THE CHINESE UNIVERSITY OF HONG KONG
DEPARTMENT OF MATHEMATICS

MMAT5210 Discrete Mathematics 2017-2018
Suggested Solution to Assignment 2

1. (a) Suppose that a, b and $n$are positive integers. Prove that if $a^n|b^n$, then$a|b$.

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

   Ans:

   (a) By our assumption, $a|b^n$. If a is prime, then proposition 3.1 in lecture note 3 implies that $a|b$. In general, we can take prime decomposition of a and b, $a = p_1^{k_1} \cdots p_r^{k_r}$ and $b = q_1^{l_1} \cdots q_s^{l_s}$. $a^n|b^n$ implies that $p_i^{nk_i}|p_i^{nl_{j_i}}$ for each i. Therefore, $k_i|l_{j_i}$. As a result, $a|b$.

   (b) Since $p|a^k$ and p is prime, we must have $p|a$ due to Proposition 3.1 in lecture note 3. Therefore, we also have $p^k|a^k$.

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.

   Ans: Write $n = a_1 + a_2 10 + \cdots 10^k a_k$. It is worth noting that $10^k = 1 \mod 3$. As a result, $n = \sum_{i=1}^k a_i \mod 3$ and $n = 0 \mod 3$ if and only if $\sum_{i=1}^k a_i = 0 \mod 3$.

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

   Ans: To find the last two digits, it suffices to compute $123^{562} \mod 100$. Note that $\varphi(100) = 32$ and $gcd(123, 100) = 1$, according to Euler' theorem, $123^{32} = 1 \mod 100$. Therefore, $123^{562} = 123^{18} \mod 100$. By the expansion of $(100 + 23)^{18}$, we know that $123^{18} = 23^{18} \mod 100$. Again, by the expansion of $(20 + 3)^{18} = 20^{18} + \cdots + C_{18}^2 20^2 \times 3^{16} + C_{18}^1 20 \times 3^{17} + 3^{18} = 20^{18} \cdots + 121 \times 3^{18}$, we have $23^{18} = 7 \times 3^{19} \mod 100$. It is easy to check that $3^5 = 243 = 43 \mod 100$ and $43^3 = (40 + 3)^3 = 40^3 + C_3^2(40)^2 + 3 \times 40 \times 3 + 3^3 = 87 \mod 100$. Therefore, $7 \times 3^{19} = 7 \times 81 \times 87 = 29 \mod 100$.

   In conclusion, the last two digits is 29.

4. RSA cryptosystem is implemented by using two primes $p = 17$ and $q = 23$.

   (a) i. Compute $\varphi(n)$, where $n = pq$.
   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?

   (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 $0 \leq m < n$.

   Ans:

   (a) i. $\varphi(17 \times 23) = 16 \times 22 = 352$.
   ii. Take $e = 31$, then $gcd(31, 352) = 1$. We need to solve the equation $31d = 1 \mod 352$. By Euclidean algorithm, we know that $d = 159$.

iii. By assumption, $C = m^e = 33^{31} = 135 \mod 391$. $C^d = 135^{159} = 33 \mod 391$. The message $m = 33$ is recovered.

(b) i. When $e = 29$, we need to solve $29d = 1 \mod 352$. By Euclidean algorithm, we know that $d = 85$.

ii. Given $C = 18$, then $m = C^d = 18^{85} = 154 \mod 391$. The original message m is 154.

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

Ans: Let $G =< a >$ and H be a subgroup of G. Note that any element in H is of the form a^i. Define $k = \min\{i > 0 | a^i \in H\}$. We claim that $H =< a^k >$ and hence H is a cyclic subgroup. By definition, $< a^k >\subset H$. Conversely, for any $a^p \in H$ and we may assume that $p > 0$ for convenience. Then we must have $k|p$. Otherwise, we can write $p = mk+r$ for some $0 < r < k$ and hence $a^r \in H$, contradict with our assumption. In conclusion, $a^p = a^{mk}$ and $H =< a^k >$.

6. 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.

Ans: For any $a, b \in H$, then $(ab)^2 = a^2b^2 = e$ by the assumption. In addition, for each $a \in H$, $a^{-1} = a \in H$ since a has order 2. In conclusion, H is a subgroup of G.

7. 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.

Ans: First of all, note that $\mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$ is not a cyclic group because of proposition 4.10 in lecture note 4.

If G contains a subgroup which is isomorphic to $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$, then by the conclusion in question 6, G is not cyclic.

Conversely, let us assume that G is not cyclic. By the fundamental theorem of abelian groups, G is isomorphic to

$$\mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \mathbb{Z}/p_2^{k_2}\mathbb{Z} \times \cdots \mathbb{Z}/p_r^{k_r}\mathbb{Z},$$

where p_i are primes but not necessary to be distinct. Under our assumption, there are $i \neq j$ such that $p_i = p_j$. Otherwise, G is cyclic because of Corollary 4.4 in lecture note 4. Therefore, G contains a subgroup $\mathbb{Z}/p^{k_i}\mathbb{Z} \times \mathbb{Z}/p^{k_j}\mathbb{Z}$ and hence G contains a subgroup $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$ for some prime p.

8. 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.

Ans: By the fundamental theorem of abelian groups, G is isomorphic to

$$\mathbb{Z}/p_1^{k_1}\mathbb{Z} \times \mathbb{Z}/p_2^{k_2}\mathbb{Z} \times \cdots \mathbb{Z}/p_r^{k_r}\mathbb{Z},$$

where p_i are primes but not necessary to be distinct.

Above classification theorem implies that $|G| = p_1^{k_1} \cdots p_r^{k_r}$. As a result, $p_1 = \cdots p_r = p$. In other words,

$$G = \mathbb{Z}/p^{k_1}\mathbb{Z} \times \mathbb{Z}/p^{k_2}\mathbb{Z} \times \cdots \mathbb{Z}/p^{k_r}\mathbb{Z}.$$

Obviously, the order of element in above group is a power of p.