THE CHINESE UNIVERSITY OF HONG KONG
DEPARTMENT OF MATHEMATICS

MMAT5510 Foundation of Advanced Mathematics 2017-2018
Assignment 3 (Due date: 30 Nov, 2017)

1. Suppose that S and T are sets such that $T \subseteq S$. Show that
   (a) if S is a finite set, then T is also a finite set;
   (b) if T is an infinite set, then S is an infinite set.
2. Prove that the set of all prime numbers is a countably infinite set.
   (Hint: You may use the fact that a subset of a countable set is countable.)
3. Let A be the set of all integers which are divisible by 5. By writing down an explicit bijection $f : \mathbb{N}^+ \to A$, where $\mathbb{N}^+$ is the set of all positive integers, show that A is a countably infinite set.
4. Let $a, b, c \in \mathbb{Z}$. Show that there exist $s, t \in \mathbb{Z}$ such that $as + bt = c$ if and only if $\gcd(a, b)|c$.
5. Solve the following equations.
   (a) $8x \equiv 3 \pmod{27}$
   (b) $7x + 32 \equiv 6 \pmod{18}$
6. (a) Compute $\varphi(15)$, where φ is the Euler's φ function.
   (b) Find the remainder when 8^{2017} is divided by 15.
   (Hint: Using Euler's Theorem.)
7. Find all integers x such that $x \equiv 3 \pmod{11}$ and $x \equiv 4 \pmod{13}$.
8. RSA cryptosystem is implemented by using two primes $p = 17$ and $q = 23$.
   (a) i. Compute $\varphi(n)$, where $n = pq$.
   Hence choose a possible number e to generate a public key (n, e).
   ii. According to your choice in part (a), generate the private key d.
   iii. What is the ciphertext c if the message $m = 33$ is encrypted?
   (Remark: Verify your answer by decrypting c by using the private key d and see if you can recover m.)
   (b) i. If $e = 29$ is chosen, generate the private key d.
   ii. Suppose that the ciphertext received is $c = 18$. Find the original message m, given that $0 \leq m < n$.
9. (Optional) If a ciphertext $c = 125$ is sent by using RSA cryptosystem while the public key using is $(n, e) = (28459, 109)$. What is the orginal message m, given that $0 \leq m < n$?