THE CHINESE UNIVERSITY OF HONG KONG
DEPARTMENT OF MATHEMATICS

MMAT5210 Discrete Mathematics 2017-2018
Assignment 2 (Due date: 22 Feb, 2017)

1. (a) Suppose that a, b and n are positive integers. Prove that if $a^n \mid b^n$, then $a \mid b$.
   (b) Suppose that p is a prime and a and k are positive integers. Prove that if $p \mid a^k$, then $p^k \mid a^k$.

2. Prove that an integer n is divisible by 3 if and only if the sum of the digits of n is divisible by 3.
   (Hint: Express n as $a_1 + 10a_2 + 10^2a_3 + \cdots + 10^k a_k$.)

3. Find the last two digits of 123^{562}.

4. 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 $0 \le m < n$.

5. (Optional) If a ciphertext $c = 273095689186$ is sent by using RSA cryptosystem while the public key using is $(n, e) = (712446816787, 6551)$. What is the orginal message m, given that $0 \le m < n$?

6. Prove that a subgroup of a cyclic group is also cyclic.

7. Let G be an abelian group. Let H be the subset of G consisting of the identity e together with all elements of G of order 2. Show that H is a subgroup of G.

8. Show that a finite abelian group is not cyclic if and only if it contains a subgroup isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ for some prime p.

9. Prove that if a finite abelian group has order a power of a prime, then the order of every element in the group is a power of p.