今までの主なレポート課題の例（01/16 配布）

問 17. n を正整数とし、不定方程式 $x^2+y^2=n$ を考える。

(1) 小さい n に対し、整数解 (x,y) が存在するかどうか調べよ。存在する場合・しない場合にどのような規則性があるか。

(2) 整数解 (x,y) が存在する場合に、それを利用して、$x^2+y^2=n$ の有理数解を全て求めよ。

問 18. 上問と同様のことを、不定方程式 $x^2+2y^2=n$ について考察するとどうなるか。また、$x^2+Dy^2=n$（$D\in\boldsymbol{N}, D>0$）で、D をいろいろ変えて考えてみよ。

問 19. 平方数で割り切れない整数を square-free（平方無縁）という。D を square-free な自然数とし、$a+b\sqrt{-D}$ $(a,b\in\boldsymbol{Z})$ 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) $N(\alpha):=\alpha\overline{\alpha}$（$\alpha$ 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) $-D\equiv 1 \pmod 4$ の時は、実は、$\sqrt{-D}$ の代わりに $\omega:=\dfrac{-1+\sqrt{-D}}{2}$ を考えて、$\boldsymbol{Z}[\omega]:=\{a+b\omega | a,b\in\boldsymbol{Z}\}$ を考えた方が何かと良い。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 20. $\boldsymbol{Z}[\sqrt{-D}]$ 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 $N(\varepsilon)=\pm1$ 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 $\varepsilon=\pm1,\pm\sqrt{-1}$ で、それ以外は $\varepsilon=\pm1$ に限る。（$D=3$ のとき、$\boldsymbol{Z}[\omega]$ で考えていれば、$\varepsilon=\pm1,\pm\omega,\pm\omega^2$ の可能性もある。）

問 21. D を square-free な正整数とし、$a+b\sqrt{D}$ $(a,b\in\boldsymbol{Z})$ 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。（見付けるのに $\sqrt{D}$ の連分数展開が利用できる。）

問 22. $\boldsymbol{Z}[\sqrt{-D}]$ 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 $\overset{\leftarrow}{\iff}$ $(\pi=\alpha\beta \Longrightarrow (\pi|\alpha \text{ または } \pi|\beta))$
- π が $\boldsymbol{Z}[\sqrt{-D}]$ の素数 $\overset{\leftarrow}{\iff}$ $(\pi|\alpha\beta \Longrightarrow (\pi|\alpha \text{ または } \pi|\beta))$

（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) 従って、$\boldsymbol{Z}[\sqrt{-D}]$ において既約数が必ず素数であれば、$\boldsymbol{Z}[\sqrt{-D}]$ に属す 0 でない数は、素数の（0 個以上の）積に分解でき、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。

(5) $D = 5$ 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。（特に、$2, 3, 1 \pm \sqrt{-5}$ は $\boldsymbol{Z}[\sqrt{-5}]$ の素数ではない。）

(6) $\boldsymbol{Z}[\sqrt{-5}]$ 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 23. 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 24. $\omega := \dfrac{-1+\sqrt{-3}}{2}$ とおき、$\boldsymbol{Z}[\omega]$ を **Eisenstein の整数環**という。これについても前問と同様なことを論ぜよ。

問 25. 整数 $a \in \boldsymbol{Z}$ に対し、その相異なる素因数全ての積を $\mathrm{rad}(a)$ と書き、a の**根基 (radical)** という：

$$\mathrm{rad}(a) := \prod_{p|a} p$$

a の根基 $\mathrm{rad}(a)$ は、或る $n \in \boldsymbol{N}$ に対して $a | r^n$ となるような自然数 r のうち最小のものである。

問 26. $a + b = c$ を満たす互いに素な正整数の組 (a, b, c) を abc-triple と呼ぼう。abc **予想**とは、abc-triple に対する次の命題のことである：

- 任意の正の実数 $\varepsilon > 0$ に対し、或る正の実数 $K = K_\varepsilon > 0$ が存在し、任意の abc-triple (a, b, c) に対して

$$c < K\mathrm{rad}(abc)^{1+\varepsilon}.$$

これは次の命題と同値である：

- 任意の正の実数 $\varepsilon > 0$ に対し、$c \geq \mathrm{rad}(abc)^{1+\varepsilon}$ となる abc-triple (a, b, c) は有限個。

問 27. abc 予想が正しければ、次を満たす正整数 N が存在する：

- 任意の abc-triple (a, b, c) に対して $c < \mathrm{rad}(abc)^N$

このとき、$n \geq 3N$ となる整数 n に対して、次の Fermat 予想の指数 n の場合が従う。

- $X^n + Y^n = Z^n$ は $XYZ \neq 0$ であるような整数解を持たない。

問 28. abc-triple (a,b,c) が abc 予想の不等式の限界に如何に “肉薄” しているか、を示す指標として、quality と呼ばれる次の値を導入する：

$$q = q(a,b,c) := \frac{\log(c)}{\log \mathrm{rad}(abc)}.$$

このとき、abc 予想は次のように言い換えられる：

- 任意の正の実数 $\varepsilon > 0$ に対し、$q(a,b,c) > 1+\varepsilon$ となる abc-triple (a,b,c) は有限個。

大きい quality の値を持つ abc-triple の例を探索せよ。（以下の問題はその例。）

問 29. r を正整数とするとき、$(a,b,c) = (1, 3^{2^r}-1, 3^{2^r})$ とすると、$q(a,b,c) > 1$ となる。（ヒント：$X^2-1 = (X-1)(X+1)$ を用いて b を繰返し分解すると、各因子が 2 で割れるので、b が 2 で多数回割れる。このことから、$\mathrm{rad}(b)$ が上から押さえられる。）この例は、quality が 1 より大きい abc-triple が無限個存在すること、即ち、$\varepsilon = 0$ では予想が成り立たないことを示している。

問 30. 上問で 3 の代わりに奇数 $5, 7, 11, 13, 15, 17, \ldots$ を用いたらどうか。また、不等式の限界に “肉薄” している度合いを比較せよ。

問 31. 平方因子を持たない正整数 N について、$\sqrt{N}$ の連分数展開の近似分数を s_n/t_n として、$s_n^2 - Nt_n^2 = C$ とおくと、C は n に関して有界、即ち、或る（N には依るが n に依らない）定数 B が存在して $|C| \le B$ となる。（特に $C = \pm 1$ となるような n が無限に（周期的に）現れる。問 21 参照。）記述の簡単のため、$C > 0$ とすると、このとき、$(a,b,c) = (C, Nt_n^2, s_n^2)$ は abc-triple で、$t_n < s_n/\sqrt{N}$ であることから、

$$\mathrm{rad}(abc) \le CN\mathrm{rad}(s_n)\mathrm{rad}(t_n) \le BNs_nt_n < B\sqrt{N}c$$

となり、$\varepsilon = 0$ のときの不等式に定数 $B\sqrt{N}$ 倍程度まで肉薄する。（$C < 0$ でも同様。）一般にはここまでだが、s_n, t_n が “偶々” 平方因子（やさらに高い冪の因子）を持つときは、$\mathrm{rad}(s_n), \mathrm{rad}(t_n)$ が小さくなって、$\mathrm{rad}(abc) > c$ 即ち $q(a,b,c) > 1$ となることが期待される。そのような例をいろいろ見つけよ。

問 32. 正整数 N, r について、N の r 乗根 $\sqrt[r]{N}$ の連分数展開の近似分数を s_n/t_n とし、$s_n^r - Nt_n^r = C$ とおいて abc-triple (a,b,c) を作ると、ほぼ、

$$\mathrm{rad}(abc) \le CN\mathrm{rad}(s_n)\mathrm{rad}(t_n) \le CNs_nt_n < CN^{1-\frac{1}{r}}c^{\frac{2}{r}}$$

となり、$r \ge 3$ のとき abc 予想に抵触する例を生み出すように見えるが、実は $r = 2$ のときと異なり、$r \ge 3$ のときは C が n につれて大きくなるので、直ちに反例となるわけではない。しかしながら、“偶々” C の値が小さくなるときには、$q(a,b,c)$ が大きい abc-triple (a,b,c) が見つかると期待される。そのような例をいろいろ見つけよ。（$\sqrt[r]{N}$ の連分数展開は近似値を用いて求めることになるだろう。現在見つかっている $q(a,b,c)$ が大きい abc-triple (a,b,c) の中にも、このようにして見つけられたと思われるものは多い。）

レポート提出について

- 締切：**2018 年 2 月 2 日 (金)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。
- 提出先：情報理工学科授業準備室（9-354 室）前のレポートポスト。授業最終回の授業終了後に提出しても良い。電子メイル（`tsuno-h@sophia.ac.jp` 宛）で提出しても良い。電子メイルで提出の場合は、原則として、**情報システム室（メディアセンター）の自分のアカウント**から送ること。
- 注意：参考にした文献があれば、その題名・著者などを記すこと。インターネット上の情報であれば、サイト名・文章題目・URL などを記すこと。但し、単なる文章の引き写しではなく、自分で理解した言葉でまとめること。他の受講者と共同で取り組んだ問題があれば、学生番号・氏名を記すこと。