$Z = X^2 + kY^2$で表される数Z

坂本　優人
学習院大学理学部数学科

Contents

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$k = 2, 3, 5, 6, 7$ の場合を調べたが、今は$k = 2, 5$ について詳しく説明する。

X^2+2Y^2 の表

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

X^2+2Y^2の値	因数分解	X^2+2Y^2 の形で表記
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
⋮	⋮	⋮
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+5Y^2 の表

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

X^2+5Y^2の値	因数分解	X^2+5Y^2 の形で表記
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
⋮	⋮	⋮
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

2. 表からわかること

$Z = X^2 + kY^2$ と因数の関係

$k = 2$ 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。

他の$k=3,7$についても同様の通りに分解できた。
これから、$k=2,3,7$のとき、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}通りに分解できることがわかった。
しかし$k=5,6$のときはこの法則を満たさないものがあった。

$k=5$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。

$k = 6$ のときも同様に法則を満たさないものがあった。
$k = 5$ では、Z が2 の因数を持つとき、$k = 6$ では、2 か3 の因数を持つとき法則を満たさないことがわかった。

3. 剰余環についての考察

$Z = X^2 + 5Y^2$ 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。

(α) による剰余環が体になる場合

$Z = 181$ とする。
$181 = (1 + 6\sqrt{-5})(1 - 6\sqrt{-5})$
$\alpha = 1 + 6\sqrt{-5}$ 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
$\mathbf{Z}[\sqrt{-5}]/(1 + 6\sqrt{-5}) \cong \mathbf{Z}[X]/J \cong (\mathbf{Z}[Y]/(Y))/J \cong \mathbf{F}_{181}$
ゆえに (α) における剰余環は体になる。

これは任意の素数$p = a^2 + 5b^2$について体になることがいえる。
$\alpha = a + b\sqrt{-5}$ とする。
$\mathbf{Z}[\sqrt{-5}]/(a + b\sqrt{-5}) \cong \mathbf{Z}[X]/(X^2 + 5, a + bX)$
$J = (X^2 + 5, a + bX)$ とする。
$b(X^2 + 5) - X(a + bX) = 5b - aX \in J$
また$a + bX \in J$
aとbは互いに素より
$1 = as + bt$ となるs, t がある。
$-s(5b - aX) + t(a + bX) = at - 5bs + (as + bt)X$
$= -5bs + at + X = Y \in J$
$(a - bX)(a + bX) = a^2 - b^2X^2 = a^2 + 5b^2 - b^2(X^2 + 5)$

これから
$p \in J$
$J_0 = (Y, p) \subset J$ とすると
$\mathbf{Z}[Y]/J_0 \cong \mathbf{Z}/(p)$
よって J_0 は極大イデアルになるので
$J_0 = J$
したがって
$\mathbf{Z}[\sqrt{-5}]/(a + b\sqrt{-5}) \cong \mathbf{F}_p$
ゆえに、(α) における剰余環は体になる。

α による剰余環が環の直和または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。

$Z = 86$ とする。
$86 = 2 \cdot 43 = (9 + \sqrt{-5})(9 - \sqrt{-5})$
$\mathbf{Z}[\sqrt{-5}]/(2) \cong \mathbf{Z}[X]/(X^2 + 5, 2)$
$J_1 = (X^2 + 5, 2)$ 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
$\mathbf{Z}[\sqrt{-5}]/(2) \cong \mathbf{Z}[Y]/J_1 \cong (\mathbf{Z}[Y]/(2))/(Y^2) \cong \mathbf{F}_2/(Y^2)$
これは無限小拡大環になる。

$\mathbf{Z}[\sqrt{-5}]/(43) \cong \mathbf{Z}[X]/(X^2+5, 43)$
$J_2 = (X^2+5, 43)$ とする。
$X^2 + 5 - 43 \cdot 2 = X^2 - 81 = (X+9)(X-9)$
$Y = X - 9$ とすると
$J_2 = (43, Y(Y+18)) \supset (43)$
これから
$\mathbf{Z}[\sqrt{-5}]/(43) \cong \mathbf{Z}[Y]/J_2 \cong (\mathbf{Z}[Y]/(43))/(Y(Y+18))$
$\cong \mathbf{F}_{43}/(Y(Y+18))$

$18x \equiv 1 \mod 43$ 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1通りに表せる。