情報基礎数学 I・構造数理　期末試験 (2005 年 7 月 29 日)

注意. 途中の計算や議論も書いて下さい. 答えが間違っていても部分点を出せる場合があるので, できる限り丁寧な答案を書くよう, 心掛けて下さい. 授業中に紹介した定理は証明なしで用いて良い.

1. 次の連立一次合同式を解け. 更に, 0 以上 1000 以下となる整数解を全て求めよ.

$$\begin{cases} x & \equiv & 2 & (\mathrm{mod} \quad 5) \\ x & \equiv & 3 & (\mathrm{mod} \quad 7) \\ x & \equiv & 2 & (\mathrm{mod} \quad 11) \end{cases}$$

2. (1) 3^{100} を 35 で割ったときの余りを求めよ.

(2) 全ての整数 a に対して, $a^{25} \equiv a \pmod{35}$ が成り立つかどうか理由をつけて答えよ.

3. (1) $\mathbb{Z}/13\mathbb{Z} = \{K(0), K(1), \ldots, K(12)\}$ において, 次の等式をみたす整数 x $(0 \leq x \leq 12)$ を求めよ. (次の式の演算は剰余環 $\mathbb{Z}/13\mathbb{Z}$ での演算である.)

$$K(x) = (K(7) + K(9)) \div K(6)$$

(2) $\mathbb{Z}/13\mathbb{Z}$ の元 $K(a)$, $K(b)$ で, $K(a)K(b) = K(0)$ かつ $0 < a, b < 13$ となるものは存在するかどうか理由をつけて答えよ.

4. 暗号化鍵 (公開鍵) が $(n, e) = (187, 23)$ となる RSA 暗号について, 次の (1) と (2) を答えよ.

(1) 復号化鍵 (秘密鍵) d を求めよ.

(2) 暗号文 $y = 3$ を復号化し, 元の平文 x を求めよ.

5. 一次合同式 $21x \equiv 9 \pmod{15}$ を解け. 更に, 15 を法としたときの解の個数を求めよ.