

応用数理情報概論 II 中間試験  
2015年6月8日

注意

- 答案用紙に3枚とも学修番号・氏名を書くこと.
- 答案用紙の裏面を用いてもよい.

問題

1. アルファベット大文字 26 文字に関するシーザー暗号を考える. 平文 “TMU” が暗号文 “CVD” に暗号化される時, 同じ鍵によって得られる暗号文

“HNB R QJEN J WDVKNA”

に対応する平文を求めよ. ただし, 空白は暗号化によって変化しないものとする.

2.  $a = 1012, b = 451$  に対し,  $a$  と  $b$  の最大公約数  $d$  と,  $\alpha a + \beta b = d$  となる整数  $\alpha, \beta$  を 1 組求めよ.
3.  $\mathbb{Z}/12\mathbb{Z}$  の可逆元をすべて求めよ.
4. 次の整数  $a, b, n$  に対して, 線形合同式  $ax \equiv b \pmod{n}$  を満たす整数  $x$  で  $0 \leq x \leq n-1$  を満たすものをすべて求めよ.
  - (a)  $a = 42, b = 16, n = 47$ .
  - (b)  $a = 91, b = 78, n = 143$ .
5.  $n$  が合成数ならば,  $2^n - 1$  も合成数であることを示せ.
6. 正の整数  $a, b, k$  に対して,

$$\gcd(a^k, b^k) = \gcd(a, b)^k$$

が成り立つことを示せ.