学術フロンティア講義 （平成 29 年度・夏学期）
数理工学のすすめ　レポート課題

高木 剛
工学部 計数工学科
takagi@mist.i.u-tokyo.ac.jp

2017 年 6 月 22 日

以下の二問のうち，一問を選んで解答すること．

問 1

1. 素数 p と整数 $a \in \{1, 2, ..., p-1\}$ に対して，次の問いに答えよ．
   (a) $a^k \equiv 1 \bmod p$ となる最小正の整数 k は，$k \,|\, (p-1)$ を満たすことを示せ．
   (b) $a^{p-1} \equiv 1 \bmod p$ かつ $0 < d < p-1$ に対して $a^d \not\equiv 1 \bmod p$ を満たす a は，$\varphi(p-1)$ 個あることを示せ．ただし，φ はオイラーの φ 関数とする．

2. 銀行のキャッシュカードの暗証番号は，10 進 4 桁の整数としてランダムに分布していると仮定する．同じ部屋にキャッシュカードを 1 枚だけ持つ人を集めた場合，少なくとも 2 人が同じ暗証番号となる確率が 0.99 より大きくなるには，何人の人を集める必要があるかを計算せよ．

問 2

量子コンピュータが RSA 暗号に与える影響に関して，書籍やインターネット等で調べ，まとめよ．