2022 年度全学共通科目「現代の数学と数理解析」　山下 (剛) 担当回レポート問題

以下の 1 〜 10 を出来る限り多く答えよ.

1 (1). 4 で割って余りが 1 になる 100 以下のすべての素数 p に対して, $p = x^2 + y^2$ となる自然数 x, y を見つけよ. (例: $5 = 2^2 + 1^2$.)
(2). 8 で割って余りが 1 か 3 になる 100 以下のすべての素数 p に対して, $p = x^2 + 2y^2$ となる自然数 x, y を見つけよ. (例: $3 = 1^2 + 2 \cdot 1^2$.)
(3). 8 で割って余りが 1 か 7 になる 100 以下のすべての素数 p に対して, $p = x^2 - 2y^2$ となる自然数 x, y を見つけよ. (例: $7 = 3^2 - 2 \cdot 1^2$.)

2 p を素数とする. 集合 $\mathbb{F}_p := \{0, 1, 2, \ldots, p-1\}$ に「常に p で割った余りで考える」ことで加減乗除を定義する. $\mathbb{F}_p$ において 0 でない元による割り算が常に可能であることを示せ.

3 p を素数, a を p と互いに素な自然数とする時, a^{p-1} を p で割った余りが 1 になることを示せ (**Fermat の小定理**). (色々な証明方法があるが, (初歩的な群論を学んでいない 1 回生向けの) ヒント: 2 項定理を用いて自然数 n, m に対し $(n+m)^p$ と $n^p + m^p$ は p で割った余りが等しいことを示せ. 次に, それを用いて a^p と a は p で割った余りが等しいことを示し, 2 を使え.)

4 素数 p に対して $\mathbb{F}_p^\times := \{1, 2, \ldots, p-1\}$ $(\subset \mathbb{F}_p)$ として (常に p で割った余りを考えて) 掛け算でこの集合に演算を入れる.

$$\mathbb{F}_p^\times = \{a, a^2, \ldots, a^{p-1}\}$$

となる $a \in \mathbb{F}_p^\times$ が存在する (つまり, $\mathbb{F}_p^\times$ **は巡回群である**) ことを以下の指示に従って示せ. (a を $\mathbb{F}_p^\times$ の **生成元** (の 1 つ) と呼ぶ.)
(1). 自然数 n に対して, n と互いに素な 1 以上 n 以下の自然数の個数を $\varphi(n)$ と置く (**Euler の φ 関数**). 任意の自然数 n に対して $n = \sum_{d|n} \varphi(d)$ を示せ. (ここで $\sum_{d|n}$ は n を割る自然数 d を走るという意味である.)
(2). $\mathbb{F}_p^\times$ の元 a に対して ($\mathbb{F}_p^\times$ の中で) $a^d = 1$ となる最小の自然数 $d \geq 1$ を a の **位数** と呼ぶことにする. 3 を使い $\mathbb{F}_p^\times$ の任意の元の位数は $p-1$ の約数であることを示せ.
(3). 与えられた自然数 d に対して, $\mathbb{F}_p^\times$ の元で位数 d となるものの個数 $f(d)$ は 0 か $\varphi(d)$ であることを示せ. (ヒント: $\mathbb{F}_p$ は 2 より加減乗除 (特に非零による割り算) が出来るため, $\mathbb{F}_p$ 係数の d 次多項式は高々 d 個の根をもつことを使え.)
(4). (1), (2), (3) から $\mathbb{F}_p^\times$ に生成元が存在することを示せ.

5 素数 p に対して **Fermat の 2 平方和の定理**

$$p = x^2 + y^2 \text{ となる自然数 } x, y \text{ が存在する} \ \Leftrightarrow \ p = 2 \text{ か } p \text{ は } 4 \text{ で割ると } 1 \text{ 余る}$$

を以下の指示に従って示せ.
(1). x, y の偶奇で場合分けして 4 で割った余りを考えることで $\Rightarrow$ を示せ.
(2). 4 を用いて, 奇素数 p に対し

$$a^2 = -1 \text{ となる元 } a \in \mathbb{F}_p^\times \text{ が存在する} \ \Leftrightarrow \ p \text{ を } 4 \text{ で割ると } 1 \text{ 余る}$$

を示せ.

裏面もあることに注意せよ.

(3). 整数 n に対して $\mathbb{F}_p$ の元と考えたものを $\overline{n}$ と書くことにする. p を 4 で割って 1 余る素数とする. a を (2) の $\Leftarrow$ により存在が言えている元 $a \in \mathbb{F}_p^\times$ とする. 自然数 x_1, x_2, y_1, y_2 に対して

$$\overline{x_1} - a\overline{y_1} = \overline{x_2} - a\overline{y_2}, \quad (x_1, y_1) \neq (x_2, y_2), \quad 0 \leq x_1, x_2, y_1, y_2 < \sqrt{p}$$

となるものが存在することを示せ. (ヒント: 鳩ノ巣原理)
(4). (3) の x_1, x_2, y_1, y_2 を用いて $p = x^2 + y^2$ となる自然数 x, y が存在することを示せ.

6 (1). 4 で割って 3 余る素数が無限個存在することを示せ. (ヒント: そのような素数が $p_1, \ldots, p_n$ と有限個だと仮定し, $4p_1 \cdots p_n - 1$ を考えよ.)
(2). 4 で割って 1 余る素数が無限個存在することを示せ. (ヒント: そのような素数が $p_1, \ldots, p_n$ と有限個だと仮定し, $(2p_1 \cdots p_n)^2 + 1$ を考え 5 の (2) の $\Rightarrow$ を使え.)

7 (1).

$$\text{素数 } p \neq 2, 5 \text{ に対して } (p) = \mathfrak{p}\overline{\mathfrak{p}} \text{ と } \mathbb{Q}(\sqrt{-5}) \text{ で分解} \Leftrightarrow p \equiv 1, 3, 7, 9 \pmod{20}$$

である ($\overline{\mathfrak{p}}$ は $\mathfrak{p}$ の $\mathbb{Q}$ 上の共役) が, 一方

$$\text{素数 } p \neq 5 \text{ が } p = x^2 + 5y^2 \, (x, y \in \mathbb{Z}) \text{ と書ける} \Leftrightarrow p \equiv 1, 9 \pmod{20}$$

と両者の合同 (による) 判定条件がズレる. この現象を「元とイデアルのズレ」及び $\mathbb{Q}(\sqrt{-5})$ の **Hilbert 類体** (=導手 (1) の**射類体**) $\mathbb{Q}(\sqrt{-5}, \sqrt{-1})$ での分解の観点から説明せよ. (余裕があれば, 上記の後者の同値を証明せよ.)
(2).

$$\text{素数 } p \neq 2, 3 \text{ に対して } (p) = \mathfrak{p}\overline{\mathfrak{p}} \text{ と } \mathbb{Q}(\sqrt{3}) \text{ で分解} \Leftrightarrow p \equiv 1, 11 \pmod{12}$$

である ($\overline{\mathfrak{p}}$ は $\mathfrak{p}$ の $\mathbb{Q}$ 上の共役) が, 一方

$$\text{素数 } p \text{ が } p = x^2 - 3y^2 \, (x, y \in \mathbb{Z}) \text{ と書ける} \Leftrightarrow p \equiv 1 \pmod{12}$$

と, $\mathbb{Q}(\sqrt{3})$ においてすべてのイデアルは 1 元で生成されるにも関わらず両者の合同 (による) 判定条件がズレる. この現象を $\mathbb{Q}(\sqrt{3})$ の基本単数 (のノルム) の性質と「イデアル類群と狭義イデアル類群のズレ」及び $\mathbb{Q}(\sqrt{3})$ の **狭義 Hilbert 類体** (=導手 $(1) \cdot \infty_1 \cdot \infty_2$ の**射類体**) $\mathbb{Q}(\sqrt{3}, \sqrt{-1})$ での分解の観点から説明せよ. (余裕があれば, 上記の後者の同値を証明せよ.)

8

$$f = q \prod_{n \geq 1} (1 - q^n)\left(1 - q^{23n}\right) = \sum_{n \geq 1} a_n q^n$$

で a_n を定める. (f は重さ 1, レベル 23, 指標 $(\frac{-23}{\bullet})$ の**正規化 Hecke 固有尖点形式**になる.) α を $x^3 - x - 1 = 0$ の根の 1 つとし,

$$H := \mathbb{Q}\left(\sqrt{-23}, \alpha\right)$$

($\mathbb{Q}(\sqrt{-23})$ の **Hilbert 類体**) とする. ($x^3 - x - 1 = 0$ の判別式は $-(4(-1)^3 + 27(-1)^2) = -23$ より H は α の取り方には依存しない.) (H の $\mathbb{Q}$ 上の Galois 群は 3 次対称群になり, 非可換である.)
(1). $p = 2, 3$ に対して (a). $a_p = -1$ を示せ. (b). $\mathbb{Q}(\sqrt{-23})$ において $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ と分解するが $\mathfrak{p}$ は H において分解しないことを示せ. (ヒント: $\mathbb{Q}(\sqrt{-23})$ の整数環は $\mathbb{Z}\left[\frac{1+\sqrt{-23}}{2}\right]$ であったことを思い出せ. また, **Hilbert 類体の理論**により, $\mathfrak{p}$ は H において (完全) 分解しないことは $\mathfrak{p}$ が (素元で) 1 元生成されない, つまり $p = x^2 + 23y^2 \, (x, y \in \mathbb{Z})$ と書けないことと同値であったことも思い出せ.)

2 枚目に続くことに注意せよ.

(2). $p = 5, 7$ に対して (a). $a_p = 0$ を示せ. (b). $\mathbb{Q}(\sqrt{-23})$ において $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ と分解しないことを示せ. (ヒント: $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ と分解すれば $\mathbb{Z}\left[\frac{1+\sqrt{-23}}{2}\right]/\mathfrak{p} \cong \mathbb{F}_p$ であったことを思い出し, $\beta := \frac{1+\sqrt{-23}}{2} \in \mathbb{Z}\left[\frac{1+\sqrt{-23}}{2}\right]$ は $\beta^2 - \beta + 6 = 0$ を満たすことを使え.)
(3). $p = 59, 101$ に対して (a). **Euler の五角数定理**

$$\prod_{n\geq 1}(1-q^n) = \sum_{n\in\mathbb{Z}}(-1)^n q^{\frac{n(3n-1)}{2}} = 1 + \sum_{n\geq 1}(-1)^n q^{\frac{n(3n-1)}{2}} + \sum_{n\geq 1}(-1)^n q^{\frac{n(3n+1)}{2}}$$

を用いて $a_p = 2$ を示せ. (b). $\mathbb{Q}(\sqrt{-23})$ において $(p) = \mathfrak{p}\overline{\mathfrak{p}}$ と分解し, $\mathfrak{p}$ も H において分解することを示せ. (ヒント: **Hilbert 類体の理論**により, $\mathfrak{p}$ は H において (完全) 分解することは $\mathfrak{p}$ が (素元で) 1 元生成される, つまり $p = x^2 + 23y^2$ $(x, y \in \mathbb{Z})$ と書けることと同値であったことを思い出せ.)
(注: 一般に, 素数 $p \neq 23$ に対して p の $\mathrm{Gal}(H/\mathbb{Q})$ での (共役を除いて定まる) **Frobenius 元** (の 1 つ) を Fr_p と書くと,

$$\begin{aligned}
a_p = 2 &\Leftrightarrow \mathrm{Fr}_p \text{の位数は} 1 \Leftrightarrow (p) \text{は} H \text{で完全分解} \Leftrightarrow p = x^2 + 23y^2\ (x, y \in \mathbb{Z}) \text{と書ける},\\
a_p = -1 &\Leftrightarrow \mathrm{Fr}_p \text{の位数は} 3 \Leftrightarrow (p) \text{は} \mathbb{Q}(\sqrt{-23}) \text{で分解するが} H \text{で完全分解しない},\\
a_p = 0 &\Leftrightarrow \mathrm{Fr}_p \text{の位数は} 2 \Leftrightarrow (p) \text{は} \mathbb{Q}(\sqrt{-23}) \text{で分解しない}
\end{aligned}$$

を示すことが出来る. 可換な時の合同式が一見消えてなくなっているように見えるが, 可換な時の「合同式」は非可換な時には「保型性」に対応している. (数体 F と F のアデール $\mathbb{A}_F$ に対して $\mathrm{GL}_1(F)\backslash\mathrm{GL}_1(\mathbb{A}_F)/K$ 上の関数 (K は $\mathrm{GL}_1(\mathbb{A}_F)$ の開コンパクト部分群) で指標になっているものに対し $\mathrm{GL}_1(F)$, K がその「合同式の法」に対応し, $\mathrm{GL}_2(F)\backslash\mathrm{GL}_2(\mathbb{A}_F)/K'$ 上の関数 (K' は $\mathrm{GL}_2(\mathbb{A}_F)$ の開コンパクト部分群) で正規化 Hecke 固有になっているものに対し $\mathrm{GL}_2(F)$, K' がその「保型性の法」に対応する.))

9 あなたの好きな定理を (名前のみではなく内容を) 述べ, その理由もあわせて書け. 定理や理由は今回の講義内容と必ずしも関係しなくてもよい (定理や理由は成績には影響しないが, 定理の主張がおかしいなどの数学的内容に不備がある場合は成績に影響する).

10 講義について感想やコメントなどを書け (成績には影響しない).