$Z = X^2 + kY^2$ で表される数 Z

坂本　優人
学習院大学理学部数学科

平成 25 年 1 月 31 日

目 次

1　目的

自然数 X ,Y が互いに素であるとき、$Z = X^2 + kY^2$ で表される数 Z を考えた。ただし、X は k で割り切れないものとする。特に $Z = X^2 + kY^2$ の規則性、剰余環について調べることを目的とする。この研究では $k = 2, 3, 5, 6, 7$ の場合を調べる。

例
$9 = 1^2 + 2 \cdot 2^2$
$46 = 1^2 + 5 \cdot 3^2$

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、$Z = X^2 + kY^2$ と Z の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(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).
```

144 と 39 を一般互除法を使って表示する例

```
1 ?- gcd(D=144*X+39*Y).
D = 3,
X = 3,
Y = -11
```

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),!.
```

48 を素因数分解してリストで表示する例

```
1 ?- factorize(48,L).
L = [2,2,2,2,3].
```

$Z = X^2 + 2Y^2$ の表示

```
bunkai2:- for(1=<100,X),for(1=<100,Y),
gcd(D=(X,Y)),X mod 2\==0,Z is X*X+2*Y*Y,Z<2000,Z mod 2=\=0,
D==1,factorize(Z,L),write(Z),tab(9),write(L),tab(9),write( X*X+2*Y*Y),nl,fail.
bunkai2.
```

上記のプログラムを実行すると

```
3          [3]          1*1+2*1*1
9          [3, 3]          1*1+2*2*2
19          [19]          1*1+2*3*3
33          [3, 11]          1*1+2*4*4
51          [3, 17]          1*1+2*5*5
73          [73]          1*1+2*6*6
99          [3, 3, 11]          1*1+2*7*7
129          [3, 43]          1*1+2*8*8
163          [163]          1*1+2*9*9
201          [3, 67]          1*1+2*10*10
```

と $Z = 2000$ まで表示される。

$Z = X^2 + 3Y^2$ の表示

```
bunkai3:- for(1=<100,X),for(1=<100,Y),
gcd(D=(X,Y)),X mod 3\==0,Z is X*X+3*Y*Y,Z<2000,Z mod 3=\=0,
D==1,factorize(Z,L),write(Z),tab(9),write(L),tab(9),write( X*X+3*Y*Y),nl,fail.
bunkai3.
```

上記のプログラムを実行すると

```
4          [2, 2]          1*1+3*1*1
13          [13]          1*1+3*2*2
28          [2, 2, 7]          1*1+3*3*3
49          [7, 7]          1*1+3*4*4
76          [2, 2, 19]          1*1+3*5*5
109          [109]          1*1+3*6*6
148          [2, 2, 37]          1*1+3*7*7
193          [193]          1*1+3*8*8
244          [2, 2, 61]          1*1+3*9*9
301          [7, 43]          1*1+3*10*10
```

と $Z = 2000$ まで表示される。

$Z = X^2 + 5Y^2$ の表示

```
bunkai5:- for(1=<100,X),for(1=<100,Y),
gcd(D=(X,Y)),X mod 5\==0,Z is X*X+5*Y*Y,Z<2000,Z mod 5=\=0,
D==1,factorize(Z,L),write(Z),tab(9),write(L),tab(9),write( X*X+5*Y*Y),nl,fail.
bunkai5.
```

上記のプログラムを実行すると

```
6          [2, 3]          1*1+5*1*1
21          [3, 7]          1*1+5*2*2
46          [2, 23]          1*1+5*3*3
81          [3, 3, 3, 3]          1*1+5*4*4
126          [2, 3, 3, 7]          1*1+5*5*5
181          [181]          1*1+5*6*6
246          [2, 3, 41]          1*1+5*7*7
321          [3, 107]          1*1+5*8*8
406          [2, 7, 29]          1*1+5*9*9
501          [3, 167]          1*1+5*10*10
```

と $Z = 2000$ まで表示される。

$Z = X^2 + 6Y^2$ の表示

```
bunkai6:- for(1=<100,X),for(1=<100,Y),
gcd(D=(X,Y)),X mod 6\==0,Z is X*X+6*Y*Y,Z<2000,Z mod 6=\=0,
D==1,factorize(Z,L),write(Z),tab(9),write(L),tab(9),write( X*X+6*Y*Y),nl,fail.
bunkai6.
```

上記のプログラムを実行すると

```
7          [7]          1*1+6*1*1
25          [5, 5]          1*1+6*2*2
55          [5, 11]          1*1+6*3*3
97          [97]          1*1+6*4*4
151          [151]          1*1+6*5*5
217          [7, 31]          1*1+6*6*6
295          [5, 59]          1*1+6*7*7
385          [5, 7, 11]          1*1+6*8*8
487          [487]          1*1+6*9*9
601          [601]          1*1+6*10*10
```

と $Z = 2000$ まで表示される。

$Z = X^2 + 7Y^2$ の表示

```
bunkai7:- for(1=<100,X),for(1=<100,Y),
gcd(D=(X,Y)),X mod 7\==0,Z is X*X+7*Y*Y,Z<2000,Z mod 7=\=0,
D==1,factorize(Z,L),write(Z),tab(9),write(L),tab(9),write( X*X+7*Y*Y),nl,fail.
bunkai7.
```

上記のプログラムを実行すると

```
8          [2, 2, 2]          1*1+7*1*1
29          [29]          1*1+7*2*2
64          [2, 2, 2, 2, 2, 2]          1*1+7*3*3
113          [113]          1*1+7*4*4
176          [2, 2, 2, 2, 11]          1*1+7*5*5
253          [11, 23]          1*1+7*6*6
344          [2, 2, 2, 43]          1*1+7*7*7
449          [449]          1*1+7*8*8
568          [2, 2, 2, 71]          1*1+7*9*9
701          [701]          1*1+7*10*10
```

と $Z = 2000$ まで表示される。

3　結果

3.1　わかったこと

$k = 2, 3, 7$ のときについて、Z が 2 個の異なる素因数を持つとき、$X^2 + kY^2$ の形に 2 通りの分解ができ、3 個の異なる素因数を持つとき、4 通りの分解ができた。このことから Z が n 個の異なる素因数を持つとき、$X^2 + kY^2$ の形には 2^{n-1} 通りに分解できると推測できた。
しかし $k = 5, 6$ のとき、n 個の異なる素因数でも 2^{n-1} 通りに分解できないものがあった。$k = 5$ では、Z が 2 の因数を持つとき、$k = 6$ では、2 か 3 の因数を持つときうまく分解できないことがわかった。

　Z の奇素数について考える。次のことがわかった。
$k = 2$ のとき、Z の値は $3, 11, 17, 19, 41, 43, 59, 67, 73, \cdots$ となり $Z \equiv 1, 3 \ mod\ 8$ を満たす。
$k = 3$ のとき、Z の値は $7, 13, 19, 31, 37, 43, 61, 67, 73, \cdots$ となり $Z \equiv 1, 7 \ mod\ 12$ を満たす。
$k = 5$ のとき、Z の値は $29, 41, 61, 89, 101, 109, 149, 181, 229, \cdots$ となり $Z \equiv 1, 9 \ mod\ 20$ を満たす。
$k = 6$ のとき、Z の値は $7, 31, 73, 79, 97, 103, 127, 151, 193, \cdots$ となり $Z \equiv 1, 7 \ mod\ 24$ を満たす。
$k = 7$ のとき、Z の値は $11, 23, 29, 37, 43, 53, 67, 71, 79, \cdots$ となり $Z \equiv 1, 9, 11, 15, 23, 25 \ mod\ 28$ を満たす。

3.2 $Z = X^2 + kY^2$ の表

表 1: Excel で $X^2 + 2Y^2$ の値を昇順に直した表

$X^2 + 2Y^2$ の値	因数分解	$X^2 + 2Y^2$ の形で表記したもの
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: Excel で 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 の形で表記したもの
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
339	[3, 113]	17·17+2·5·5

表 1: Excel で 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 の形で表記したもの
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
531	[3, 3, 59]	17·17+2·11·11
531	[3, 3, 59]	23·23+2·1·1

表 1: Excel で 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 の形で表記したもの
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
691	[691]	23·23+2·9·9
697	[17, 41]	7·7+2·18·18
697	[17, 41]	25·25+2·6·6

表 1: Excel で 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 の形で表記したもの
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
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

表 1: Excel で 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 の形で表記したもの
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

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
373	[373]	19·19+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
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
556	[2, 2, 139]	23·23+3·3·3
559	[13, 43]	14·14+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
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
757	[757]	13·13+3·14·14
763	[7, 109]	16·16+3·13·13
763	[7, 109]	20·20+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
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
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

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
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

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
441	[3, 3, 7, 7]	11·11+5·8·8

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]	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
654	[2, 3, 109]	7·7+5·11·11
654	[2, 3, 109]	23·23+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
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
861	[3, 7, 41]	29·29+5·2·2
881	[881]	6·6+5·13·13
886	[2, 443]	29·29+5·3·3

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
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

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
433	[433]	7·7+6·8·8

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
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
655	[5, 131]	13·13+6·9·9
655	[5, 131]	19·19+6·7·7

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
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
865	[5, 173]	29·29+6·2·2
879	[3, 293]	27·27+6·5·5
886	[2, 443]	20·20+6·9·9

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
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

$X^2 + 7Y^2$ 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
487	[487]	12·12+7·7·7

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
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
737	[11, 67]	17·17+7·8·8
737	[11, 67]	25·25+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
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
989	[23, 43]	17·17+7·10·10
989	[23, 43]	31·31+7·2·2
991	[991]	12·12+7·11·11

3.3　うまく分解できる場合

$k = 2$ のとき

$Z = 51$ とする。
$51 = 3 \cdot 17 = 1^2 + 2 \cdot 5^2 = 7^2 + 2 \cdot 1^2$
異なる素因数は 3 と 17 の 2 個である。このとき 2 通り分解できる。

$Z = 627$ とする。
$627 = 3 \cdot 11 \cdot 19 = 7^2 + 2 \cdot 17^2 = 17^2 + 2 \cdot 13^2 = 23^2 + 2 \cdot 7^2 = 25^2 + 2 \cdot 1^2$
異なる素因数は 3 と 11 と 19 の 3 個である。このとき 4 通り分解できる。

$k = 3$ のとき

$Z = 91$ とする。
$91 = 7 \cdot 13 = 4^2 + 3 \cdot 5^2 = 8^2 + 3 \cdot 3^2$
異なる素因数は 7 と 13 の 2 個である。このとき 2 通り分解できる。

$z = 532$ とする。$532 = 2^2 \cdot 7 \cdot 19 = 5^2 + 3 \cdot 13^2 = 13^2 + 3 \cdot 11^2 = 17^2 + 3 \cdot 9^2 = 23^2 + 3 \cdot 1^2$
異なる素因数は 2 と 7 と 19 の 3 個である。このとき 4 通り分解できる。

$k = 5$ のとき

$z = 21$ とする。
$21 = 3 \cdot 7 = 1^2 + 5 \cdot 2^2 = 4^2 + 5 \cdot 1^2$
異なる素因数は 3 と 7 の 2 個である。このとき 2 通り分解できる。

$k = 6$ のとき

$z = 55$ とする。
$55 = 5 \cdot 11 = 1^2 + 6 \cdot 3^2 = 7^2 + 6 \cdot 1^2$
異なる素因数は 5 と 11 の 2 個である。このとき 2 通り分解できる。

$k = 7$ のとき

$z = 88$ とする。
$88 = 2^3 \cdot 11 = 5^2 + 7 \cdot 3^2 = 9^2 + 7 \cdot 1^2$
異なる素因数は 2 と 11 の 2 個である。このとき 2 通り分解できる。

3.4　うまく分解できない場合

$k = 5$ のとき

$z = 86$ とする。
$86 = 2 \cdot 43 = 9^2 + 5 \cdot 1^2$
異なる素因数は 2 と 43 の 2 個あるが、1 通りしか分解できない。

$z = 174$ とする。
$174 = 2 \cdot 3 \cdot 29 = 7^2 + 5 \cdot 5^2 = 13^2 + 5 \cdot 1^2$
異なる素因数は 2 と 3 と 29 の 3 個あるが、2 通りしか分解できない。

$k = 6$ のとき

$z = 58$ とする。
$58 = 2 \cdot 29 = 2^2 + 6 \cdot 3^2$
異なる素因数は 2 と 29 の 2 個あるが、1 通りしか分解できない。

$z = 105$ とする。
$105 = 3 \cdot 5 \cdot 7 = 3^2 + 6 \cdot 4^2 = 9^2 + 6 \cdot 2^2$
異なる素因数は 3 と 5 と 7 の 3 個あるが、2 通りしか分解できない。

4　考察

4.1　平方剰余を用いた mod を使って表せる証明

まず証明のために必要な定義や定理を簡単に書く。

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 が平方剰余であるならば、a と b も平方剰余である。
(　)ab が平方非剰余であるならば、a と b の一方が平方非剰余である。

これらを使い $k = 7$ のとき、$Z \equiv 1, 9, 11, 15, 23, 25 \bmod 28$ を満たすことを証明する。

$Z = X^2 + 7X^2$ となる奇素数 Z について考える。p を任意の素数とし、$X \neq 0 \bmod p$ とする。
Z が 7 で割り切れるとき、$Z = X^2 + 7Y^2$ を $\bmod p$ で考えると
$X^2 \equiv -7Y^2 \bmod p$
$Y \bmod p$ の逆元を U とすると
$(UX)^2 \equiv -7 \bmod p$
このとき $(\frac{-7}{p}) = 1$ となる p を調べる。
$(\frac{-7}{p}) = (\frac{-1}{p})(\frac{7}{p}) = (-1)^{\frac{p-1}{2}}(\frac{7}{p})$
このとき任意の自然数 n に対して
$Z = 4n+1, 4n+3$
なので
$p = 4n+1, 4n+3$
だから
$(\frac{-7}{p}) = (-1)^{2n}(\frac{7}{p}) = (\frac{7}{p}) \quad (p = 4n+1)$
$(\frac{-7}{p}) = (-1)^{2n+1}(\frac{7}{p}) = -(\frac{7}{p}) \quad (p = 4n+3)$
平方剰余の相互法則より
$(\frac{7}{p})(\frac{p}{7}) = (-1)^{\frac{p-1}{2}\cdot 3} = (-1)^{3\cdot 2n} = 1 \quad (p = 4n+1)$
$(\frac{7}{p})(\frac{p}{7}) = (-1)^{\frac{p-1}{2}\cdot 3} = (-1)^{3(2n+1)} = -1 \quad (p = 4n+3)$
$(\frac{p}{7}) = 1$ となる p は、$p \equiv 1, 2, 4 \bmod 7$
一方
$(\frac{-1}{p}) = 1$ となる p は、$p \equiv 1 \bmod 4$
$(\frac{-1}{p}) = -1$ となる p は、$p \equiv 3 \bmod 4$
これらを合わせると、$p \equiv 1, 9, 11, 15, 23, 25 \bmod 28$ となる。

4.2 剰余環についての考察

規則性を満たさなかった $Z = X^2 + 5Y^2$ について、任意の α に対して、(α) による剰余環 $R = \mathbf{Z}[\sqrt{-5}]/(\alpha)$ を調べる。

4.2.1 (α) が体になる場合

$\mathbf{Z}[\sqrt{-5}] = a + b\sqrt{-5} | a, b \in \mathbf{Z}$ 上で考える。

例 1 $Z = 29$

$29 = (3 + 2\sqrt{-5})(3 - 2\sqrt{-5})$
$\alpha = 3 + 2\sqrt{-5}$ とする。
$\mathbf{Z}[\sqrt{-5}]/(3 + 2\sqrt{-5}) \cong \mathbf{Z}[X]/(X^2 + 5, 3 + 2X)$
$J = (X^2 + 5, 3 + 2X)$ とする。
$2(X^2 + 5) - (X - 1)(3 + 2X) = 13 - X = Y$
これから
$X = 13 - Y$
$X^2 + 5 = (13 - Y)^2 + 5 = Y^2 - 26Y + 174$
$3 + 2X = 3 + 2(13 - Y) = -2Y + 29$
したがって
$J = (Y^2 - 26Y + 174, -2Y + 29) \supset (Y)$
このとき
$174 = 6 \cdot 29$
なので
$\mathbf{Z}[X]/J \cong (\mathbf{Z}[Y]/(Y))/J \cong \mathbf{F}_{29}$
ゆえに、α による剰余環は体になる。

例 2 $Z = 41$

$41 = (6 + \sqrt{-5})(6 - \sqrt{-5})$
$\alpha = 6 + \sqrt{-5}$ とする。
$\mathbf{Z}[\sqrt{-5}]/(6 + \sqrt{-5}) \cong \mathbf{Z}[X]/(X^2 + 5, 6 + X)$
$J = (X^2 + 5, 6 + X)$ とする。
$6 + X = Y$ とする。
$X^2 + 5 = (Y - 6)^2 + 5 = Y^2 - 12Y + 41$
したがって
$J = (Y, Y^2 - 12Y + 41) \supset (Y)$ よって
$\mathbf{Z}[X]/J \cong (\mathbf{Z}[Y]/(Y))/J \cong \mathbf{F}_{41}$
ゆえに、α による剰余環は体になる。

例 3 $Z = 61$

$61 = (4 + 3\sqrt{-5})(4 - 3\sqrt{-5})$
$\alpha = 4 + 3\sqrt{-5}$ とする。
$\mathbf{Z}[\sqrt{-5}]/(4 + 3\sqrt{-5}) \cong \mathbf{Z}[X]/(X^2 + 5, 4 + 3X)$
$J = (X^2 + 5, 4 + 3X)$ とする。
$3(X^2 + 5) - (X - 1)(4 + 3X) = 19 - X = Y$
これから
$X = 19 - Y$
$X^2 + 5 = (19 - Y)^2 + 5 = Y^2 - 38Y + 366$
$4 + 3X = 4 + 3(19 - Y) = -3Y + 61$
したがって
$J = (Y^2 - 38Y + 366, -3Y + 61) \supset (Y)$
このとき
$366 = 2 \cdot 3 \cdot 61$
なので
$\mathbf{Z}[X]/J \cong (\mathbf{Z}[Y]/(Y))/J \cong \mathbf{F}_{61}$
ゆえに、α による剰余環は体になる。

例 4 $Z = 89$

$89 = (3 + 4\sqrt{-5})(3 - 4\sqrt{-5})$
$\alpha = 3 + 4\sqrt{-5}$ とする。
$\mathbf{Z}[\sqrt{-5}]/(3 + 4\sqrt{-5}) \cong \mathbf{Z}[X]/(X^2 + 5, 3 + 4X)$
$J = (X^2 + 5, 3 + 4X)$ とする。
$4(X^2 + 5) - (X - 1)(3 + 4X) = X + 23 = Y$
これから
$X = Y - 23$
$X^2 + 5 = (Y - 23)^2 + 5 = Y^2 - 46Y + 534$
$3 + 4X = 3 + 4(Y - 23) = 4Y - 89$
したがって
$J = (Y^2 - 46Y + 534, 4Y - 89) \supset (Y)$
このとき
$534 = 5 \cdot 89$
なので
$\mathbf{Z}[X]/J \cong (\mathbf{Z}[Y]/(Y))/J \cong \mathbf{F}_{89}$
ゆえに、α による剰余環は体になる。

例 5 $Z = 101$

$101 = (9 + 2\sqrt{-5})(9 - 2\sqrt{-5})$
$\alpha = 9 + 2\sqrt{-5}$ とする。
$\mathbf{Z}[\sqrt{-5}]/(9 + 2\sqrt{-5}) \cong \mathbf{Z}[X]/(X^2 + 5, 9 + 2X)$
$J = (X^2 + 5, 9 + 2X)$ とする。
$2(X^2 + 5) - (X - 4)(9 + 2X) = 46 - X = Y$
これから
$X = 46 - Y$
$X^2 + 5 = (46 - Y)^2 + 5 = Y^2 - 92Y + 2121$
$9 + 2X = 9 + 2(46 - Y) = -2Y + 101$
したがって
$J = (Y^2 - 92Y + 2121, -2Y + 101) \supset (Y)$
このとき
$2121 = 3 \cdot 7 \cdot 101$
なので
$\mathbf{Z}[X]/J \cong (\mathbf{Z}[Y]/(Y))/J \cong \mathbf{F}_{101}$
ゆえに、α による剰余環は体になる。

例 6 $Z = 109$

$109 = (8 + 3\sqrt{-5})(8 - 3\sqrt{-5})$
$\alpha = 8 + 3\sqrt{-5}$ とする。
$\mathbf{Z}[\sqrt{-5}]/(8 + 3\sqrt{-5}) \cong \mathbf{Z}[X]/(X^2 + 5, 8 + 3X)$
$J = (X^2 + 5, 8 + 3X)$ とする。
$3(X^2 + 5) - (X - 3)(8 + 3X) = X + 39 = Y$
これから
$X = Y - 39$
$X^2 + 5 = (Y - 39)^2 + 5 = Y^2 - 78Y + 1526$
$8 + 3X = 8 + 3(Y - 39) = 3Y - 109$
したがって
$J = (Y^2 - 78Y + 1526, 3Y - 109) \supset (Y)$
このとき
$1526 = 2 \cdot 7 \cdot 109$
なので
$\mathbf{Z}[X]/J \cong (\mathbf{Z}[Y]/(Y))/J \cong \mathbf{F}_{109}$
ゆえに、α による剰余環は体になる。

例 7 $Z = 149$

$149 = (12 + \sqrt{-5})(12 - \sqrt{-5})$
$\alpha = 12 + \sqrt{-5}$ とする。
$\mathbf{Z}[\sqrt{-5}]/(12 + \sqrt{-5}) \cong \mathbf{Z}[X]/(X^2 + 5, 12 + X)$
$J = (X^2 + 5, 12 + X)$ とする。
$12 + X = Y$ とする。
$X^2 + 5 = (Y - 12)^2 + 5 = Y^2 - 24Y + 149$
したがって
$J = (Y, Y^2 - 24Y + 149) \supset (Y)$ よって
$\mathbf{Z}[X]/J \cong (\mathbf{Z}[Y]/(Y))/J \cong \mathbf{F}_{149}$
ゆえに、α による剰余環は体になる。

例 8 $Z = 181$

$109 = (1 + 6\sqrt{-5})(1 - 6\sqrt{-5})$
$\alpha = 1 + 6\sqrt{-5}$ とする。
$\mathbf{Z}[\sqrt{-5}]/(1 + 6\sqrt{-5}) \cong \mathbf{Z}[X]/(X^2 + 5, 1 + 6X)$
$J = (X^2 + 5, 1 + 6X)$ とする。
$30(X^2 + 5) - (5X - 1)(1 + 6X) = X + 151 = Y$
これから
$X = Y - 151$
$X^2 + 5 = (Y - 151)^2 + 5 = Y^2 - 302Y + 22806$
$1 + 6X = 1 + 6(Y - 151) = 6Y - 905$
したがって
$J = (Y^2 - 302Y + 22806, 6Y - 905) \supset (Y)$
このとき
$22806 = 2 \cdot 3^2 \cdot 7 \cdot 181$
$905 = 5 \cdot 181$
なので
$\mathbf{Z}[X]/J \cong (\mathbf{Z}[Y]/(Y))/J \cong \mathbf{F}_{181}$
ゆえに、α による剰余環は体になる。

例 **9** $Z = 229$

$229 = (7 + 6\sqrt{-5})(7 - 6\sqrt{-5})$
$\alpha = 7 + 6\sqrt{-5}$ とする。
$\mathbf{Z}[\sqrt{-5}]/(7 + 6\sqrt{-5}) \cong \mathbf{Z}[X]/(X^2 + 5, 7 + 6X)$
$J = (X^2 + 5, 7 + 6X)$ とする。
$6(X^2 + 5) - (X - 1)(7 + 6X) = 37 - X = Y$
これから
$X = 37 - Y$
$X^2 + 5 = (37 - Y)^2 + 5 = Y^2 - 74Y + 1374$
$7 + 6X = 7 + 6(37 - Y) = -6Y + 229$
したがって
$J = (Y^2 - 74Y + 1374, -6Y + 229) \supset (Y)$
このとき
$1374 = 2 \cdot 3 \cdot 229$
なので
$\mathbf{Z}[X]/J \cong (\mathbf{Z}[Y]/(Y))/J \cong \mathbf{F}_{229}$
ゆえに、α による剰余環は体になる。

例 **10** $Z = 241$

$241 = (14 + 3\sqrt{-5})(14 - 3\sqrt{-5})$
$\alpha = 14 + 3\sqrt{-5}$ とする。
$\mathbf{Z}[\sqrt{-5}]/(14 + 3\sqrt{-5}) \cong \mathbf{Z}[X]/(X^2 + 5, 14 + 3X)$
$J = (X^2 + 5, 14 + 3X)$ とする。
$3(X^2 + 5) - (X - 5)(14 + 3X) = X + 85 = Y$
これから
$X = Y - 85$
$X^2 + 5 = (Y - 85)^2 + 5 = Y^2 - 170Y + 7230$
$14 + 3X = 14 + 3(Y - 85) = 3Y - 241$
したがって
$J = (Y^2 - 170Y + 7230, 3Y - 241) \supset (Y)$
このとき
$7230 = 2 \cdot 3 \cdot 5 \cdot 241$
なので
$\mathbf{Z}[X]/J \cong (\mathbf{Z}[Y]/(Y))/J \cong \mathbf{F}_{241}$
ゆえに、α による剰余環は体になる。

例 **11** $Z = 269$

$269 = (12 + 5\sqrt{-5})(12 - 5\sqrt{-5})$
$\alpha = 12 + 5\sqrt{-5}$ とする。
$\mathbf{Z}[\sqrt{-5}]/(12 + 5\sqrt{-5}) \cong \mathbf{Z}[X]/(X^2 + 5, 12 + 5X)$
$J = (X^2 + 5, 12 + 5X)$ とする。
$10(X^2 + 5) - (2X - 5)(12 + 5X) = X + 110 = Y$
これから
$X = Y - 110$
$X^2 + 5 = (Y - 110)^2 + 5 = Y^2 - 220Y + 12105$
$12 + 5X = 12 + 5(Y - 110) = 5Y - 538$
したがって
$J = (Y^2 - 220Y + 12105, 5Y - 538) \supset (Y)$
このとき
$12105 = 3^2 \cdot 5 \cdot 269$
$538 = 2 \cdot 269$
なので
$\mathbf{Z}[X]/J \cong (\mathbf{Z}[Y]/(Y))/J \cong \mathbf{F}_{269}$
ゆえに、α による剰余環は体になる。

例 **12** $Z = 281$

$281 = (6 + 7\sqrt{-5})(6 - 7\sqrt{-5})$
$\alpha = 6 + 7\sqrt{-5}$ とする。
$\mathbf{Z}[\sqrt{-5}]/(6 + 7\sqrt{-5}) \cong \mathbf{Z}[X]/(X^2 + 5, 6 + 7X)$
$J = (X^2 + 5, 6 + 7X)$ とする。
$7(X^2 + 5) - (X - 1)(6 + 7X) = X + 41 = Y$
これから
$X = Y - 41$
$X^2 + 5 = (Y - 41)^2 + 5 = Y^2 - 82Y + 1686$
$6 + 7X = 6 + 7(Y - 41) = 7Y - 281$
したがって
$J = (Y^2 - 82Y + 1686, 7Y - 281) \supset (Y)$
このとき
$1686 = 2 \cdot 3 \cdot 281$
なので
$\mathbf{Z}[X]/J \cong (\mathbf{Z}[Y]/(Y))/J \cong \mathbf{F}_{281}$
ゆえに、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

(α) が、既約元であるが素元でない場合がある。

例 1 $Z = 6$

$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$
$\mathbf{Z}[\sqrt{-5}]/(2) \cong \mathbf{Z}[X]/(X^2 + 5, 2)$
$J_1 = (X^2 + 5, 2)$ とする。
$X^2 + 5 - 3 \cdot 2 = X^2 - 1 = (X + 1)(X - 1)$
$Y = X - 1$ とすると
$J_1 \supset (2)$
なので
$X - 1 = X + 1 = Y$
これから
$\mathbf{Z}[\sqrt{-5}]/(3) \cong \mathbf{Z}[Y]/J_1 \cong (\mathbf{Z}[Y]/(2))/(Y^2) \cong \mathbf{F}_2/(Y^2)$
これは無限小拡大環になる。

$\mathbf{Z}[\sqrt{-5}]/(3) \cong \mathbf{Z}[X]/(X^2 + 5, 3)$
$J_2 = (X^2 + 5, 3)$ とする。
$X^2 + 5 - 3 \cdot 2 = X^2 - 1 = (X + 1)(X - 1)$
$Y = X - 1$ とすると
$J_2 = (3, Y(Y + 2)) \supset (3)$
これから
$\mathbf{Z}[\sqrt{-5}]/(3) \cong \mathbf{Z}[Y]/J_2 \cong (\mathbf{Z}[Y]/(3))/(Y(Y + 2)) \cong \mathbf{F}_3/(Y(Y + 2))$
$2x \equiv 1 \mod 3$ を満たす x を求めるために、$3a + 2b = 1$ を満たす a, b を求めると
$a = 1, b = -1$ となり、$x = -1$ となる。
これから
$A = -(Y + 2), B = Y$ とすると $AB = -Y(Y + 2) \in (Y(Y + 2))$
$\mathbf{F}_3$ 上において、$-2 \equiv 1 \mod 3$ なので
$A + B = -2 = 1$
したがって
$\mathbf{Z}[\sqrt{-5}]/(3) \cong \mathbf{F}_3[Y]/(A) \oplus \mathbf{F}_3[Y]/(B)$
このとき
$\mathbf{F}_3[Y]/(A) \cong \mathbf{F}_3, \mathbf{F}_3[Y]/(B) \cong \mathbf{F}_3$
なので
$\mathbf{Z}[\sqrt{-5}]/(3) \cong \mathbf{F}_3 \oplus \mathbf{F}_3$
よって、(3) による剰余環は、環の直和になる。

$\alpha = 1 + \sqrt{-5}$ とする。
$\mathbf{Z}[\sqrt{-5}]/(1+\sqrt{-5}) \cong \mathbf{Z}[X]/(X^2+5, 1+X)$
$I = (X^2+5, 1+X)$ とする。
$1 + X = Y$ とする。
$X^2 + 5 = (Y-1)^2 + 5 = Y^2 - 2Y + 6$
したがって
$I = (Y, Y^2 - 2Y + 6) \supset (Y)$
よって
$\mathbf{Z}[X]/I \cong (\mathbf{Z}[Y]/(Y))/I \cong \mathbf{Z}/(6) \cong \mathbf{Z}/(2) \oplus \mathbf{Z}/(3) = \mathbf{F}_2 \oplus \mathbf{F}_3$
よって、$(\alpha) = (1+\sqrt{-5})$ による剰余環は、環の直和になる。

ここで
$j_1 = (1+\sqrt{-5}, 2), j_2 = (1+\sqrt{-5}, 3)$ とする。
$j_1 j_2 = (-4 + 2\sqrt{-5}, 3 + 3\sqrt{-5}, 2 + 2\sqrt{-5}, 6)$
このとき
$3 + 3\sqrt{-5} = 3(1+\sqrt{-5}), 2 + 2\sqrt{-5} = 2(1+\sqrt{-5}),$
$6 = (1-\sqrt{-5})(1+\sqrt{-5}), 6 + (-4 + 2\sqrt{-5}) = 2(1+\sqrt{-5})$
なので
$j_1 j_2 = (1+\sqrt{-5})$ となる。
これから
$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{5}) = j_1 j_2 \bar{j_1} \bar{j_2}$
となり素イデアルの積で表せる。

例 2 $Z = 14$

$14 = 2 \cdot 7 = (3 + \sqrt{-5})(3 - \sqrt{-5})$
例 1 より、(2) による剰余環は、無限小拡大環になる。
$\mathbf{Z}[\sqrt{-5}]/(7) \cong \mathbf{Z}[X]/(X^2 + 5, 7)$
$J = (X^2 + 5, 7)$ とする。
$X^2 + 5 - 7 \cdot 2 = X^2 - 9 = (X + 3)(X - 3)$
$Y = X - 3$ とすると
$J = (7, Y(Y + 6)) \supset (7)$
これから
$\mathbf{Z}[\sqrt{-5}]/(7) \cong \mathbf{Z}[Y]/J \cong (\mathbf{Z}[Y]/(7))/(Y(Y + 6)) \cong \mathbf{F}_7/(Y(Y + 6))$
$6x \equiv 1 \mod 7$ を満たす x を求めるために、$7a + 6b = 1$ を満たす a, b を求めると
$a = 1, b = -1$ となり、$x = -1$ となる。
これから
$A = -(Y + 6), B = Y$ とすると $AB = -Y(Y + 6) \in (Y(Y + 6))$
$\mathbf{F}_7$ 上において、$-6 \equiv 1 \mod 7$ なので
$A + B = -6 = 1$
したがって
$\mathbf{Z}[\sqrt{-5}]/(7) \cong \mathbf{F}_7[Y]/(A) \oplus \mathbf{F}_7[Y]/(B)$
このとき
$\mathbf{F}_7[Y]/(A) \cong \mathbf{F}_7, \mathbf{F}_7[Y]/(B) \cong \mathbf{F}_7$
なので
$\mathbf{Z}[\sqrt{-5}]/(7) \cong \mathbf{F}_7 \oplus \mathbf{F}_7$
よって、(7) による剰余環は、環の直和になる。

$\alpha = 3 + \sqrt{-5}$ とする。
$\mathbf{Z}[\sqrt{-5}]/(3 + \sqrt{-5}) \cong \mathbf{Z}[X]/(X^2 + 5, 3 + X)$
$I = (X^2 + 5, 3 + X)$ とする。
$3 + X = Y$ とする。
$X^2 + 5 = (Y - 3)^2 + 5 = Y^2 - 6Y + 14$
したがって
$I = (Y, Y^2 - 6Y + 14) \supset (Y)$
よって
$\mathbf{Z}[X]/I \cong (\mathbf{Z}[Y]/(Y))/I \cong \mathbf{Z}/(14) \cong \mathbf{Z}/(2) \oplus \mathbf{Z}/(7) = \mathbf{F}_2 \oplus \mathbf{F}_7$
よって、$(\alpha) = (3 + \sqrt{-5})$ による剰余環は、環の直和になる。

ここで
$j_1 = (3+\sqrt{-5}, 2), j_2 = (3+\sqrt{-5}, 7)$ とする。
$j_1 j_2 = (4+6\sqrt{-5}, 21+7\sqrt{-5}, 6+2\sqrt{-5}, 14)$
このとき
$21+7\sqrt{-5} = 7(3+\sqrt{-5}), 6+2\sqrt{-5} = 2(3+\sqrt{-5}),$
$14 = (3-\sqrt{-5})(3+\sqrt{-5}), 14+(4+6\sqrt{-5}) = 6(3+\sqrt{-5})$
なので
$j_1 j_2 = (3+\sqrt{-5})$ となる。
これから
$14 = 2 \cdot 7 = (3+\sqrt{-5})(3-\sqrt{5}) = j_1 j_2 \bar{j_1} \bar{j_2}$
となり素イデアルの積で表せる。

例 3 $Z = 46$

$46 = 2 \cdot 23 = (1+3\sqrt{-5})(1-3\sqrt{-5})$
例 1 より、(2) による剰余環は、無限小拡大環になる。
$\mathbf{Z}[\sqrt{-5}]/(23) \cong \mathbf{Z}[X]/(X^2+5, 23)$
$J = (X^2+5, 23)$ とする。
$X^2+5-23 \cdot 3 = X^2-64 = (X+8)(X-8)$
$Y = X-8$ とすると
$J = (23, Y(Y+16)) \supset (23)$
これから
$\mathbf{Z}[\sqrt{-5}]/(23) \cong \mathbf{Z}[Y]/J \cong (\mathbf{Z}[Y]/(23))/(Y(Y+16)) \cong \mathbf{F}_{23}/(Y(Y+16))$
$16x \equiv 1 \mod 23$ を満たす x を求めるために、$23a+16b = 1$ を満たす a, b を求めると
$a = 7, b = -10$ となり、$x = -10$ となる。
これから
$A = -10(Y+16), B = 10Y$ とすると $AB = -100Y(Y+16) \in (Y(Y+16))$
$\mathbf{F}_{23}$ 上において、$-160 \equiv 1 \mod 23$ なので
$A+B = -160 = 1$
したがって
$\mathbf{Z}[\sqrt{-5}]/(23) \cong \mathbf{F}_{23}[Y]/(A) \oplus \mathbf{F}_{23}[Y]/(B)$
このとき
$\mathbf{F}_{23}[Y]/(A) \cong \mathbf{F}_{23}, \mathbf{F}_{23}[Y]/(B) \cong \mathbf{F}_{23}$
なので
$\mathbf{Z}[\sqrt{-5}]/(23) \cong \mathbf{F}_{23} \oplus \mathbf{F}_{23}$
よって、(23) による剰余環は、環の直和になる。

$\alpha = 1 + 3\sqrt{-5}$ とする。
$\mathbf{Z}[\sqrt{-5}]/(1 + 3\sqrt{-5}) \cong \mathbf{Z}[X]/(X^2 + 5, 1 + 3X)$
$I = (X^2 + 5, 1 + 3X)$ とする。
$6(X^2 + 5) - (2X - 1)(1 + 3X) = X + 31 = Y$
これから
$X = Y - 31$
$X^2 + 5 = (Y - 31)^2 + 5 = Y^2 - 62Y + 966$
$1 + 3X = 1 + 3(Y - 31) = 3Y - 92$
したがって
$I = (Y^2 - 62Y + 966, 3Y - 92) \supset (Y)$
このとき
$966 = 2 \cdot 3 \cdot 7 \cdot 23$
$92 = 2^2 \cdot 23$
なので
$\mathbf{Z}[X]/I \cong (\mathbf{Z}[Y]/(Y))/I \cong \mathbf{Z}/(46) \cong \mathbf{Z}/(2) \oplus \mathbf{Z}/(23) = \mathbf{F}_2 \oplus \mathbf{F}_{23}$
よって、$(\alpha) = (1 + 3\sqrt{-5})$ による剰余環は、環の直和になる。

ここで
$j_1 = (1 + 3\sqrt{-5}, 2), j_2 = (1 + 3\sqrt{-5}, 23)$ とする。
$j_1 j_2 = (-44 + 6\sqrt{-5}, 23 + 69\sqrt{-5}, 2 + 6\sqrt{-5}, 46)$
このとき
$23 + 69\sqrt{-5} = 23(1 + 3\sqrt{-5}), 2 + 6\sqrt{-5} = 2(1 + 3\sqrt{-5}),$
$46 = (1 - 3\sqrt{-5})(1 + 3\sqrt{-5}), 46 + (-44 + 6\sqrt{-5}) = 2(1 + 3\sqrt{-5})$
なので
$j_1 j_2 = (1 + 3\sqrt{-5})$ となる。
これから
$46 = 2 \cdot 23 = (1 + 3\sqrt{-5})(1 - 3\sqrt{5}) = j_1 j_2 \bar{j}_1 \bar{j}_2$
となり素イデアルの積で表せる。

例 4 $Z = 86$

$86 = 2 \cdot 43 = (9 + \sqrt{-5})(9 - \sqrt{-5})$
例 1 より、(2) による剰余環は、無限小拡大環になる。
$\mathbf{Z}[\sqrt{-5}]/(43) \cong \mathbf{Z}[X]/(X^2 + 5, 43)$
$J = (X^2 + 5, 43)$ とする。
$X^2 + 5 - 43 \cdot 2 = X^2 - 81 = (X + 9)(X - 9)$
$Y = X - 9$ とすると
$J = (43, Y(Y + 18)) \supset (43)$
これから
$\mathbf{Z}[\sqrt{-5}]/(43) \cong \mathbf{Z}[Y]/J \cong (\mathbf{Z}[Y]/(43))/(Y(Y + 18)) \cong \mathbf{F}_{43}/(Y(Y + 18))$
$18x \equiv 1 \mod 43$ を満たす x を求めるために、$43a + 18b = 1$ を満たす a, b を求めると
$a = -5, b = 12$ となり、$x = 12$ となる。
これから
$A = 12(Y + 18), B = -12Y$ とすると $AB = -144Y(Y + 18) \in (Y(Y + 18))$
$\mathbf{F}_{43}$ 上において、$216 \equiv 1 \mod 43$ なので
$A + B = 216 = 1$
したがって
$\mathbf{Z}[\sqrt{-5}]/(43) \cong \mathbf{F}_{43}[Y]/(A) \oplus \mathbf{F}_{43}[Y]/(B)$
このとき
$\mathbf{F}_{43}[Y]/(A) \cong \mathbf{F}_{43}, \mathbf{F}_{43}[Y]/(B) \cong \mathbf{F}_{43}$
なので
$\mathbf{Z}[\sqrt{-5}]/(43) \cong \mathbf{F}_{43} \oplus \mathbf{F}_{43}$
よって、(43) による剰余環は、環の直和になる。

$\alpha = 9 + \sqrt{-5}$ とする。
$\mathbf{Z}[\sqrt{-5}]/(9 + \sqrt{-5}) \cong \mathbf{Z}[X]/(X^2 + 5, 9 + X)$
$I = (X^2 + 5, 9 + X)$ とする。
$9 + X = Y$ とする。
$X^2 + 5 = (Y - 9)^2 + 5 = Y^2 - 18Y + 86$
したがって
$I = (Y, Y^2 - 18Y + 86) \supset (Y)$
ゆえに
$\mathbf{Z}[X]/I \cong (\mathbf{Z}[Y]/(Y))/I \cong \mathbf{Z}/(86) \cong \mathbf{Z}/(2) \oplus \mathbf{Z}/(43) = \mathbf{F}_2 \oplus \mathbf{F}_{43}$
よって、$(\alpha) = (9 + \sqrt{-5})$ による剰余環は、環の直和になる。

ここで
$j_1 = (9+\sqrt{-5}, 2), j_2 = (9+\sqrt{-5}, 43)$ とする。
$j_1 j_2 = (76+18\sqrt{-5}, 387+43\sqrt{-5}, 18+2\sqrt{-5}, 86)$
このとき
$387+43\sqrt{-5} = 43(9+\sqrt{-5}), 18+2\sqrt{-5} = 2(9+\sqrt{-5}),$
$86 = (9-\sqrt{-5})(9+\sqrt{-5}), 86+(76+18\sqrt{-5}) = 18(9+\sqrt{-5})$
なので
$j_1 j_2 = (9+\sqrt{-5})$ となる。
これから
$86 = 2 \cdot 43 = (9+\sqrt{-5})(9-\sqrt{5}) = j_1 j_2 \bar{j_1} \bar{j_2}$
となり素イデアルの積で表せる。

例 5 $Z = 94$

$94 = 2 \cdot 47 = (7+3\sqrt{-5})(7-3\sqrt{-5})$
例 1 より、(2) による剰余環は、無限小拡大環になる。
$\mathbf{Z}[\sqrt{-5}]/(47) \cong \mathbf{Z}[X]/(X^2+5, 47)$
$J = (X^2+5, 47)$ とする。
$X^2+5-47 \cdot 2 = X^2-324 = (X+18)(X-18)$
$Y = X-18$ とすると
$J = (47, Y(Y+36)) \supset (47)$
これから
$\mathbf{Z}[\sqrt{-5}]/(47) \cong \mathbf{Z}[Y]/J \cong (\mathbf{Z}[Y]/(47))/(Y(Y+36)) \cong \mathbf{F}_{47}/(Y(Y+36))$
$36x \equiv 1 \mod 47$ を満たす x を求めるために、$47a+36b = 1$ を満たす a, b を求めると
$a = -13, b = 17$ となり、$x = 17$ となる。
これから
$A = 17(Y+36), B = -17Y$ とすると $AB = -289Y(Y+36) \in (Y(Y+36))$
$\mathbf{F}_{47}$ 上において、$612 \equiv 1 \mod 47$ なので
$A+B = 612 = 1$
したがって
$\mathbf{Z}[\sqrt{-5}]/(47) \cong \mathbf{F}_{47}[Y]/(A) \oplus \mathbf{F}_{47}[Y]/(B)$
このとき
$\mathbf{F}_{47}[Y]/(A) \cong \mathbf{F}_{47}, \mathbf{F}_{47}[Y]/(B) \cong \mathbf{F}_{47}$
なので
$\mathbf{Z}[\sqrt{-5}]/(47) \cong \mathbf{F}_{47} \oplus \mathbf{F}_{47}$
よって、(47) による剰余環は、環の直和になる。

$\alpha = 7 + 3\sqrt{-5}$ とする。
$\mathbf{Z}[\sqrt{-5}]/(7 + 3\sqrt{-5}) \cong \mathbf{Z}[X]/(X^2 + 5, 7 + 3X)$
$I = (X^2 + 5, 7 + 3X)$ とする。
$3(X^2 + 5) - (X - 2)(7 + 3X) = 29 - X = Y$
これから
$X = 29 - Y$
$X^2 + 5 = (29 - Y)^2 + 5 = Y^2 - 58Y + 846$
$7 + 3X = 7 + 3(29 - Y) = -3Y + 94$
したがって
$I = (Y^2 - 58Y + 846, -3Y + 94) \supset (Y)$
このとき
$846 = 2 \cdot 3^2 \cdot 47$
$94 = 2 \cdot 47$
なので
$\mathbf{Z}[X]/I \cong (\mathbf{Z}[Y]/(Y))/I \cong \mathbf{Z}/(94) \cong \mathbf{Z}/(2) \oplus \mathbf{Z}/(47) = \mathbf{F}_2 \oplus \mathbf{F}_{47}$
よって、$(\alpha) = (7 + 3\sqrt{-5})$ による剰余環は、環の直和になる。

ここで
$j_1 = (7 + sqrt{-5}, 2), j_2 = (7 + 3\sqrt{-5}, 47)$ とする。
$j_1 j_2 = (4 + 42\sqrt{-5}, 329 + 141\sqrt{-5}, 14 + 6\sqrt{-5}, 94)$
このとき
$329 + 141\sqrt{-5} = 47(7 + 3\sqrt{-5}), 14 + 6\sqrt{-5} = 2(7 + 3\sqrt{-5}),$
$94 = (3 - 7\sqrt{-5})(3 + 7\sqrt{-5}), 94 + (4 + 42\sqrt{-5}) = 14(7 + 3\sqrt{-5})$
なので
$j_1 j_2 = (7 + 3\sqrt{-5})$ となる。
これから
$94 = 2 \cdot 47 = (7 + 3\sqrt{-5})(7 - 3\sqrt{5}) = j_1 j_2 \bar{j_1} \bar{j_2}$
となり素イデアルの積で表せる。