

2014 年度 前期 中間試験 (問題 兼 解答用紙)

開講学部	評点
理工学部	

問題枚数	両面印刷	別紙解答用紙	試験時間	試験科目名	クラス	出題者
1/1	有	なし	80 分	代 数 学 I <small>木曜 2 時限, 教科書 : A.Weil 著「初学者のための整数論」</small>	A	大 西 良 博
持込許可物件	所属学部	所属学科	学年	学 籍 番 号 (9 桁)	氏 名	
なし	理工学部	数学科	2 年			

- 注意 1. 最終的な答に至る途中の説明をできるだけ詳しく書くこと。最終結果だけでは得点できない。  
 注意 2. 学生証, 記名用のペン, 鉛筆またはシャープペンシル, 消しゴム以外は机の上に置かないこと。  
 注意 3. 試験場の静粛を保つために, 退出は開始 60 分後の時点の一回限りとする。

1 (15 点)  $F_1 = F_2 = 1, F_{n+2} = F_{n+1} + F_n (n \geq 1)$  で定まる数列  $\{F_n\}$  について  $\gcd(F_n, F_{n+1}) = 1$  となることを証明せよ。

2 (15 点)  $703x + 481y = \gcd(703, 481)$  となる  $x, y$  を全て求めよ。

3 (20 点)  $\gcd(a, b) = 1$  で  $a^2 - b^2$  が完全平方数であれば  $a + b$  と  $a - b$  はともに完全平方数であるか, ともに完全平方数の 2 倍であるかのどちらかであることを示せ。

4 (15点)  $S$  は群  $G$  の有限部分集合とする.  $S$  が  $G$  の群演算で閉じているならば,  $S$  は部分群になることを示せ.

5 (15点)  $d = \gcd(m, n)$  とする. 連立方程式

$$x \equiv a \pmod{m}, x \equiv b \pmod{n}$$

が解を持つためには,  $a \equiv b \pmod{d}$  であることが必要十分であることを示せ. また  $d = 1$  であれば, 解は法  $mn$  に関して唯一つであることを示せ.

6 (20点)  $m > 0, n > 0, \in \mathbb{Z}$  とし,  $\gcd(m, n) = 1$  とする. このとき  $\varphi(mn) = \varphi(m)\varphi(n)$  であることを証明せよ.

(Hint : 5 の結果を使う.)

## 既習事項のまとめ

- ( 1)  $\mathbb{Z}$  は整数全体のなす環,
- ( 2)  $\mathbb{Q}$  は有理数全体のなる体.
- ( 3)  $a, b, \dots, c \in \mathbb{Z}$  に対して,

$$\{ax + by + \dots + cz \mid x, y, \dots, z \in \mathbb{Z}\} = d\mathbb{Z}$$

となる  $d \in \mathbb{Z}$  ( $d \geq 0$ ) が唯 1 つ存在する. このときは  $d = (a, b, \dots, c)$  または  $d = \gcd(a, b, \dots, c)$  と表す.

- ( 4) 群とは演算  $G \times G \rightarrow G : (a, b) \rightarrow ab$  が定義された集合  $G$  であって,
  - (i) 単位元が存在し, かつ
  - (ii) 各元の逆元が存在するもののことである.この講義ではさらに, 可換性, つまり任意の  $a, b \in G$  に対して,  $ab = ba$  も仮定している.
- ( 5) 部分群とは群の部分集合であって, その群の演算について, それ自体で群になっているもののことである.
- ( 6) 群  $G$  といくつかの元の部分集合  $\{a, b, \dots, c\} \subset G$  について, これらの元の逆元をとること, あるいは, それらの間のできる限りの演算をほどこすことによって得られる (生成される) 元を集め, さらに, そうして得られた (生成された) あらゆる元に対して同様のことを行う. これを何度も繰り返して得られた (生成された) 元を全て集めてできる群を,  $\{a, b, \dots, c\}$  で 生成される (部分) 群と呼ぶ.
- ( 7) 巡回群とは 1 つの元で生成される群のことである.
- ( 8)  $G$  を  $x$  で生成された位数  $m$  の巡回群とする.  $G$  の任意の部分群  $H$  はまた巡回群であり,  $d \mid m$  なる  $d$  が存在して,  $x^d$  が  $H$  を生成する.
- ( 9)  $\mathbb{Z}/m\mathbb{Z}$  は法  $m$  による剰余類 ( $k \bmod m$ ) ( $= \bar{k}$  と略記する) 達のなす (可換) 環.  
例えば  $\mathbb{Z}/5\mathbb{Z} = \{(0 \bmod 5), (1 \bmod 5), (2 \bmod 5), (3 \bmod 5), (4 \bmod 5)\} = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}\}$ .
- ( 10)  $m$  が素数  $p$  のとき,  $\mathbb{Z}/m\mathbb{Z} = \mathbb{F}_p$  と略記する.
- ( 11)  $(\mathbb{Z}/m\mathbb{Z})^\times = \{(j \bmod m) \in \mathbb{Z}/m\mathbb{Z} \mid \gcd(j, m) = 1\}$ . これは積に関して群をなす. 法  $m$  に関する 既約剰余類群 と呼ばれる.
- ( 12)  $\varphi(n) = “(\mathbb{Z}/n\mathbb{Z})^\times$  の要素の個数” = “ $1, \dots, n-1$  の中で  $n$  と互いに素なものの個数”.  
ただし  $\varphi(1) = 1$ .