代数入門演習中間試験　　　　　　　　　　　　　2012. 12.18

(**注意**)

1. まず, すべての解答用紙に学籍番号と名前を書いてください.
2. 解答用紙は 3 枚です. 表裏を使って構いません. 各問題の解答は解答用紙のまとまった場所に書くこと.
3. 式の羅列ばかりでは数学の解答にはなりません. 説明が足りないものは大いに減点します.
4. 120 点満点です.

問題 1. (各 10 点)　p を 2 以上の自然数とする.

(1) p が素数であることの定義を書け. 約数の定義も書くこと.

(2) p が素数となるための必要十分条件 (特徴付け) を正確に述べよ.

問題 2. m を 2 以上の自然数とし, a, b を整数とする.

(1) (10 点)　合同式 $a \equiv b \mod m$ の定義を書け.

(2) (15 点)　a で代表される剰余類を

$$\bar{a} := \{x \in \mathbb{Z} \mid x \equiv a \mod m\}$$

と表わす. $\bar{a} = \bar{b}$ かつ $\gcd(a, m) = 1$ ならば, $\gcd(b, m) = 1$ となることを示せ.

問題 3. ((1) は 10 点, (2) は 15 点)　次の合同式を解け.

(1) $82x \equiv 1 \mod 121$　　(2) $\begin{cases} 82x \equiv 1 \mod 121 \\ x \equiv 2 \mod 8 \end{cases}$

問題 4. (各 10 点)　m を自然数とし, $\bar{a}$ を既約剰余類群 $(\mathbb{Z}/m\mathbb{Z})^\times$ の元とする.

(1) a が mod m の原始根であることの定義を書け. 位数の定義も書くこと. ただし φ で Euler 関数を表わす.

(2) $m = 7$ と取る. 既約剰余類群 $(\mathbb{Z}/7\mathbb{Z})^\times$ の各元 $\bar{1}, \bar{2}, \ldots, \bar{6}$ の位数を求めよ. また原始根をすべて求めよ. その個数はいくつか答えよ.

問題 5. (各 15 点)　n, a, b, c, d を自然数とする. 次を証明せよ.

(1) $5^n \equiv 1 \mod 16$ ならば $4 \mid n$.

(2) $(-1)^a 5^c \equiv (-1)^b 5^d \mod 16$ ならば $a \equiv b \mod 2$, $c \equiv d \mod 4$.