方程式 $x^2 + py^2 = z$ の解の研究

齋藤　孝仁

2013 年 2 月 2 日

目次

0　はじめに

有理数体は整数環を含み、２次体は有理数体を含む体である。２次体の整数環は一般の整数環とは一味違っていて、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。

そこで今回虚２次体の整数環である$\mathbb{Z}\left[\sqrt{-p}\right](p = 3,7)$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。

今回の研究における計算は Prolog を用いたプログラムによるものである。

1　準備

いくつか定義をし、定理や命題等については証明を省略する。

定義 1,1（２次体）

mを平方数でない整数とする。有理数体$\mathbb{Q}$と$\sqrt{m}$を含む最小の体を$\mathbb{Q}(\sqrt{m})$で表す。すなわち$\mathbb{Q}(\sqrt{m})$は、有理数と$\sqrt{m}$を用いて加減乗除で得られるすべての数の集合である。体$\mathbb{Q}(\sqrt{m})$を**２次体**と呼ぶ。

$m > 0$ならば$\mathbb{Q}(\sqrt{m})$を**実２次体**と呼ぶ。

$m < 0$ならば$\mathbb{Q}(\sqrt{m})$を**虚２次体**と呼ぶ。

命題 1,2

$\mathbb{Q}(\sqrt{m}) = \{a + b\sqrt{m} | a, b \in \mathbb{Q}\}$が成り立つ。

定義 1,3（共役）

２次体$\mathbb{Q}(\sqrt{m})$の元$\alpha = a + b\sqrt{m}(a, b \in \mathbb{Q})$に対して、$\bar{\alpha} = a - b\sqrt{m}$とおき、$\bar{\alpha}$を$\alpha$の**共役**と呼ぶ。

定義 1,4（ノルムとトレース）

２次体$\mathbb{Q}(\sqrt{m})$の元$\alpha = a + b\sqrt{m}(a, b \in \mathbb{Q})$に対して、

αの**ノルム**$N(\alpha)$を$N(\alpha) = \alpha\bar{\alpha} = a^2 - mb^2$により定義する。

αの**トレース**$T(\alpha)$ を$T(\alpha) = \alpha + \bar{\alpha} = 2a$により定義する。

命題 1,5

$\alpha, \beta \in \mathbb{Q}(\sqrt{m})$に対して、$N(\alpha\beta) = N(\alpha)N(\beta)$が成り立つ。

定義 1,6（２次体の整数環）

２次体$K = \mathbb{Q}(\sqrt{m})$に対して、$O_K := \{\alpha \in K | N(\alpha), T(\alpha) \in \mathbb{Z}\}$を$K$の整数環と呼ぶ。$O_K$の元を$K$の整数と呼ぶ。

※２次体の整数と区別するために、$\mathbb{Z}$の元を**有理整数**と呼ぶことにする。

定義 1,7（約数と倍数）

整数$\alpha,\beta \in O_K$に対して、$\beta = \alpha\gamma$をみたす整数$\gamma \in O_K$が存在するとき、「αはβを割り切る」といい、$\alpha \mid \beta$と表す。このときαをβの**約数**と呼び、βをαの**倍数**と呼ぶ。またαがβを割り切らないときは、$\alpha \nmid \beta$と表す。

定義 1,8（単数）

整数環O_Kにおける 1 の約数をO_Kの**単数**と呼ぶ。

言い換えれば$\varepsilon(\neq 0) \in O_K$が単数であるとは、$1/\varepsilon \in O_K$となることである。

また整数$\alpha,\beta \in O_K$に対し、$\alpha = \varepsilon\beta$となる単数$\varepsilon$が存在するとき、

αとβは**同伴**であるという。任意の整数αに対し、任意の単数及びαと同伴な任意の整数は常にαの約数である。これらをαの**自明な約数**と呼ぶ。

命題 1,9

整数$\alpha \in O_K$が単数であるためには$N(\alpha) = \pm 1$であることが必要十分である。

定義 1,10（素数）

πをO_Kの 0 でも単数でもない整数とする。πの約数が自明な約数に限るとき、πを**素数**と呼ぶ。

※２次体の素数と区別するために、$\mathbb{Z}$の素数を**有理素数**と呼ぶことにする。

定義 1,11（既約元と素元）

整数環O_Kの素数πに対して、

“πと同伴な整数は素数である”をみたすものを**既約元**と呼ぶ。

“πの共役$\bar{\pi}$も素数である”をみたすものを**素元**と呼ぶ。

定義 1,12（一意分解整域：UFD）

整数環O_Kの（0 でも単数でもない）元αに対し、

分解$\alpha = \pi_1\pi_2 \ldots \pi_r$（$\pi_1,\ldots,\pi_r$は$O_K$の素数）を$\alpha$の素因数分解と呼ぶ。

O_Kの元が一意的に素因数分解できるとき、O_Kを**一意分解整域**と呼ぶ。

定義 1,13（イデアル）

整数環O_Kの部分集合$A \neq \phi$が次の二つの条件をみたすとき、

AをO_Kの**イデアル**と呼ぶ。

（ｉ）任意の$\alpha, \beta \in A$に対して$\alpha + \beta \in A$

（ii）任意の$\alpha \in A$と$\gamma \in O_K$に対して$\alpha\gamma \in A$

また任意の$\alpha_1, \ldots, \alpha_n \in O_K$に対して、

$(\alpha_1, \ldots, \alpha_n) = \{\alpha_1\xi_1 + \cdots +, \alpha_n\xi_n | \xi_1, \ldots \xi_n \in O_K\}$とおいて、

$(\alpha_1, \ldots, \alpha_n)$を$\alpha_1, \ldots, \alpha_n$で生成される$O_K$のイデアルと呼ぶ。

特に整数$\alpha \in O_K$に対して、

$(\alpha) = \alpha O_K = \{\alpha\xi | \xi \in O_K\}$とおいて、

(α)をαで生成されるO_Kの単項イデアルと呼ぶ。

$(1) = O_K, (0) = \{0\}$である。

命題 1,14

整数$\alpha, \beta \in O_K$に対して次が成り立つ。

（ｉ）$(\alpha) \supset (\beta) \Leftrightarrow \alpha \mid \beta$

（ii）$(\alpha) = (\beta) \Leftrightarrow \alpha$と$\beta$は同伴

（iii）$(\alpha) = O_K \Leftrightarrow \alpha$は$O_K$の単数

定義 1,15（割り算原理とユークリッド整域）

任意の$\alpha, \beta \in O_K (\beta \neq 0)$に対して、

$\alpha = \beta\kappa + \lambda$かつ$|N(\lambda)| < |N(\beta)|$をみたす$\kappa, \lambda \in O_K$が存在するとき、

O_Kを**ユークリッド整域**と呼ぶ。

定義 1,16（単項イデアル整域：PID）

整数環O_Kの任意のイデアルが単項イデアルであるとき、

O_Kを単項イデアル整域と呼ぶ。

定理 1,17

ユークリッド整域は PID である。

定理 1,18

整数環O_Kが UFD であるためには、O_Kの任意の素数が(∗)をみたすことが必要十分である。

(∗) $\alpha, \beta \in O_K$について、π | αβ ⇒ π | αまたはπ | βが成り立つ。

定理 1,19

整数環O_Kが PID ならば UFD である。

定理 1,20

整数環O_Kが UFD ならば PID である。

補題 1,21

有理素数pがO_Kの素数でなければ、pはO_Kのある素数πを用いて、$p = \pm\pi\bar{\pi}$と素因数分解される。

命題 1,22

可換環RのイデアルIに関して次のことが成り立つ。

(ⅰ) Iは素イデアル⇔剰余環R/Iは整域

(ⅱ) Iは極大イデアル⇔剰余環R/Iは体

(ⅲ) 極大イデアルは素イデアルである

2　素因数分解の一意性

2.1 ガウス整数環$\mathbb{Z}[i]$

虚２次体の整数環を考えていくうえで大概は素因数分解の一意性が成り立たない。今回研究対象とする$\mathbb{Z}\left[\sqrt{-p}\right](p = 3,7)$も素因数分解の一意性が成り立たない例の一部である。（具体例は 2.2 で）
しかし虚２次体の整数環でもガウス整数環$\mathbb{Z}[i]$は素因数分解の一意性が成立する。（つまり UFD である。）

$\mathbb{Z}[i]$はユークリッド整域であり PID なので UFD である。
よって$\mathbb{Z}[i]$では単数倍を無視して素因数分解の一意性が成り立つ。
ただし$\mathbb{Z}[i]$の単数は$\pm 1, \pm i$である。

例）$\mathbb{Z}[i]$における 10 の素因数分解

$$10 = (1+i)(1-i)(2+i)(2-i)$$
$$10 = -i(1+i)^2(1+2i)(1-2i)$$

一見上式と下式の分解は異なっているように見えるが、次のように単数をかけて調整すれば同じになり、分解は１通りとなる。

$$1-i = -i(1+i)$$
$$2+i = i(1-2i)$$
$$2-i = -i(1+2i)$$

$\mathbb{Z}[i]$が PID になることを示す
証明）$\mathbb{Z}[i]$の元が定めるガウス平面の点を$1, i$を基にした格子点とみる。
これらの格子点は幅が 1、高さが 1 の正方形を単位とする。
与えられた格子点でない複素数zに最も近い格子点は、
zとの距離が$\sqrt{2}/2(< 1)$以内にある。
これから割り算原理が成立しユークリッド整域である。
それゆえ$\mathbb{Z}[i]$ではイデアルがすべて単項となる。終
以上から$\mathbb{Z}[i]$においては素因数分解の一意性が成り立つ。

2.2 $\mathbb{Z}[\sqrt{-3}]$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。

$\mathbb{Z}[\sqrt{-3}]$について

$\mathbb{Z}[\sqrt{-3}]$の元が定めるガウス平面の点を$1, \sqrt{-3}$を基にした格子点とし、
これらの格子点は幅が 1、高さが$\sqrt{3}$の長方形を単位とする。
与えられた格子点でない複素数zに最も近い格子点は、
zとの距離が1以内にある。
それゆえ割り算がうまくできずイデアルがすべて単項とならない。

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。

$\mathbb{Z}[\sqrt{-7}]$について

$\mathbb{Z}[\sqrt{-7}]$の元が定めるガウス平面の点を$1, \sqrt{-7}$を基にした格子点とし、これらの格子点は幅が 1、高さが$\sqrt{7}$の長方形を単位とする。

与えられた格子点でない複素数zに最も近い格子点は、

zとの距離が$\sqrt{2}(> 1)$以内にある。

それゆえ割り算がうまくできずイデアルがすべて単項とならない。

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。

以上から$\mathbb{Z}[\sqrt{-p}](p = 3,7)$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。

2.3 素因数分解の一意性不成立の理由

これまでのことから虚 2 次体の整数環では素因数分解の一意性が成り立たないことがしばしばあることがわかる。それではなぜ素因数分解の一意性が成り立たないのだろうか。

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。

ちなみに素イデアル分解の一意性こそがイデアルというものが考えだされた起源であり、理想数（ideal number）からきている。

3　二平方和問題

3.1 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$\mathbb{Z}[\sqrt{-p}](p = 3,7)$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。

3.2 $\mathbb{Z}[\sqrt{-3}]$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。

左から$z, x, y, \mathbb{Z}$におけるzの素因数分解となっている。

※今回は$z = x^2 + py^2$をみたす素数zの二平方和を重点的に考えるため、なるべく合成数が現れないよう奇数のみに限定した。
またzをpで割れないようにした理由は、
方程式の解であるx, yが互いに素となるためである。

$\mathbb{Z}[\sqrt{-3}]$の二平方和表

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 8	5 3	$7 * 13$
97	7	4	97
103	10	1	103
109	1	6	109
127	10	3	127
133	5 11	6 2	$7 * 19$
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

z	x	y	因数分解
211	8	7	211
217	5 13	8 4	$7 * 31$
223	14	3	223
229	11	6	229
241	7	8	241
247	2 10	9 7	$13 * 19$
259	4 16	9 1	$7 * 37$
271	14	5	271
277	13	6	277
283	16	3	283
301	1 17	10 2	$7 * 43$
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

z	x	y	因数分解
403	16 20	7 1	$13 * 31$
409	19	4	409
421	11	10	421
427	8 20	11 3	$7 * 61$
433	1	12	433
439	14	9	439
457	5	12	457
463	10	11	463
469	13 19	10 6	$7 * 67$
481	7 17	12 8	$13 * 37$
487	22	1	487
499	16	9	499

z	x	y	因数分解
1729	1 23 31 41	24 20 16 4	$7 * 13 * 19$
2821	11 37 43 53	30 22 18 2	$7 * 13 * 31$
53599	46 82 118 134 206 214 218 226	131 125 115 109 61 51 45 29	$7 * 13 * 19$ $* 31$
2000089	283 499 517 667 1139 1229 1331 1381	800 764 760 720 484 404 276 176	$7 * 13 * 31$ $* 709$

$\mathbb{Z}[\sqrt{-7}]$の二平方和表

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 15	6 2	$11 * 23$

z	x	y	因数分解
263	16	1	263
277	5	6	277
281	13	4	281
317	17	2	317
319	12 16	5 3	$11 * 29$
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 20	7 1	$11 * 37$
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 19	8 4	$11 * 43$
487	12	7	487
491	22	1	491
499	18	5	499

z	x	y	因数分解
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 24	9 1	$11 * 53$
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 18	9 7	$23 * 29$
673	15	8	673
683	26	1	683
701	1	10	701
709	3	10	709
737	17 25	8 4	$11 * 67$
739	26	3	739
743	20	7	743
751	24	5	751
757	27	2	757

z	x	y	因数分解
204479	136 284 416 452	163 133 67 5	$11 * 29 * 641$
207391	52 228 396 452	171 149 85 21	$23 * 71 * 127$
315491	62 146 302 442 454 482 538 554	211 205 179 131 125 109 61 35	$11 * 23 * 29$ $* 43$

上の表で考察されることは、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。

また$\mathbb{Z}[\sqrt{-3}]$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、

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

という考察ができる。

3.3 $\mathbb{Z}[\sqrt{-3}]$の素元

上の表から 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。

以下途中の計算は省略する。

●$19=(4+\sqrt{-3})(4-\sqrt{-3})$ について
$I=(X^2+3,4+X)$とする。
$4+X=Y$とおけば$I=(Y,19)$となるから、
$R_1/I\cong\mathbb{Z}[Y]/(Y,19)\cong F_{19}$
R_1/I が体になったので、$4+\sqrt{-3}$は素元である。

●$31=(2+3\sqrt{-3})(2-3\sqrt{-3})$について
$I=(X^2+3,2+3X)$とする。
$3(X^2+3)-X(2+3X)=9-2X\in I$
$(2+3X)+(9-2X)=X+11\in I$より$X+11=Y$とおけば
$I=(Y,31)$となるから、$R_1/I\cong\mathbb{Z}[Y]/(Y,31)\cong F_{31}$
R_1/I が体になったので、$2+3\sqrt{-3}$は素元である。

●$37=(5+2\sqrt{-3})(5-2\sqrt{-3})$について
$I=(X^2+3,5+2X)$とする。
$2(X^2+3)-X(5+2X)=6-5X\in I$
$3(5+2X)+(6-5X)=X+21\in I$より$X+21=Y$とおけば
$I=(Y,37)$となるから、$R_1/I\cong\mathbb{Z}[Y]/(Y,37)\cong F_{37}$
R_1/I が体になったので、$5+2\sqrt{-3}$は素元である。

●$43=(4+3\sqrt{-3})(4-3\sqrt{-3})$について

$I=(X^2+3,4+3X)$とする。

$3(X^2+3)-X(4+3X)=9-4X\in I$

$-(9-4X)-(4+3X)=X-13\in I$より$X-13=Y$とおけば

$I=(Y,43)$となるから、$R_1/I\cong\mathbb{Z}[Y]/(Y,43)\cong F_{43}$

R_1/I が体になったので、$4+3\sqrt{-3}$は素元である。

●$49=(1+4\sqrt{-3})(1-4\sqrt{-3})$について

$I=(X^2+3,1+4X)$とする。

$4(X^2+3)-X(1+4X)=12-X\in I$ より$12-X=Y$とおけば

$I=(Y,49)$となるから、

$R_1/I\cong\mathbb{Z}[Y]/(Y,49)\cong\mathbb{Z}_{49}$

R_1/I は体にならないので、$1+4\sqrt{-3}$は素元でない。

もともと$49=7^2$であり$7=(2+\sqrt{-3})(2-\sqrt{-3})$なので、

$49=\left(2+\sqrt{-3}\right)^2\left(2-\sqrt{-3}\right)^2$となる。

実際$1+4\sqrt{-3}=\left(2+\sqrt{-3}\right)^2$となるので、$1+4\sqrt{-3}$は既約元でもない。

●$61=(7+2\sqrt{-3})(7-2\sqrt{-3})$について

$I=(X^2+3,7+2X)$とする。

$2(X^2+3)-X(7+2X)=6-7X\in I$

$4(7+2X)+(6-7X)=X+34\in I$より$X+34=Y$とおけば

$I=(Y,61)$となるから、$R_1/I\cong\mathbb{Z}[Y]/(Y,61)\cong F_{61}$

R_1/I が体になったので、$7+2\sqrt{-3}$は素元である。

●$67=(8+\sqrt{-3})(8-\sqrt{-3})$ について

$I=(X^2+3,8+X)$とする。

$8+X=Y$とおけば$I=(Y,67)$となるから、

$R_1/I\cong\mathbb{Z}[Y]/(Y,67)\cong F_{67}$

R_1/I が体になったので、$8+\sqrt{-3}$は素元である。

●$73=(5+4\sqrt{-3})(5-4\sqrt{-3})$について

$I=(X^2+3,5+4X)$とする。

$4(X^2+3)-X(5+4X)=12-5X\in I$

$-(5+4X)-(12-5X)=X-17\in I$より$X-17=Y$とおけば

$I=(Y,73)$となるから、$R_1/I\cong\mathbb{Z}[Y]/(Y,73)\cong F_{73}$

R_1/I が体になったので、$5+4\sqrt{-3}$は素元である。

●$79=(2+5\sqrt{-3})(2-5\sqrt{-3})$について

$I=(X^2+3,2+5X)$とする。

$5(X^2+3)-X(2+5X)=15-2X\in I$

$(2+5X)+2(15-2X)=X+32\in I$より$X+32=Y$とおけば

$I=(Y,79)$となるから、$R_1/I\cong\mathbb{Z}[Y]/(Y,79)\cong F_{79}$

R_1/I が体になったので、$2+5\sqrt{-3}$は素元である。

●$91=\left(4+5\sqrt{-3}\right)\left(4-5\sqrt{-3}\right)=\left(8+3\sqrt{-3}\right)\left(8-3\sqrt{-3}\right)$について

$I_1=(X^2+3,4+5X)$とする。

$5(X^2+3)-X(4+5X)=15-4X\in I$

$(4+5X)+(15-4X)=X+19\in I$より$X+19=Y$とおけば

$I=(Y,91)$となるから、$R_1/I_1\cong\mathbb{Z}[Y]/(Y,91)\simeq\mathbb{Z}_{91}$

R_1/I_1 は体にならないので、$4+5\sqrt{-3}$は素元でない。

$I_2=(X^2+3,8+3X)$とする。

$3(X^2+3)-X(8+3X)=9-8X\in I$

$2(8+3X)+(9-8X)=25-2X\in I$

$(8+3X)+(25-2X)=X+33\in I$より$X+33=Y$とおけば

$I_2=(Y,91)$となるから、$R_1/I_2\cong\mathbb{Z}[Y]/(Y,91)\cong\mathbb{Z}_{91}$

R_1/I_2 は体にならないので、$8+3\sqrt{-3}$は素元でない。

もともと$91=7\times13$であり

$7=(2+\sqrt{-3})(2-\sqrt{-3})$で、$13=(1+2\sqrt{-3})(1-2\sqrt{-3})$だから、

$7=\alpha\bar{\alpha}$（但し$\alpha=2+\sqrt{-3}$）、$13=\beta\bar{\beta}$（但し$\beta=1+2\sqrt{-3}$）と思えば、

$91=\alpha\bar{\alpha}\beta\bar{\beta}=\alpha\beta\left(\overline{\alpha\beta}\right)=\alpha\bar{\beta}(\bar{\alpha}\beta)$と表せる。

$\alpha\beta = \left(2+\sqrt{-3}\right)\left(1+2\sqrt{-3}\right) = -4+5\sqrt{-3}$なので、
$4+5\sqrt{-3} = -\overline{\alpha\beta}$となり既約元でもない。
また$X=4, Y=5$とみれば 91 の平方和となっている。
同様に、
$\alpha\bar{\beta} = \left(2+\sqrt{-3}\right)\left(1-2\sqrt{-3}\right) = 8-3\sqrt{-3}$なので、
$8+3\sqrt{-3} = \bar{\alpha}\beta$となり既約元でもない。
また$X=8, Y=3$とみれば 91 の平方和となっている。

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、
$b(X^2+3) - X(a+bX) = 3b-aX \in J$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。

ここまでいくつか例を挙げたが 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出てこなかった。しかし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。
また合成数に関しては素因数分解したときに現れる素因数（素数）を上に述べたように素元分解し、その素元たちの組み合わせによるものであるといえる。

では“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、今回の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
先にも述べたように 2 も$1 \pm \sqrt{-3}$も既約元である。
そこでこれらによる剰余環を考える。

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

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。

また

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

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。

3.4 $\mathbb{Z}[\sqrt{-7}]$の素元

3.3 と同様に考える。

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

$R_1 := \mathbb{Z}[X] \supset I$

●$11 = (2+\sqrt{-7})(2-\sqrt{-7})$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。

●$29 = (1+2\sqrt{-7})(1-2\sqrt{-7})$について

$I = (X^2+7, 1+2X)$とする。

$2(X^2+7) - X(1+2X) = 14 - X \in I$より$14 - X = Y$とおけば

$I = (X^2+7, 1+2X, 14-X) = (203-2Y+Y^2, 29-2Y, Y)$

$= (Y, 29, 203) = (Y, 29)$となるから、

$R_1/I \cong \mathbb{Z}[Y]/(Y, 37) \cong F_{37}$

R_1/I が体になったので、$1+2\sqrt{-7}$は素元である。

●$121=(3+4\sqrt{-7})(3-4\sqrt{-7})$について

$I=(X^2+7,3+4X)$とする。

$4(X^2+7)-X(3+4X)=28-3X\in I$

$(3+4X)+(28-3X)=X+31\in I$より$X+31=Y$とおけば

$I=(Y,121)$となるから、

$R_1/I\cong\mathbb{Z}[Y]/(Y,121)\cong\mathbb{Z}_{121}$

R_1/I は体にならないので、$3+4\sqrt{-7}$は素元でない。

もともと$121=11^2$であり$11=(2+\sqrt{-7})(2-\sqrt{-7})$なので、

$121=\left(2+\sqrt{-7}\right)^2\left(2-\sqrt{-7}\right)^2$となる。

実際$3+4\sqrt{-7}=-\left(2-\sqrt{-7}\right)^2$となるので、$3+4\sqrt{-7}$は既約元でもない。

●$253=\left(1+6\sqrt{-7}\right)\left(1-6\sqrt{-7}\right)=\left(15+2\sqrt{-7}\right)\left(15-2\sqrt{-7}\right)$

について

$I_1=(X^2+7,1+6X)$とする。

$6(X^2+7)-X(1+6X)=42-X\in I$ より$42-X=Y$とおけば

$I=(Y,253)$となるから、$R_1/I_1\cong\mathbb{Z}[Y]/(Y,253)\cong\mathbb{Z}_{253}$

R_1/I_1 は体にならないので、$1+6\sqrt{-7}$は素元でない。

$I_2=(X^2+7,15+2X)$とする。

$2(X^2+7)-X(15+2X)=14-15X\in I$

$8(15+2X)+(14-15X)=X+134\in I$より$X+134=Y$とおけば

$I_2=(Y,253)$となるから、$R_1/I_2\cong\mathbb{Z}[Y]/(Y,253)\cong\mathbb{Z}_{253}$

R_1/I_2 は体にならないので、$15+2\sqrt{-7}$は素元でない。

もともと$253=11\times23$であり

$11=(2+\sqrt{-7})(2-\sqrt{-7})$で、$23=(4+\sqrt{-7})(4-\sqrt{-7})$だから、

$11=\alpha\bar{\alpha}$（但し$\alpha=2+\sqrt{-7}$）、$23=\beta\bar{\beta}$（但し$\beta=4+\sqrt{-7}$）と思えば、

$253=\alpha\bar{\alpha}\beta\bar{\beta}=\alpha\beta\left(\overline{\alpha\beta}\right)=\alpha\bar{\beta}(\bar{\alpha}\beta)$と表せる。

$\alpha\beta=\left(2+\sqrt{-7}\right)\left(4+\sqrt{-7}\right)=1+6\sqrt{-7}$なので、

$1+6\sqrt{-7}=\alpha\beta$となり既約元でもない。

また$X=1,Y=6$とみれば 253 の平方和となっている。

同様に、
$\alpha\bar{\beta} = (2+\sqrt{-7})(4-\sqrt{-7}) = 15+2\sqrt{-7}$なので、
$15+2\sqrt{-7} = \alpha\bar{\beta}$となり既約元でもない。
また$X = 15, Y = 2$とみれば 253 の平方和となっている。

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$\mathbb{Z}[\sqrt{-7}]$の素元になる。

証明）$J = (X^2+7, a+bX)$とおくと、
$b(X^2+7)-X(a+bX) = 7b-aX \in J$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、
$\mathbb{Z}[\sqrt{-7}]/(a+b\sqrt{-7}) \cong F_p$であり、
$a+b\sqrt{-7}$は$\mathbb{Z}[\sqrt{-7}]$の素元になる。

ここでも 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出てこなかった。しかし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。
また合成数に関しては素因数分解したときに現れる素因数（素数）を上に述べたように素元分解し、その素元たちの組み合わせによるものであるといえる。
では“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、今回の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
先にも述べたように 2 も$1 \pm \sqrt{-7}$も既約元である。
そこでこれらによる剰余環を考える。

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

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。

また

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

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 となれない理由は、
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。

4　考察と今後の課題

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$q=x^2+3y^2$と表せる有理素数qは、
$q\equiv 1\ (mod6)$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) $\mathbb{Z}[\sqrt{-7}]$において$q=x^2+7y^2$と表せる有理素数qは、
$q\equiv 1,5(mod6)$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$\mathbb{Z}[\sqrt{-7}]$の素元になる。
(7) $\mathbb{Z}[\sqrt{-7}]$の素元でない既約元は“2 と$1\pm\sqrt{-7}$”だけである。
ということが考察される。

今後の課題として、
・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
などが挙げられる。

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