数学集中講義

素数の秘密　複素数での素数とは？

吉田　信夫

大学への数学　15 年 3 月号　掲載

素数については様々な秘密があり，その解明は現代数学にも直結している．そんな素数の秘密の中から，複素数を考えることで見えてくるものを取り上げてみたい．

まず，いくつかの予備知識から．1 つ目は合同式の方程式 $x^2 \equiv -1 \pmod{p}$ の解についてである．

予備知識 1

p が素数のとき，

$$x^2 \equiv -1 \pmod{p} \quad (1 \leqq x \leqq p-1)$$

を満たす x は，

1)　$p=2$ のとき，$x=1$

2)　p が 4 で割って 3 余るとき，存在しない

3)　p が 4 で割って 1 余るとき，

$$x \equiv \left(\frac{p-1}{2}\right)!\ ,\ -\left(\frac{p-1}{2}\right)! \pmod{p}$$

となる 2 つの x が解である

3) の 2 解は，和が p なので，1 つが偶数，もう 1 つが奇数である．これを応用することで次の結果が得られる．

予備知識 2

自然数 x に対し，x^2+1 は 4 で割って 3 余るような素数を素因数にもたない．特に，x が偶数のとき，x^2+1 の素因数は 4 で割って 1 余るもののみである．

証明については，本誌 2014 年 6 月号を参照していただきたい．

合わせて，複素数平面の基本を確認しておこう．

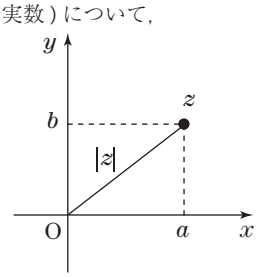
複素数 $z=a+bi$ (a，b は実数) について，

$$|z|=\sqrt{a^2+b^2}$$

を z の絶対値という．簡単な計算により，実数と同様の

$$|zw|=|z|\times|w|$$

という「絶対値の積の法則」が成り立つことも分かる．



これらを受けて，今回はもっと深く掘り下げていこう．

4 で割って 1 余る素数

5，13，17，29，37，41，……

と，4 で割って 3 余る素数

3，7，11，19，23，31，……

の決定的な違いについてである．実は，前者は

$4+1$，$9+4$，$16+1$，$25+4$，$36+1$，

$25+16$，……

と 2 つの平方数の和で表すことができる（これを一般的に示すことが本稿の目標である）．和で奇数を作っているので，(偶数)^2+(奇数)^2 の形になっている．

また，2 は

$$2=1+1$$

と，2 つの平方数の和で表すことができる．

では，4 で割って 3 余る素数は？

問題 1.　4 で割って 3 余る素数は，2 つの平方数の和で表すことができないことを示せ．

解　まず，平方数を 4 で割った余りについて考える．

整数 m に対し，

$$(2m)^2=4m^2$$

は 4 の倍数であり，

$$(2m-1)^2=4m^2-4m+1$$

は 4 で割って 1 余る．

よって，2 つの平方数の和を 4 で割った余りは，

0，1，2

のいずれかである．

これで，4 で割って 3 余る素数は，2 つの平方数の和で表すことができないことが示された．

＊　　＊

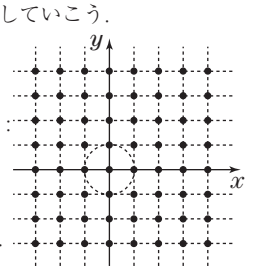
これが何を意味するか，確認していこう．

実は，複素数を用いると意味が分かってくる．複素数平面での格子点を表すようなもの：

$$z=a+bi$$

(a，b は整数)

を複素整数と呼ぶことにしよう．



すると，この世界でも「複素素数」というものを考えることができる．例えば，5 は普通の整数の世界では素数であるが，複素数として考えると

$$5=4+1=(2+i)(2-i)$$

と，複素整数の積で表すことができる．つまり，「複素素数」ではないのである．

一方，7 はどうだろうか？

$$7=(-7i)\cdot i=(7i)\cdot(-i)=(-7)\cdot(-1)$$

という積で表すことができるが，こう表されるからといって，「7 が複素素数でない」とは言いがたい．そこで，絶対値が 1 の複素整数 1，-1，i，$-i$ は特別扱いにしておき，「複素整数の積で表したとき，積の片割れが絶対値 1 になる複素整数」を複素素数と呼ぶことにしよう．もちろん，絶対値が 1 のものは複素素数とは呼ばない．

ちなみに，5 についての説明に登場した $2+i$，$2-i$ は複素素数である．$2+i$ について確認してみよう．

$$2+i=(a+bi)(c+di)\ (a,\ b,\ c,\ d \text{ は整数})$$

とおくと，両辺の絶対値の 2 乗を考えて

$$5=(a^2+b^2)(c^2+d^2)$$

となる．ここで，絶対値の積の法則を用いた．すると

$$\{a^2+b^2,\ c^2+d^2\}=\{1,\ 5\}$$

となり，$a+bi$ または $c+di$ の絶対値が 1 となる．

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

などの形にしか書けないので，複素素数である．

1 つ補足しておこう．$1-2i$ も複素素数なので，

$$5=i(1-2i)(2-i)=(1-2i)(1+2i)$$

も 5 の素因数分解になるが，複素整数では，±1，$\pm i$ 倍の違いがあっても同じ素数と見なすことになっている．

ここで，本稿の主題となる定理を紹介しよう．

定理

p を素数とする．

1) $p=2$ のとき，複素素数でない

2) 4 で割って 3 余るとき，p は複素素数である

3) 4 で割って 1 余るとき，p は複素素数でない

$p=2$ については，

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

より，複素素数ではない．**定理** 1) は正しい．

次に，4 で割って 3 余る素数 $p=7$ について考えよう．

問題 2. a，b，c，d を整数とし，

$$\alpha=a+bi,\ \beta=c+di$$

とおく．ただし，$|\alpha|\geqq|\beta|$ とする．$\alpha\beta=7$ となる α，β を求めよ．

解 $\alpha\beta=7$ の両辺の絶対値の 2 乗を考えて，

$$(a^2+b^2)(c^2+d^2)=49$$

が成り立つ．ここで，7 が 2 つの平方数の和で表すことができない素数であるため，

$$a^2+b^2=49,\ c^2+d^2=1$$

となる．後者から

$$(c,\ d)=(1,\ 0),\ (-1,\ 0),\ (0,\ 1),\ (0,\ -1)$$

しかないことが分かる．順に $\beta=1$，-1，i，$-i$ なので $\alpha\beta=7$ となる組を探すと，

$$(\alpha,\ \beta)=(7,\ 1),\ (-7,\ -1),\ (-7i,\ i),\ (7i,\ -i)$$

となる．

＊　　＊

以上で，7 が複素素数であることが分かった．同様にして，一般に，4 で割って 3 余る素数は複素素数であることが分かる．つまり，**定理** 2) は正しい．

では，次が本題．**定理** 3) の「p が 4 で割って 1 余るとき，複素素数でない」を示していこう．険しい道になるので，具体例を挙げながら丁寧に見ていくことにする．

ポイントとなるのは，**予備知識 1** の 3) から分かる

> p が 4 で割って 1 余る素数のとき，
> $x^2\equiv-1\pmod p$　$(1\leqq x\leqq p-1)$
> を満たす偶数 x が存在する．

である．x を偶数の方にしておくと，(偶数)$^2+1$ の素因数に関する**予備知識 2** を用いて論証をスムーズに行うことができる．これを元に，

> 4 で割って 1 余る素数は，2 つの平方数の和で表すことができる．

を示す．これが分かれば，

$$p=a^2+b^2=(a+bi)(a-bi)$$

となるので，複素素数でないと結論づけることができる（$p=5$ の場合と同様，p の素因数分解になる）．

さて，先ほどは 41 までを平方数の和で表したので，53 について考えてみよう．見た瞬間に平方数の和で表すことができるが，一般論に近づくため，気づかなかったことにしておこう！

まず，**予備知識 1** の 3) から，

$$x^2\equiv-1\pmod{53}\quad(1\leqq x\leqq52)$$

を満たす偶数 x が存在するはずなので，それを求める．

$$x^2=53k-1\ (k \text{ は自然数})$$

を考えたいので，$53k-1$ と表される数を並べていくと，

52，105，158，211，264，317，370，423，
476，529，582，……

となる．この中で，$23^2=529$ が平方数であるから，偶数の x は，

$$x=53-23=30$$

である．確かに，

$$30^2\equiv(-23)^2=529\equiv-1 \pmod{53}$$

となっている．これは，直接的に

$$30^2=900=16\cdot53+52\equiv-1 \pmod{53}$$

としても良い（$17\cdot53=901$ となるのである）．

さて，

$$30^2+1=17\cdot53$$

と分かったのであるが，複素整数で表記してみると，

$$(30+i)(30-i)=(4+i)(4-i)\cdot53$$

となる．ここで，実験的に

$$\frac{30+i}{4+i}=\frac{(30+i)(4-i)}{17}=\frac{121-26i}{17},$$
$$\frac{30+i}{4-i}=\frac{(30+i)(4+i)}{17}=\frac{119+34i}{17}=7+2i$$

と計算しておこう．

これを利用できる．後者において，共役を考えたら

$$\frac{30-i}{4+i}=7-2i$$

となる．ゆえに，

$$53=\frac{(30+i)(30-i)}{(4+i)(4-i)}=\frac{30+i}{4-i}\cdot\frac{30-i}{4+i}$$
$$=(7+2i)(7-2i)=7^2+2^2$$

が導かれるのである．

これが一般化できれば，証明できそうである．流れは見えてきただろうか？

4 で割って 1 余る素数を小さい方から順に

$$q_1,\ q_2,\ q_3,\ \cdots\cdots$$

とおき，素数に付けられた番号に関する数学的帰納法で証明するのである．

ここから長い証明に入る．丁寧に議論していこう．

まず，$q_1=5$ は $4+1$ と表すことができる．

次に，

$$q_1,\ q_2,\ q_3,\ \cdots\cdots,\ q_k$$

が 2 つの平方数の和で表されると仮定して，q_{k+1} が 2 つの平方数の和で表されることを示す．これができれば証明完了となる．そのためのヒントが上記である．

$$x^2\equiv-1 \pmod{q_{k+1}}\quad(1\leqq x\leqq q_{k+1}-1)$$

を満たす偶数 x が存在するので，

$$x^2+1=Aq_{k+1}\ (A\text{ は自然数})$$

と表すことができる．そして，(偶数)$^2+1$ の素因数は 4 で割って 1 余るもののみであることも分かっている．

$$x^2+1\leqq(q_{k+1}-1)^2+1={q_{k+1}}^2-2q_{k+1}+2<{q_{k+1}}^2$$

なので，x^2+1 は q_{k+1} で割り切れるが，${q_{k+1}}^2$ では割り切れない．さらに，q_N $(N\geqq k+2)$ でも割り切れない（もし割り切れたら，

$$x^2+1\geqq q_{k+1}q_N>{q_{k+1}}^2$$

となってしまい，不適）．

これで，x^2+1 は

・4 で割って 1 余る素数 q_1，q_2，q_3，……しか素因数にもたない

・q_{k+1} を 1 つしか含まない

・q_{k+1} より大きい素因数をもたない

が分かった．よって，素因数分解は

$$x^2+1={q_1}^{r_1}\cdot{q_2}^{r_2}\cdot\cdots\cdots\cdot{q_k}^{r_k}\cdot q_{k+1}$$

とおける．ただし，r_l $(l=1,\ 2,\ \cdots\cdots,\ k)$ は 0 以上の整数である（$r_l=0$ となる q_l は素因数に含まれない，ということ）．

帰納法の仮定から，各 q_l $(l=1,\ 2,\ \cdots\cdots,\ k)$ は 2 つの自然数 a_l，b_l を用いて

$$q_l={a_l}^2+{b_l}^2$$

と表すことができる．よって，複素整数を用いると

$$(x+i)(x-i)$$
$$=\{(a_1+b_1i)(a_1-b_1i)\}^{r_1}\cdot\{(a_2+b_2i)(a_2-b_2i)\}^{r_2}\cdot$$
$$\cdots\cdots\cdot\{(a_k+b_ki)(a_k-b_ki)\}^{r_k}\cdot q_{k+1}$$

ということである．

ここで，次を示そう．

問題 3. x，y，a，b，k を自然数とし，

$$a^2+b^2=p:\text{素数}$$
$$x^2+y^2=(a^2+b^2)k$$

が成り立つとする．

（1）$|(x+yi)(a-bi)|^2$，$|(x+yi)(a+bi)|^2$ が p^2 の倍数であることを示せ．

（2）$(ax+by)(-bx+ay)(ax-by)(bx+ay)$ が p の倍数であることを示せ．

（3）$\dfrac{x+yi}{a+bi}$，$\dfrac{x+yi}{a-bi}$ のいずれか一方は複素整数であることを示せ．

解 （1）後で計算過程を参照するので，法則を用いずに計算すると，

$$|(x+yi)(a-bi)|^2=|(ax+by)+(-bx+ay)i|^2$$
$$=(ax+by)^2+(-bx+ay)^2$$
$$=(a^2+b^2)(x^2+y^2)$$
$$=p^2k,$$

$$|(x+yi)(a+bi)|^2=|(ax-by)+(bx+ay)i|^2$$
$$=(ax-by)^2+(bx+ay)^2$$
$$=(a^2+b^2)(x^2+y^2)$$
$$=p^2k$$

である．よって，いずれも p^2 の倍数である．

（2）展開すると，

$$(ax+by)(-bx+ay)(ax-by)(bx+ay)$$
$$=(a^2x^2-b^2y^2)(-b^2x^2+a^2y^2)$$
$$=(a^4+b^4)x^2y^2-(x^4+y^4)a^2b^2$$

である．ここで，

$$(x^2+y^2)^2=x^4+2x^2y^2+y^4$$
$$\therefore\quad x^4+y^4\equiv-2x^2y^2\pmod p$$
$$(a^2+b^2)^2=a^4+2a^2b^2+b^4$$
$$\therefore\quad a^4+b^4\equiv-2a^2b^2\pmod p$$

である．これらを代入して，

$$(ax+by)(-bx+ay)(ax-by)(bx+ay)$$
$$\equiv-2a^2b^2x^2y^2+2x^2y^2a^2b^2$$
$$=0\pmod p$$

となる．これで示された．

（3）分母を実数化すると，

$$\frac{x+yi}{a+bi}=\frac{(x+yi)(a-bi)}{a^2+b^2}$$
$$=\frac{(ax+by)+(-bx+ay)i}{p},$$
$$\frac{x+yi}{a-bi}=\frac{(x+yi)(a+bi)}{a^2+b^2}$$
$$=\frac{(ax-by)+(bx+ay)i}{p}$$

である．ここで，（2）より，

$$ax+by,\ -bx+ay,\ ax-by,\ bx+ay$$

のいずれかは p の倍数である．さらに，（1）の計算過程から

$$(ax+by)^2+(-bx+ay)^2,\ (ax-by)^2+(bx+ay)^2$$

が p の倍数なので，「$ax+by$ と $-bx+ay$ がともに p の倍数」または「$ax-by$ と $bx+ay$ がともに p の倍数」の少なくとも一方が成り立つ．前者の場合は

$$\frac{x+yi}{a+bi}=\frac{(ax+by)+(-bx+ay)i}{p}$$

が複素整数であり，後者の場合は

$$\frac{x+yi}{a-bi}=\frac{(ax-by)+(bx+ay)i}{p}$$

が複素整数である．以上で示された．

＊　　＊

本問の結果は重要である．先ほど，

$$(30+i)(30-i)=(4+i)(4-i)\cdot53$$

から，$53=7^2+2^2$ を作るときに

$$\frac{30+i}{4+i}=\frac{(30+i)(4-i)}{17}=\frac{121-26i}{17},$$
$$\frac{30+i}{4-i}=\frac{(30+i)(4+i)}{17}=\frac{119+34i}{17}=7+2i$$

という計算を行った．後者が複素整数になってくれたために，

$$53=(7+2i)(7-2i)$$

を導けたのであった．これを

$$(x+i)(x-i)$$
$$=\{(a_1+b_1i)(a_1-b_1i)\}^{r_1}\cdot\{(a_2+b_2i)(a_2-b_2i)\}^{r_2}\cdot$$
$$\cdots\cdots\cdot\{(a_k+b_ki)(a_k-b_ki)\}^{r_k}\cdot q_{k+1}$$

に当てはめるとどうなるだろうか？

$r_1\neq0$ としたら，$q_1={a_1}^2+{b_1}^2$ から 問題 3（3）を使うことができて，$\dfrac{x+i}{a_1+b_1i}$，$\dfrac{x+i}{a_1-b_1i}$ のいずれかが複素整数となる．それを $A+Bi$ とおこう．すると，

$$(A+Bi)(A-Bi)$$
$$=\{(a_1+b_1i)(a_1-b_1i)\}^{r_1-1}\cdot\{(a_2+b_2i)(a_2-b_2i)\}^{r_2}\cdot$$
$$\cdots\cdots\cdot\{(a_k+b_ki)(a_k-b_ki)\}^{r_k}\cdot q_{k+1}$$

となる．この作業を $r_1+r_2+\cdots\cdots+r_k$ 回繰り返すと，

$$(a+bi)(a-bi)=q_{k+1}\ (a,\ b\text{ は整数})$$

を得る．つまり，

$$q_{k+1}=a^2+b^2\ (a,\ b\text{ は整数})$$

となった．絶対値を考えることで，a，b は自然数であるとしても良い．

以上で，

$$q_1,\ q_2,\ q_3,\ \cdots\cdots,\ q_k$$

が 2 つの平方数の和で表されるなら，q_{k+1} も 2 つの平方数の和で表されることを示すことができた．

数学的帰納法により，4 で割って 1 余るすべての素数

$$q_1,\ q_2,\ q_3,\ \cdots\cdots$$

に関して，

$$q_l={a_l}^2+{b_l}^2\ (a_l,\ b_l\text{ は整数})$$

と表されることが示された．

＊　　＊

ハードな道だったが，何とか「4 で割って 1 余る素数は複素素数でない」も示すことができて，**定理**は正しいことが分かった．漫然と素数を眺めていても気づくことはないが，4 で割った余りによって素数の性質はあまりに異なるのである．こんな秘密がたくさんあるのが素数の魅力である．

（よしだ　のぶお，予備校講師）