

情報基礎数学 I テスト問題

2007.07.27. 実施 (吉原)

1 一次合同式 $66x \equiv 2 \pmod{17}$ を解け。

2 p を素数とするとき、以下の問に答えよ。

- (1) 整数 r が $0 < r < p$ をみたすとき、 ${}_p C_r$ は p の倍数であることを示せ。
- (2) a, b は正の整数とするとき、 $(a+b)^p \equiv a^p + b^p \pmod{p}$ を示せ。
- (3) a を正の整数とするとき、 $a^p \equiv a \pmod{p}$ を示せ。
- (4) $1^{17} + 2^{17} + 3^{17} + \dots + 16^{17}$ を 17 で割った余りを求めよ。

3 以下の問に答えよ。

- (1) 自然数 n に対して、 $1, 2, \dots, n$ の中で n と互いに素なものの個数が 4 となるような n をすべて求めよ。
- (2) 自然数 n に対して、 $1, 2, \dots, n$ の中で n と互いに素なものの個数が 5 となるような n をすべて求めよ。

4 暗号化鍵 $(n, e) = (35, 13)$ をもつ暗号文 $y = 16$ を解読せよ。すなわち、暗号化鍵 $(35, 13)$ から復号化鍵 d を求め、暗号文 y を復号化し、もとの文 x を求めよ。