今までの主なレポート課題の例 (01/08 配布)

問 16. D を自然数で、平方数で割り切れないもの (square-free (平方無縁) という) とし、$a+b\sqrt{-D}$ $(a,b\in \boldsymbol{Z})$ の形の複素数全体

$$\boldsymbol{Z}[\sqrt{-D}] := \{a+b\sqrt{-D} | a,b\in \boldsymbol{Z}\}$$

を考える。

(1) $\boldsymbol{Z}[\sqrt{-D}]$ に属す数同士の和・差・積は再び $\boldsymbol{Z}[\sqrt{-D}]$ に属す (和・差・積で閉じているという) ことを示せ。($\boldsymbol{Z}[\sqrt{-D}]$ が**環 (ring)** を成すという。)

(2) $\alpha = a+b\sqrt{-D}\in \boldsymbol{Z}[\sqrt{-D}]$ に対し、その複素共役 $\overline{\alpha} := a-b\sqrt{-D}$ を考えると、

$$\overline{\alpha}+\overline{\beta} = \overline{\alpha+\beta}, \qquad \overline{\alpha}\overline{\beta} = \overline{\alpha\beta}$$

が成り立つことを示せ。

(3) $N(\alpha) := \alpha\overline{\alpha}$ (α のノルムという) と置くと、$N(\alpha)\in \boldsymbol{Z}$ であり、$N(\alpha\beta) = N(\alpha)N(\beta)$ が成り立つことを示せ。

(4) $D\equiv 3 \pmod 4$ の時は、実は、$\omega := \dfrac{-1+\sqrt{-D}}{2}$ を考えて、$\boldsymbol{Z}[\omega] := \{a+b\omega | a,b\in \boldsymbol{Z}\}$ を考えた方が良い。ω を根とする整数係数の 2 次多項式 $f(X)\in \boldsymbol{Z}[X]$ を求めよ。また、$\boldsymbol{Z}[\omega]$ が和・差・積で閉じていることを示せ。

問 17. $\boldsymbol{Z}[\sqrt{-D}]$ において、$\boldsymbol{Z}$ の時と同様に、$\alpha=\beta\gamma$ となる $\gamma\in \boldsymbol{Z}[\sqrt{-D}]$ が存在するとき、α が β で割り切れる (α が β の倍数、β が α の約数) といい、$\beta|\alpha$ と書く。

(1) $a,b\in \boldsymbol{Z}$ に対して、$\boldsymbol{Z}[\sqrt{-D}]$ での意味で $b|a$ であることと、$\boldsymbol{Z}$ での意味で $b|a$ であることとは同値。

(2) $\beta|\alpha$ ならば、$N(\beta)|N(\alpha)$.

(3) $\varepsilon\in \boldsymbol{Z}[\sqrt{-D}]$ に対し、$\varepsilon|1$ となることと $N(\varepsilon)=\pm 1$ となることとは同値。(このような 1 の約数を単数という。約数・倍数を考えるときは単数倍の違いは区別できない (のでしない)。)

(4) $\boldsymbol{Z}[\sqrt{-D}]$ の単数は、$D=1$ のとき $\varepsilon=\pm 1,\pm\sqrt{-1}$ で、それ以外は $\varepsilon=\pm 1$ に限る。($D=3$ のとき、$\boldsymbol{Z}[\omega]$ で考えていれば、$\varepsilon=\pm 1,\pm\omega,\pm\omega^2$ の可能性もある。)

問 18. D を square-free な自然数とし、$a+b\sqrt{D}$ $(a,b\in \boldsymbol{Z})$ の形の実数全体

$$\boldsymbol{Z}[\sqrt{D}] := \{a+b\sqrt{D} | a,b\in \boldsymbol{Z}\}$$

について同様なことを考える。このとき一般に、$\varepsilon|1$ となる $\varepsilon\in \boldsymbol{Z}[\sqrt{D}]$ は無限個存在する (ので、数論がいろいろ難しくなる)。$D=2,3,5,6,7,\ldots$ に対し、そのような ε を見出せ。$D=61,199$ などではどうか。

問 19. $\boldsymbol{Z}[\sqrt{-D}]$ において、素数・既約数を次で定義する。単数でも 0 でもない $\pi\in \boldsymbol{Z}[\sqrt{-D}]$ について、

- π が $\boldsymbol{Z}[\sqrt{-D}]$ の既約数 $\overset{\leftarrow}{\iff}$ ($\pi=\alpha\beta \Longrightarrow$ ($\pi|\alpha$ または $\pi|\beta$))
- π が $\boldsymbol{Z}[\sqrt{-D}]$ の素数 $\overset{\leftarrow}{\iff}$ ($\pi|\alpha\beta \Longrightarrow$ ($\pi|\alpha$ または $\pi|\beta$))

(π は p に対応するギリシャ文字だから使ったが、勿論ここでは円周率ではない。)

(1) 素数は既約数でもある。

(2) $\boldsymbol{Z}[\sqrt{-D}]$ に属す数は、単数でも 0 でもなければ、既約数の積に分解できる。(ヒント：$N(\alpha)$ に関する帰納法)

(3) $\boldsymbol{Z}[\sqrt{-D}]$ に属す数が素数の積に分解できるならば、その分解は掛ける順番と各素因数の単数倍の違いを除いて一意的である。(ヒント：上の定義にある素数の性質があれば、$\boldsymbol{Z}$ での時と全く同様に証明できる。)

(4) $D=5$ のとき、$\boldsymbol{Z}[\sqrt{-5}]$ 内で、6 は $6=2\cdot 3=(1+\sqrt{-5})(1-\sqrt{-5})$ と分解される。この時、各因数 $2,3,1\pm\sqrt{-5}$ は $\boldsymbol{Z}[\sqrt{-5}]$ の既約数であり、どれも互いに単数倍ではない。従って、既約数への分解の一意性は成立しない。

(5) $\boldsymbol{Z}[\sqrt{-5}]$ 内で、他に既約数の積に 2 通りに分解される例を見付けよ。($\boldsymbol{Z}[\sqrt{-6}]$ などでも同様の現象が起きるので、そこでの例でも可。)

問 20. 特に $\boldsymbol{Z}[\sqrt{-1}]$ を **Gauss の整数環**という。$\boldsymbol{Z}[\sqrt{-1}]$ では $\boldsymbol{Z}$ と類似の互除法が出来ることから、素因数分解の一意可能性が成立する。これを以下の順を追って示そう。

(1) $\xi \in \boldsymbol{C}$ に対し、$N(\xi - \gamma) < 1$ となる $\gamma \in \boldsymbol{Z}[\sqrt{-1}]$ が存在することを示せ。(ヒント：$\xi = x + y\sqrt{-1} \in \boldsymbol{C}$ を平面の点 (x, y) に対応させるとき (複素数平面・Gauss 平面などという)、$N(\xi) = x^2 + y^2$ は原点から (x, y) までの距離の平方である。)

(2) 任意の $\alpha, \beta \in \boldsymbol{Z}[\sqrt{-1}], \beta \neq 0$ に対して、$\alpha = \beta\gamma + \delta, N(\delta) < N(\beta)$ となる γ, δ が存在することを示せ。(ヒント：$\xi = \alpha/\beta$ について前問を適用せよ。これさえあれば以下の議論は $\boldsymbol{Z}$ の場合と殆ど同様に出来る。)

(3) 任意の $\alpha, \beta \in \boldsymbol{Z}[\sqrt{-1}]$ に対して、次を満たす $\delta \in \boldsymbol{Z}[\sqrt{-1}]$ が存在することを示せ。
- $\delta | \alpha, \delta | \beta$
- $\delta' | \alpha, \delta' | \beta \Longrightarrow \delta' | \delta$

このような δ は単数倍の違いを除いて一意的である。(その違いを気にせずに) $\delta = \gcd(\alpha, \beta)$ と書いて、α, β の最大公約数と呼ぶ。

(4) このとき、$\alpha\xi + \beta\eta = \delta$ となる $\xi, \eta \in \boldsymbol{Z}[\sqrt{-1}]$ が存在する。

(5) $\gcd(\alpha, \beta) = 1$ のとき、α, β は互いに素であるという。このとき、$\alpha | \beta\gamma \Longrightarrow \alpha | \gamma$.

(6) $\boldsymbol{Z}[\sqrt{-1}]$ では、既約数は素数でもある。(ヒント：π が既約数のとき、$\pi | \alpha$ でなければ π, α が互いに素であることを示す。)

(7) これより、$\boldsymbol{Z}[\sqrt{-1}]$ では素因数分解の一意可能性が成立する。

問 21. (Fermat の小定理) p を素数とする。p と互いに素な整数 a に対し、

$$a^{p-1} \equiv 1 \pmod{p} \qquad (a^p \equiv a \pmod{p} \text{と言っても同じ})$$

が成り立つ。これを次の 2 つの方法で示せ。

(1) (加法的方法) 二項定理により $(a+b)^p \equiv a^p + b^p \pmod{p}$ を示し、帰納法を用いる。

(2) (乗法的方法) $x = 1, \ldots, p-1$ に対して、$ax \bmod p$ が全て異なり 1 回づつ現れることから、$(p-1)!$ を 2 通りに計算して比較する。

問 22. (本問は Mathematica などの計算代数ソフトウェアを用いると良い。)
$N = 1316383,\ e = 3617$ とし、自分の学生番号の先頭のアルファベットを除いた 7 桁の数字で出来る自然数を P とする。

(1) N を法、e を暗号化鍵 (公開鍵) として、RSA 暗号で P を暗号化し、暗号文 C を求めよ。

(2) N を素因数分解して、これから復号鍵 (秘密鍵) d を求めよ。

(3) 求めた復号鍵 d を用いて、暗号文 C から平文 P を復元せよ。

問 23. 暗号・符号など、数理が利用されている実用技術について調べて述べよ。

レポート提出について

- 締切：**2013 年 2 月 4 日 (月)20 時頃**まで
- 内容：配布プリントのレポート課題の例のような内容、及び授業に関連する内容で、授業内容の理解または発展的な取組みをアピールできるようなもの
- 分量：プリントのレポート課題を全部提出する必要はなく、問題の重さによって適宜判断して数問取り組めば良い。内容に関しては、このプリントの例に必ずしも拘らず、意欲的な取組みを望む。