3·7·7
403	[13, 31]	20·20+3·1·1
409	[409]	19·19+3·4·4
412	[2, 2, 103]	7·7+3·11·11
412	[2, 2, 103]	13·13+3·9·9
421	[421]	11·11+3·10·10
427	[7, 61]	8·8+3·11·11
427	[7, 61]	20·20+3·3·3
433	[433]	1·1+3·12·12
436	[2, 2, 109]	17·17+3·7·7
436	[2, 2, 109]	19·19+3·5·5
439	[439]	14·14+3·9·9
457	[457]	5·5+3·12·12
463	[463]	10·10+3·11·11
469	[7, 67]	13·13+3·10·10
469	[7, 67]	19·19+3·6·6
481	[13, 37]	7·7+3·12·12
481	[13, 37]	17·17+3·8·8
487	[487]	22·22+3·1·1
499	[499]	16·16+3·9·9
508	[2, 2, 127]	1·1+3·13·13
508	[2, 2, 127]	19·19+3·7·7
511	[7, 73]	2·2+3·13·13
511	[7, 73]	22·22+3·3·3
523	[523]	4·4+3·13·13
532	[2, 2, 7, 19]	5·5+3·13·13
532	[2, 2, 7, 19]	13·13+3·11·11
532	[2, 2, 7, 19]	17·17+3·9·9
532	[2, 2, 7, 19]	23·23+3·1·1
541	[541]	23·23+3·2·2
547	[547]	20·20+3·7·7
553	[7, 79]	11·11+3·12·12
553	[7, 79]	19·19+3·8·8
556	[2, 2, 139]	7·7+3·13·13

表 2: X^2+3Y^2 の値を昇順に直した表

X^2+3Y^2 の値	因数分解	X^2+3Y^2 の形で表記
556	[2, 2, 139]	23·23+3·3·3
559	[13, 43]	14·14+3·11·11
559	[13, 43]	22·22+3·5·5
571	[571]	8·8+3·13·13
577	[577]	23·23+3·4·4
589	[19, 31]	1·1+3·14·14
589	[19, 31]	17·17+3·10·10
601	[601]	13·13+3·12·12
604	[2, 2, 151]	19·19+3·9·9
604	[2, 2, 151]	23·23+3·5·5
607	[607]	10·10+3·13·13
613	[613]	5·5+3·14·14
619	[619]	16·16+3·11·11
628	[2, 2, 157]	11·11+3·13·13
628	[2, 2, 157]	25·25+3·1·1
631	[631]	22·22+3·7·7
637	[7, 7, 13]	23·23+3·6·6
637	[7, 7, 13]	25·25+3·2·2
643	[643]	20·20+3·9·9
652	[2, 2, 163]	17·17+3·11·11
652	[2, 2, 163]	25·25+3·3·3
661	[661]	19·19+3·10·10
673	[673]	25·25+3·4·4
676	[2, 2, 13, 13]	1·1+3·15·15
676	[2, 2, 13, 13]	23·23+3·7·7
679	[7, 97]	2·2+3·15·15
679	[7, 97]	26·26+3·1·1
691	[691]	4·4+3·15·15
703	[19, 37]	14·14+3·13·13
703	[19, 37]	26·26+3·3·3
709	[709]	11·11+3·14·14
721	[7, 103]	17·17+3·12·12
721	[7, 103]	23·23+3·8·8
724	[2, 2, 181]	7·7+3·15·15
724	[2, 2, 181]	19·19+3·11·11
727	[727]	22·22+3·9·9
733	[733]	25·25+3·6·6
739	[739]	8·8+3·15·15
751	[751]	26·26+3·5·5

表 2: X^2+3Y^2 の値を昇順に直した表

X^2+3Y^2 の値	因数分解	X^2+3Y^2 の形で表記
757	[757]	13·13+3·14·14
763	[7, 109]	16·16+3·13·13
763	[7, 109]	20·20+3·11·11
769	[769]	1·1+3·16·16
772	[2, 2, 193]	23·23+3·9·9
772	[2, 2, 193]	25·25+3·7·7
787	[787]	28·28+3·1·1
793	[13, 61]	5·5+3·16·16
793	[13, 61]	19·19+3·12·12
796	[2, 2, 199]	11·11+3·15·15
796	[2, 2, 199]	17·17+3·13·13
811	[811]	28·28+3·3·3
817	[19, 43]	7·7+3·16·16
817	[19, 43]	25·25+3·8·8
823	[823]	26·26+3·7·7
829	[829]	23·23+3·10·10
844	[2, 2, 211]	13·13+3·15·15
844	[2, 2, 211]	29·29+3·1·1
853	[853]	29·29+3·2·2
859	[859]	28·28+3·5·5
868	[2, 2, 7, 31]	1·1+3·17·17
868	[2, 2, 7, 31]	19·19+3·13·13
868	[2, 2, 7, 31]	25·25+3·9·9
868	[2, 2, 7, 31]	29·29+3·3·3
871	[13, 67]	2·2+3·17·17
871	[13, 67]	14·14+3·15·15
877	[877]	17·17+3·14·14
883	[883]	4·4+3·17·17
889	[7, 127]	11·11+3·16·16
889	[7, 127]	29·29+3·4·4
892	[2, 2, 223]	5·5+3·17·17
892	[2, 2, 223]	23·23+3·11·11
907	[907]	20·20+3·13·13
916	[2, 2, 229]	7·7+3·17·17
916	[2, 2, 229]	29·29+3·5·5
919	[919]	26·26+3·9·9
931	[7, 7, 19]	8·8+3·17·17
931	[7, 7, 19]	16·16+3·15·15
937	[937]	13·13+3·16·16

表 2: X^2+3Y^2 の値を昇順に直した表

X^2+3Y^2 の値	因数分解	X^2+3Y^2 の形で表記
949	[13, 73]	19·19+3·14·14
949	[13, 73]	29·29+3·6·6
961	[31, 31]	23·23+3·12·12
964	[2, 2, 241]	17·17+3·15·15
964	[2, 2, 241]	31·31+3·1·1
967	[967]	10·10+3·17·17
973	[7, 139]	1·1+3·18·18
973	[7, 139]	31·31+3·2·2
988	[2, 2, 13, 19]	11·11+3·17·17
988	[2, 2, 13, 19]	25·25+3·11·11
988	[2, 2, 13, 19]	29·29+3·7·7
988	[2, 2, 13, 19]	31·31+3·3·3
991	[991]	22·22+3·13·13
997	[997]	5·5+3·18·18

3.4 X^2+5Y^2 の表

表 3: X^2+5Y^2 の値を昇順に直した表

X^2+5Y^2 の値	因数分解	X^2+5Y^2 の形で表記
6	[2, 3]	1·1+5·1·1
9	[3, 3]	2·2+5·1·1
14	[2, 7]	3·3+5·1·1
21	[3, 7]	1·1+5·2·2
21	[3, 7]	4·4+5·1·1
29	[29]	3·3+5·2·2
41	[41]	6·6+5·1·1
46	[2, 23]	1·1+5·3·3
49	[7, 7]	2·2+5·3·3
54	[2, 3, 3, 3]	7·7+5·1·1
61	[61]	4·4+5·3·3
69	[3, 23]	7·7+5·2·2
69	[3, 23]	8·8+5·1·1
81	[3, 3, 3, 3]	1·1+5·4·4
86	[2, 43]	9·9+5·1·1
89	[89]	3·3+5·4·4
94	[2, 47]	7·7+5·3·3
101	[101]	9·9+5·2·2
109	[109]	8·8+5·3·3
126	[2, 3, 3, 7]	1·1+5·5·5
126	[2, 3, 3, 7]	11·11+5·1·1
129	[3, 43]	2·2+5·5·5
129	[3, 43]	7·7+5·4·4
134	[2, 67]	3·3+5·5·5
141	[3, 47]	4·4+5·5·5
141	[3, 47]	11·11+5·2·2
149	[149]	12·12+5·1·1
161	[7, 23]	6·6+5·5·5
161	[7, 23]	9·9+5·4·4
166	[2, 83]	11·11+5·3·3
174	[2, 3, 29]	7·7+5·5·5
174	[2, 3, 29]	13·13+5·1·1
181	[181]	1·1+5·6·6
189	[3, 3, 3, 7]	8·8+5·5·5
189	[3, 3, 3, 7]	13·13+5·2·2
201	[3, 67]	11·11+5·4·4
201	[3, 67]	14·14+5·1·1
206	[2, 103]	9·9+5·5·5

表 3: X^2+5Y^2 の値を昇順に直した表

X^2+5Y^2 の値	因数分解	X^2+5Y^2 の形で表記
214	[2, 107]	13·13+5·3·3
229	[229]	7·7+5·6·6
241	[241]	14·14+5·3·3
246	[2, 3, 41]	1·1+5·7·7
246	[2, 3, 41]	11·11+5·5·5
249	[3, 83]	2·2+5·7·7
249	[3, 83]	13·13+5·4·4
254	[2, 127]	3·3+5·7·7
261	[3, 3, 29]	4·4+5·7·7
261	[3, 3, 29]	16·16+5·1·1
269	[269]	12·12+5·5·5
281	[281]	6·6+5·7·7
294	[2, 3, 7, 7]	13·13+5·5·5
294	[2, 3, 7, 7]	17·17+5·1·1
301	[7, 43]	11·11+5·6·6
301	[7, 43]	16·16+5·3·3
309	[3, 103]	8·8+5·7·7
309	[3, 103]	17·17+5·2·2
321	[3, 107]	1·1+5·8·8
321	[3, 107]	14·14+5·5·5
326	[2, 163]	9·9+5·7·7
329	[7, 47]	3·3+5·8·8
329	[7, 47]	18·18+5·1·1
334	[2, 167]	17·17+5·3·3
349	[349]	13·13+5·6·6
366	[2, 3, 61]	11·11+5·7·7
366	[2, 3, 61]	19·19+5·1·1
369	[3, 3, 41]	7·7+5·8·8
369	[3, 3, 41]	17·17+5·4·4
381	[3, 127]	16·16+5·5·5
381	[3, 127]	19·19+5·2·2
389	[389]	12·12+5·7·7
401	[401]	9·9+5·8·8
406	[2, 7, 29]	1·1+5·9·9
406	[2, 7, 29]	19·19+5·3·3
409	[409]	2·2+5·9·9
414	[2, 3, 3, 23]	13·13+5·7·7
414	[2, 3, 3, 23]	17·17+5·5·5
421	[421]	4·4+5·9·9

表 3: X^2+5Y^2 の値を昇順に直した表

X^2+5Y^2 の値	因数分解	X^2+5Y^2 の形で表記
441	[3, 3, 7, 7]	11·11+5·8·8
441	[3, 3, 7, 7]	19·19+5·4·4
446	[2, 223]	21·21+5·1·1
449	[449]	18·18+5·5·5
454	[2, 227]	7·7+5·9·9
461	[461]	21·21+5·2·2
469	[7, 67]	8·8+5·9·9
469	[7, 67]	17·17+5·6·6
486	[2, 3, 3, 3, 3, 3]	19·19+5·5·5
489	[3, 163]	13·13+5·8·8
489	[3, 163]	22·22+5·1·1
501	[3, 167]	1·1+5·10·10
501	[3, 167]	16·16+5·7·7
509	[509]	3·3+5·10·10
521	[521]	21·21+5·4·4
526	[2, 263]	11·11+5·9·9
529	[23, 23]	22·22+5·3·3
534	[2, 3, 89]	17·17+5·7·7
534	[2, 3, 89]	23·23+5·1·1
541	[541]	19·19+5·6·6
549	[3, 3, 61]	7·7+5·10·10
549	[3, 3, 61]	23·23+5·2·2
566	[2, 283]	21·21+5·5·5
569	[569]	18·18+5·7·7
574	[2, 7, 41]	13·13+5·9·9
574	[2, 7, 41]	23·23+5·3·3
581	[7, 83]	9·9+5·10·10
581	[7, 83]	24·24+5·1·1
601	[601]	14·14+5·9·9
606	[2, 3, 101]	1·1+5·11·11
606	[2, 3, 101]	19·19+5·7·7
609	[3, 7, 29]	2·2+5·11·11
609	[3, 7, 29]	17·17+5·8·8
609	[3, 7, 29]	22·22+5·5·5
609	[3, 7, 29]	23·23+5·4·4
614	[2, 307]	3·3+5·11·11
621	[3, 3, 3, 23]	4·4+5·11·11
621	[3, 3, 3, 23]	11·11+5·10·10
641	[641]	6·6+5·11·11

表 3: X^2+5Y^2 の値を昇順に直した表

X^2+5Y^2 の値	因数分解	X^2+5Y^2 の形で表記
654	[2, 3, 109]	7·7+5·11·11
654	[2, 3, 109]	23·23+5·5·5
661	[661]	16·16+5·9·9
669	[3, 223]	8·8+5·11·11
669	[3, 223]	13·13+5·10·10
681	[3, 227]	19·19+5·8·8
681	[3, 227]	26·26+5·1·1
686	[2, 7, 7, 7]	9·9+5·11·11
694	[2, 347]	17·17+5·9·9
701	[701]	24·24+5·5·5
709	[709]	23·23+5·6·6
721	[7, 103]	1·1+5·12·12
721	[7, 103]	26·26+5·3·3
729	[3, 3, 3, 3, 3, 3]	22·22+5·7·7
734	[2, 367]	27·27+5·1·1
749	[7, 107]	12·12+5·11·11
749	[7, 107]	27·27+5·2·2
761	[761]	21·21+5·8·8
766	[2, 383]	19·19+5·9·9
769	[769]	7·7+5·12·12
774	[2, 3, 3, 43]	13·13+5·11·11
774	[2, 3, 3, 43]	23·23+5·7·7
789	[3, 263]	17·17+5·10·10
789	[3, 263]	28·28+5·1·1
801	[3, 3, 89]	14·14+5·11·11
801	[3, 3, 89]	26·26+5·5·5
809	[809]	27·27+5·4·4
821	[821]	24·24+5·7·7
829	[829]	28·28+5·3·3
841	[29, 29]	11·11+5·12·12
846	[2, 3, 3, 47]	1·1+5·13·13
846	[2, 3, 3, 47]	29·29+5·1·1
849	[3, 283]	2·2+5·13·13
849	[3, 283]	23·23+5·8·8
854	[2, 7, 61]	3·3+5·13·13
854	[2, 7, 61]	27·27+5·5·5
861	[3, 7, 41]	4·4+5·13·13
861	[3, 7, 41]	16·16+5·11·11
861	[3, 7, 41]	19·19+5·10·10

表 3: X^2+5Y^2 の値を昇順に直した表

X^2+5Y^2 の値	因数分解	X^2+5Y^2 の形で表記
861	[3, 7, 41]	29·29+5·2·2
881	[881]	6·6+5·13·13
886	[2, 443]	29·29+5·3·3
889	[7, 127]	13·13+5·12·12
889	[7, 127]	22·22+5·9·9
894	[2, 3, 149]	7·7+5·13·13
894	[2, 3, 149]	17·17+5·11·11
909	[3, 3, 101]	8·8+5·13·13
909	[3, 3, 101]	28·28+5·5·5
921	[3, 307]	26·26+5·7·7
921	[3, 307]	29·29+5·4·4
926	[2, 463]	9·9+5·13·13
929	[929]	18·18+5·11·11
934	[2, 467]	23·23+5·9·9
941	[941]	21·21+5·10·10
966	[2, 3, 7, 23]	11·11+5·13·13
966	[2, 3, 7, 23]	19·19+5·11·11
966	[2, 3, 7, 23]	29·29+5·5·5
966	[2, 3, 7, 23]	31·31+5·1·1
974	[2, 487]	27·27+5·7·7
981	[3, 3, 109]	1·1+5·14·14
981	[3, 3, 109]	31·31+5·2·2
989	[23, 43]	3·3+5·14·14
989	[23, 43]	12·12+5·13·13

3.5 X^2+6Y^2 の表

表 4: X^2+6Y^2 の値を昇順に直した表

X^2+6Y^2 の値	因数分解	X^2+6Y^2 の形で表記
7	[7]	1·1+6·1·1
10	[2, 5]	2·2+6·1·1
15	[3, 5]	3·3+6·1·1
22	[2, 11]	4·4+6·1·1
25	[5, 5]	1·1+6·2·2
31	[31]	5·5+6·1·1
33	[3, 11]	3·3+6·2·2
49	[7, 7]	5·5+6·2·2
55	[5, 11]	1·1+6·3·3
55	[5, 11]	7·7+6·1·1
58	[2, 29]	2·2+6·3·3
70	[2, 5, 7]	4·4+6·3·3
70	[2, 5, 7]	8·8+6·1·1
73	[73]	7·7+6·2·2
79	[79]	5·5+6·3·3
87	[3, 29]	9·9+6·1·1
97	[97]	1·1+6·4·4
103	[103]	7·7+6·3·3
105	[3, 5, 7]	3·3+6·4·4
105	[3, 5, 7]	9·9+6·2·2
106	[2, 53]	10·10+6·1·1
118	[2, 59]	8·8+6·3·3
121	[11, 11]	5·5+6·4·4
127	[127]	11·11+6·1·1
145	[5, 29]	7·7+6·4·4
145	[5, 29]	11·11+6·2·2
151	[151]	1·1+6·5·5
154	[2, 7, 11]	2·2+6·5·5
154	[2, 7, 11]	10·10+6·3·3
159	[3, 53]	3·3+6·5·5
166	[2, 83]	4·4+6·5·5
175	[5, 5, 7]	11·11+6·3·3
175	[5, 5, 7]	13·13+6·1·1
177	[3, 59]	9·9+6·4·4
193	[193]	13·13+6·2·2
199	[199]	7·7+6·5·5
202	[2, 101]	14·14+6·1·1
214	[2, 107]	8·8+6·5·5

表 4: X^2+6Y^2 の値を昇順に直した表

X^2+6Y^2 の値	因数分解	X^2+6Y^2 の形で表記
217	[7, 31]	1·1+6·6·6
217	[7, 31]	11·11+6·4·4
223	[223]	13·13+6·3·3
231	[3, 7, 11]	9·9+6·5·5
231	[3, 7, 11]	15·15+6·1·1
241	[241]	5·5+6·6·6
249	[3, 83]	15·15+6·2·2
250	[2, 5, 5, 5]	14·14+6·3·3
262	[2, 131]	16·16+6·1·1
265	[5, 53]	7·7+6·6·6
265	[5, 53]	13·13+6·4·4
271	[271]	11·11+6·5·5
295	[5, 59]	1·1+6·7·7
295	[5, 59]	17·17+6·1·1
298	[2, 149]	2·2+6·7·7
303	[3, 101]	3·3+6·7·7
310	[2, 5, 31]	4·4+6·7·7
310	[2, 5, 31]	16·16+6·3·3
313	[313]	17·17+6·2·2
319	[11, 29]	5·5+6·7·7
319	[11, 29]	13·13+6·5·5
321	[3, 107]	15·15+6·4·4
337	[337]	11·11+6·6·6
343	[7, 7, 7]	17·17+6·3·3
346	[2, 173]	14·14+6·5·5
358	[2, 179]	8·8+6·7·7
367	[367]	19·19+6·1·1
375	[3, 5, 5, 5]	9·9+6·7·7
385	[5, 7, 11]	1·1+6·8·8
385	[5, 7, 11]	13·13+6·6·6
385	[5, 7, 11]	17·17+6·4·4
385	[5, 7, 11]	19·19+6·2·2
393	[3, 131]	3·3+6·8·8
394	[2, 197]	10·10+6·7·7
406	[2, 7, 29]	16·16+6·5·5
406	[2, 7, 29]	20·20+6·1·1
409	[409]	5·5+6·8·8
415	[5, 83]	11·11+6·7·7
415	[5, 83]	19·19+6·3·3

表 4: X^2+6Y^2 の値を昇順に直した表

X^2+6Y^2 の値	因数分解	X^2+6Y^2 の形で表記
433	[433]	7·7+6·8·8
439	[439]	17·17+6·5·5
447	[3, 149]	21·21+6·1·1
454	[2, 227]	20·20+6·3·3
457	[457]	19·19+6·4·4
463	[463]	13·13+6·7·7
465	[3, 5, 31]	9·9+6·8·8
465	[3, 5, 31]	21·21+6·2·2
487	[487]	1·1+6·9·9
490	[2, 5, 7, 7]	2·2+6·9·9
490	[2, 5, 7, 7]	22·22+6·1·1
502	[2, 251]	4·4+6·9·9
505	[5, 101]	11·11+6·8·8
505	[5, 101]	17·17+6·6·6
511	[7, 73]	5·5+6·9·9
511	[7, 73]	19·19+6·5·5
519	[3, 173]	15·15+6·7·7
535	[5, 107]	7·7+6·9·9
535	[5, 107]	23·23+6·1·1
537	[3, 179]	21·21+6·4·4
538	[2, 269]	22·22+6·3·3
550	[2, 5, 5, 11]	8·8+6·9·9
550	[2, 5, 5, 11]	16·16+6·7·7
553	[7, 79]	13·13+6·8·8
553	[7, 79]	23·23+6·2·2
577	[577]	19·19+6·6·6
583	[11, 53]	17·17+6·7·7
583	[11, 53]	23·23+6·3·3
586	[2, 293]	10·10+6·9·9
591	[3, 197]	21·21+6·5·5
601	[601]	1·1+6·10·10
607	[607]	11·11+6·9·9
609	[3, 7, 29]	3·3+6·10·10
609	[3, 7, 29]	15·15+6·8·8
625	[5, 5, 5, 5]	23·23+6·4·4
631	[631]	25·25+6·1·1
634	[2, 317]	22·22+6·5·5
649	[11, 59]	7·7+6·10·10
649	[11, 59]	25·25+6·2·2

表 4: X^2+6Y^2 の値を昇順に直した表

X^2+6Y^2 の値	因数分解	X^2+6Y^2 の形で表記
655	[5, 131]	13·13+6·9·9
655	[5, 131]	19·19+6·7·7
673	[673]	17·17+6·8·8
679	[7, 97]	23·23+6·5·5
679	[7, 97]	25·25+6·3·3
681	[3, 227]	9·9+6·10·10
682	[2, 11, 31]	14·14+6·9·9
682	[2, 11, 31]	26·26+6·1·1
694	[2, 347]	20·20+6·7·7
721	[7, 103]	11·11+6·10·10
721	[7, 103]	25·25+6·4·4
727	[727]	1·1+6·11·11
730	[2, 5, 73]	2·2+6·11·11
730	[2, 5, 73]	26·26+6·3·3
735	[3, 5, 7, 7]	3·3+6·11·11
735	[3, 5, 7, 7]	27·27+6·1·1
742	[2, 7, 53]	4·4+6·11·11
742	[2, 7, 53]	16·16+6·9·9
745	[5, 149]	19·19+6·8·8
745	[5, 149]	23·23+6·6·6
751	[751]	5·5+6·11·11
753	[3, 251]	27·27+6·2·2
769	[769]	13·13+6·10·10
775	[5, 5, 31]	7·7+6·11·11
775	[5, 5, 31]	17·17+6·9·9
778	[2, 389]	22·22+6·7·7
790	[2, 5, 79]	8·8+6·11·11
790	[2, 5, 79]	28·28+6·1·1
807	[3, 269]	9·9+6·11·11
823	[823]	23·23+6·7·7
825	[3, 5, 5, 11]	21·21+6·8·8
825	[3, 5, 5, 11]	27·27+6·4·4
826	[2, 7, 59]	10·10+6·11·11
826	[2, 7, 59]	26·26+6·5·5
838	[2, 419]	28·28+6·3·3
841	[29, 29]	25·25+6·6·6
847	[7, 11, 11]	19·19+6·9·9
847	[7, 11, 11]	29·29+6·1·1
865	[5, 173]	1·1+6·12·12

表 4: X^2+6Y^2 の値を昇順に直した表

X^2+6Y^2 の値	因数分解	X^2+6Y^2 の形で表記
865	[5, 173]	29·29+6·2·2
879	[3, 293]	27·27+6·5·5
886	[2, 443]	20·20+6·9·9
889	[7, 127]	5·5+6·12·12
889	[7, 127]	17·17+6·10·10
895	[5, 179]	13·13+6·11·11
895	[5, 179]	29·29+6·3·3
913	[11, 83]	7·7+6·12·12
913	[11, 83]	23·23+6·8·8
919	[919]	25·25+6·7·7
922	[2, 461]	14·14+6·11·11
934	[2, 467]	28·28+6·5·5
937	[937]	29·29+6·4·4
951	[3, 317]	15·15+6·11·11
961	[31, 31]	19·19+6·10·10
967	[967]	31·31+6·1·1
970	[2, 5, 97]	22·22+6·9·9
970	[2, 5, 97]	26·26+6·7·7
982	[2, 491]	16·16+6·11·11
985	[5, 197]	11·11+6·12·12
985	[5, 197]	31·31+6·2·2
991	[991]	29·29+6·5·5

3.6 $X^2 + 7Y^2$ の表

表 5: $X^2 + 7Y^2$ の値を昇順に直した表

$X^2 + 7Y^2$ の値	因数分解	$X^2 + 7Y^2$ の形で表記
8	[2, 2, 2]	1·1+7·1·1
11	[11]	2·2+7·1·1
16	[2, 2, 2, 2]	3·3+7·1·1
23	[23]	4·4+7·1·1
29	[29]	1·1+7·2·2
32	[2, 2, 2, 2, 2]	5·5+7·1·1
37	[37]	3·3+7·2·2
43	[43]	6·6+7·1·1
53	[53]	5·5+7·2·2
64	[2, 2, 2, 2, 2, 2]	1·1+7·3·3
67	[67]	2·2+7·3·3
71	[71]	8·8+7·1·1
79	[79]	4·4+7·3·3
88	[2, 2, 2, 11]	5·5+7·3·3
88	[2, 2, 2, 11]	9·9+7·1·1
107	[107]	10·10+7·1·1
109	[109]	9·9+7·2·2
113	[113]	1·1+7·4·4
121	[11, 11]	3·3+7·4·4
127	[127]	8·8+7·3·3
128	[2, 2, 2, 2, 2, 2, 2]	11·11+7·1·1
137	[137]	5·5+7·4·4
149	[149]	11·11+7·2·2
151	[151]	12·12+7·1·1
163	[163]	10·10+7·3·3
176	[2, 2, 2, 2, 11]	1·1+7·5·5
176	[2, 2, 2, 2, 11]	13·13+7·1·1
179	[179]	2·2+7·5·5
184	[2, 2, 2, 23]	3·3+7·5·5
184	[2, 2, 2, 23]	11·11+7·3·3
191	[191]	4·4+7·5·5
193	[193]	9·9+7·4·4
197	[197]	13·13+7·2·2
211	[211]	6·6+7·5·5
232	[2, 2, 2, 29]	13·13+7·3·3
232	[2, 2, 2, 29]	15·15+7·1·1
233	[233]	11·11+7·4·4
239	[239]	8·8+7·5·5

表 5: $X^2 + 7Y^2$ の値を昇順に直した表

$X^2 + 7Y^2$ の値	因数分解	$X^2 + 7Y^2$ の形で表記
253	[11, 23]	1·1+7·6·6
253	[11, 23]	15·15+7·2·2
256	[2, 2, 2, 2, 2, 2, 2, 2]	9·9+7·5·5
263	[263]	16·16+7·1·1
277	[277]	5·5+7·6·6
281	[281]	13·13+7·4·4
296	[2, 2, 2, 37]	11·11+7·5·5
296	[2, 2, 2, 37]	17·17+7·1·1
317	[317]	17·17+7·2·2
319	[11, 29]	12·12+7·5·5
319	[11, 29]	16·16+7·3·3
331	[331]	18·18+7·1·1
337	[337]	15·15+7·4·4
344	[2, 2, 2, 43]	1·1+7·7·7
344	[2, 2, 2, 43]	13·13+7·5·5
347	[347]	2·2+7·7·7
352	[2, 2, 2, 2, 2, 11]	3·3+7·7·7
352	[2, 2, 2, 2, 2, 11]	17·17+7·3·3
359	[359]	4·4+7·7·7
368	[2, 2, 2, 2, 23]	5·5+7·7·7
368	[2, 2, 2, 2, 23]	19·19+7·1·1
373	[373]	11·11+7·6·6
379	[379]	6·6+7·7·7
389	[389]	19·19+7·2·2
401	[401]	17·17+7·4·4
407	[11, 37]	8·8+7·7·7
407	[11, 37]	20·20+7·1·1
421	[421]	13·13+7·6·6
424	[2, 2, 2, 53]	9·9+7·7·7
424	[2, 2, 2, 53]	19·19+7·3·3
431	[431]	16·16+7·5·5
443	[443]	10·10+7·7·7
449	[449]	1·1+7·8·8
457	[457]	3·3+7·8·8
463	[463]	20·20+7·3·3
464	[2, 2, 2, 2, 29]	11·11+7·7·7
464	[2, 2, 2, 2, 29]	17·17+7·5·5
473	[11, 43]	5·5+7·8·8
473	[11, 43]	19·19+7·4·4

表 5: $X^2 + 7Y^2$ の値を昇順に直した表

$X^2 + 7Y^2$ の値	因数分解	$X^2 + 7Y^2$ の形で表記
487	[487]	12·12+7·7·7
491	[491]	22·22+7·1·1
499	[499]	18·18+7·5·5
512	[2, 2, 2, 2, 2, 2, 2, 2, 2]	13·13+7·7·7
529	[23, 23]	9·9+7·8·8
536	[2, 2, 2, 67]	19·19+7·5·5
536	[2, 2, 2, 67]	23·23+7·1·1
541	[541]	17·17+7·6·6
547	[547]	22·22+7·3·3
557	[557]	23·23+7·2·2
568	[2, 2, 2, 71]	1·1+7·9·9
568	[2, 2, 2, 71]	15·15+7·7·7
569	[569]	11·11+7·8·8
571	[571]	2·2+7·9·9
583	[11, 53]	4·4+7·9·9
583	[11, 53]	24·24+7·1·1
592	[2, 2, 2, 2, 37]	5·5+7·9·9
592	[2, 2, 2, 2, 37]	23·23+7·3·3
599	[599]	16·16+7·7·7
613	[613]	19·19+7·6·6
617	[617]	13·13+7·8·8
631	[631]	8·8+7·9·9
632	[2, 2, 2, 79]	17·17+7·7·7
632	[2, 2, 2, 79]	25·25+7·1·1
641	[641]	23·23+7·4·4
653	[653]	25·25+7·2·2
659	[659]	22·22+7·5·5
667	[23, 29]	10·10+7·9·9
667	[23, 29]	18·18+7·7·7
673	[673]	15·15+7·8·8
683	[683]	26·26+7·1·1
688	[2, 2, 2, 2, 43]	11·11+7·9·9
688	[2, 2, 2, 2, 43]	25·25+7·3·3
701	[701]	1·1+7·10·10
704	[2, 2, 2, 2, 2, 2, 11]	19·19+7·7·7
704	[2, 2, 2, 2, 2, 2, 11]	23·23+7·5·5
709	[709]	3·3+7·10·10
736	[2, 2, 2, 2, 2, 23]	13·13+7·9·9
736	[2, 2, 2, 2, 2, 23]	27·27+7·1·1

表 5: $X^2 + 7Y^2$ の値を昇順に直した表

$X^2 + 7Y^2$ の値	因数分解	$X^2 + 7Y^2$ の形で表記
737	[11, 67]	17·17+7·8·8
737	[11, 67]	25·25+7·4·4
739	[739]	26·26+7·3·3
743	[743]	20·20+7·7·7
751	[751]	24·24+7·5·5
757	[757]	27·27+7·2·2
781	[11, 71]	9·9+7·10·10
781	[11, 71]	23·23+7·6·6
809	[809]	19·19+7·8·8
821	[821]	11·11+7·10·10
823	[823]	16·16+7·9·9
827	[827]	22·22+7·7·7
841	[29, 29]	27·27+7·4·4
848	[2, 2, 2, 2, 53]	1·1+7·11·11
848	[2, 2, 2, 2, 53]	29·29+7·1·1
851	[23, 37]	2·2+7·11·11
851	[23, 37]	26·26+7·5·5
856	[2, 2, 2, 107]	3·3+7·11·11
856	[2, 2, 2, 107]	17·17+7·9·9
863	[863]	4·4+7·11·11
869	[11, 79]	13·13+7·10·10
869	[11, 79]	29·29+7·2·2
872	[2, 2, 2, 109]	5·5+7·11·11
872	[2, 2, 2, 109]	23·23+7·7·7
877	[877]	25·25+7·6·6
883	[883]	6·6+7·11·11
904	[2, 2, 2, 113]	27·27+7·5·5
904	[2, 2, 2, 113]	29·29+7·3·3
907	[907]	30·30+7·1·1
911	[911]	8·8+7·11·11
919	[919]	24·24+7·7·7
928	[2, 2, 2, 2, 2, 29]	9·9+7·11·11
928	[2, 2, 2, 2, 2, 29]	19·19+7·9·9
947	[947]	10·10+7·11·11
953	[953]	29·29+7·4·4
967	[967]	20·20+7·9·9
968	[2, 2, 2, 11, 11]	25·25+7·7·7
968	[2, 2, 2, 11, 11]	31·31+7·1·1
977	[977]	23·23+7·8·8

表 5: $X^2 + 7Y^2$ の値を昇順に直した表

$X^2 + 7Y^2$ の値	因数分解	$X^2 + 7Y^2$ の形で表記
989	[23, 43]	17·17+7·10·10
989	[23, 43]	31·31+7·2·2
991	[991]	12·12+7·11·11

3.7　Z の異なる素因数の個数と方程式 $Z = X^2 + pY^2$ の解の個数の関係

3.7.1　$Z = X^2 + 2Y^2$ の場合

例 **1**、$Z = 11$ のとき

素因数分解 11（異なる素因数は 1 個）,
$Z = 3^2 + 2 \cdot 1^2$（1 個の解）

例 **2**、$Z = 177$ のとき

素因数分解 $3 \cdot 59$（異なる素因数は 2 個）,
$Z = 7^2 + 2 \cdot 8^2$
$= 13^2 + 2 \cdot 2^2$（2 個の解）

例 **3**、$Z = 627$ のとき

素因数分解 $3 \cdot 11 \cdot 19$（異なる素因数は 3 個）,
$Z = 7^2 + 2 \cdot 17^2$
$= 17^2 + 2 \cdot 13^2$
$= 23^2 + 2 \cdot 7^2$
$= 25^2 + 2 \cdot 1^2$（4 個の解）

例 **4**、$Z = 561$ のとき

素因数分解 $3 \cdot 11 \cdot 17$（異なる素因数は 3 個）,
$Z = 7^2 + 2 \cdot 16^2$
$= 13^2 + 2 \cdot 14^2$
$= 19^2 + 2 \cdot 10^2$
$= 23^2 + 2 \cdot 4^2$（4 個の解）

したがって、方程式 $Z = X^2 + 2Y^2$ は Z の異なる素因数が n 個なら 2^{n-1} 個の解を持つ。

（例 4 の補足）素因数分解の因数は 3 と 11 と 17 である。
$Z = 3, 11, 17$ はそれぞれ X, Y の解がある。
$3 = 1^2 + 2 \cdot 1^2$,$11 = 3^2 + 2 \cdot 1^2$,$17 = 3^2 + 2 \cdot 2^2$

$\mathbf{Z}[\sqrt{-2}]$ において
$561 = \left(7 + 16\sqrt{-2}\right)\left(7 - 16\sqrt{-2}\right)$
$= \left(13 + 14\sqrt{-2}\right)\left(13 - 14\sqrt{-2}\right)$
$= \left(19 + 10\sqrt{-2}\right)\left(19 - 10\sqrt{-2}\right)$
$= \left(23 + 4\sqrt{-2}\right)\left(23 - 4\sqrt{-2}\right)$
$3 = \left(1 + \sqrt{-2}\right)\left(1 - \sqrt{-2}\right)$,$11 = \left(3 + \sqrt{-2}\right)\left(3 - \sqrt{-2}\right)$,$17 = \left(3 + 2\sqrt{-2}\right)\left(3 - 2\sqrt{-2}\right)$ となる。
$\alpha = 1 + \sqrt{-2}$,$\beta = 3 + \sqrt{-2}$,$\gamma = 3 + 2\sqrt{-2}$ とおく。
$\alpha\beta\gamma = 13 + 14\sqrt{-2}$, $\alpha\beta\bar{\gamma} = 19 + 10\sqrt{-2}$,
$\alpha\bar{\beta}\gamma = 7 + 16\sqrt{-2}$,$\bar{\alpha}\beta\gamma = 23 + 4\sqrt{-2}$
$Z = \alpha\beta\gamma \cdot \bar{\alpha}\bar{\beta}\bar{\gamma} = \alpha\beta\bar{\gamma} \cdot \bar{\alpha}\bar{\beta}\gamma = \alpha\bar{\beta}\gamma \cdot \bar{\alpha}\beta\bar{\gamma} = \bar{\alpha}\beta\gamma \cdot \alpha\bar{\beta}\bar{\gamma}$

3.7.2　$Z = X^2 + 3Y^2$ の場合

例 1、$Z = 7$

　素因数分解 7（異なる素因数は 1 個），
$Z = 2^2 + 3 \cdot 1^2$（1 個の解）

例 2、$Z = 52$

　素因数分解 $2 \cdot 2 \cdot 13$（異なる素因数は 2 個），
$Z = 5^2 + 3 \cdot 3^2$
$= 7^2 + 3 \cdot 1^2$（2 個の解）

例 3、$Z = 76$

　素因数分解 $2 \cdot 2 \cdot 19$（異なる素因数は 2 個），
$Z = 1^2 + 3 \cdot 5^2$
$= 7^2 + 3 \cdot 3^2$（2 個の解）

例 4、$Z = 364$

　素因数分解 $2 \cdot 2 \cdot 7 \cdot 13$（異なる素因数は 3 個），
$Z = 1^2 + 3 \cdot 11^2$
$= 11^2 + 3 \cdot 9^2$
$= 17^2 + 3 \cdot 5^2$
$= 19^2 + 3 \cdot 1^2$（4 個の解）

　したがって、方程式 $Z = X^2 + 3Y^2$ は Z の異なる素因数が n 個なら 2^{n-1} 個の解を持つ。

（例 4 の補足）素因数分解の因数は 2 と 7 と 13 である。
$Z = 7, 13$ はそれぞれ X, Y の解がある。
$7 = 2^2 + 3 \cdot 1^2$,$13 = 1^2 + 3 \cdot 2^2$
$Z = 2$ は解がないので仕方ないので、解のある $Z = 4$ を使う。
$4 = 1^2 + 3 \cdot 1^2$

$\mathbf{Z}[\sqrt{-3}]$ において
$364 = \left(1 + 11\sqrt{-3}\right)\left(1 - 11\sqrt{-3}\right)$
$= \left(11 + 9\sqrt{-3}\right)\left(11 - 9\sqrt{-3}\right)$
$= \left(17 + 5\sqrt{-3}\right)\left(17 - 5\sqrt{-3}\right)$
$= \left(19 + \sqrt{-3}\right)\left(19 - \sqrt{-3}\right)$
$4 = \left(1 + \sqrt{-3}\right)\left(1 - \sqrt{-3}\right)$,$7 = \left(2 + \sqrt{-3}\right)\left(2 - \sqrt{-3}\right)$,$13 = \left(1 + 2\sqrt{-3}\right)\left(1 - 2\sqrt{-3}\right)$ となる。
$\alpha = 1 + \sqrt{-3}$,$\beta = 2 + \sqrt{-3}$,$\gamma = 1 + 2\sqrt{-3}$ とおく。
$\alpha\beta\gamma = -19 + \sqrt{-3}$, $\alpha\beta\bar{\gamma} = 17 + 5\sqrt{-3}$,
$\alpha\bar{\beta}\gamma = -1 + 11\sqrt{-3}$,$\bar{\alpha}\beta\gamma = 11 + 9\sqrt{-3}$
$364 = \alpha\beta\gamma \cdot \bar{\alpha}\bar{\beta}\bar{\gamma} = \alpha\beta\bar{\gamma} \cdot \bar{\alpha}\bar{\beta}\gamma = \alpha\bar{\beta}\gamma \cdot \bar{\alpha}\beta\bar{\gamma} = \bar{\alpha}\beta\gamma \cdot \alpha\bar{\beta}\bar{\gamma}$

3.7.3　$Z = X^2 + 7Y^2$ の場合

例 1、$Z = 16$

　素因数分解 $2 \cdot 2 \cdot 2 \cdot 2$ （異なる素因数は 1 個），
$X^2 + 7Y^2 = 5^2 + 7 \cdot 3^2$（1 個の解）

例 2、$Z = 176$

　素因数分解 $2 \cdot 2 \cdot 2 \cdot 2 \cdot 11$ （異なる素因数は 2 個），
$Z = 1^2 + 7 \cdot 5^2$
$= 13^2 + 7 \cdot 1^2$（2 個の解）

例 3、$Z = 352$

　素因数分解 $2 \cdot 2 \cdot 2 \cdot 2 \cdot 2 \cdot 11$ （異なる素因数は 2 個），
$Z = 3^2 + 7 \cdot 7^2$
$= 17^2 + 7 \cdot 3^2$（2 個の解）

　したがって、方程式 $Z = X^2 + 7Y^2$ は Z の異なる素因数が n 個なら 2^{n-1} 個の解を持つ。

　（例 3 の補足）素因数分解の因数は 2 と 11 である。
$Z = 11$ はそれぞれ X, Y の解がある。
$11 = 2^2 + 7 \cdot 1^2$
$Z = 2$ は解がないので仕方ないので、解のある $Z = 32$ を使う。
$32 = 5^2 + 7 \cdot 2^2$

$\mathbf{Z}[\sqrt{-7}]$ において
$352 = \left(3 + 7\sqrt{-7}\right)\left(3 - 7\sqrt{-3}\right)$
　$= \left(17 + 3\sqrt{-7}\right)\left(17 - 3\sqrt{-3}\right)$
$11 = \left(2 + \sqrt{-7}\right)\left(2 - \sqrt{-7}\right)$,$32 = \left(5 + \sqrt{-7}\right)\left(5 - \sqrt{-7}\right)$ となる。
$\alpha = 2 + \sqrt{-7}$,$\beta = 5 + \sqrt{-7}$ とおく。
$\alpha\beta = 3 + 7\sqrt{-3}$,　$\alpha\bar{\beta} = 17 + 3\sqrt{-3}$,
$352 = \alpha\beta \cdot \bar{\alpha}\bar{\beta} = \alpha\bar{\beta} \cdot \bar{\alpha}\beta$

3.7.4　$Z = X^2 + 5Y^2$ の場合

例 1、$Z = 161$

　素因数分解 $7 \cdot 23$（異なる素因数は 2 個）
$Z = 6^2 + 5 \cdot 5^2$
$= 9^2 + 5 \cdot 4^2$ （2 個の解）

例 2、$Z = 609$

　素因数分解 $3 \cdot 7 \cdot 29$（異なる素因数は 3 個）
$Z = 2^2 + 5 \cdot 11^2$
$= 17^2 + 5 \cdot 8^2$
$= 22^2 + 5 \cdot 5^2$
$= 23^2 + 5 \cdot 4^2$ （4 個の解）

反例 1、$Z = 14$

　素因数分解 $2 \cdot 7$（異なる素因数は 2 個）
$Z = 3^2 + 5 \cdot 1^2$ （1 個の解）

反例 2、$Z = 126$

　素因数分解 $2 \cdot 3 \cdot 3 \cdot 7$（異なる素因数は 3 個）
$Z = 1^2 + 5 \cdot 5^2$
$= 11^2 + 5 \cdot 1^2$ （2 個の解）

　方程式 $Z = X^2 + 5Y^2$ は、必ずしも異なる素因数が n 個なら、$2^n - 1$ 個の分解になるとは限らない。
反例 1，2 のように Z が 2 の倍数のとき、規則性が乱れてる。

3.7.5　$Z = X^2 + 6Y^2$ の場合

例 1、$Z = 55$

　素因数分解 $5 \cdot 11$（異なる素因数は 2 個）
$Z = 1^2 + 6 \cdot 3^2$
$= 7^2 + 6 \cdot 1^2$ （2 個の解）

例 2、$Z = 385$

　素因数分解 $5 \cdot 7 \cdot 11$（異なる素因数は 3 個）
$Z = 1^2 + 6 \cdot 8^2$
$= 13^2 + 6 \cdot 6^2$
$= 17^2 + 6 \cdot 4^2$
$= 19^2 + 6 \cdot 2^2$ （4 個の解）

（例 2 の補足）素因数分解の因数は 5 と 7 と 11 である。
$Z=7$ はそれぞれ X,Y の解がある。
$7=1^2+6\cdot 1^2$
$Z=5,11$ は解がないし、$Z=55$ は解が 2 つでるので使えない。
$\mathbf{Z}[\sqrt{-6}]$ において 5,11 は既約元だが、素元ではない。
後に既約元 (3), (11) について剰余環で考える。

$\mathbf{Z}[\sqrt{-6}]$ において
$385=\left(1+8\sqrt{-6}\right)\left(1-8\sqrt{-6}\right)$
$\quad=\left(13+6\sqrt{-6}\right)\left(13-6\sqrt{-6}\right)$
$\quad=\left(17+4\sqrt{-6}\right)\left(17-4\sqrt{-6}\right)$
$\quad=\left(19+2\sqrt{-6}\right)\left(19-2\sqrt{-6}\right)$
$7=\left(1+\sqrt{-6}\right)\left(1-\sqrt{-6}\right)$

5,11 をどう扱うか？
$55=\left(7+\sqrt{-6}\right)\left(7-\sqrt{-6}\right)=\left(1+3\sqrt{-6}\right)\left(1-3\sqrt{-6}\right)$
$J_1=(5,7+\sqrt{-6}),\ \ J_2=(11,7+\sqrt{-6})$
$J_1J_2=(5\cdot 11,7+\sqrt{-6},11(7+\sqrt{-6}),5(3+2\sqrt{-6}))$
$5\cdot 11=\left(7+\sqrt{-6}\right)\left(7-\sqrt{-6}\right)$
$15+12\sqrt{-6}=(7+\sqrt{-6})^2$
よって、$J_1J_2=(7+\sqrt{-6})$
したがって $5\cdot 11=J_1J_2\bar{J}_1\bar{J}_2$ であり、素イデアルの積で表せる。

$J_3=(5,1+3\sqrt{-6}),\ \ J_4=(11,1+3\sqrt{-6})$
$J_3J_4=(5\cdot 11,-17+6\sqrt{-6},11(1+3\sqrt{-6}),5(1+3\sqrt{-6}))$
$5\cdot 11=\left(1+3\sqrt{-6}\right)\left(1-3\sqrt{-6}\right)$
$-17+6\sqrt{-6}=(1+3\sqrt{-6})^2$
よって、$J_3J_4=(1+3\sqrt{-6})$
したがって $5\cdot 11=J_3J_4\bar{J}_3\bar{J}_4$ であり、素イデアルの積で表せる。

$\alpha=1+\sqrt{-6}$ とおく。
$385=\alpha\bar{\alpha}J_1J_2\bar{J}_1\bar{J}_2=\alpha\bar{\alpha}J_3J_4\bar{J}_3\bar{J}_4$

反例 1、$Z = 22$

素因数分解 $2 \cdot 11$（異なる素因数は 2 個）
$Z = 4^2 + 6 \cdot 1^2$（1 個の解）

反例 2、$Z = 231$

素因数分解 $3 \cdot 7 \cdot 11$（異なる素因数は 3 個）
$Z = 9^2 + 6 \cdot 5^2$
$= 15^2 + 6 \cdot 1^2$ （2 個の解）

（反例 2 の補足）素因数分解の因数は 3 と 7 と 11 である。
$Z = 7$ はそれぞれ X, Y の解がある。
$7 = 1^2 + 6 \cdot 1^2$
$Z = 3, 11$ は解がないので仕方ないので、解のある $Z = 33$ を使う。
$33 = 3 \cdot 11 = 3^2 + 6 \cdot 2^2$
しかし、$\mathbf{Z}[\sqrt{-6}]$ において 3,11 は既約元だが、素元ではない。
後に既約元 (3), (11) について剰余環で考える。

$33 = \left(3 + 2\sqrt{-6}\right)\left(3 - 2\sqrt{-6}\right)$
$J_1 = (3, 3 + 2\sqrt{-6})$, $J_2 = (11, 3 + 2\sqrt{-6})$
$J_1 J_2 = (3 \cdot 11, 15 + 12\sqrt{-6}, 11(3 + 2\sqrt{-6}), 3(3 + 2\sqrt{-6}))$
$3 \cdot 11 = \left(3 + 2\sqrt{-6}\right)\left(3 - 2\sqrt{-6}\right)$
$15 + 12\sqrt{-6} = (3 + 2\sqrt{-6})^2$
よって、$J_1 J_2 = (3 + 2\sqrt{-6})$
したがって $3 \cdot 11 = J_1 J_2 \bar{J_1} \bar{J_2}$ であり、素イデアルの積で表せる。

$\alpha = 1 + \sqrt{-6}$ とおく。
$231 = \alpha\bar{\alpha} J_1 J_2 \bar{J_1} \bar{J_2}$

方程式 $Z = X^2 + 6Y^2$ は、必ずしも異なる素因数が n 個なら、$2^n - 1$ 個の分解になるとは限らない。
反例 1，2 のように Z が 2 の倍数または 3 の倍数のとき、規則性が乱れてる。
方程式 $Z = X^2 + 6Y^2$ については剰余環を使って Z の数を調べる。

4　考察

4.1　平方剰余を用いた証明

結果で書いたように、Z から奇素数だけを取り出して考えると、$p = 6$ のとき、$Z \equiv 1, 7 \bmod 24$ を満たすという証明を平方剰余の相互法則などを用いて証明する。
以下、証明に必要な定義や法則を記述する。

平方剰余

定義

a は p を法とするとき平方数 x^2 と合同とする。すなわち、$x^2 \equiv a \bmod p$ として x が解を持つとき、a は p を法として平方剰余であるといい、$(\frac{a}{p}) = 1$ と記述する。x が解を持たないとき、a は p を法として平方非剰余であるといい、$(\frac{a}{p}) = -1$ と記述する。

平方剰余の相互法則

平方剰余の相互法則は整数 a が奇素数 p を法として平方剰余であるか判定する法則である。
p, q を相異なる奇素数とするとき、$(\frac{p}{q})(\frac{q}{p}) = (-1)^{(\frac{p-1}{2})(\frac{q-1}{2})}$ が成り立つ。

第一補充法則

p を奇素数とするとき、$(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}}$ が成り立つ。

第二補充法則

p を奇素数とするとき、$(\frac{2}{p}) = (-1)^{\frac{p^2-1}{8}}$ が成り立つ。

その他

☒ p と a, b が素であれば、$(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$ が成り立つ。
☒ ab が平方剰余 $\Longleftrightarrow$ a と b も平方剰余である。
☒ ab が平方非剰余 $\Longleftrightarrow$ a と b の一方が平方非剰余である。

証明

$Z = X^2 + 6Y^2$, Z は奇素数, 任意の奇素数 k に対して、$X \neq 0 \mod k$ とする。
k で Z が割り切れるとき、$Z = X^2 + 6Y^2$ を $\mod k$ で考えると、

$$X^2 = -6Y^2 \mod k$$

$Y \mod k$ の逆元を U とすると、

$$(UX)^2 = -6 \mod k$$

-6 が k を法として平方剰余になる必要十分条件は $(\frac{-6}{k}) = 1$ である。
$(\frac{-6}{k}) = 1$ になる必要十分条件が $k \equiv 1, 7 \mod 24$ であることを平方剰余を用いて証明する。
平方剰余の定義より、$x^2 \equiv a \bmod k$ として x が解を持つとき、$(\frac{a}{k}) = 1$ である。
今、$(\frac{-6}{k}) = 1$ になる必要十分条件を考えているので、$a = -6$ とおき、$(\frac{-6}{k}) = 1$ となる k を調べる。
その他☒より $(\frac{-6}{k}) = (\frac{-1}{k})(\frac{2}{k})(\frac{3}{k})$ とできる。
$(\frac{-1}{k})(\frac{2}{k})(\frac{3}{k}) = 1$ を考える。

☒、$(\frac{-1}{k})$ について
任意の自然数 n に対して、$k = 8n + 1$ とおくと、第一補充法則を用いて、$(\frac{-1}{k}) = (-1)^{\frac{k-1}{2}} = (-1)^{\frac{8n}{2}} = 1$,
$k = 8n - 1$ とおくと、$(\frac{-1}{k}) = (-1)^{\frac{k-1}{2}} = (-1)^{\frac{8n-2}{2}} = -1$ となる。
よって、$(\frac{-1}{k}) = 1 \Longleftrightarrow k \equiv 1 \mod 8, (\frac{-1}{k}) = -1 \Longleftrightarrow k \equiv 7 \mod 8$
☒、$(\frac{2}{k})$ について
☒と同様に、$k = 8n + 1$ とおくと、第二補充法則を用いて、$(\frac{2}{k}) = (-1)^{\frac{k^2-1}{8}} = (-1)^{\frac{64n^2+16n}{8}} = 1$,
$k = 8n - 1$ とおくと、$(\frac{2}{k}) = (-1)^{\frac{k^2-1}{8}} = (-1)^{\frac{64n^2-16n}{8}} = 1$ となる。
よって、$(\frac{-1}{k}) = 1 \Longleftrightarrow k \equiv 1, 7 \mod 8$
☒、平方剰余の相互法則より、$(\frac{3}{k})(\frac{k}{3}) = (-1)^{(\frac{3-1}{2})(\frac{k-1}{2})} = 1$
その他☒より、$(\frac{k}{3}) = 1 \Longleftrightarrow k \equiv 1 \mod 3$

したがって、
・$k \equiv 1, 7 \mod 8 \to 1, 7, 9, 15, 17, 23, 25, 31, 33, 39, 41, 47, 49, 55, \cdots$
・$k \equiv 1 \mod 3 \to 1, 4, 7, 10, 13, 16, 19, 22, 25, 28, 31, 34, 37, 40, 43, 46, 49, 52, 55, \cdots$
2 つの共通部分を抜き出すと $1, 7, 25, 31, 49, 55, \cdots$ となり、これは、 $k \equiv 1, 7 \mod 24$ を満たす。

$p = 2, 3, 5, 7$ の場合も $p = 6$ の場合と同様にできる。

4.2　剰余環とイデアル分解

$\mathbf{Z}[\sqrt{-6}] = \left\{a + b\sqrt{-6} : a, b \in \mathbf{Z}\right\}$ において、既約元 α について、(α) による剰余環が体になるか、環の直和または体の無限小拡大環になることを例を出しながら確認する。
$\mathbf{Z}[\sqrt{-5}]$ については同じ研究課題の坂本君のを参考にしてください。

$Z = X^2 + 6Y^2$ の場合

$\mathbf{Z}[\sqrt{-6}] = \left\{a + b\sqrt{-6} : a, b \in \mathbf{Z}\right\}$ 上で考える。
$\mathbf{Z}[\sqrt{-6}]$ の剰余環は、$\mathbf{Z}[\sqrt{-6}] \cong \mathbf{Z}[X]/(X^2 + 6)$ である。

4.2.1　(α) による剰余環が体になる場合

$\mathbf{Z}[\sqrt{-6}]$ において、既約元 (α) が素元になる場合

例 1、$Z = 7$

$$7 = (1 + \sqrt{-6})(1 - \sqrt{-6})$$

$\alpha = 1 + \sqrt{-6}$,$J = (X^2 + 6, 1 + X)$ とおく。
$\mathbf{Z}[\sqrt{-6}]/(\alpha) \cong \mathbf{Z}[X]/J$
$1 + X$ を Y とおく（$X = Y - 1$）と $J = (Y^2 - 2Y + 7, Y) \supset (Y)$ となる。
よって $\mathbf{Z}[X]/J \cong (\mathbf{Z}[Y]/(Y))/J \cong \mathbf{Z}/(7) \cong \mathbf{F}_7$
したがって、(α) による剰余環は体になる。

例 2、$Z = 31$

$$31 = (5 + \sqrt{-6})(5 - \sqrt{-6})$$

$\alpha = 5 + \sqrt{-6}$,$J = (X^2 + 6, 5 + X)$ とおく。
$\mathbf{Z}[\sqrt{-6}]/(\alpha) \cong \mathbf{Z}[X]/J$
$5 + X$ を Y とおく（$X = Y - 5$）と $J = (Y^2 - 10Y + 31, Y) \supset (Y)$ となる。
よって $\mathbf{Z}[X]/J \cong (\mathbf{Z}[Y]/(Y))/J \cong \mathbf{Z}/(31) \cong \mathbf{F}_{31}$
したがって、(α) による剰余環は体になる。

例 3、$Z = 73$

$$73 = (7 + 2\sqrt{-6})(7 - 2\sqrt{-6})$$

$\alpha = 7 + 2\sqrt{-6}$,$J = (X^2 + 6, 7 + 2X)$ とおく。

$\mathbf{Z}[\sqrt{-6}]/(\alpha) \cong \mathbf{Z}[X]/J$
$2\left(X^2+6\right)-(X-3)(7+2X)=33-X$
$33-X$ を Y とおく（$X=33-Y$）と $J=(Y^2-66Y+1095, 73-2Y)$ となる。
$1095=73\cdot 5$ より、 $\mathbf{Z}[X]/J \cong (\mathbf{Z}[Y]/(Y))/J \cong \mathbf{Z}/(73) \cong \mathbf{F}_{73}$
したがって、(α) による剰余環は、体になる。

例 4、$Z=79$

$$73=(5+3\sqrt{-6})(5-3\sqrt{-6})$$

$\alpha=5+3\sqrt{-6}$,$J=(X^2+6, 5+3X)$ とおく。
$\mathbf{Z}[\sqrt{-6}]/(\alpha) \cong \mathbf{Z}[X]/J$
$3\left(X^2+6\right)-(X-2)(5+3X)=X+28$
$X+28$ を Y とおく（$X=Y-28$）と $J=(Y^2-56Y+790, 3Y-79)$ となる。
$790=79\cdot 10$ より、 $\mathbf{Z}[X]/J \cong (\mathbf{Z}[Y]/(Y))/J \cong \mathbf{Z}/(79) \cong \mathbf{F}_{79}$
したがって、(α) による剰余環は、体になる。

例 5、$Z=97$

$$97=(1+4\sqrt{-6})(1-4\sqrt{-6})$$

$\alpha=1+4\sqrt{-6}$,$J=(X^2+6, 1+4X)$ とおく。
$\mathbf{Z}[\sqrt{-6}]/(\alpha) \cong \mathbf{Z}[X]/J$
$4\left(X^2+6\right)-X(1+4X)=24-X$
$24-X$ を Y とおく（$X=24-Y$）と $J=(Y^2-2Y+582, 97-4Y)$ となる。
$582=97\cdot 6$ より、 $\mathbf{Z}[X]/J \cong (\mathbf{Z}[Y]/(Y))/J \cong \mathbf{Z}/(97) \cong \mathbf{F}_{97}$
したがって、(α) による剰余環は、体になる。

例 6、$Z=103$

$$103=(7+3\sqrt{-6})(7-3\sqrt{-6})$$

$\alpha=7+3\sqrt{-6}$,$J=(X^2+6, 7+3X)$ とおく。
$\mathbf{Z}[\sqrt{-6}]/(\alpha) \cong \mathbf{Z}[X]/J$
$3\left(X^2+6\right)-(X-2)(7+3X)=32-X$
$32-X$ を Y とおく（$X=32-Y$）と $J=(Y^2-2Y+1030, 103-3Y)$ となる。
$1030=103\cdot 10$ より、 $\mathbf{Z}[X]/J \cong (\mathbf{Z}[Y]/(Y))/J \cong \mathbf{Z}/(103) \cong \mathbf{F}_{103}$
したがって、(α) による剰余環は、体になる。

例 **7**、$Z = 127$

$$127 = (11 + \sqrt{-6})(11 - \sqrt{-6})$$

$\alpha = 11 + \sqrt{-6}$,$J = (X^2 + 6, 11 + X)$ とおく。
$\mathbf{Z}[\sqrt{-6}]/(\alpha) \cong \mathbf{Z}[X]/J$
$\left(X^2 + 6\right) - (X - 12)(11 + X) = X + 138$
$X + 138$ を Y とおく（$X = Y - 138$）と $J = (Y^2 - 276Y + 19050, Y - 127)$ となる。
$19050 = 127 \cdot 150$ より、 $\mathbf{Z}[X]/J \cong (\mathbf{Z}[Y]/(Y))/J \cong \mathbf{Z}/(127) \cong \mathbf{F}_{127}$
したがって、(α) による剰余環は、体になる。

例 **8**、$Z = 151$

$$151 = (1 + 5\sqrt{-6})(1 - 5\sqrt{-6})$$

$\alpha = 1 + 5\sqrt{-6}$,$J = (X^2 + 6, 1 + 5X)$ とおく。
$\mathbf{Z}[\sqrt{-6}]/(\alpha) \cong \mathbf{Z}[X]/J$
$5\left(X^2 + 6\right) - X(1 + 5X) = 30 - X$
$30 - X$ を Y とおく（$X = 30 - Y$）と $J = (Y^2 - 60Y + 906, 151 - 5Y)$ となる。
$906 = 6 \cdot 151$ より、 $\mathbf{Z}[X]/J \cong (\mathbf{Z}[Y]/(Y))/J \cong \mathbf{Z}/(151) \cong \mathbf{F}_{151}$
したがって、(α) による剰余環は、体になる。

例 **9**、$Z = 199$

$$199 = (7 + 5\sqrt{-6})(7 - 5\sqrt{-6})$$

$\alpha = 7 + 5\sqrt{-6}$,$J = (X^2 + 6, 7 + 5X)$ とおく。
$\mathbf{Z}[\sqrt{-6}]/(\alpha) \cong \mathbf{Z}[X]/J$
$15\left(X^2 + 6\right) - (3X - 4)(7 + 5X) = 118 - X$
$118 - X$ を Y とおく（$X = 118 - Y$）と $J = (Y^2 - 236Y + 13930, 597 - 5Y)$ となる。
$13930 = 199 \cdot 3,\ 597 = 199 \cdot 70$ より、 $\mathbf{Z}[X]/J \cong (\mathbf{Z}[Y]/(Y))/J \cong \mathbf{Z}/(199) \cong \mathbf{F}_{199}$
したがって、(α) による剰余環は、体になる。

例 **10**、$Z = 223$

$$223 = (13 + 3\sqrt{-6})(13 - 3\sqrt{-6})$$

$\alpha = 13 + 3\sqrt{-6}$,$J = (X^2 + 6, 13 + 3X)$ とおく。
$\mathbf{Z}[\sqrt{-6}]/(\alpha) \cong \mathbf{Z}[X]/J$
$3\left(X^2 + 6\right) - (X - 4)(13 + 3X) = 70 - X$

$70-X$ を Y とおく（$X=70-Y$）と $J=(Y^2-140Y+4906, 223-3Y)$ となる。
$4906=223\cdot 22$ より、 $\mathbf{Z}[X]/J\cong(\mathbf{Z}[Y]/(Y))/J\cong\mathbf{Z}/(223)\cong\mathbf{F}_{223}$
したがって、(α) による剰余環は、体になる。

例 **11**、$Z=241$

$$73=(5+6\sqrt{-6})(5-6\sqrt{-6})$$

$\alpha=5+6\sqrt{-6}$,$J=(X^2+6, 5+6X)$ とおく。
$\mathbf{Z}[\sqrt{-6}]/(\alpha)\cong\mathbf{Z}[X]/J$
$2\left(X^2+6\right)-(X-1)(5+6X)=41-X$
$41-X$ を Y とおく（$X=41-Y$）と $J=(Y^2-82Y+1687, 6Y-241)$ となる。
$1687=241\cdot 7$ より、 $\mathbf{Z}[X]/J\cong(\mathbf{Z}[Y]/(Y))/J\cong\mathbf{Z}/(241)\cong\mathbf{F}_{241}$
したがって、(α) による剰余環は、体になる。

例 **12**、$Z=271$

$$271=(11+5\sqrt{-6})(11-5\sqrt{-6})$$

$\alpha=11+5\sqrt{-6}$,$J=(X^2+6, 11+5X)$ とおく。
$\mathbf{Z}[\sqrt{-6}]/(\alpha)\cong\mathbf{Z}[X]/J$
$5\left(X^2+6\right)-(X-2)(11+5X)=52-X$
$52-X$ を Y とおく（$X=52-Y$）と $J=(Y^2-104Y+2710, 271-5Y)$ となる。
$2710=271\cdot 10$ より、 $\mathbf{Z}[X]/J\cong(\mathbf{Z}[Y]/(Y))/J\cong\mathbf{Z}/(271)\cong\mathbf{F}_{271}$
したがって、(α) による剰余環は、体になる。

例 **13**、$Z=313$

$$313=(17+2\sqrt{-6})(17-2\sqrt{-6})$$

$\alpha=17+2\sqrt{-6}$,$J=(X^2+6, 17+2X)$ とおく。
$\mathbf{Z}[\sqrt{-6}]/(\alpha)\cong\mathbf{Z}[X]/J$
$2\left(X^2+6\right)-(X-8)(17+2X)=148-X$
$148-X$ を Y とおく（$X=148-Y$）と $J=(Y^2-296Y+21910, 313-2Y)$ となる。
$21910=313\cdot 70$ より、 $\mathbf{Z}[X]/J\cong(\mathbf{Z}[Y]/(Y))/J\cong\mathbf{Z}/(313)\cong\mathbf{F}_{313}$
したがって、(α) による剰余環は、体になる。

例 14、$Z = 367$

$$367 = (19 + \sqrt{-6})(19 - \sqrt{-6})$$

$\alpha = 19 + \sqrt{-6}$,$J = (X^2 + 6, 19 + X)$ とおく。
$\mathbf{Z}[\sqrt{-6}]/(\alpha) \cong \mathbf{Z}[X]/J$
$X^2 + 6 - (X - 20)(19 + X) = X + 386$
$X + 386$ を Y とおく（$X = Y - 386$) と $J = (Y^2 - 772Y + 149002, Y - 367)$ となる。
$149002 = 367 \cdot 406$ より、 $\mathbf{Z}[X]/J \cong (\mathbf{Z}[Y]/(Y))/J \cong \mathbf{Z}/(367) \cong \mathbf{F}_{367}$
したがって、(α) による剰余環は、体になる。

4.2.2 (α) による剰余環が環の直和または体の無限小拡大環になる場合

$\mathbf{Z}[\sqrt{-6}]$ において、既約元 (α) が素元にならない場合

例 **1**、$Z = 10$

$2 \cdot 5 = (2 + \sqrt{-6})(2 - \sqrt{-6})$

$J = (X^2 + 6, 5)$ とおく。
$\mathbf{Z}[\sqrt{-6}]/(5) \cong \mathbf{Z}[X]/J$
$X^2 + 6 - 5 \cdot 2 = X^2 - 4 = (X - 2)(X + 2)$
$X + 2$ を Y とおく（$X = Y - 2$) と $(X - 2)(X + 2) = Y(Y + 4)$
$J_1 = (Y(Y + 4), 5) \supset (5)$ とおく。
$\mathbf{Z}[X]/J = \mathbf{Z}[Y]/J_1 \cong (\mathbf{Z}[Y]/(5))/(Y(Y + 4)) \cong \mathbf{F}_5[Y]/(Y(Y + 4)) \cdots \Delta$
$4x \equiv 1 \bmod 5$ を満たす x を求めるため、$5a + 4b = 1$ を満たす a, b の解を出す。$5a + 4b = 1$ を満たす a, b は、$a = 1, b = -1$ であり、 $x = -1$ である。
$A = -(Y + 4),\ B = Y$ とおく。 （$-(Y + 4) \bmod 5 \equiv 1 - Y$）
$AB \in (Y^2 + 4Y),\ A + B = 1$
$\mathbf{F}_5[Y]/(1 - Y) = \mathbf{F}_5$
$\mathbf{F}_5[Y]/(B) = \mathbf{F}_5$
Δ より $\mathbf{Z}[X]/J \cong \mathbf{F}_5[Y]/(Y(Y + 4)) \cong \mathbf{F}_5[Y]/(A) \oplus \mathbf{F}_5[Y]/(B) \cong \mathbf{F}_5 \oplus \mathbf{F}_5$
したがって、(5) による剰余環は、環の直和になる。

$J = (X^2 + 6, 2)$ とおく。
$\mathbf{Z}[\sqrt{-6}]/(2) \cong \mathbf{Z}[X]/J$
$X^2 + 6 - 2 \cdot 3 = X^2$
したがって、(2) による剰余環は、無限小拡大環になる。

$\alpha = 2 + \sqrt{-6}$,$J = (X^2 + 6, 2 + X)$ とおく。
$\mathbf{Z}[\sqrt{-6}]/(\alpha) \cong \mathbf{Z}[X]/J$
$X + 2$ を Y とおく（$X = Y - 2$) と $J = (Y^2 - 4Y + 10, Y) \supset (Y)$ となる。
$\mathbf{Z}[X]/J \cong (\mathbf{Z}[Y]/(Y))/J \cong \mathbf{Z}/(10) \cong \mathbf{Z}/(2) \oplus \mathbf{Z}/(5) = \mathbf{F}_2 \oplus \mathbf{F}_5$
したがって、(α) による剰余環は、環の直和になる。

例 **2**、$Z = 15$

$3 \cdot 5 = (3 + \sqrt{-6})(3 - \sqrt{-6})$

例 1 より、(5) による剰余環は、$\mathbf{Z}[\sqrt{-6}]/(5) \cong \mathbf{F}_5 \oplus \mathbf{F}_5$ となり、環の直和になる。
$J = (X^2 + 6, 3)$ とおく。
$\mathbf{Z}[\sqrt{-6}]/(3) \cong \mathbf{Z}[X]/J$
$X^2 + 6 - 3 \cdot 2 = X^2$
したがって、(3) による剰余環は、無限小拡大環になる。

$\alpha = 3 + \sqrt{-6}$,$J = (X^2 + 6, 3 + X)$ とおく。
$\mathbf{Z}[\sqrt{-6}]/(\alpha) \cong \mathbf{Z}[X]/J$
$X + 3$ を Y とおく（$X = Y - 3$) と $J = (Y^2 - 6Y + 15, Y) \supset (Y)$ となる。
$\mathbf{Z}[X]/J \cong (\mathbf{Z}[Y]/(Y))/J \cong \mathbf{Z}/(15) \cong \mathbf{Z}/(3) \oplus \mathbf{Z}/(5) = \mathbf{F}_3 \oplus \mathbf{F}_5$
したがって、(α) による剰余環は、環の直和になる。

例 3、$Z = 22$

$2 \cdot 11 = (4 + \sqrt{-6})(4 - \sqrt{-6})$

例 1 より、(2) による剰余環は、無限小拡大環になる。

$J = (X^2 + 6, 11)$ とおく。
$\mathbf{Z}[\sqrt{-6}]/(11) \cong \mathbf{Z}[X]/J$
$X^2 + 6 - 11 \cdot 2 = X^2 - 16 = (X - 4)(X + 4)$
$X + 4$ を Y とおく（$X = Y - 4$) と $(X - 4)(X + 4) = Y(Y + 8)$
$J_1 = (Y(Y + 8), 11) \supset (11)$ とおく。
$\mathbf{Z}[X]/J = \mathbf{Z}[Y]/J_1 \cong (\mathbf{Z}[Y]/(11))/(Y(Y + 8)) \cong \mathbf{F}_{11}[Y]/(Y(Y + 8)) \cdots \Delta$
$8x \equiv 1 \bmod 11$ を満たす x を求めるため、$11a + 8b = 1$ を満たす a, b の解を出す。$11a + 8b = 1$ を満たす a, b は、$a = 3, b = -4$ であり、 $x = -4$ である。
$A = -4(Y + 8)$, $B = 4Y$ （ $-4(Y + 8) \bmod 11 \equiv 1 - 4Y$ ）
$AB \in (Y^2 + 8Y)$, $A + B = 1$
$\mathbf{F}_{11}[Y]/(1 - 4Y) = \mathbf{F}_{11}$
$\mathbf{F}_{11}[Y]/(B) = \mathbf{F}_{11}$
Δ より $\mathbf{Z}[X]/J \cong \mathbf{F}_{11}[Y]/(Y(Y + 8)) \cong \mathbf{F}_{11}[Y]/(A) \oplus \mathbf{F}_{11}[Y]/(B) \cong \mathbf{F}_{11} \oplus \mathbf{F}_{11}$
したがって、(11) による剰余環は、環の直和になる。

$\alpha = 4 + \sqrt{-6}$,$J = (X^2 + 6, 4 + X)$ とおく。
$\mathbf{Z}[\sqrt{-6}]/(\alpha) \cong \mathbf{Z}[X]/J$
$X + 4$ を Y とおく（$X = Y - 4$) と $J = (Y^2 - 8Y + 22, Y) \supset (Y)$ となる。
$\mathbf{Z}[X]/J \cong (\mathbf{Z}[Y]/(Y))/J \cong \mathbf{Z}/(22) \cong \mathbf{Z}/(2) \oplus \mathbf{Z}/(11) = \mathbf{F}_2 \oplus \mathbf{F}_{11}$
したがって、(α) による剰余環は、環の直和になる。

例 **4**、$Z = 154$

$2 \cdot 7 \cdot 11 = (2 + 5\sqrt{-6})(2 - 5\sqrt{-6}) = (10 + 3\sqrt{-6})(10 - 3\sqrt{-6})$

例 1 より、(2) による剰余環は、無限小拡大環になる。

$J = (X^2 + 6, 7)$ とおく。
$\mathbf{Z}[\sqrt{-6}]/(7) \cong \mathbf{Z}[X]/J$
$X^2 + 6 - 7 = X^2 - 1 = (X - 1)(X + 1)$
$X - 1$ を Y とおく（$X = Y + 1$) と $(X - 1)(X + 1) = Y(Y + 2)$
$J_1 = (Y(Y + 2), 7) \supset (7)$ とおく。
$\mathbf{Z}[X]/J = \mathbf{Z}[Y]/J_1 \cong (\mathbf{Z}[Y]/(7))/(Y(Y + 2)) \cong \mathbf{F}_7[Y]/(Y(Y + 2)) \cdots \Delta$
$2x \equiv 1 \bmod 7$ を満たす x を求めるため、$7a + 2b = 1$ を満たす a, b の解を出す。
$7a + 2b = 1$ を満たす a, b は、$a = 1, b = -3$ であり、 $x = -3$ である。
$A = -3(Y + 2),\ B = 3Y$ （ $-3(Y + 2) \bmod 7 \equiv 1 - 3Y$ ）
$AB \in (Y^2 + 2Y),\ A + B = 1$
$\mathbf{F}_7[Y]/(A) = \mathbf{F}_7$
$\mathbf{F}_7[Y]/(B) = \mathbf{F}_7$
Δ より $\mathbf{Z}[X]/J \cong \mathbf{F}_7[Y]/(Y(Y + 2)) \cong \mathbf{F}_7[Y]/(A) \oplus \mathbf{F}_7[Y]/(B) \cong \mathbf{F}_7 \oplus \mathbf{F}_7$
したがって、(7) による剰余環は、環の直和になる。

例 3 より (11) による剰余環は、環の直和になる。

$\alpha = 2 + 5\sqrt{-6}$,$J = (X^2 + 6, 2 + 5X)$ とおく。
$\mathbf{Z}[\sqrt{-6}]/(\alpha) \cong \mathbf{Z}[X]/J$
$10(X^2 + 6) - (2X - 1)(2 + 5X) = X + 62$
$X + 62$ を Y とおく（$X = Y - 62$) と $J = (Y^2 - 124Y + 3850, 5Y - 308)$ となる。
$3850 = 154 \cdot 25$ より $\mathbf{Z}[X]/J \cong (\mathbf{Z}[Y]/(Y))/J \cong \mathbf{Z}/(154) \cong \mathbf{Z}/(2) \oplus \mathbf{Z}/(7) \oplus \mathbf{Z}/(11) = \mathbf{F}_2 \oplus \mathbf{F}_7 \oplus \mathbf{F}_{11}$
したがって、(α) による剰余環は、環の直和になる。

$\alpha = 10 + 3\sqrt{-6}$,$J = (X^2 + 6, 10 + 3X)$ とおく。
$\mathbf{Z}[\sqrt{-6}]/(\alpha) \cong \mathbf{Z}[X]/J$
$3(X^2 + 6) - (X - 3)(10 + 3X) = -X + 48$
$-X + 48$ を Y とおく（$X = -Y + 48$) と $J = (Y^2 - 96Y + 2310, -3Y - 154)$ となる。
$2310 = 154 \cdot 15$ より $\mathbf{Z}[X]/J \cong (\mathbf{Z}[Y]/(Y))/J \cong \mathbf{Z}/(154) \cong \mathbf{Z}/(2) \oplus \mathbf{Z}/(7) \oplus \mathbf{Z}/(11) =$

$\mathbf{F}_2 \oplus \mathbf{F}_7 \oplus \mathbf{F}_{11}$
したがって、(α) による剰余環は、環の直和になる。

例 5、$Z = 385$

$5 \cdot 7 \cdot 11 = (1+8\sqrt{-6})(1-8\sqrt{-6}) = (13+6\sqrt{-6})(13-6\sqrt{-6}) = (17+4\sqrt{-6})(17-4\sqrt{-6}) = (19+2\sqrt{-6})(19-2\sqrt{-6})$

例 1 より、 (5) による剰余環は、環の直和になる。

例 4 より、 (7) による剰余環は、環の直和になる。

例 3 より (11) による剰余環は、環の直和になる。

$\alpha = 1+8\sqrt{-6}$,$J = (X^2+6, 1+8X)$ とおく。
$\mathbf{Z}[\sqrt{-6}]/(\alpha) \cong \mathbf{Z}[X]/J$
$72(X^2+6) - (9X-1)(1+8X) = -X+433$
$-X+433$ を Y とおく（$X = -Y+433$) と $J = (Y^2 - 866Y + 187495, 3465 - 8Y)$ となる。
$187495 = 487 \cdot 385$, $3465 = 385 \cdot 9$ より $\mathbf{Z}[X]/J \cong (\mathbf{Z}[Y]/(Y))/J \cong \mathbf{Z}/(385) \cong \mathbf{Z}/(5) \oplus \mathbf{Z}/(7) \oplus \mathbf{Z}/(11) = \mathbf{F}_5 \oplus \mathbf{F}_7 \oplus \mathbf{F}_{11}$
したがって、(α) による剰余環は、環の直和になる。

$\alpha = 13+6\sqrt{-6}$,$J = (X^2+6, 13+6X)$ とおく。
$\mathbf{Z}[\sqrt{-6}]/(\alpha) \cong \mathbf{Z}[X]/J$
$6(X^2+6) - (X-2)(13+6X) = -X+62$
$-X+62$ を Y とおく（$X = -Y+62$) と $J = (Y^2 - 124Y + 3850, 385 - 6Y)$ となる。
$\mathbf{Z}[X]/J \cong (\mathbf{Z}[Y]/(Y))/J \cong \mathbf{Z}/(385) \cong \mathbf{Z}/(5) \oplus \mathbf{Z}/(7) \oplus \mathbf{Z}/(11) = \mathbf{F}_5 \oplus \mathbf{F}_7 \oplus \mathbf{F}_{11}$
したがって、(α) による剰余環は、環の直和になる。

$\alpha = 17+4\sqrt{-6}$,$J = (X^2+6, 17+4X)$ とおく。
$\mathbf{Z}[\sqrt{-6}]/(\alpha) \cong \mathbf{Z}[X]/J$
$4(X^2+6) - (X-4)(17+4X) = -X+92$
$-X+92$ を Y とおく（$X = -Y+92$) と $J = (Y^2 - 184Y + 8470, 385 - 4Y)$ となる。
$8470 = 385 \cdot 22$ より $\mathbf{Z}[X]/J \cong (\mathbf{Z}[Y]/(Y))/J \cong \mathbf{Z}/(385) \cong \mathbf{Z}/(5) \oplus \mathbf{Z}/(7) \oplus \mathbf{Z}/(11) = \mathbf{F}_5 \oplus \mathbf{F}_7 \oplus \mathbf{F}_{11}$
したがって、(α) による剰余環は、環の直和になる。

$\alpha = 19 + 2\sqrt{-6}$,$J = (X^2 + 6, 19 + 2X)$ とおく。
$\mathbf{Z}[\sqrt{-6}]/(\alpha) \cong \mathbf{Z}[X]/J$
$2(X^2 + 6) - (X - 9)(19 + 2X) = -X + 183$
$-X + 183$ を Y とおく（$X = -Y + 183$) と $J = (Y^2 - 366Y + 33495, 385 - 2Y)$ となる。
$33495 = 87 \cdot 385$ より $\mathbf{Z}[X]/J \cong (\mathbf{Z}[Y]/(Y))/J \cong \mathbf{Z}/(385) \cong \mathbf{Z}/(5) \oplus \mathbf{Z}/(7) \oplus \mathbf{Z}/(11) = \mathbf{F}_5 \oplus \mathbf{F}_7 \oplus \mathbf{F}_{11}$
したがって、(α) による剰余環は、環の直和になる。

例 6、$Z = 58$

$2 \cdot 29 = (2 + 3\sqrt{-6})(2 - 3\sqrt{-6})$

例 1 より、(2) による剰余環は、無限小拡大環になる。

$J = (X^2 + 6, 29)$ とおく。
$\mathbf{Z}[\sqrt{-6}]/(29) \cong \mathbf{Z}[X]/J$
$X^2 + 6 - 29 \cdot 3 = X^2 - 81 = (X - 9)(X + 9)$
$X - 9$ を Y とおく（$X = Y + 9$) と $(X - 9)(X + 9) = Y(Y + 18)$
$J_1 = (Y(Y + 18), 29) \supset (29)$ とおく。
$\mathbf{Z}[X]/J = \mathbf{Z}[Y]/J_1 \cong (\mathbf{Z}[Y]/(29))/(Y(Y + 18)) \cong \mathbf{F}_{29}[Y]/(Y(Y + 18)) \cdots \Delta$
$18x \equiv 1 \bmod 29$ を満たす x を求めるため、$29a + 18b = 1$ を満たす a, b の解を出す。
$29a + 18b = 1$ を満たす a, b は、$a = 5, b = -8$ であり、 $x = -8$ である。
$A = -8(Y + 18)$, $B = 8Y$ （ $-8(Y + 18) \bmod 29 \equiv 1 - 8Y$ ）
$AB \in (Y^2 + 18Y)$, $A + B = 1$
$\mathbf{F}_{29}[Y]/(A) = \mathbf{F}_{29}$
$\mathbf{F}_{29}[Y]/(B) = \mathbf{F}_{29}$
Δ より $\mathbf{Z}[X]/J \cong \mathbf{F}_{29}[Y]/(Y(Y + 18)) \cong \mathbf{F}_{29}[Y]/(A) \oplus \mathbf{F}_{29}[Y]/(B) \cong \mathbf{F}_{29} \oplus \mathbf{F}_{29}$
したがって、(29) による剰余環は、環の直和になる。

$\alpha = 2 + 3\sqrt{-6}$,$J = (X^2 + 6, 2 + 3X)$ とおく。
$\mathbf{Z}[\sqrt{-6}]/(\alpha) \cong \mathbf{Z}[X]/J$
$6(X^2 + 6) - (2X - 1)(2 + 3X) = 38 - X$
$38 - X$ を Y とおく（$X = 38 - Y$) と $J = (Y^2 - 76Y + 1450, -3Y + 116)$ となる。
$1450 = 25 \cdot 58$,$116 = 58 \cdot 2$ より $\mathbf{Z}[X]/J \cong (\mathbf{Z}[Y]/(Y))/J \cong \mathbf{Z}/(58) \cong \mathbf{Z}/(2) \oplus \mathbf{Z}/(29) = \mathbf{F}_2 \oplus \mathbf{F}_{29}$
したがって、(α) による剰余環は、環の直和になる。

例 **7**、$Z = 106$

$$2 \cdot 53 = (10 + \sqrt{-6})(10 - \sqrt{-6})$$

例 1 より、(2) による剰余環は、無限小拡大環になる。

$J = (X^2 + 6, 53)$ とおく。
$\mathbf{Z}[\sqrt{-6}]/(53) \cong \mathbf{Z}[X]/J$
$X^2 + 6 - 53 \cdot 2 = X^2 - 100 = (X - 10)(X + 10)$
$X - 10$ を Y とおく（$X = Y + 10$) と $(X - 10)(X + 10) = Y(Y + 20)$
$J_1 = (Y(Y + 20), 53) \supset (53)$ とおく。
$\mathbf{Z}[X]/J = \mathbf{Z}[Y]/J_1 \cong (\mathbf{Z}[Y]/(53))/(Y(Y + 20)) \cong \mathbf{F}_{53}[Y]/(Y(Y + 20)) \cdots \Delta$
$20x \equiv 1 \bmod 53$ を満たす x を求めるため、$53a + 20b = 1$ を満たす a, b の解を出す。
$29a + 18b = 1$ を満たす a, b は、$a = -3, b = 8$ であり、 $x = 8$ である。
$A = 8(Y + 20)$, $B = -8Y$ （ $8(Y + 20) \bmod 53 \equiv 1 + 8Y$ ）
$AB \in (Y^2 + 20Y)$, $A + B = 1$
$\mathbf{F}_{53}[Y]/(A) = \mathbf{F}_{53}$
$\mathbf{F}_{53}[Y]/(B) = \mathbf{F}_{53}$
Δ より $\mathbf{Z}[X]/J \cong \mathbf{F}_{53}[Y]/(Y(Y + 20)) \cong \mathbf{F}_{53}[Y]/(A) \oplus \mathbf{F}_{53}[Y]/(B) \cong \mathbf{F}_{53} \oplus \mathbf{F}_{53}$
したがって、(53) による剰余環は、環の直和になる。

$\alpha = 10 + \sqrt{-6}$,$J = (X^2 + 6, 10 + X)$ とおく。
$\mathbf{Z}[\sqrt{-6}]/(\alpha) \cong \mathbf{Z}[X]/J$
$X^2 + 6 - (X - 11)(10 + X) = X + 116$
$X + 116$ を Y とおく（$X = Y - 116$) と $J = (Y^2 - 232Y + 13462, Y - 106)$ となる。
$13462 = 106 \cdot 127$ より $\mathbf{Z}[X]/J \cong (\mathbf{Z}[Y]/(Y))/J \cong \mathbf{Z}/(106) \cong \mathbf{Z}/(2) \oplus \mathbf{Z}/(53) = \mathbf{F}_2 \oplus \mathbf{F}_{53}$
したがって、(α) による剰余環は、環の直和になる。

例 **8**、$Z = 415$

$$5 \cdot 83 = (11 + 7\sqrt{-6})(11 - 7\sqrt{-6})$$

例 1 より、 (5) による剰余環は、環の直和になる。

$J = (X^2 + 6, 83)$ とおく。
$\mathbf{Z}[\sqrt{-6}]/(83) \cong \mathbf{Z}[X]/J$
$X^2 + 6 - 83 \cdot 14 = X^2 - 1156 = (X - 34)(X + 34)$
$X - 34$ を Y とおく（$X = Y + 34$) と $(X - 34)(X + 34) = Y(Y + 68)$

$J_1 = (Y(Y+68), 83) \supset (83)$ とおく。
$\mathbf{Z}[X]/J = \mathbf{Z}[Y]/J_1 \cong (\mathbf{Z}[Y]/(83))/(Y(Y+68)) \cong \mathbf{F}_{83}[Y]/(Y(Y+68)) \cdots \Delta$
$68x \equiv 1 \bmod 83$ を満たす x を求めるため、$83a + 68b = 1$ を満たす a, b の解を出す。
$83a + 68b = 1$ を満たす a, b は、$a = -9, b = 11$ であり、 $x = 11$ である。
$A = 11(Y+68)$, $B = -11Y$ （ $11(Y+68) \bmod 83 \equiv 1 + 11Y$ ）
$AB \in (Y^2 + 68Y)$, $A + B = 1$
$\mathbf{F}_{83}[Y]/(A) = \mathbf{F}_{83}$
$\mathbf{F}_{83}[Y]/(B) = \mathbf{F}_{83}$
Δ より $\mathbf{Z}[X]/J \cong \mathbf{F}_{83}[Y]/(Y(Y+68)) \cong \mathbf{F}_{83}[Y]/(A) \oplus \mathbf{F}_{83}[Y]/(B) \cong \mathbf{F}_{83} \oplus \mathbf{F}_{83}$
したがって、(83) による剰余環は、環の直和になる。

$\alpha = 11 + 7\sqrt{-6}$,$J = (X^2 + 6, 11 + 7X)$ とおく。
$\mathbf{Z}[\sqrt{-6}]/(\alpha) \cong \mathbf{Z}[X]/J$
$14(X^2 + 6) - (2X - 3)(11 + 7X) = -X + 117$
$-X + 117$ を Y とおく（$X = -Y + 117$) と $J = (Y^2 - 234Y + 13695, -7Y + 830)$ となる。
$13695 = 415 \cdot 33$,$830 = 2 \cdot 415$ より $\mathbf{Z}[X]/J \cong (\mathbf{Z}[Y]/(Y))/J \cong \mathbf{Z}/(415) \cong \mathbf{Z}/(5) \oplus \mathbf{Z}/(83) = \mathbf{F}_2 \oplus \mathbf{F}_{53}$
したがって、(α) による剰余環は、環の直和になる。