計算数学特論 レポート課題

機械知能工学専攻　16344217　津上 祐典

課題 1

(1) $(Z_p*, \times)$ が群の構造を持つことを示せ.

条件 1. 演算 $\times$ が閉じている.

演算 $\times$ が閉じている，つまり $a, b \in Z_p*(a, b$ は自然数) のとき，$a \times b(\mathrm{mod\ p}) \in Z_p*$ であることを示せば良い．一般に $a \times b(\mathrm{mod\ p}) = 0, 1, \cdots, p-1$ である $Z_p* = \{1, 2, \cdots, p-1\}$

(2) (1) を用いて，フェルマーの小定理 $a^{p-1}(\mathrm{mod\ \ p}) = 1$($a$ は Z_p* の任意の要素) を示せ.

おおお

課題 2

(1) $p = 7, q = 13$ で公開鍵 e と秘密鍵 d を設定せよ.

おお

(2) コーディングを以下とする．a=1,b=1$\cdots$,z=26,A=27,B=28,$\cdots$,Z=52,0=60,1=61$\cdots$,9=69