MAT246H1S LEC0101 - Concepts In Abstract Mathematics

Solutions for Term Test 1 - February 6, 2019

Time allotted: 105 minutes. Aids permitted: None.

General Comments:

- NO HALF MARKS, Please
- ~~Do not~~ - Deduct marks for imprecise, sloppy, or logically incorrect statements.
- Don't waste a lot of time trying to figure out what students are doing; they are supposed to make it clear what they are doing.

Breakdown of Results: ? students wrote this test. The marks ranged from ?% to ?%, and the average was ?%. Some statistics on grade distribution are in the table on the left, and a histogram of the marks (by decade) is on the right.

Grade	%	Decade	%
		90-100%	%
A	%	80-89%	%
B	%	70-79%	%
C	%	60-69%	%
D	%	50-59%	%
F	%	40-49%	%
		30-39%	%
		20-29%	%
		10-19%	%
		0-9%	%

- Only look at pages 12, 13 or 14 if a student directs you to it. Don't enter any marks on pages 12, 13 or 14; all marks should be included ~~in~~ on the page for the question.
- Leave some kind of comment, sign, or other indication, to show students where they lost marks.

Thanks, Diedrich

1.(a) [6 marks] Let a, p, m and n be natural numbers. Define the following:

(2) each

(i) a is a divisor of n

1 1

Solution: a is a divisor of n if there is a natural number k such that $n = k \cdot a$.

(ii) p is a prime number

1

Solution: a natural number p greater than 1 is a prime number if the only natural number divisors of p are 1 and itself.

1

(iii) m is a composite number

1 1

Solution: a natural number m greater than 1 is a composite number if it is not a prime number. (That's the definition in the book.)

Or: a natural number m greater than 1 is a composite number if there are natural numbers a, b with $1 < a, b < m$ and $m = a \cdot b$.

1.(b) [4 marks] State precisely the following theorems.

(2) each

(i) Fermat's Theorem

1 for correct hypotheses

Solution: if p is a prime number and a is any natural number not divisible by p, then

$$a^{p-1} \equiv 1 \ (\text{mod} p).$$

1 for correct conclusion

(ii) Wilson's Theorem

Solution: if p is prime then $(p-1)! + 1 \equiv 0 \ (\text{mod} p)$.

1 for correct hypothesis

1 for correct conclusion

2.(a) [3 marks] State the Well-Ordering Principle.

(1) (1) (1)

Solution: every non-empty set of natural numbers contains a least element.

Or: if $S \subseteq \mathbb{N}$ and $S \neq \emptyset$, then there is an $m \in S$ such that $m \leq n$ for all $n \in S$.

2.(b) [7 marks] Let a and b be positive integers, and assume that $a > b$. Use the Well-Ordering Principle to prove there are non-negative integers q and r, with $0 \leq r \leq b-1$, such that $a = qb + r$.

Method I **Proof:** if $a = k\,b$ for $k \in \mathbb{N}$, take $q = k$ and $r = 0$. Now assume b does not divide a. Let

(1)

$$S = \{a - q \cdot b \mid q \in \mathbb{N} \text{ and } a - q \cdot b > 0\}.$$

Since $a > b$, the number $a - b = a - 1 \cdot b > 0$, so $a - b$ is in S, and $S \neq \emptyset$. By the well-ordering principle, S has a *least* element, call it r. Then $r > 0$, because it is in S, and there is a number $q \in \mathbb{N}$ such that

$$a - q\,b = r \Leftrightarrow a = q\,b + r.$$

(3)

We claim $r < b$. We shall show $r \geq b$ is impossible:

- If $r = b$, then $a = q\,b + b = (q+1)\,b$ and $b \mid a$, contradicting our assumption.
- If $r > b$, then $a = q\,b + r > q\,b + b = (q+1)b$, and so $a - (q+1)b > 0$, which means $a - (q+1)b$ is in S. Since $a - (q+1)b < r$, this is a contradiction. That is, $r = a - qb$ and

$$\begin{aligned} & a - (q+1)b < a - qb \\ \Leftrightarrow\ & -(q+1)b < -qb \\ \Leftrightarrow\ & qb < qb + b \\ \Leftrightarrow\ & 0 < b, \text{ which is true.} \end{aligned}$$

(3)

Method II **Alternate Proof:** let $S = \{a - kb \mid k \in \mathbb{N} \text{ and } a - kb > 0\}$. Then $S \neq \emptyset$, since for $k = 1$ the expression $a - 1 \cdot b = a - b > 0$. By the Well Ordering Principle S contains a least element, call it r, which must be positive because $r \in S$. Then there is a $q \in \mathbb{N}$ such that

$$a - qb = r \Leftrightarrow a = qb + r.$$

(3)

We claim $r \leq b$: if $r > b$, then $a - qb > b \Leftrightarrow a - (q+1)b > 0$, so $a - (q+1)b \in S$. But then

$$a - (q+1)b < a - qb,$$

(3)

which contradicts the fact that $a - qb$ is the least element in S. Thus $r < b$, in which case we're finished; or $r = b$. In this latter case we can write $a = qb + r = qb + b = (q+1)b + 0$.

(1)

3.(a) [3 marks] State the Principle of Mathematical Induction.

Solution: if S is any set of natural numbers such that (1)

- 1 is in S, and
- $k+1$ is in S whenever k is in S, (1)

then $S = \mathbb{N}$. (1)

3.(b) [7 marks] Let q be any real number such that $q \neq 1$. Use the Principle of Mathematical Induction to prove that

$$1 + 2q + 3q^2 + \cdots + nq^{n-1} = \frac{1-(n+1)q^n + nq^{n+1}}{(1-q)^2} \qquad (\dagger)$$

for every natural number n.

Proof: let $S = \{n \in \mathbb{N} \mid (\dagger) \text{ is true}\}$. (1) $1 \in S$, since for $n = 1$ the left side of $(\dagger)$ is 1 and the right side of $(\dagger)$ is

$$\frac{1-2q+q^2}{(1-q)^2} = \frac{(1-q)^2}{(1-q)^2} = 1. \quad (2)$$

Now assume $k \in S$. Then

$$\begin{aligned}
& 1 + 2q + 3q^2 + \cdots + kq^{k-1} + (k+1)q^k \\
= \; & \frac{1-(k+1)q^k + kq^{k+1}}{(1-q)^2} + (k+1)q^k \\
= \; & \frac{1-(k+1)q^k + kq^{k+1} + (k+1)q^k(1-q)^2}{(1-q)^2} \\
= \; & \frac{1-(k+1)q^k + kq^{k+1} + (k+1)q^k - 2(k+1)q^{k+1} + (k+1)q^{k+2}}{(1-q)^2} \\
= \; & \frac{1-(k+2)q^{k+1} + (k+1)q^{k+2}}{(1-q)^2}
\end{aligned} \quad (3)$$

Thus the formula $(\dagger)$ is true for $n = k+1$ as well, and by the Principle of Mathematical Induction, $S = \mathbb{N}$.

(1)

4.(a) [3 marks] State the Principle of Complete Mathematical Induction.

Solution: if S is any set of natural numbers with the properties that 1

- A: 1 is in S, and
- B: $k + 1$ is in S whenever k is a natural number and *all* the natural numbers from 1 through k are in S, 1

then $S = \mathbb{N}$. 1

4.(b) [7 marks] Show that the Well-Ordering Principle is a consequence of the Principle of Complete Mathematical Induction. That is, use the Principle of Complete Mathematical Induction to prove the Well-Ordering Principle.

1

Proof: suppose W is a set of natural numbers that has no least element. Let $S = \{n \in \mathbb{N} : n \notin W\}$. Then 4

- A: $1 \in S$: if $1 \in W$ it would be the least element of W.
- B: suppose natural numbers $1, 2, \ldots, k$ are all in S. Then none of $1, 2, \ldots, k$ are in W, by definition of S. Thus $k + 1 \notin W$, else $k + 1$ would be the least element of W. Thus $k + 1 \in S$.

By the Principle of Complete Mathematical Induction, $S = \mathbb{N}$, and consequently 1 $W = \emptyset$. Thus:

If W is any non-empty set of natural numbers, it must have a least element. 1

There may be other ways to prove this!
The ~~prove above is basically by con~~!

5.(a) [3 marks] Let n be a natural number other than 1. Define the canonical factorization of n into a product of primes.

Solution: if $n > 1$ then the canonical factorization of n is

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}, \quad (1)$$

(1)

where each p_i is a prime, $p_i < p_{i+1}$, and α_i is a natural number. (1)

5.(b) [7 marks] Find the canonical factorization of 1940400.

Solution: 1940400 is even, ends in a zero, and the sum of its digits is divisible by 9; so 2, 9 and 5 all divide it. We have

(1) for each correct prime factor

(2) more if all exponents are correct

- $16 \mid 1940400$ since $1940400 = 16 \cdot 121275$
- $9 \mid 121275$ since $121275 = 9 \cdot 13475$
- $25 \mid 13475$ since $13475 = 25 \cdot 539$

Is 539 divisible by 7? Yes: $539 = 7 \cdot 77 = 7^2 \cdot 11$. Thus the canonical factorization of 1940400 is

$$1940400 = 2^4 \cdot 3^2 \cdot 5^2 \cdot 7^2 \cdot 11.$$

Altrante Calculations: obviously, $1940400 = 100 \cdot 19404$. Since the sum of the digits of 19404 is 18, which is divisible by 9, 9 divides 19404 as well. In particular

$$19404 = 9 \cdot 2156.$$

Now 4 divides 2156:

$$2156 = 4 \cdot 539.$$

And $539 = 7 \cdot 77$. Putting it all together

$$1940400 = 100 \cdot 9 \cdot 4 \cdot 7 \cdot 77 = 4 \cdot 25 \cdot 9 \cdot 4 \cdot 7 \cdot 77 = 2^4 \cdot 3^2 \cdot 5^2 \cdot 7^2 \cdot 11.$$

Really! for 6a) part marks are at your discretion, since I have no idea how they will do this one!

6.(a) [6 marks] Suppose that a and n are natural numbers and p is a prime number. Assume that p^4 divides a^n but p^5 does not divide a^n. Prove that n divides 4.

2

Proof: let p^k be the highest power of p that divides a. Then $a = p^k m$ for some natural number m not divisible by p. Then $a^n = p^{nk} m^n$. If p^4 divides a^n, then $4 \leq nk$; if p^5 does not divide a^n, then $nk \leq 4$. Combining these two inequalities gives $nk = 4$, which means n is a divisor of 4.

1 1 1 1

6.(b) [4 marks] A natural number is a *perfect square* if it has the form n^2, for some natural number n. Find all primes p such that $5p + 1$ is a perfect square.

Solution: since $5 \cdot 5 + 1 = 26$ is not a perfect square, $p \neq 5$. Let $5p + 1 = n^2$. Then $n > 3$ and

$$5p = n^2 - 1 = (n-1)(n+1).$$

2 for setting up

By the Fundamental Theorem of Arithmetic, there are two possibilities:

1. $n - 1 = 5$ and $p = n + 1$, in which case $n = 6$ and $p = 7$; 1
2. $n + 1 = 5$ and $p = n - 1$, in which case $n = 4$ and $p = 3$. 1

NB: If they just find $p=7$ and $p=3$ by "trial and error", give them 2 marks and ask, "how do you know there are no more?"

7.(a) [5 marks] Prove that there are no integer solutions to the equation $x^2 + y^2 = 4007$.

Solution: consider the equation as a congruency modulo 4. If x is an integer then

$$x \equiv 0, 1, 2 \text{ or } 3 \pmod 4 \Rightarrow x^2 = 0, 1, 4 \text{ or } 9 \equiv 0, 1, 0 \text{ or } 1 \pmod 4.$$ 2

Similarly, if y is an integer, then

$$y \equiv 0, 1, 2 \text{ or } 3 \pmod 4 \Rightarrow y^2 = 0, 1, 4 \text{ or } 9 \equiv 0, 1, 0 \text{ or } 1 \pmod 4.$$ 1

Therefore, for any integers x and y the possibilities are

$$x^2 + y^2 \equiv 0 + 0, 0 + 1, 1 + 0 \text{ or } 1 + 1 \equiv 0, 1, 1 \text{ or } 2 \pmod 4.$$ 1

But

$$4007 \equiv 3 \pmod 4,$$ 1

so there can be no integer solutions to the equation $x^2 + y^2 = 4007$.

7.(b) [5 marks] Let a and b be integers, let p and q be distinct primes. Prove that if $a \equiv b \pmod p$ and $a \equiv b \pmod q$, then $a \equiv b \pmod{pq}$.

1

Proof: $a \equiv b \pmod p \Rightarrow p \mid a - b \Rightarrow a - b = p \cdot m$, for some integer m. Also,

$$a \equiv b \pmod q \Rightarrow q \mid a - b \Rightarrow q \mid p \cdot m.$$ 1

Since q is prime,

$$q \mid p \text{ or } q \mid m.$$ 2

Since p and q are distinct primes, we must have $q \mid m$. Thus $m = q \cdot n$, for some integer n, and

$$a - b = p \cdot m = p \cdot q \cdot n,$$ 1

which means $a \equiv b \pmod{pq}$.

8.(a) [7 marks] Find gcd(1292, 14440), the greatest common divisor of 1292 and 14440, and express it as an integral linear combination of the numbers 1292 and 14440.

Solution: use the Euclidean algorithm.

$$\begin{aligned} 14440 &= 11 \cdot 1292 + 228 && (1) \\ 1292 &= 5 \cdot 228 + 152 && (2) \\ 228 &= 1 \cdot 152 + 76 && (3) \\ 152 &= 2 \cdot 76 && (4) \end{aligned}$$

Thus

$$\gcd(1292, 14440) = 76.$$

4

Now use 'backward substitution' to express it as an integral combination of 1292 and 14440:

3

(3) $\Rightarrow 76 = 228 - 152;$

(2) $\Rightarrow 76 = 228 - (1292 - 5 \cdot 228) = 6 \cdot 228 - 1292;$

(1) $\Rightarrow 76 = 6(14440 - 11 \cdot 1292) - 1292 = 6 \cdot 14440 - 67 \cdot 1292$. Thus

$$76 = 6 \cdot 14440 - 67 \cdot 1292.$$

Alternate Calculation: you could find the greatest common divisor by using the prime factorizations of the two numbers:

$$1292 = 2^2 \cdot 17 \cdot 19 \text{ and } 14440 = 2^3 \cdot 5 \cdot 19^2.$$

Thus

$$\gcd(1292, 14440) = 2^2 \cdot 19 = 76.$$

But this method doesn't help you with the second part of the problem.

8.(b) [3 marks] Find an integral solution to the equation $1292x + 14440y = 228$.

Solution: observe that $228 = 3 \cdot 76$. So 1

$$\begin{aligned} 76 = 6 \cdot 14440 - 67 \cdot 1292 \quad &\Rightarrow \quad 228 = 3(6 \cdot 14440 - 67 \cdot 1292) \\ &\Rightarrow \quad 228 = -201 \cdot 1292 + 18 \cdot 14440, \end{aligned}$$

1

so one integral solution is $(x, y) = (-201, 18)$. 1

9.(a) [4 marks] Let m, n be natural numbers. Define the following:

(2) each

(*i*) m and n are relatively prime. (2) basically, all or nothing!

Solution: the natural numbers m and n are relatively prime if $\gcd(m, n) = 1$.

Or: the natural numbers m and n are relatively prime if their greatest common divisor is 1.

(*ii*) a multiplicative inverse of n modulo m, if $m > 1$.

Solution: a multiplicative inverse of n modulo m is an integer a such that (1)

$$a \cdot n \equiv 1 \pmod{m}.$$

(1)

9.(b) [6 marks] Find a multiplicative inverse of 17 modulo 60 and use it to find a solution to the congruency $17x \equiv 4 \pmod{60}$.

Solution: use the Euclidean algorithm with 17 and 60:

(4)

$$\begin{aligned} 60 &= 3 \cdot 17 + 9 && (5) \\ 17 &= 1 \cdot 9 + 8 && (6) \\ 9 &= 1 \cdot 8 + 1 && (7) \\ 8 &= 8 \cdot 1 && (8) \end{aligned}$$

Then

(7) $\Rightarrow 1 = 9 - 8$;

(6) $\Rightarrow 1 = 9 - (17 - 9) = 2 \cdot 9 - 17$;

(5) $\Rightarrow 1 = 2(60 - 3 \cdot 17) - 17 = 2 \cdot 60 - 7 \cdot 17$. Thus

$$-7 \cdot 17 \equiv 1 \pmod{60},$$

and -7 is a multiplicative inverse of 17, modulo 60. (So is $-7 + 60 = 53$.) Consequently, there are actually infinitely many correct sols

(2)

$$\begin{aligned} 17x \equiv 4 \pmod{60} &\Rightarrow -7 \cdot 17x \equiv -7 \cdot 4 \pmod{60} \\ &\Rightarrow x \equiv -28 \pmod{60}, \end{aligned}$$

so one solution is $x = -28$; another solution is $x = -28 + 60 = 32$.

10. [10 marks] Find the remainder when $2^{47829} - 7^{6593} + 19! + 15!$ is divided by 17.

Solution: make use of Fermat's Theorem and Wilson's Theorem. Consider the four terms separately:

3

1. By Fermat's Theorem, $2^{16} \equiv 1 \pmod{17}$. And $47829 = 16 \cdot 2989 + 5$, so

$$2^{47829} = (2^{16})^{2989} \cdot 2^5 \equiv (1)^{2989} \cdot 2^5 \equiv 1 \cdot 32 \equiv 15 \pmod{17}.$$

2

2. By Fermat's Theorem, $7^{16} \equiv 1 \pmod{17}$. And $6593 = 16 \cdot 412 + 1$, so

$$7^{6593} = (7^{16})^{412} \cdot 7 \equiv (1)^{412} \cdot 7 \equiv 7 \pmod{17}.$$

1

3. $17 \mid 19!$, so

$$19! \equiv 0 \pmod{17}.$$

2

4. By Wilson's Theorem, $16! \equiv -1 \pmod{17}$. Consequently,

$$\begin{aligned} 16! \equiv -1 \pmod{17} \quad &\Rightarrow \quad 16 \cdot 15! \equiv -1 \pmod{17} \\ &\Rightarrow \quad -15! \equiv -1 \pmod{17} \\ &\Rightarrow \quad 15! \equiv 1 \pmod{17} \end{aligned}$$

Putting it all together we have

$$\begin{aligned} 2^{47829} - 7^{6593} + 19! + 15! &\equiv 15 - 7 + 0 + 1 \pmod{17} \\ &\equiv 9 \pmod{17}. \end{aligned}$$

2

Thus the remainder when $2^{47829} - 7^{6593} + 19! + 15!$ is divided by 17 is 9.

This is correct final answer, not this.

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.