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

Contents

1. 研究内容

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。剰余環やイデアル分解を使って Z の数の性質について研究することが目的である。

この研究では $p = 2, 3, 5, 6, 7$ の場合を調べたが、ここでは $Z = X^2 + 6Y^2$ の解について発表する。

2. $Z = X^2 + 6Y^2$ の表

Zの値	Zの因数分解	$X^2 + 6Y^2$ 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

Zの値	Zの因数分解	X^2+6Y^2 で表記
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

Zの値	Zの因数分解	X^2+6Y^2 で表記
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
⋮	⋮	⋮
⋮	⋮	⋮

3. 表から分かる規則性

・$Z = X^2 + 6Y^2$ の解については、必ずしも Z の異なる素因数が n 個なら 2^{n-1} 個の異なる解が出るとは限らない。Z が2の倍数または3の倍数のとき規則性が乱れる。

この規則性の乱れを研究するため、$\mathbf{Z}[\sqrt{-6}]$ において、既約元 α について (α) による剰余環を調べた。

4. 剰余環とイデアル分解の例

$\mathbf{Z}[\sqrt{-6}] = \left\{a + b\sqrt{-6} : a, b \in \mathbf{Z}\right\}$ 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。

$\mathbf{Z}[\sqrt{-6}] = \left\{a + b\sqrt{-6} : a, b \in \mathbf{Z}\right\}$ において、既約元 α について (α) による剰余環を調べると、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がわかった。

それぞれ例を出して確かめる。

(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、$Z = 271$

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

$\alpha = 11 + 5\sqrt{-6}, J = (X^2 + 6, 11 + 5X)$ 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。

$X^2+6Y^2=P$ （P:素数）のときの一般論

このとき、$a+b\sqrt{-6}$ は素元である。

$J=(X^2+6, a+bX)$ とおく。

$b(X^2+6)-(a+bX)X=6b-aX\in J,\ \ a+bX\in J$

$1=as+bt$ となる s,t がある。

$s(6b-aX)-t(a+bX)=-X+6sb-ta$

$-X+6sb-ta=Y$ とおく。

$Y\in J,\ (a-bX)(a+bX)=a^2-b^2X^2=a^2+6b^2-b^2(X^2+6)$

$P=a^2+6b^2\in J$

$(Y,p)=J_0\subset J$

$\mathbf{Z}[Y]/J_0\cong\mathbf{Z}/(P)$

$J_0=J,\ \ \mathbf{Z}[Y]/(a+b\sqrt{-6})\cong\mathbf{F}/(P)$

一般論から $-X+6sb-ta=Y$ とおけばうまくいくことを確かめる。

$271=(11+5\sqrt{-6})(11-5\sqrt{-6})$
$\alpha=11+5\sqrt{-6}, J=(X^2+6, 11+5X)$ とおく。
$1=11s+5t$ となる s,t がある。
$s=1,\ t=-2$
$-X+6sb-ta=52-X$
$52-X$ を Y とおくと $J=(Y^2-104Y+2710, 271-5Y)$ 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。

(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、$Z = 231$

$$
\begin{aligned}
Z = 231 &= 3 \cdot 7 \cdot 11 \\
&= \left(9 + 5\sqrt{-6}\right)\left(9 - 5\sqrt{-6}\right) \\
&= \left(15 + \sqrt{-6}\right)\left(15 - \sqrt{-6}\right)
\end{aligned}
$$

既約元 (3), (11), $\left(9 + 5\sqrt{-6}\right)$ による剰余環の例を出す。

$J = (X^2 + 6, 3)$ 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。

$J = (X^2 + 6, 11)$ 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 とおくと $(X - 4)(X + 4) = Y(Y + 8)$
$J_1 = (Y(Y + 8), 11) \supset (11)$ とおく。
$$\begin{aligned}\mathbf{Z}[\sqrt{-6}]/(11) = \mathbf{Z}[Y]/J_1 &\cong (\mathbf{Z}[Y]/(11))/(Y(Y + 8)) \\ &\cong \mathbf{F}_{11}[Y]/(Y(Y + 8))\end{aligned}$$

$8x \equiv 1 \bmod 11$ 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。

$A = -4\,(Y + 8),\ \ B = 4Y$ （ $-4\,(Y + 8) \bmod 11 \equiv 1 - 4Y$ ）

$AB \in (Y^2 + 8Y),\ \ A + B = 1$

$\mathbf{F}_{11}[Y]/\,(1 - 4Y) = \mathbf{F}_{11}$

$\mathbf{F}_{11}[Y]/\,(B) = \mathbf{F}_{11}$

$\mathbf{Z}[\sqrt{-6}]/(11) \cong \mathbf{F}_{11}[Y]/\,(Y\,(Y + 8))$

$\cong \mathbf{F}_{11}[Y]/\,(A) \oplus \mathbf{F}_{11}[Y]/\,(B) \cong \mathbf{F}_{11} \oplus \mathbf{F}_{11}$

したがって、(11) による剰余環は、環の直和になる。

$\alpha = 9 + 5\sqrt{-6}, J = (X^2 + 6, 9 + 5X)$ とおく。

$\mathbf{Z}[\sqrt{-6}]/(\alpha) \cong \mathbf{Z}[X]/J$

$5(X^2 + 6) - (X - 2)(9 + 5X) = X + 48$

$X + 48$ を Y とおくと $J = (Y^2 - 96Y + 2310, 5Y - 231)$ となる。

$2310 = 231 \cdot 10$ より

$$\mathbf{Z}[\sqrt{-6}]/(\alpha) \cong (\mathbf{Z}[Y]/(Y))/J \cong \mathbf{Z}/(231)$$
$$\cong \mathbf{Z}/(3) \oplus \mathbf{Z}/(7) \oplus \mathbf{Z}/(11) = \mathbf{F}_3 \oplus \mathbf{F}_7 \oplus \mathbf{F}_{11}$$

したがって、(α) による剰余環は、環の直和になる。

5. $\mathbf{Z}[\sqrt{-6}]$ において方程式 $Z = X^2 + 6Y^2$ を考察

例、$Z = 231 = 3 \cdot 7 \cdot 11$

$\mathbf{Z}[\sqrt{-6}]$ において

$$231 = \left(9 + 5\sqrt{-6}\right)\left(9 - 5\sqrt{-6}\right)$$
$$= \left(15 + \sqrt{-6}\right)\left(15 - \sqrt{-6}\right)$$

$7 = \left(1 + \sqrt{-6}\right)\left(1 - \sqrt{-6}\right) = \alpha\bar{\alpha}$ とおく。

$Z = 3, 11$ は解がないので、解のある $Z = 33$ を使う。

$33 = 3 \cdot 11 = \left(3 + 2\sqrt{-6}\right)\left(3 - 2\sqrt{-6}\right) = \beta\bar{\beta}$ とおく。

$\alpha\beta = -9 + 5\sqrt{-6}$, $\alpha\bar{\beta} = 15 + \sqrt{-6}$

$231 = 7 \cdot 33 = \alpha\beta \cdot \bar{\alpha}\bar{\beta} = \alpha\bar{\beta} \cdot \bar{\alpha}\beta$

$\mathbf{Z}[\sqrt{-6}]$ において $3, 11$ は既約元だが、素元ではない。

3,11 をどう扱うか？

$7 = \left(1+\sqrt{-6}\right)\left(1-\sqrt{-6}\right) = \alpha\bar{\alpha}$

$33 = 3\cdot 11 = \left(3+2\sqrt{-6}\right)\left(3+2\sqrt{-6}\right) = \beta\bar{\beta}$

$J_1 = (3, 3+2\sqrt{-6}),\ \ J_2 = (11, 3+2\sqrt{-6})$

$J_1J_2 = (3\cdot 11,\ 15+12\sqrt{-6},\ 11(3+2\sqrt{-6}),\ 3(3+2\sqrt{-6}))$

$3\cdot 11 = \left(3+2\sqrt{-6}\right)\left(3-2\sqrt{-6}\right)$

$15+12\sqrt{-6} = (3+2\sqrt{-6})^2$

よって、$J_1J_2 = (3+2\sqrt{-6})$

$3\cdot 11 = \left(3+2\sqrt{-6}\right)\left(3-2\sqrt{-6}\right) = J_1J_2\bar{J}_1\bar{J}_2$ であり、

33 は素イデアルの積で1通りに表せる。

$231 = 7\cdot 33 = \alpha\bar{\alpha}\beta\bar{\beta} = \alpha\bar{\alpha}J_1J_2\bar{J}_1\bar{J}_2$