MAT246H1S LEC0101 - Concepts In Abstract Mathematics

Solutions to Term Test 2 - March 13, 2019

Time allotted: 105 minutes. Aids permitted: None.

Solutions and guide to part marks.

General Comments:

- (1) no half-marks please!
- (2) students must explain their work; ~~don't accept~~ deduct marks if ~~no~~ no explanation is given
- (3) don't waste a lot of time trying to figure out what students are doing, they are supposed to make it clear.
- (4) only look at p 12, 13 or 14 if student directs you there. Enter no marks on p 12, 13, or 14. Any part marks for work on p 12, 13 or 14 should go into total for page the question is orginally on.
- (5) watch out for alternate correct solutions.

Thanks. LB

1.(a) [3 marks] Define the Euler ϕ function.

1

Solution: let m be a natural number greater than 1. $\phi(m)$ is the number of elements in the set 1 $\{1, 2, 3, \ldots, m-1\}$ which are relatively prime to m.

1

1.(b) [4 marks] Calculate $\phi(675)$.

1

Solution: the prime factorization of 675 is $675 = 3^3 \cdot 5^2$, so

$$\phi(675) = \underbrace{\phi(3^3)\phi(5^2)}_{1} = \underbrace{(3^3 - 3^2) \cdot (5^2 - 5) = 18 \cdot 20 = 360}_{2}.$$

1.(c) [3 marks] Suppose m is a natural number with $m > 1$. Prove that $\phi(m) = m - 1$ if and only if m is a prime.

Proof: suppose m is prime. It was proved in the book that $\phi(m) = m - 1$. 1

OR: suppose m is prime and k is a number in the set $\{1, 2, \ldots, m-1\}$. If $\gcd(k, m) = d$, then in particular d divides m, which means $d = 1$ or $d = m$. But d also divides k and $k < m$. So $d = 1$ for each k and consequently $\phi(m) = m - 1$. 2 if they prove it.

2 Conversely, suppose every number k in the set $\{1, 2, \ldots, m-1\}$ is relatively prime to m. In particular, if $k > 1$ then k cannot divide m; otherwise $\gcd(m, k) = k$. Thus m has no divisors other than 1 and itself. That is, m is prime.

So: students can get 4/3 on this part if they prove

m prime $\Rightarrow \phi(m) = m-1$

2.(a) [2 marks] State Euler's Theorem.

Solution: if m is a natural number greater than 1 and a is a natural number that is relatively prime to m, then $a^{\phi(m)} \equiv 1 \pmod{m}$. (1)

(1)

2.(b) [3 marks] Calculate the multiplicative inverse of 3^{19} modulo 16. Give your answer as a natural number less than 16.

Solution: since 3 and 16 are relatively prime, and $\phi(16) = \phi(2^4) = 2^4 - 2^3 = 8$, Euler's Theorem implies

(1)

$$3^8 \equiv 1 \pmod{16}.$$

Thus $(3^8)^3 = 3^{24} \equiv 1 \pmod{16}$, which means a multiplicative inverse of 3^{19} is 3^5. But

(1)

$$3^5 = 3^4 \cdot 3 \equiv 1 \cdot 3 \pmod{16},$$

so the answer is 3. (1)

2.(c) [5 marks] Suppose that a and m are relatively prime natural numbers, $m > 1$, and k is the smallest natural number such that $a^k \equiv 1 \pmod{m}$. Prove that k divides $\phi(m)$.

(1)

Proof: by Euler's Theorem, $a^{\phi(m)} \equiv 1 \pmod{m}$. Thus, by definition of k, we have $k \leq \phi(m)$.
(1) Suppose k does not divide $\phi(m)$. Then by the division algorithm there are natural numbers n and r such that $r < k$ and

$$\phi(m) = n \cdot k + r.$$

Consequently

(3)

$$a^{\phi(m)} = a^{n \cdot k + r} = (a^k)^n \cdot a^r$$

and

$$\begin{aligned} (a^k)^n \cdot a^r &\equiv a^{\phi(m)} \pmod{m} \\ \Rightarrow (1)^n \cdot a^r &\equiv 1 \pmod{m} \\ \Rightarrow a^r &\equiv 1 \pmod{m} \end{aligned}$$

for using division algorithm and

Since $r < k$, this contradicts the definition of k as the the smallest natural number such that

$$a^k \equiv 1 \pmod{m}.$$

getting contradiction

Hence k must divide $\phi(m)$.

3.(a) [6 marks] Use the Rational Roots Theorem to find all the rational roots of the polynomial

$$f(x) = 2x^3 - 5x^2 + 5x - 3.$$

Solution: if

$$r = \frac{m}{n}$$

(2) is a rational root of $f(x)$, in lowest terms, then by the Rational Roots Theorem, m must divide 3 and n must divide 2. Thus $m = \pm 1$ or ± 3; and $n = \pm 1$ or ± 2. This gives eight possible rational roots r of $f(x)$. However if $r < 0$ then $f(r) < 0$. So we need only check the four positive possibilities for r to see if $f(r) = 0$:

r	$f(r)$	is r a root?
1	$2 - 5 + 5 - 3 = -1 \neq 0$	no
$\frac{1}{2}$	$\frac{2}{8} - \frac{5}{4} + \frac{5}{2} - 3 = -\frac{3}{2} \neq 0$	no
3	$54 - 45 + 15 - 3 = 21 \neq 0$	no
$\frac{3}{2}$	$\frac{54}{8} - \frac{45}{4} + \frac{15}{2} - 3 = 0$	yes

(4) for checking.

So the only rational root of $f(x)$ is $r = \frac{3}{2}$.

3.(b) [4 marks] Find the non-rational solutions to the equation $f(x) = 0$. (They will be complex numbers.)

Solution: long division by the factor $2x - 3$ gives

$$f(x) = (2x - 3)(x^2 - x + 1).$$ (1)

Using the quadratic formula, the non-rational roots of $f(x)$ are

$$x = \frac{1 \pm \sqrt{1-4}}{2} = \frac{1}{2} \pm \frac{\sqrt{3}}{2} i.$$ (2) – 1 each.

Alternate Division: if the linear factor is taken to be $x - 3/2$, then

$$f(x) = \left(x - \frac{3}{2}\right)(2x^2 - 2x + 2).$$

Of course the complex roots, are still the same.

4. [10 marks] Prove that the following numbers are irrational.

(a) [5 marks] $\sqrt[3]{5}+\sqrt{3}$

1

Proof: suppose $\sqrt[3]{5}+\sqrt{3}=r$, where $r=\dfrac{m}{n}$ is a rational number. Then

3

$$\begin{aligned}\sqrt[3]{5}+\sqrt{3}=r \quad &\Rightarrow \quad \sqrt[3]{5}=r-\sqrt{3}\\ &\Rightarrow \quad 5=(r-\sqrt{3})^3=r^3-3r^2\sqrt{3}+9r-3\sqrt{3}\\ &\Rightarrow \quad \sqrt{3}=\frac{r^3+9r-5}{3+3r^2},\end{aligned}$$

which would imply that $\sqrt{3}$ is rational. This contradicts the result proved in the book that $\sqrt{p}$ is irrational for every prime p. So $\sqrt[3]{5}+\sqrt{3}$ must be irrational.

1

(b) [5 marks] $\sqrt{n}$, if $n \equiv \pm 2 \pmod 5$.

Proof: by contraposition. Suppose $\sqrt{n}$ is rational. Then by a Theorem in the book, $\sqrt{n}=k$, for some natural number k. Thus $n=k^2$. Consider the five possibilities:

2

2

1. if $k \equiv 0\,(\text{mod}5)$, then $n=0^2 \equiv 0 \pmod 5$
2. if $k \equiv 1\,(\text{mod}5)$, then $n=1^2 \equiv 1 \pmod 5$
3. if $k \equiv 2\,(\text{mod}5)$, then $n=2^2 \equiv 4 \pmod 5$
4. if $k \equiv 3\,(\text{mod}5)$, then $n=3^2 \equiv 4 \pmod 5$
5. if $k \equiv 4\,(\text{mod}5)$, then $n=4^2 \equiv 1 \pmod 5$

That is, if $\sqrt{n}$ is rational, then $n \equiv 0, 1$ or $4 \pmod 5$.

Equivalently: if $n \equiv 2$ or $3 \pmod 5$, then $\sqrt{n}$ must be irrational.

1

5.(a) [3 marks] State De Moivre's Theorem.

Solution: for every natural number n and any real numbers r, θ, 1 1

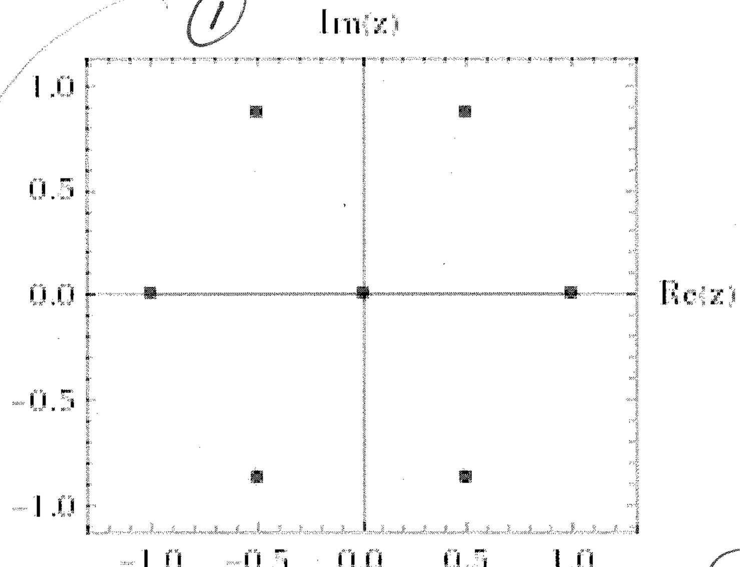
$$(r(\cos\theta + i\sin\theta))^n = r^n(\cos(n\theta) + i\sin(n\theta)).$$

1

5.(b) [7 marks] Find all the roots of the polynomial $z^7 - z$.

Solution 1: $z = 0$ or $z^6 = 1$. Let $z = \cos\theta + i\,\sin\theta$. Then $z^6 = 1$ implies, by De Moivre's Theorem,

1



$$\cos(6\theta) + i\,\sin(6\theta) = 1$$
$$\Rightarrow \quad 6\,\theta = 0 + 2\pi k$$
$$\Rightarrow \quad \theta = \frac{\pi k}{3}$$

The six distinct non-zero solutions for z are given by

$$\theta = 0,\ \pi,\ \pm\frac{\pi}{3},\ \pm\frac{2\pi}{3}.$$

3

The seven distinct solutions to $z^7 = z$ are

3

$$z = 0,\ z = \pm 1,\ \text{and } z = \pm\frac{1}{2} \pm \frac{\sqrt{3}}{2}i.$$

They should simplify $\sin\frac{\pi}{3} = \frac{\sqrt{3}}{2}$ etc

They are all plotted in the figure above left.

Solution 2: just factor.

$$z^7 - z = z(z^6 - z) = z(z^3 - 1)(z^3 + 1) = z(z-1)(z^2 + z + 1)(z+1)(z^2 - z + 1).$$

Thus

$$\begin{aligned} z^7 = z \quad \Rightarrow z \quad &= 0,\ z = \pm 1,\ z^2 + z + 1 = 0,\ \text{or } z^2 - z + 1 = 0 \\ \Rightarrow \quad & z = 0,\ z = \pm 1,\ z = \frac{-1 \pm \sqrt{-3}}{2},\ z = \frac{1 \pm \sqrt{-3}}{2} \\ \Rightarrow \quad & z = 0,\ z = \pm 1, z = -\frac{1}{2} \pm \frac{\sqrt{3}}{2}i,\ z = \frac{1}{2} \pm \frac{\sqrt{3}}{2}i, \end{aligned}$$

as before.

6. [10 marks] An exercise in the textbook says that if p and q are distinct primes, then the system of congruences

$$x \equiv a \pmod{p}, \ \ x \equiv b \pmod{q}$$

has a unique solution modulo pq. Illustrate this result by solving the following system modulo 187 :

$$x \equiv 2 \pmod{11}, \ \ x \equiv 5 \pmod{17}.$$

Solution:

$$x \equiv 2 \pmod{11} \Rightarrow x = 2 + 11\,j, \text{ for some integer } j. \quad 2$$

Then

$$\begin{aligned} x \equiv 5 \pmod{17} \quad &\Rightarrow \quad 2 + 11\,j \equiv 5 \pmod{17} \quad 2 \\ &\Rightarrow \quad 11\,j \equiv 3 \pmod{17} \\ &\Rightarrow \quad (-3) \cdot 11\,j \equiv -9 \pmod{17} \quad 2 \\ (\text{since } -33 \equiv 1 \pmod{17}) \quad &\Rightarrow \quad j \equiv 8 \pmod{17} \end{aligned}$$

Thus $j = 8 + 17\,k$, for some integer k, and so

$$x = 2 + 11(8 + 17\,k) = 90 + 187\,k, \quad 2$$

for some integer k. Thus

$$x = 90 \quad 2$$

is the unique solution, modulo 187, to the given system of congruences.

Note: you could also find the multiplicative inverse of 11, modulo 17, as follows:

$$\begin{aligned} 17 &= 1 \cdot 11 + 6 \\ 11 &= 1 \cdot 6 + 5 \\ 6 &= 1 \cdot 5 + 1, \end{aligned}$$

implying

$$1 = 6 - 5 = 6 - (11 - 6) = 2 \cdot 6 - 11 = 2(17 - 11) - 11 = 2 \cdot 17 - 3 \cdot 11,$$

from which you can see that -3 (or 14) is the multiplicative inverse of 11, modulo 17.

7.(a) [5 marks] Assume that m is a natural number with $m > 1$. Prove that a has a multiplicative inverse modulo m if and only if a and m are relatively prime.

1 **Proof:** there is an integer x such that $a\,x \equiv 1 \pmod{m}$

1 if and only if there is an integer y such that $a\,x - 1 = y\,m$

1 if and only if $a\,x - y\,m = 1$

1 it and only if $\gcd(a, m) = 1$,

1 since if d divides both a and m then d divides $a\,x - y\,m = 1$, which means $d \mid 1$.

7.(b) [5 marks] Assume that a and b are natural numbers greater than 1. Prove that $\gcd(a, b)$ is the smallest natural number n such that n is an integral linear combination of a and b.

Proof: let $\gcd(a, b) = d$. Let e be the smallest natural number n such that n is an integral linear combination of a and b. We claim $e = d$. To show this we shall show $e \leq d$ and $d \leq e$.

3
- $e \leq d$: since $d = \gcd(a, b)$, there are integers x and y such that $d = x\,a + y\,b$. Thus d can be written as an integral linear combination of a and b, and so $e \leq d$, by definition of e.

2
- $d \leq e$: there are integers s and t such that $e = s\,a + t\,b$. Since $d \mid a$ and $d \mid b$, it follows that $d \mid e$. Thus $d \leq e$.

ie 3 for one inequality
2 for the other.

NB: there may be alternate solutions for this one

8. [10 marks] Suppose $a \geq 2$ and $b \geq 2$ are relatively prime natural numbers. Prove that

$$a^{\phi(b)} + b^{\phi(a)} \equiv 1 \,(\mathrm{mod}\; ab).$$

Proof: by Euler's Theorem

$$a^{\phi(b)} \equiv 1 \,(\mathrm{mod}\; b) \Leftrightarrow a^{\phi(b)} - 1 = j\, b,$$ 2

for some natural number j. Similarly,

$$b^{\phi(a)} \equiv 1 \,(\mathrm{mod}\; a) \Leftrightarrow b^{\phi(a)} - 1 = k\, a,$$ 2

for some natural number k. Then

$$j\, b\, k\, a = \left(a^{\phi(b)} - 1\right)\left(b^{\phi(a)} - 1\right) = a^{\phi(b)} b^{\phi(a)} - a^{\phi(b)} - b^{\phi(a)} + 1.$$ 3

3 Since $a\, b$ divides the left side of this equation, and $a\, b$ divides the term $a^{\phi(b)} b^{\phi(a)}$ on the right side of this equation, it follows that $a\, b$ divides the rest of the right side of the above equation. That is,

$$a\, b \mid 1 - a^{\phi(b)} - b^{\phi(a)} \Leftrightarrow a^{\phi(b)} + b^{\phi(a)} \equiv 1 \,(\mathrm{mod}\; ab).$$

9.(a) [6 marks] Let $\mathcal{S}$ and $\mathcal{T}$ be sets. Define the following:

1. $\mathcal{S}$ is countable.

   Solution: the set $\mathcal{S}$ is countable if it is finite or has the same cardinality as $\mathbb{N}$.

   1 2

2. $|\mathcal{S}| = |\mathcal{T}|$.

   Solution: two sets $\mathcal{S}$ and $\mathcal{T}$ have the same cardinality, or satisfy $|\mathcal{S}| = |\mathcal{T}|$, if there is a function 1 $f : \mathcal{S} \longrightarrow \mathcal{T}$ such that f is one-to-one and onto. (Or as the book puts it: f is a one-to-one correspondence.) 1 1

9.(b) [4 marks] Prove that the set $\mathcal{S} = \{n^{1/k} \mid n, k \in \mathbb{N}\}$ is countable.

Solution 1: let $\mathcal{S}_k = \{n^{1/k} \mid n \in \mathbb{N}\} = \{1^{1/k}, 2^{1/k}, 3^{1/k}, \ldots, n^{1/k}, \ldots\}$. Then $\mathcal{S}_k$ is countable and 2

$$\mathcal{S} = \mathcal{S}_1 \cup \mathcal{S}_2 \cup \cdots \cup \mathcal{S}_k \cup \cdots = \bigcup_{k=1}^{\infty} \mathcal{S}_k;$$ 1

1 that is, $\mathcal{S}$ is the union of a countable number of countable sets, so it is countable. (By a Theorem in the book.)

Solution 2: list the elements in $\mathcal{S}$ as

$$\begin{array}{cccccc}
1^{1/1} & 2^{1/1} & 3^{1/1} & 4^{1/1} & 5^{1/1} & \cdots \\
1^{1/2} & 2^{1/2} & 3^{1/2} & 4^{1/2} & 5^{1/2} & \cdots \\
1^{1/3} & 2^{1/3} & 3^{1/3} & 4^{1/3} & 5^{1/3} & \cdots \\
1^{1/4} & 2^{1/4} & 3^{1/4} & 4^{1/4} & 5^{1/4} & \cdots \\
1^{1/5} & 2^{1/5} & 3^{1/5} & 4^{1/5} & 5^{1/5} & \cdots \\
\vdots & \vdots & \vdots & \vdots & \vdots &
\end{array}$$

and then count them in the usual zig-zag manner, starting in the top left corner, skipping any repetitions. This is really the same as Solution 1, since the k-th row in the above array consists of all the elements in $\mathcal{S}_k$.

10.(a) [4 marks] Find a function $f : [-1, 0) \longrightarrow [1, \infty)$ that is one-to-one and onto, and show your function *is* one-to-one and onto.

Solution: one obvious choice is

$$f(x) = -\frac{1}{x}.$$ 1

We have

1. $-1 \le x < 0 \Rightarrow 1 \ge -x > 0$ and $f(x) = -\dfrac{1}{x} \ge 1$.
2. f is one-to-one:
$$f(x_1) = f(x_2) \Rightarrow -\frac{1}{x_1} = -\frac{1}{x_2} \Rightarrow x_2 = x_1$$
3. f is onto: let $y \ge 1$. Then $-1/y \in [-1, 0)$ and
$$f\left(-\frac{1}{y}\right) = -1/(-1/y) = y.$$

3 for verifying properties

10.(b) [6 marks] Show that $|(0,1)| = |(0,1) \cup (4,5)|$ by constructing an explicit one-to-one and onto function $g : (0,1) \longrightarrow (0,1) \cup (4,5)$, and verifying that g is one-to-one and onto. Use the next page if you need more space.

Solution: here is one possibility. Let $g : (0,1) \longrightarrow (0,1) \cup (4,5)$ be defined in two pieces:

1

1. Define $g : (1/2, 1) \longrightarrow (4,5)$ by $g(x) = 2x + 3$, which is clearly one-to-one and onto.
2. Define $g : (0, 1/2] \longrightarrow (0,1)$ in two steps:

4

Step 1: map $x \in (0, 1/2]$ to $2x \in (0, 1]$, by $h(x) = 2x$, which is clearly one-to-one and onto.

Step 2: now map $(0,1] \longrightarrow (0,1)$, using some techniques from the book, as in Theorem 10.2.6:

Define $k : (0,1] \longrightarrow (0,1)$ by

$$k(x) = \begin{cases} \dfrac{1}{n+1} & \text{if} \quad x = \dfrac{1}{n},\ n \in \mathbb{N} \\[2ex] x \quad , & \text{otherwise} \end{cases}$$

Then $k : \{1/1, 1/2, 1/3, \ldots, 1/n, \ldots\} \longrightarrow \{1/2, 1/3, 1/4, \ldots, 1/(n+1), \ldots\}$ and fixes all numbers x which are not reciprocals of a natural number. Thus the range of k is $(0,1)$. And k is also one-to-one: $f(1/n) = f(1/m) \Rightarrow 1/(n+1) = 1/(m+1) \Rightarrow n+1 = m+1 \Rightarrow n = m$; for non-reciprocal x, f is just the identity.

1

Then $g = k \circ h : (0, 1/2] \longrightarrow (0,1)$, and it is one-to-one and onto, since the composition of one-to-one and onto maps is also one-to-one and onto.

This page is for rough work or for extra space to finish a previous problem. It will not be marked unless you have indicated in a previous question to look at this page.

This page is for rough work or for extra space to finish a previous problem. It will not be marked unless you have indicated in a previous question to look at this page.

This page is for rough work or for extra space to finish a previous problem. It will not be marked unless you have indicated in a previous question to look at this page.