応用数学６ 2010 年 11 月 11 日

第 2 回小テスト

講師: 安永憲司

問題 2 と 3 は，電卓等の電子計算機は使わずに，手で計算してください．

問題 1.

一方向性関数 f の逆計算の困難性の定義として，様々なものが考えられる．以下の二つについて，(a) と (b) を比べたとき，逆関数の困難性が強い方を，その根拠とともに答えよ．

1. (a) 以下を満たす PPT アルゴリズム A は存在しない．

$$\forall x, \Pr[A(f(x)) \in f^{-1}(f(x))] = 1.$$

(b) 以下を満たす確率的アルゴリズム A は存在しない．

$$\forall x, \Pr[A(f(x)) \in f^{-1}(f(x))] = 1.$$

2. (a) 任意の PPT アルゴリズム A に対し，無視できる関数 $\epsilon(\cdot)$ が存在し，すべての $n \in \mathbb{N}$ に対して，

$$\Pr[f(x') = y \mid x \xleftarrow{R} \{0,1\}^n, y = f(x), x' \leftarrow A(1^n, y)] \leq \epsilon(n).$$

(b) 任意の PPT アルゴリズム A に対し，ある多項式 $p(\cdot)$ が存在し，すべての $n \in \mathbb{N}$ に対して，

$$\Pr[f(x') = y \mid x \xleftarrow{R} \{0,1\}^n, y = f(x), x' \leftarrow A(1^n, y)] \leq 1 - \frac{1}{p(n)}.$$

問題 2.

1. 拡張 Euclid 互除法を用いて，素数 61 と 79 に対して，$61x + 79y = 1$ となる整数 x, y を求めよ．
2. 乗法群 $\mathbb{Z}_{79}^*$ において，61 の逆元を求めよ．
3. $\mathbb{Z}_7^*$ における生成元をすべて求めよ．

問題 3.

Alice と Bob は RSA 暗号を用いて秘匿通信を行った．Bob はパラメータ $N = 91, e = 29$ を選び，暗号化関数 $f_{N,e}(x) = x^e \bmod N$ を用いて，暗号文 $c = 2$ という結果を得た．そしてそれを Alice に送った．しかし，Bob の選んだパラメータ N はあまり大きくないため，暗号文からメッセージを計算することができる．Bob の送ったメッセージ x を求めよ．