THE CHINESE UNIVERSITY OF HONG KONG
DEPARTMENT OF MATHEMATICS

MMAT5210 Discrete Mathematics 2017-2018
Suggested Solution to Midterm Examination

1. Define a relation $\sim$ on $\mathbb{R}$ such that $x \sim y$ if and only if $x - y$ is an integer.

   (a) Show that the relation $\sim$ is an equivalence relation.

   (b) Let $x, y, x', y' \in \mathbb{R}$. Show that if $x \sim x'$ and $y \sim y'$, then $x + y \sim x' + y'$.

   (c) Let $x, y, x', y' \in \mathbb{R}$. If $x \sim x'$ and $y \sim y'$, is it always true that $xy \sim x'y'$? Why?

   Ans:

   (a) i. (Reflexive) Let $x \in \mathbb{R}$. Then, $x - x = 0$ which is an integer and so $x \sim x$.

   ii. (Symmetric) Let $x, y \in \mathbb{R}$ such that $x \sim y$.
   Then $x - y$ is an integer, so $y - x = -(x - y)$ is also an integer and we have $y \sim x$.

   iii. (Transitive) Let $x, y, z \in \mathbb{R}$ such that $x \sim y$ and $y \sim z$.
   Then $x - y$ and $y - z$ are integers, so $x - z = (x - y) + (y - z)$ is also an integer and we have $x \sim z$.

   Therefore, $\sim$ is an equivalence relation on $\mathbb{R}$.

   (b) Let $x, y, x', y' \in \mathbb{R}$ such that $x \sim x'$ and $y \sim y'$. Then $x - x'$ and $y - y'$ are integers.
   Therefore, $(x+y)-(x'+y') = (x-x')+(y-y')$ is also an integer and we have $x+y \sim x'+y'$.

   (c) No. If $x = 0.5$, $x' = 1.5$, $y = 0.2$ and $y' = 1.2$, then we have $x \sim x'$ and $y \sim y'$ but $xy - x'y' = 0.1 - 1.8 = -1.7$ which is not an integer.

2. Let $f, g : \mathbb{Z}^+ \to \mathbb{R}$ be two functions.

   (a) State the definition of $f(n) = O(g(n))$.

   (b) Suppose that $f(n) = O(g(n))$. Show that for every positive integer k, $[f(n)]^k = O([g(n)]^k)$.

   Ans:

   (a) $f(n) = O(g(n))$ if there exist $C > 0$ and $K \in \mathbb{Z}^+$ such that $|f(n)| \leq C|g(n)|$ for all $n \geq K$.

   (b) Suppose that $f(n) = O(g(n))$. Then there exist $C > 0$ and $K \in \mathbb{Z}^+$ such that $|f(n)| \leq C|g(n)|$ for all $n \geq K$. For any positive integer k and $n \geq K$, we have

   $$\begin{aligned} |[f(n)]^k| &= |f(n)|^k \\ &\leq (C|g(n)|)^k \\ &= C^k|[g(n)]^k| \end{aligned}$$

   and so $[f(n)]^k = O([g(n)]^k)$.

3. Let a, b, c, n be integers. Prove that

   (a) if $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.

   (b) if $a \mid n$ and $b \mid n$ with $\gcd(a, b) = 1$, then $ab \mid n$.

   Ans:

(a) Since $a \mid bc$, $bc = am$ for some integer m.

Since $\gcd(a, b) = 1$, there exist integers r and s such that $ar + bs = 1$. Then,

$$\begin{aligned} c &= acr + bcs \\ &= acr + ams \\ &= a(cr + ms) \end{aligned}$$

where $cr + ms$ is an integer. Therefore, $a \mid c$.

(b) Since $b \mid n$, $n = bq$ for some integer q.

Then $a \mid n = bq$ with $\gcd(a, b) = 1$. By (a), we have $a \mid q$, i.e. $q = ar$ for some integer r.

We have $n = bq = abr$ and so $ab \mid n$.

4. (a) Prove that a positive integer n is divisible by 9 if and only if the sum of the digits of n is divisible by 9.

(b) By using (a), determine whether 12345678987654321 is divisible by 9.

Ans:

(a) Let $n = a_k \times 10^k + a_{k-1} \times 10^{k-1} + \cdots + a_1 \times 10 + a_0$. Since $10 \equiv 1 \pmod 9$, $10^r \equiv 1^r \equiv 1 \pmod 9$ for all positive integer r. Then,

$$\begin{aligned} n &\equiv a_k \times 10^k + a_{k-1} \times 10^{k-1} + \cdots + a_1 \times 10 + a_0 \pmod 9 \\ &\equiv a_k \times 1 + a_{k-1} \times 1 + \cdots + a_1 \times 1 + a_0 \pmod 9 \\ &\equiv a_k + a_{k-1} + \cdots + a_1 + a_0 \pmod 9 \end{aligned}$$

and so n is divisible by 9 if and only if the sum of the digits of n is divisible by 9.

(b) Sum of the digits of the given number is 81 which is divisible by 9, therefore the given number is also divisible by 9.

5. Use Pohlig-Hellman algorithm, Baby Step, Giant Step or the Index Calculus to find an integer x such that $3^x \equiv 25 \pmod{29}$.

Ans:

$x = 20$.

6. Let E be the elliptic curve given by the equation $y^2 \equiv x^3 + x + 6 \pmod{11}$. Find

(a) $(2, 4) + (2, 7)$;

(b) $(2, 4) + (3, 5)$;

(c) $2(2, 4)$.

Ans:

(a) ∞

(b) $(7, 2)$

(c) $(5, 9)$

7. (a) Prove that a subgroup of a cyclic group is also cyclic.

(b) i. What is the order of the group $(\mathbb{Z}/120\mathbb{Z})^\times$?

ii. Find the inverse of 23 in $(\mathbb{Z}/120\mathbb{Z})^\times$.

iii. By considering the subgroup $\{1, 11, 19, 89\}$ of $(\mathbb{Z}/120\mathbb{Z})^{\times}$, determine whether $(\mathbb{Z}/120\mathbb{Z})^{\times}$ is a cyclic group.

Ans:

(a) Let G be a cyclic group. Then all the elements of G is of the form a^n for some integer n.

Let H be a subgroup of G. If H is the trivial group, then H is already a cyclic subgroup.

Otherwise, note that if $a^n \in H$, then $a^{-n} \in H$, so H must contain an element a^n for some positive integer n.

Therefore, we let d be the least positive integer such that $a^d \in H$ and we claim every element of H is of the form a^{md} for some integer m.

Suppose the contrary, there exists an integer s such that s is not a multiple of d but $a^s \in H$. Then by division algorithm, there exist integer q and r with $0 < r < d$ such that $s = dq + r$. Since a^s and a^d are elements in H, $a^r = a^{s-dq}$ is also an element in H which contradicts to that d is the least positive integer such that $a^d \in H$. Therefore, $H = \langle a^d \rangle$, i.e. H is cyclic.

(b) i. The order of the group $(\mathbb{Z}/120\mathbb{Z})^{\times} = \varphi(120) = \varphi(8) \times \varphi(3) \times \varphi(5) = 4 \times 2 \times 4 = 32$.

ii. By extended Euclidean algorithm, we have $1 = 23 \times 47 + 120 \times (-9)$, and so $23 \times 47 \equiv 1 \pmod{120}$. Therefore, $23^{-1} = 47$.

iii. Note that $11^2 \equiv 121 \equiv 1$, $19^2 \equiv 361 \equiv 1$ and $89^2 \equiv 7921 \equiv 1 \bmod 120$. Therefore, every element except 1 of the given subgroup is of order 2, which is not a primitive element. Therefore, the given subgroup is not a cyclic subgroup.
By (a), $(\mathbb{Z}/120\mathbb{Z})^{\times}$ is not a cyclic group.

8. The RSA Algorithm:

(1) Bob chooses secret primes p and q and compute $n = pq$.

(2) Bob chooses e with $\gcd(e, (p-1)(q-1)) = 1$.

(3) Bob computes d with $de \equiv 1 \pmod{(p-1)(q-1)}$.

(4) Bob publishes the public key (n, e), and keeps p, q, d secret.

(5) Alice encrptys the message m as $c \equiv m^e \pmod{n}$ and sends c to Bob.

(6) Bob decrypts by computing $m \equiv c^d \pmod{n}$.

Suppose that the RSA algorithm is implemented with $n = 391$.

(a) Suppose that the ciphertext $c = 20$ was obtained while $e = 29$. Using the factorization $391 = 17 \times 23$, find the messgae m.

You may use the following table:

j	0	1	2	4	8	16	32	64	128	256
$20^j \pmod{391}$	1	20	9	81	305	358	307	18	324	188

(b) Suppose that a message $0 \le m < 391$ is encrypted twice with the RSA algorithm using $e = 37$ and $e' = 91$ and the ciphertexts are $c \equiv m^e \equiv 359 \pmod{391}$ and $c' \equiv m^{e'} \equiv 366 \pmod{391}$. By considering the fact that $\gcd(e, e') = \gcd(37, 91) = 1$, find the message m.

You may use the fact that $359^{32} \equiv 18 \pmod{391}$ and $366^{-13} \equiv 270 \pmod{391}$.

Ans:

(a) Let $p = 17$ and $q = 23$, then $(p-1)(q-1) = 16 * 22 = 352$.

Note that $\gcd(e,(p-1)(q-1)) = \gcd(29,352) = 1$, by extended Euclidean algorithm, we have $1 = 352 \times (-7) + 29 \times 85$. Therefore, the equation $de \equiv 1 \pmod{(p-1)(q-1)}$ gives $d \equiv 85 \pmod{352}$.

Then, we have $m \equiv c^d \equiv 20^{85} \equiv 362 \pmod{391}$

(b) Note that $\gcd(e,e') = \gcd(37,91) = 1$, by extended Euclidean algorithm, we have $1 = 37 \times 32 + 91 \times (-13)$. Then,

$$m \equiv m^1 \equiv (m^e)^{32} \cdot (m^{e'})^{-13} \equiv c^{32} \cdot (c')^{-13} \equiv 359^{32} \times 366^{-13} \equiv 18 \times 270 \equiv 168 \pmod{391}$$

9. (a) Let p be a prime and let α be an integer such that $1 \le \alpha \le p-1$.

Suppose that $p-1$ can be factorized as $\prod_{i=1}^{m} p_i^{d_i}$ where p_i are primes and d_i are positive integers, and $N_i = \dfrac{p-1}{p_i}$.

Prove that $\alpha^d \equiv 1 \pmod{p}$ for some $d \mid p-1$ with $1 \le d < p-1$ if and only if $\alpha^{N_i} \equiv 1 \pmod{p}$ for some $i = 1, 2, \ldots, m$.

(b) By using (a), show that 2 is a primitive root mod 19.

(c) List all the primitive roots mod 19.

(Hint: From (b), $(\mathbb{Z}/19\mathbb{Z})^\times$ is a cyclic group and isomorphic to $\mathbb{Z}/18\mathbb{Z}$.)

Ans:

(a) ($\Leftarrow$) Suppose that $\alpha^{N_i} \equiv 1 \pmod{p}$ for some $1 \le i \le m$, since $N_i \mid p-1$, then the result follows.

($\Rightarrow$) Suppose that $\alpha^d \equiv 1 \pmod{p}$ for some $d \mid p-1$ with $1 \le d < p-1$. Since $d \mid p-1 = \prod_{i=1}^{m} p_i^{d_i}$, $d = \prod_{i=1}^{m} p_i^{k_i}$ where $0 \le k_i \le d_i$ for $i = 1, 2, \ldots, m$.

Also, since $d < p-1$, there must be some $1 \le j \le m$, such that $k_j < d_j$, i.e. $k_j \le d_j - 1$. Therefore, we have $d \mid N_j$ and $\alpha^d \equiv 1 \pmod{p}$ implies $\alpha^{N_j} \equiv 1 \pmod{p}$.

(b) Note that $19 - 1 = 18 = 2 \times 3^2$. Also, we have $2^6 \equiv 64 \equiv 7 \pmod{19}$ and $2^9 \equiv 512 \equiv 18 \pmod{19}$.

By (a), 2^d is not congruent to 1 for all $d \mid 18$ with $1 \le d < 18$ (also note that the order of 2 must be a divisor of 18), therefore 2 is a primitive root mod 19.

(c) Note that $(\mathbb{Z}/19\mathbb{Z})^\times$ is a cyclic group and isomorphic to $\mathbb{Z}/18\mathbb{Z}$ and the primitive elements of $\mathbb{Z}/18\mathbb{Z}$ are those integers $1 \le d \le 18$ which are relatively prime with 18, and they are 1, 5, 7, 11, 13, 17.

Therefore, the primitive roots mod 19 are $2^1 \equiv 2$, $2^5 \equiv 13$, $2^7 \equiv 14$, $2^{11} \equiv 15$, $2^{13} \equiv 3$, $2^{17} \equiv 10$.