実施：2014 年 8 月 4 日 (木) 13:10-14:40, 4-410 室

開講学部	評点
理工学部	

2014 年度　**前 期　定 期 試 験**　(問題 兼 解答用紙)

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 木曜 2 時限，教科書：A.Weil 著「初学者のための整数論」	A, B	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)　x, y, $z \in \mathbb{Z}$ で $x^2 + y^2 = z^2$ ならば $xyz \equiv 0 \pmod{60}$ であることを証明せよ．

2 (15 点)　$551x + 377y = \gcd(551, 377)$ 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 (10 点) p は素数とする. このとき $(p-1)! \equiv -1 \pmod{p}$ であることを示せ.

(Hint : $(\mathbb{Z}/p\mathbb{Z})^{\times}$ の各元とその逆元を組にしてみる.)

5 (20 点) $d = \gcd(m, n)$ とする. 連立方程式

$$x \equiv a (\mathrm{mod} m),\ x \equiv b (\mathrm{mod} n)$$

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 1 つであるとを示せ.

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.)

ここより下に記入しないで下さい.

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, $\cdots$, $c \in \mathbb{Z}$ に対して,

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

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

(4) 群 とは演算 $G \times G \to G : (a, b) \to ab$ 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 $\{a, b, \cdots, c\} \subset G$ 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, $\{a, b, \cdots, c\}$ 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, $d|m$ 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 $(k \mod m)$ $(= \overline{k}$ と略記する) 達のなす (可換) 環.
例えば $\mathbb{Z}/5\mathbb{Z} = \{(0 \mod 5), (1 \mod 5), (2 \mod 5), (3 \mod 5), (4 \mod 5)\} = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$.

(10) m が素数 p のとき, $\mathbb{Z}/m\mathbb{Z} = \mathbb{F}_p$ と略記する.

(11) $(\mathbb{Z}/m\mathbb{Z})^\times = \{(j \bmod m) \in \mathbb{Z}/m\mathbb{Z} \,|\, \gcd(j, g) = 1\}$. 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” = “$1, \cdots, n-1$ の中で n と互いに素なものの個数”.
ただし $\varphi(1) = 1$.