方程式 $x^2 + py^2 = z$ の解の研究

齋藤　孝仁

2013年2月2日

0.はじめに

- ２次体の整数環は普段当たり前だと思われている素因数分解の一意性が成り立たないことが多い。
- そこで虚２次体の整数環である$\mathbb{Z}[\sqrt{-p}](p = 3,7)$について考え、素因数分解の一意性が成り立たない中にも何か規則があるのではないかというのが今回の研究の目的である。また素因数分解の一意性と関連して二平方和問題の類似（整数zがある2つの整数x, yの平方を用いて$z = x^2 + py^2$と表せるかという問題）の研究も試みた。
- 計算はPrologを用いたプログラムによるものである。

1.素因数分解の一意性

1.1. $\mathbb{Z}[\sqrt{-3}]$ と $\mathbb{Z}[\sqrt{-7}]$

次は素因数分解の一意性が成り立たない例を見てみたいと思う。

例）$\mathbb{Z}[\sqrt{-3}]$における4の因数分解

- $4 = 2^2$
- $4 = (1+\sqrt{-3})(1-\sqrt{-3})$

2も$1 \pm \sqrt{-3}$も既約元より因数分解が2通りある。
よって素因数分解の一意性が成り立たない。

例）$\mathbb{Z}[\sqrt{-7}]$における8の因数分解

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

2も$1 \pm \sqrt{-7}$も既約元より因数分解が2通りある。
よって素因数分解の一意性が成り立たない。

1.2.素因数分解の一意性不成立の理由

- $\mathbb{Z}[\sqrt{-p}](p = 3,7)$では素因数分解の一意性が成り立たないことが分かった。

この原因は何か？

- 整数環$\mathbb{Z}$では素因数分解をすれば因数が必ず素数となる。
- しかし2次体の整数環では素因数分解をしても因数が必ず素元になるとは限らず、既約元となる場合がある。これが理由である。
- つまり2次体の整数環には素数が少ないのではないかと考えられる。
- そこで**デデキント(1831-1916)**は素数の代わりに素イデアルを利用し、素イデアル分解を考えることにより分解の一意性を回復させることを考えた。

2.二平方和問題

2.1.二平方和問題

- 二平方和問題とは
「$z = x^2 + y^2$と表せる有理整数zはどんな数か」という問題である。

- そこで今回$\mathbb{Z}\left[\sqrt{-p}\right](p = 3,7)$を研究するにあたって、二平方和問題の類似として、
「$z = x^2 + py^2(p = 3,7)$と表せる有理整数zはどんな数か」という研究を行うことにした。

2.2. $\mathbb{Z}[\sqrt{-3}]$と$\mathbb{Z}[\sqrt{-7}]$の二平方和

- $\mathbb{Z}[\sqrt{-3}]$の二平方和について
  $z = x^2 + 3y^2$と表せる有理奇数zについて、
  方程式の解であるx, yを表にまとめた。
  ただしzは3で割れない数とする。

- $\mathbb{Z}[\sqrt{-7}]$の二平方和について
  $z = x^2 + 7y^2$と表せる有理奇数zについて、
  方程式の解であるx, yを表にまとめた。
  ただしzは7で割れない数とする。

$\mathbb{Z}[\sqrt{-3}]$の二平方和

$z = x^2 + 3y^2$

z	x	y	因数分解
7	2	1	7
13	1	2	13
19	4	1	19
31	2	3	31
37	5	2	37
43	4	3	43
49	1	4	7^2
61	7	2	61
67	8	1	67
73	5	4	73
79	2	5	79
91	4	5	$7 * 13$
	8	3	
97	7	4	97
103	10	1	103
109	1	6	109
127	10	3	127
133	5	6	$7 * 19$
	11	2	
139	8	5	139
151	2	7	151
157	7	6	157
163	4	7	163
169	11	4	13^2
181	13	2	181
193	1	8	193
199	14	1	199
211	8	7	211
217	5	8	$7 * 31$
	13	4	
223	14	3	223
229	11	6	229
241	7	8	241
247	2	9	$13 * 19$
	10	7	
259	4	9	$7 * 37$
	16	1	
271	14	5	271
277	13	6	277
283	16	3	283
301	1	10	$7 * 43$
	17	2	
307	8	9	307
313	11	8	313
331	16	5	331
337	17	4	337
343	10	9	7^3
349	7	10	349
361	13	8	19^2
367	2	11	367
373	19	2	373
379	4	11	379
397	17	6	397
403	16	7	$13 * 31$
	20	1	
409	19	4	409
421	11	10	421
427	8	11	$7 * 61$
	20	3	
433	1	12	433
439	14	9	439
457	5	12	457
463	10	11	463
469	13	10	$7 * 67$
	19	6	
481	7	12	$13 * 37$
	17	8	
487	22	1	487
499	16	9	499

$\mathbb{Z}[\sqrt{-3}]$の二平方和　　$z = x^2 + 3y^2$

z	x	y	因数分解
1729	1	24	$7 * 13 * 19$
	23	20	
	31	16	
	41	4	
2821	11	30	$7 * 13 * 31$
	37	22	
	43	18	
	53	2	

z	x	y	因数分解
53599	46	131	$7 * 13 * 19 * 31$
	82	125	
	118	115	
	134	109	
	206	61	
	214	51	
	218	45	
	226	29	
2000089	283	800	$7 * 13 * 31 * 709$
	499	764	
	517	760	
	667	720	
	1139	484	
	1229	404	
	1331	276	
	1381	176	

$\mathbb{Z}[\sqrt{-7}]$の二平方和

$z = x^2 + 7y^2$

z	x	y	因数分解
11	2	1	11
23	4	1	23
29	1	2	29
37	3	2	37
43	6	1	43
53	5	2	53
67	2	3	67
71	8	1	71
79	4	3	79
107	10	1	107
109	9	2	109
113	1	4	113
121	3	4	11^2
127	8	3	127
137	5	4	137
149	11	2	149
151	12	1	151
163	10	3	163
179	2	5	179
191	4	5	191
193	9	4	193
197	13	2	197
211	6	5	211
233	11	4	233
239	8	5	239
253	1	6	$11 * 23$
	15	2	
263	16	1	263
277	5	6	277
281	13	4	281
317	17	2	317
319	12	5	$11 * 29$
	16	3	
331	18	1	331
337	15	4	337
347	2	7	347
359	4	7	359
373	11	6	373
379	6	7	379
389	19	2	389
401	17	4	401
407	8	7	$11 * 37$
	20	1	
421	13	6	421
431	16	5	431
443	10	7	443
449	1	8	449
457	3	8	457
463	20	3	463
473	5	8	$11 * 43$
	19	4	
487	12	7	487
491	22	1	491
499	18	5	499
529	9	8	23^2
541	17	6	541
547	22	3	547
557	23	2	557
569	11	8	569
571	2	9	571
583	4	9	$11 * 53$
	24	1	
599	16	7	599
613	19	6	613
617	13	8	617
631	8	9	631
641	23	4	641
653	25	2	653
659	22	5	659
667	10	9	$23 * 29$
	18	7	
673	15	8	673
683	26	1	683
701	1	10	701
709	3	10	709
737	17	8	$11 * 67$
	25	4	
739	26	3	739
743	20	7	743
751	24	5	751
757	27	2	757

$\mathbb{Z}[\sqrt{-7}]$の二平方和　　$z = x^2 + 7y^2$

z	x	y	因数分解
204479	136	163	$11 * 29 * 641$
	284	133	
	416	67	
	452	5	
207391	52	171	$23 * 71 * 127$
	228	149	
	396	85	
	452	21	

z	x	y	因数分解
315491	62	211	$11 * 23 * 29 * 43$
	146	205	
	302	179	
	442	131	
	454	125	
	482	109	
	538	61	
	554	35	

表から考察されること①

べき乗を1つの因数とみなせば、

- zが$\mathbb{Z}$で相異なる2つの素数で分解されるとき、二平方和は2通りある
- zが$\mathbb{Z}$で相異なる3つの素数で分解されるとき、二平方和は4通りある
- zが$\mathbb{Z}$で相異なる4つの素数で分解されるとき、二平方和は8通りある

これから推測できることは、

- zが$\mathbb{Z}$で相異なるn個の素数で分解されるとき、二平方和は2^{n-1}通りある

ということである。

表から考察されること②

- $\mathbb{Z}[\sqrt{-3}]$において

  $z = x^2 + 3y^2$と表せる有理素数qは、

  $$q \equiv 1 \ (mod 6)$$

- $\mathbb{Z}[\sqrt{-7}]$において

  $z = x^2 + 7y^2$と表せる有理素数qは、

  $$q \equiv 1,5 (mod 6)$$

  と表せる。

2.3. $\mathbb{Z}[\sqrt{-3}]$の素元

- 表から7の$\mathbb{Z}[\sqrt{-3}]$における因数分解は、
$$7 = 2^2 + 3 \times 1^2 = (2 + \sqrt{-3})(2 - \sqrt{-3})$$
となることがわかる。

- これを利用して有理素数を$\mathbb{Z}[\sqrt{-3}]$で因数分解したときの因数が素元であるかどうかを確かめるため、その因数によるイデアルを考え剰余環が体になるかどうかを考える。

- $R_0 := \mathbb{Z}[\sqrt{-3}] \cong \mathbb{Z}[X]/(X^2 + 3)$
- $R_1 := \mathbb{Z}[X] \supset I$

$7 = (2 + \sqrt{-3})(2 - \sqrt{-3})$について

$I = (X^2 + 3, 2 + X)$とする。

$2 + X = Y$とおけば

$$I = (Y^2 - 4Y + 7, Y) = (Y, 7)$$

となるから、

$$R_1/I \cong \mathbb{Z}[Y]/(Y, 7) \cong F_7$$

R_1/I が体になったので、$2 + \sqrt{-3}$は素元である。

$13 = (1 + 2\sqrt{-3})(1 - 2\sqrt{-3})$について

$I = (X^2 + 3, 1 + 2X)$とする。

$$2(X^2 + 3) - X(1 + 2X) = 6 - X \in I$$

より$6 - X = Y$とおけば

$$I = (X^2 + 3, 1 + 2X, 6 - X)$$
$$= (Y^2 - 2Y + 39, -2Y + 13, Y)$$
$$= (39, 13, Y) = (Y, 13)$$

となるから、

$$R_1/I \cong \mathbb{Z}[Y]/(Y, 13) \cong F_{13}$$

R_1/I が体になったので、$1 + 2\sqrt{-3}$は素元である。

より一般化して、
$p = a^2 + 3b^2$と表せる有理素数pに対して、
$a + b\sqrt{-3}$は$\mathbb{Z}\left[\sqrt{-3}\right]$の素元になる。

証明）
$J = (X^2 + 3, a + bX)$とおくと、
$b\left(X^2 + 3\right) - X(a + bX) = 3b - aX \in J$である。
$as + bt = 1$となる整数s, tがあるので、
$-s(3b - aX) + t(a + bX) = X + at - 3bs =: Y \in J$とおく。
$(a + bX)(a - bX) = a^2 - b^2X^2 = (a^2+3b^2) - b^2(X^2 + 3)$より、
$p = a^2 + 3b^2 \in J$である。
$(Y, p) = J_0 \subset J$とすれば、$\mathbb{Z}[Y]/J_0 \cong F_p$となり体になる。
J_0は極大イデアルだから$J_0 = J$となるから、
$\mathbb{Z}\left[\sqrt{-3}\right]/(a + b\sqrt{-3}) \cong F_p$であり、
$a + b\sqrt{-3}$は$\mathbb{Z}\left[\sqrt{-3}\right]$の素元になる。

- この結果から表の平方和の2つの整数を$x \pm y\sqrt{-3}$の形の因数と思えば、表に出てきたすべての素数は$x \pm y\sqrt{-3}$を素元としてうまく素元分解ができるといえる。

- ではUFD不成立には欠かせない存在である“素元でない既約元はなんなのだろうか”ということを考えるべく、表には出てこなかった数を考えたいと思う。

$4 = 2^2 = (1+\sqrt{-3})(1-\sqrt{-3})$について

$$R_0/(2) \cong R_1/(X^2+3,2) = R_1/(X^2-1,2)$$
$$\cong F_2[X]/(X^2-1) = F_2[X]/((X+1)(X-1))$$

ここで$X+1=A, 1-X=B$とおけば、

$A+B=2\equiv 0(mod2)$より$B=-A$とできるので、

$$R_0/(2) \cong F_2[X]/(A^2) = F_2[A]/(A^2)$$

という無限小拡大環となるので、2は素元ではない。

$$R_0/(1+\sqrt{-3}) \cong R_1/(X^2+3,1+X) \cong \mathbb{Z}[Y]/(Y,4) \cong \mathbb{Z}_4$$

という環になり体ではないので、

$1+\sqrt{-3}$も素元ではない。

- 以上の考察から$\mathbb{Z}[\sqrt{-3}]$がUFDとなれない理由は、素元でない既約元“2と$1 \pm \sqrt{-3}$”の存在であるといえ、なおかつ素元でない既約元はこの3つだけに限られると考えられる。

2.4.$\mathbb{Z}[\sqrt{-7}]$の素元

- $R_0 := \mathbb{Z}[\sqrt{-7}] \cong \mathbb{Z}[X]/(X^2 + 7)$
- $R_1 := \mathbb{Z}[X] \supset I$

$11 = (2 + \sqrt{-7})(2 - \sqrt{-7})$について

$I = (X^2 + 7, 2 + X)$とする。

$2 + X = Y$とおけば

$$I = (Y^2 - 4Y + 11, Y) = (Y, 11)$$

となるから、

$$R_1/I \cong \mathbb{Z}[Y]/(Y, 11) \cong F_{11}$$

R_1/I が体になったので、$2 + \sqrt{-7}$は素元である。

$23 = (4 + \sqrt{-7})(4 - \sqrt{-7})$について

$I = (X^2 + 7, 4 + X)$とする。

$4 + X = Y$とおけば

$$I = (Y^2 - 8Y + 23, Y) = (Y, 23)$$

となるから、

$$R_1/I \cong \mathbb{Z}[Y]/(Y, 23) \cong F_{23}$$

R_1/I が体になったので、$4 + \sqrt{-7}$は素元である。

より一般化して、
$p = a^2 + 7b^2$と表せる有理素数pに対して、
$a + b\sqrt{-7}$は$\mathbb{Z}\left[\sqrt{-7}\right]$の素元になる。

証明）
$J = (X^2 + 7, a + bX)$とおくと、
$b\left(X^2 + 7\right) - X(a + bX) = 7b - aX \in J$である。
$as + bt = 1$となる整数s, tがあるので、
$-s(7b - aX) + t(a + bX) = X + at - 7bs =: Y \in J$とおく。
$(a + bX)(a - bX) = a^2 - b^2X^2 = (a^2 + 7b^2) - b^2(X^2 + 7)$より、
$p = a^2 + 7b^2 \in J$である。
$(Y, p) = J_0 \subset J$とすれば、$\mathbb{Z}[Y]/J_0 \cong F_p$となり体になる。
J_0は極大イデアルだから$J_0 = J$となるから、
$\mathbb{Z}\left[\sqrt{-7}\right]/(a + b\sqrt{-7}) \cong F_p$であり、
$a + b\sqrt{-7}$は$\mathbb{Z}\left[\sqrt{-7}\right]$の素元になる。

- この結果から表の平方和の2つの整数を$x \pm y\sqrt{-7}$の形の因数と思えば、表に出てきたすべての素数は$x \pm y\sqrt{-7}$を素元としてうまく素元分解ができるといえる。

- ではUFD不成立には欠かせない存在である“素元でない既約元はなんなのだろうか”ということを考えるべく、表には出てこなかった数を考えたいと思う。

$8 = 2^3 = (1+\sqrt{-7})(1-\sqrt{-7})$について

$$R_0/(2) \cong R_1/(X^2+7,2) = R_1/(X^2-1,2)$$
$$\cong F_2[X]/(X^2-1) = F_2[X]/((X+1)(X-1))$$

ここで$X+1=A, 1-X=B$とおけば、

$A+B=2\equiv 0(mod2)$より$B=-A$とできるので、

$$R_0/(2) \cong F_2[X]/(A^2) = F_2[A]/(A^2)$$

という無限小拡大環となるので、2は素元ではない。

$$R_0/(1+\sqrt{-7}) \cong R_1/(X^2+7,1+X) \cong \mathbb{Z}[Y]/(Y,8) \cong \mathbb{Z}_8$$

という環になり体ではないので、$1+\sqrt{-7}$も素元ではない。

- 以上の考察から$\mathbb{Z}[\sqrt{-7}]$がUFDとならない理由は、素元でない既約元“2と$1 \pm \sqrt{-7}$”の存在であるといえ、なおかつ素元でない既約元はこの3つだけに限られると考えられる。

3.まとめと今後の課題

3.1.まとめ

今回方程式$x^2 + py^2 = z$の解の研究ということで$\mathbb{Z}[\sqrt{-3}]$と$\mathbb{Z}[\sqrt{-7}]$に焦点を当てて研究をした。その結果としては、

(1)有理奇数zにおいて方程式$x^2 + py^2 = z\ (p \nmid z)$をみたす互いに素な整数解$x, y$（二平方和の表し方）は、$z$が相異なる$n$個の素数で分解されるとき二平方和は$2^{n-1}$通りある（べき乗を1つの因数とみなす）。

(2)$\mathbb{Z}[\sqrt{-3}]$において$z = x^2 + 3y^2$と表せる
　有理素数qは、$q \equiv 1 \ (mod 6)$である。

(3) $p = a^2 + 3b^2$と表せる有理素数pに対して、
$a + b\sqrt{-3}$は$\mathbb{Z}[\sqrt{-3}]$の素元になる。

(4)$\mathbb{Z}[\sqrt{-3}]$の素元でない既約元は、
　“2と$1 \pm \sqrt{-3}$”だけである。

(5)$\mathbb{Z}\left[\sqrt{-7}\right]$において$z = x^2 + 7y^2$と表せる
有理素数qは、$q \equiv 1, 5(mod 6)$である。

(6) $p = a^2 + 7b^2$と表せる有理素数pに対して、
$a + b\sqrt{-7}$は$\mathbb{Z}\left[\sqrt{-7}\right]$の素元になる。

(7)$\mathbb{Z}\left[\sqrt{-7}\right]$の素元でない既約元は、
“2と$1 \pm \sqrt{-7}$”だけである。

3.2.今後の課題

- 他の虚2次体の整数環ではどうなるのかを調べること
- 素イデアル分解も考えてこれとの関係性を調べること
- 正規化環$\mathbb{Z}[\omega]$（但しωは虚数立方根）と関連して調べること

3.3.参考文献

[1] 青木昇 「素数と2次体の整数論」共立出版 2012

[2] 中島匠一 「代数と数論の基礎」共立出版 2009

[3] 山本芳彦 「数論入門」岩波書店 2009

[4] 飯高茂 「環論、これはおもしろい」共立出版 2012

[5] Miles Reid 「Undergraduate Commutative Algebra」Cambridge University Press 1995

終