自然数を $N = A^2 + 2B^2$ と表す方法の総数

慶應義塾大学 理工学部 1年フ組
60205503
加藤 祐子

1 背景と概略

与えられた正の数 N に対して,

$$D_1 = (N \text{ を割る整数 } d \text{ で } d \equiv 1 \pmod 4 \text{ を満たす数の個数}),$$

$$D_3 = (N \text{ を割る整数 } d \text{ で } d \equiv 3 \pmod 4 \text{ を満たす数の個数})$$

とおく. このとき N は2つの平方数の和にちょうど

$$R(N) = 4(D_1 - D_3) \quad \text{通り}$$

に表すことができる.

上の定理は、2平方和定理 (ルジャンドル) として知られている。(文献 [1] p.245)
これは次の命題 (文献 [3] 命題 0.2) を用いて証明できる (文献 [1] p.246)。

p が 4 でわると 1 余る素数なら

$$p = x^2 + y^2$$

となる自然数 x, y が存在するが, 4 でわると 3 あまる素数 p については, $p = x^2 + y^2$ となる有理数 x, y さえ存在しない.

これらを踏まえ、次に述べる命題を用いて $N = A^2 + 2B^2$ の表し方の総数を求める式を導いた。

2 命題 (文献 [3] 命題 0.3)

p が 8 でわると 1 または 3 余る素数ならば

$$p = x^2 + 2y^2$$

となる自然数 x, y が存在するが、8 でわると 5 または 7 余る素数 p については、$p = x^2 + 2y^2$ となる有理数 x, y さえ存在しない。

3　主定理

与えられた正の数 N に対して,

$$D_1 = (N \text{ を割る整数 } d \text{ で } d \equiv 1 \pmod 8 \text{ を満たす数の個数}),$$
$$D_3 = (N \text{ を割る整数 } d \text{ で } d \equiv 3 \pmod 8 \text{ を満たす数の個数}),$$
$$D_5 = (N \text{ を割る整数 } d \text{ で } d \equiv 5 \pmod 8 \text{ を満たす数の個数}),$$
$$D_7 = (N \text{ を割る整数 } d \text{ で } d \equiv 7 \pmod 8 \text{ を満たす数の個数})$$

とおく. このとき N は $N = A^2 + 2B^2$ $(A, B \in \mathbb{Z})$ という和にちょうど

$$R(N) = 2(D_1 + D_3 - D_5 - D_7) \quad \text{通り}$$

に表すことができる.

4　証明

証明は2つのステップで進める。最初に $R(N)$ に対する公式を導き、次に $D_1 + D_3 - (D_5 + D_7)$ に対する公式を証明し、2つの公式を比較することにより証明完了とする。

4.1　$R(N)$ に対する公式

正の数を $N = 2^t \underbrace{{p_1}^{e_1}{p_2}^{e_2}\cdots{p_r}^{e_r}}_{\text{素数}\equiv 1,3 \mod 8} \cdot \underbrace{{q_1}^{f_1}{q_2}^{f_2}\cdots{q_s}^{f_s}}_{\text{素数}\equiv 5,7 \mod 8}$ と分解する。

補題より、p_j は　$p_j = {a_j}^2 + 2{b_j}^2 = (a_j + \sqrt{2}b_j i)(a_j - \sqrt{2}b_j i)$　$(j = 1, 2, 3, \cdots, r)$　と $\mathbb{Z}[\sqrt{-2}] = \{a + \sqrt{2}bi; a, b \in \mathbb{Z}\}$ の中で積の形に分解でき、q_j は分解できない。また、整数 2 は $2 = (\sqrt{2})^2$ と分解されるので、N を素元分解すると

$$N = (\sqrt{2})^{2t}\Big((a_1 + \sqrt{2}b_1 i)(a_1 - \sqrt{2}b_1 i)\Big)^{e_1}\Big((a_2 + \sqrt{2}b_2 i)(a_2 - \sqrt{2}b_2 i)\Big)^{e_2}$$
$$\cdots\Big((a_r + \sqrt{2}b_r i)(a_r - \sqrt{2}b_r i)\Big)^{e_r} \cdot {q_1}^{f_1}{q_2}^{f_2}\cdots{q_s}^{f_s}$$

となる。

今、N を $N = A^2 + 2B^2$ と表したいので、この式を

$$N = (A + \sqrt{2}Bi)(A - \sqrt{2}Bi)$$

とする。素元分解の一意性[*1]により、$A + \sqrt{2}Bi$ は N を割る素元の積であり、$A - \sqrt{2}Bi$ は残った素元の積になる。

[*1] ＜素元＞ $\mathbb{Z}[\sqrt{-2}]$ の元 α が**素元**であるとは、α は 0 でも単数でもない、かつ、$ab \in \mathbb{Z}[\sqrt{-2}]$ で ab が α で割り切れれば、a または b が α で割り切れる、を満たすことである。

＜素元分解の法則＞ $\mathbb{Z}[\sqrt{-2}]$ の 0 でも単数でもない元 a は、

$$a = \alpha_1 \cdots \alpha_r \quad (r \geq 1, \alpha_1, \cdots, \alpha_r \text{は } \mathbb{Z}[\sqrt{-2}] \text{ の素元})$$

という素元の積の形にひととおりに分解される (文献 [3] p.108)。

また、$A+\sqrt{2}Bi$ と $A-\sqrt{2}Bi$ はお互い共役なので、ある素元のべき乗 $(a+\sqrt{2}bi)^e$ が $A+\sqrt{2}Bi$ を割れば、共役の素元のべき乗 $(a-\sqrt{2}bi)^e$ は $A-\sqrt{2}Bi$ を割る。

同じ理由で、q^f が $A+\sqrt{2}Bi$ を割れば、$A-\sqrt{2}Bi$ も割る。

よって、指数 $f_1, f_2, \cdots, f_s$ のどれかが奇数であれば、N は $N=A^2+2B^2$ と表せないので、$R(N)=0$ である。

よって、$f_1, f_2, \cdots, f_s$ はすべて偶数とすると、N は $N=A^2+2B^2$ と表せ、$A+\sqrt{2}Bi$ は、上記の理由より

$$A+\sqrt{2}Bi = u(\sqrt{2})^t \left((a_1+\sqrt{2}b_1 i)^{x_1}(a_1-\sqrt{2}b_1 i)^{e_1-x_1}\right) \cdots \left((a_r+\sqrt{2}b_r i)^{x_r}(a_r-\sqrt{2}b_r i)^{e_r-x_r}\right) \cdot {q_1}^{f_1/2}{q_2}^{f_2/2}\cdots{q_s}^{f_s/2}$$
$$(\ \ 0\le x_1\le e_1\ ,\ 0\le x_2\le e_2\ ,\ \cdots\ ,\ 0\le x_r\le e_r\ \ )$$

と表せる。ここで u は単数であり、$\mathbb{Z}[\sqrt{-2}]$ では、±1 の 2 つである。[*2]

$A+\sqrt{2}Bi$ の選択の可能性の総数は、$N=A^2+2B^2$ と表す方法の総数で、

$$2(e_1+1)(e_2+1)\cdots(e_r+1)$$

だけあることがわかる。

まとめると、

$N=2^t \underbrace{{p_1}^{e_1}{p_2}^{e_2}\cdots{p_r}^{e_r}}_{\text{素数}\equiv 1,3 \mod 8} \cdot \underbrace{{q_1}^{f_1}{q_2}^{f_2}\cdots{q_s}^{f_s}}_{\text{素数}\equiv 5,7 \mod 8}$ と分解されたとき

$$R(N) := \big(N=A^2+2B^2\ (A,B\in\mathbb{Z})\ \text{と表す方法の総数}\big) = \begin{cases} 2(e_1+1)(e_2+1)\cdots(e_r+1) & f_1,\cdots,f_s\text{はすべて偶数} \\ 0 & f_1,\cdots,f_s\text{の中に奇数がある} \end{cases}$$

4.2 例

どのような N が A^2+2B^2 で表せるか調べようと、表計算ソフトで、A, B に 1 から整数を代入していった。N の例を挙げてみる。

・$N=225=3^2\times5^2$ のとき $(A,B)=(\pm5,\pm10)$ (複合任意), $(\pm15,0)$ となり、6 通りである。
$p_1=3,\ e_1=2,\ q_1=5,\ f_1=2$ であるので、上記の $R(N)$ の式を使うと、$R(N)=2\times(e_1+1)=6$ となり、事実と一致する。

・$N=2811=3\times937$ のとき $(A,B)=(\pm53,\pm1),\ (\pm19,\pm35)$ (複合任意) となり、8 通りである。 $p_1=3,\ p_2=937,\ e_1=e_2=1$ であるので、$R(N)=2\times(e_1+1)(e_2+1)=8$ となり、これも事実と一致する。

[*2] <証明> $\alpha=a+\sqrt{2}bi\ (a,b\in\mathbb{Z})$ が単数であるとすると、ある整数 c,d が存在して、$\beta=c+\sqrt{2}di$ とおいたとき、$\alpha\beta=1$ となる。この両辺で共役複素数を取ると、α, $\overline{\alpha}$ はともに単数であることがわかり、$\alpha\overline{\alpha}=a^2+2b^2$ も単数となる。これは正の整数なので、$a^2+2b^2=1$ となるしかない。このような a,b は $b=0$ のときしかなく、$a=\pm1$ の 2 個となる。

・$N=33=3\times 11$ のとき　$(A,B)=(\pm 5,\pm 2),\ (\pm 1,\pm 4)$ (複合任意) となり、８通り。
$p_1=3,p_2=11,e_1=e_2=1$ であるので、$R(N)=2\times(e_1+1)(e_2+1)=8$
また、33 の約数をあげると、1,3,11,33。$D_1=2,D_3=2$ なので、$R(N)=2(2+2)=8$
・$N=75=3\times 5^2$ 同じように $R(N)$ を求めると、$R(N)=4$. 約数をあげると、$1,3,5,9,15,25,75$
より、$D_1=D_3=2,D_5=D_7=1$　ここで、$D_1+D_3-D_5-D_7=2$

ルジャンドルの二平方和定理や、上の例より

$$(e_1+1)(e_2+1)\cdots(e_r+1)=D_1+D_3-(D_5+D_7)$$

と予想できる。

4.3　$D_1+D_3-(D_5+D_7)$ に対する公式

整数 N を有理整数の積

$$N=2^t\underbrace{{p_1}^{e_1}{p_2}^{e_2}\cdots{p_r}^{e_r}}_{\text{素数}\equiv 1,3 \mod 8}\cdot\underbrace{{q_1}^{f_1}{q_2}^{f_2}\cdots{q_s}^{f_s}}_{\text{素数}\equiv 5,7 \mod 8}$$

に分解したとする。

$$\begin{aligned}
D_1&=(N\text{ を割る整数 }d\text{ で }d\equiv 1 \pmod 8\text{ を満たす数の個数}),\\
D_3&=(N\text{ を割る整数 }d\text{ で }d\equiv 3 \pmod 8\text{ を満たす数の個数}),\\
D_5&=(N\text{ を割る整数 }d\text{ で }d\equiv 5 \pmod 8\text{ を満たす数の個数}),\\
D_7&=(N\text{ を割る整数 }d\text{ で }d\equiv 7 \pmod 8\text{ を満たす数の個数})
\end{aligned}$$

とおく。このとき $D_1+D_3-(D_5+D_7)$ は規則

$$D_1+D_3-(D_5+D_7)=\begin{cases}(e_1+1)(e_2+1)\cdots(e_r+1) & f_1,\cdots,f_s\text{はすべて偶数}\\ 0 & f_1,\cdots,f_s\text{の中に奇数がある}\end{cases}$$

により与えられる。

証明.　s に関する帰納法で証明する。

(I)　$s=0$ のとき　　$N=2^t{p_1}^{e_1}{p_2}^{e_2}\cdots{p_r}^{e_r}$
$d={p_1}^{u_1}{p_2}^{u_2}\cdots{p_r}^{u_r}\ \ (1\le u_i\le e_i)$ は N の奇数の約数で、$d\equiv 1,3 \pmod 8$ を満たす。
よって、

$$D_1+D_3-(D_5+D_7)=D_1+D_3=(e_1+1)(e_2+1)\cdots(e_r+1)$$

(II)　$s=k-1$ のとき成り立つと仮定して、$s=k$ のとき成り立つことを示す。

$$N=2^t{p_1}^{e_1}{p_2}^{e_2}\cdots{p_r}^{e_r}\cdot{q_1}^{f_1}{q_2}^{f_2}\cdots{q_{k-1}}^{f_{k-1}}\cdot{q_k}^{f_k}$$

ここで、$n = 2^t {p_1}^{e_1} {p_2}^{e_2} \cdots {p_r}^{e_r} \cdot {q_1}^{f_1} {q_2}^{f_2} \cdots {q_{k-1}}^{f_{k-1}}$ とおく。

(i)　f_k:奇数の場合

N の奇数の約数は ${q_k}^i d$ $(0 \leq i \leq f_k$, d は奇数で n の約数$)$ で得られる。

n の各約数 d に対して、N の奇数の約数は $f_k + 1$ 個 $(q_k^0 d, q_k^1 d, \cdots, q_k^{f_k} d)$ ある。

これらの約数の半分が 8 で割って 1 または 3 余る数で、残りの半分が 8 で割って 5 または 7 余る数になる。

よって

$$D_1 + D_3 = D_5 + D_7$$
$$\therefore \qquad D_1 + D_3 - (D_5 + D_7) = 0$$

(ii)　f_k:偶数の場合

(i) と同じ理由で、n の各約数 d に対して、

N の奇数の約数　$q_k^0 d, q_k^1 d, \cdots, q_k^{f_k - 1} d$ の f_k 個については、半分が 8 で割って 1 または 3 余り、残りの半分が 8 で割って 5 または 7 余る。

N の奇数の約数 ${q_k}^{f_k}$ について、　f_k は偶数であるから、

$${q_k}^{f_k} \equiv 1, 3 \pmod 8$$

$$\begin{aligned}
&d \equiv 1 \pmod 8 \text{ ならば} \quad {q_k}^{f_k} d \equiv 1, 3 \pmod 8 \\
&d \equiv 3 \pmod 8 \text{ ならば} \quad {q_k}^{f_k} d \equiv 1, 3 \pmod 8 \\
&d \equiv 5 \pmod 8 \text{ ならば} \quad {q_k}^{f_k} d \equiv 5, 7 \pmod 8 \\
&d \equiv 7 \pmod 8 \text{ ならば} \quad {q_k}^{f_k} d \equiv 5, 7 \pmod 8
\end{aligned}$$

すなわち、　d は n の約数であるので、

$$(N \text{ に対する } D_1 + D_3 - (D_5 + D_7)) = (n \text{ に対する } D_1 + D_3 - (D_5 + D_7))$$

帰納法の仮定より

$$(n \text{ に対する } D_1 + D_3 - (D_5 + D_7)) = \begin{cases} (e_1 + 1)(e_2 + 1) \cdots (e_r + 1) & f_1, \cdots, f_{k-1} \text{はすべて偶数} \\ 0 & f_1, \cdots, f_{k-1} \text{の中に奇数がある} \end{cases}$$

が成り立つので、

$$(N \text{ に対する } D_1 + D_3 - (D_5 + D_7)) = \begin{cases} (e_1 + 1)(e_2 + 1) \cdots (e_r + 1) & f_1, \cdots, f_k \text{はすべて偶数} \\ 0 & f_1, \cdots, f_k \text{の中に奇数がある} \end{cases}$$

が成り立つ。

よって、0 以上のすべての整数 s について成り立つ。　□

4.1 , 4.3 より

$$R(N) = 2(D_1 + D_3 - D_5 - D_7)$$

が示された。 □

5 考察

今回は $\mathbb{Z}[i]$ と $\mathbb{Z}[\sqrt{-2}]$ の性質が似ていたため、ルジャンドルの二平方和定理と同じように証明することができ、公式も同じようにきれいな式になった。また、具体的に $A^2 + 2B^2$ を書き出せば、$R(N)$ を数えることもできたので、確認することができた。しかし、$A^2 - 2B^2$ などは A, B を大きくしていっても小さな N が出てくることがありえるので、証明しにくい。整数環の中には素元分解の法則が成立しないことがあったりと、他の場合の証明は複雑になるかもしれないが、いろいろな場合についてこれからも考えていきたいと思う。

参考文献

[1] ジョセフ・H・シルヴァーマン著、鈴木治郎 訳：「はじめての数論」
（ピアソン・エデュケーション）
[2] 加藤和也 著：「解決！フェルマーの最終定理」（日本評論社）
[3] 加藤和也・黒川信重・斎藤毅 著：「数論１」（岩波書店）