複素整数の素因数分解について

—— $4n+1$型の素数をめぐって ——

岡田（おかだ） 恭二（きょうじ）

1学期の終わりころ，3年生の生徒が職員室にきて，「先生，$4n+1$型の素数は，2つの整数の平方和として表されるんですね」と言いにきました．その生徒は，例えば，$5=1^2+2^2$，$29=2^2+5^2$などの例を示しながら，驚いたように話していきました．その時は，軽く受け流しておきましたが，証明は大変だろうナと予感していました．

夏休みになって，時間ができたのでいよいよ証明にかかってみました．すると，そのことに付随して複素数の因数分解の一意性という興味ある問題も含まれていることが分かりました．では，少し準備をしていきます．

1．ガウスの整数

aとbを整数として，$a+bi$をガウスの整数または複素整数という．ただし，$i=\sqrt{-1}$，以下ギリシア文字で表す．

1）約数

整数α，βの商$\frac{\beta}{\alpha}=\gamma$が整数であるとき，

αはβの約数，βはαの倍数という．

2）単数

すべての整数の約数を単数という．

単数は次の4つである．1，-1，i，$-i$

3）同伴数

$\frac{\beta}{\alpha}$が単数に等しいとき，α，βを互いに同伴数という．

4）ノルム

整数$\mu=a+bi$に対して，$\bar{\mu}=a-bi$を共役複素数といい，$\mu\bar{\mu}=|\mu|^2=a^2+b^2$を$\mu$のノルムという．

$N\mu$の記号を用いる．

（問）$\alpha\beta=\gamma$ならば$N\alpha N\beta=N\gamma$であることを証明せよ．

（証明）$\alpha=a+bi$, $\beta=c+di$とすると

$$\gamma=(ac-bd)+(ad+bc)i$$

$$N\gamma=(ac-bd)^2+(ad+bc)^2$$

$$=a^2c^2-2abcd+b^2d^2+a^2d^2+2abcd+b^2c^2$$

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

$$=N\alpha N\beta$$ （証明終）

（定理）α，βを任意の整数とする．（$\beta\neq0$）

$\alpha=\beta\times\delta+\rho$ （ただし，$|\rho|<|\beta|$）

となるような整数δ，ρが存在する．

（証明）$\frac{\alpha}{\beta}$を計算して，$\frac{\alpha}{\beta}=x+yi$となったとする．

x，yは実数である．このような複素数は正方格子点内にあるから，いま1番近い頂点をδとすれば，$x+yi$との距離は1より小さいので，

$\left|\frac{\alpha}{\beta}-\delta\right|<1$，そこで$\alpha-\beta\times\delta=\rho$と定めれば，

$|\rho|<|\beta|$がいえる．

5）最大公約数

2つ以上の整数に共通な約数（1を含む）をそれらの公約数という．その中のノルムの最も大きいものを最大公約数という．

6）素数

単数とそれ自身以外に約数をもたないものを素数という．

7）素因数分解

素数でない数（合成数）をいくつかの素数の積に表すことをいう．ただし，同伴数を同じとみなす．

（問）ノルム$N\alpha$が素数ならば，αは素数であることを示せ．

(証明) もしも α が素数でないとすると，$\alpha=\beta\gamma$ と書けることになり，$N\alpha=N\beta N\gamma$ であるから $N\alpha$ が合成数となり矛盾する．

(問) ノルムの小さい順に素数を書き並べよ．

(答) ノルム2のものは $1+i$，$1-i$
ノルム3のものはない．ノルム4は合成数．
ノルム5のものは $1+2i$，$1-2i$
(注意：$2+i$ はノルム5の素数であるが $2+i=i\times(1-2i)$ であるから同伴数であり，同一視する)

(問) 次の複素数を素因数分解せよ．
1) $1+i$　　2) $3+4i$
3) $13-i$

(答) 複素数を α としノルムを考える．
1) $N\alpha=1^2+1^2=2$ であるから素数である．
2) $N\alpha=3^2+4^2=25$ であるからノルム5のものを因数にもつ．$3+4i=(2+i)^2$
3) $N\alpha=13^2+1^2=170$ であるからノルム2と5と17のものを因数にもつ．
$13-i=(1-i)(1-2i)(-1+4i)$

(定理) 2つの整数 α，β の積が素数 λ で割り切れるならば，どちらか一方は λ で割り切れる．

(証明) α と β の最大公約数を考える．それは λ の約数であるから，単数 ε または λ に等しい．
$(\alpha,\ \lambda)=\lambda$ のとき α は λ で割り切れる．
$(\alpha,\ \lambda)=\varepsilon$ のとき β は λ で割り切れる．

> (定理) 合成数は素数の積に分解することができる．かつ，その分解は同伴数を同じとみなせば一意である．

(証明) まず，ノルムが最小の2においては，
$2=(1+i)(1-i)$ であるから定理は成り立つ．次にノルムについて，数学的帰納法を用いて証明する．α を合成数として，α よりノルムが小さい合成数に対しては定理が成り立つとする．

分解の可能性：
α は合成数であるから2つ以上の積で表される．
$\alpha=\beta\gamma$ とすると，β も γ もともにノルムは α のノルムより小さい．β も γ も素数であれば定理は証明されており，合成数ならば帰納法の仮定により，素数の積に分解することができる．

分解の一意性：
α を素因数に分解したとき，2通りに分解されたとする．
$$\alpha=\lambda\lambda'\lambda''\cdots\cdots=\mu\mu'\mu''\cdots\cdots$$
$\lambda\lambda'\lambda''\cdots\cdots$ は素数 μ で割り切れるから，$\lambda\lambda'\lambda''\cdots\cdots$ の中に μ で割り切れるものがある．λ が μ で割り切れるとすれば，どちらも素数であるから，
$\lambda=\varepsilon\mu$ である．(ε は単数)
ゆえに $\lambda'\lambda''\cdots\cdots=\varepsilon\mu'\mu''\cdots\cdots$
この等しい数を β とすると，β のノルムは α のノルムより小さいので，帰納法の仮定により2つの分解は同一となる．

では，だいぶガウスの整数に慣れてきましたので，その応用として次の定理へ進んでいきましょう．

> (定理) $4n+3$ 型の有理素数は p は複素整数としても素数であり，$4n+1$ 型の有理素数は p は2つの複素整数 $\pi\overline{\pi}$ とで因数分解される．

この証明は大変ですのでいくつかに分けて証明することにします．

(補助命題) 有理素数 p が複素素数 π で因数分解されるならば，$p=\pi\overline{\pi}$ である．

(証明) p の因数分解を $p=\pi\tau$ と仮定すると，ノルムを考えて，$Np=p^2=N\pi N\tau$ である．p^2 の約数は　1，p，p^2 であるが π も τ も単数でないから，$N\pi=N\tau=p$ に限る．
さて，π と τ を極形式で表して，
$\pi=\sqrt{p}\,(\cos\alpha+i\sin\alpha)$，
$\tau=\sqrt{p}\,(\cos\beta+i\sin\beta)$ とすると
$p=\pi\tau=p\{\cos(\alpha+\beta)+i\sin(\alpha+\beta)\}$ となるから，
$\beta=-\alpha$ でなければならない．
ゆえに，$\tau=\overline{\pi}$ であり，$p=\pi\overline{\pi}$

このことから，$\pi=x+yi$ とおくと，有理素数 p が因数分解されれば，$p=(x+yi)(x-yi)=x^2+y^2$ となり，2つの整数の平方和で表されることが分かる．

(問) $4n+3$ 型の有理素数 p は因数分解できないことを示せ．

(答) もしも因数分解できたとすると，$p=x^2+y^2$ と

なる．さて，左辺は奇数であるから，x と y は一方が奇数，他方が偶数でなければならない．しかるに，$x=2n$，$y=2m+1$ とおくと
$x^2+y^2=4n^2+4m^2+4m+1$ となり，p が $4n+3$ 型の有理素数であることに矛盾する．

(平方剰余の相互法則)
$4n+1$ 型の有理素数 p に対して，$r^2=-1(\mathrm{mod}\,p)$ となる有理整数 r が存在する．

この証明は省略する．

(補助命題) $4n+1$ 型の有理素数 p は，複素素数 π を約数にもつ．

(証明) 平方剰余の相互法則により，$4n+1$ 型の有理素数 p に対して，$r^2=-1(\mathrm{mod}\,p)$ となる有理整数 r が存在するので，$r^2+1=(r+i)(r-i)$ が p で割り切れる．
そこで，p と $r-i$ の最大公約数なるものを考えると，それは p の約数であるから，1 または p または π である．この証明の目的は，このような π の存在をいえばよい．

(Ⅰ) p と $r-i$ の最大公約数が 1 のとき
p は共役複素数 $r+i$ とも互いに素であるから，$(r+i)(r-i)=r^2+1$ とも互いに素になり，矛盾する．

(Ⅱ) p と $r-i$ の最大公約数が p のとき $r-i$ が p で割り切れることになり，それは不可能である．
したがって，p と $r-i$ の最大公約数は π でなければならない．

(証明終)

今回，1 人の生徒の話から，大変いい勉強をさせてもらったと感謝しています．おかげで，今まで当たり前と思っていた複素数の素因数分解まで，改めて考えることが出きました．

(参考文献)
「初等整数論講義」(高木　貞治著，共立出版)

(京都府立朱雀高等学校)