MATH 406 (JWG) Exam 2 Spring 2021

Solutions

Exam Logistics:

1. From the moment you download this exam you have three hours to take the exam and submit to Gradescope. This includes the entire upload and tag procedure so do not wait until the last minute to do these things.
2. Tag your problems! Please! Pretty please!
3. You may print the exam, write on it, scan and upload.
4. Or you may just write on it on a tablet and upload.
5. Or you are welcome to write the answers on separate pieces of paper if other options don't appeal to you, then scan and upload.

Exam Rules:

1. You may ask for clarification on questions but you may not ask for help on questions!
2. You are permitted to use official class resources which means your own written notes, class Panopto recordings and the textbook.
3. You are not permitted to use other resources. Thus no friends, internet, calculators, Wolfram Alpha, etc.
4. By taking this exam you agree that if you are found in violation of these rules that the minimum penalty will be a grade of 0 on this exam.

Exam Work:

1. Show all work as appropriate for and using techniques learned in this course.
2. Any pictures, work and scribbles which are legible and relevant will be considered for partial credit.
3. Arithmetic calculations do not need to be simplified unless specified.

1. Identify which of $0, 1, ..., 13$ are coprime to 14 and for each which is coprime determine the order of each mod 14. Then state which are primitive roots. [6 pts]

   Solution:

   Just do it!

2. Calculate $\phi(\sigma(\tau(1000)))$ and simplify. [5 pts]

Solution:

Just do it! The answer is 30.

3. Find all numbers n satisfying both $\phi(n) = 20$ and $\tau(n) \mid 4$. [10 pts]

Solution:

If $p \mid n$ then $(p-1)|\phi(n) = 20$ so $p-1 = 1, 2, 4, 5, 10, 20$ so $p = 2, 3, 5, 11$. Thus $n = 2^a \cdot 3^b \cdot 5^c \cdot 11^d$ for some positive integers a, b, c, d.

If $a > 0$ then $2^{a-1}|20$ so $a - 1 = 0, 1, 2$ so $a = 1, 2, 3$. Also possibly $a = 0$.

If $b > 0$ then $3^{b-1}|20$ so $b - 1 = 0$ so $b = 1$. Also possibly $b = 0$.

If $c > 0$ then $5^{c-1}|20$ so $c - 1 = 0, 1$ so $c = 1, 2$. Also possibly $c = 0$.

If $d > 0$ then $11^{d-1}|20$ so $d - 1 = 0$ so $d = 1$. Also possibly $d = 0$.

However $\tau(n) = (a+1)(b+1)(c+1)(c+1) \mid 4$ which means that the only permissible combinations are:

$(a+1)(b+1)(c+1)(d+1) = 1$ in which case $a = b = c = d = 0$. Yields: $n = 1$.

$(a+1)(b+1)(c+1)(d+1) = 2$ in which case one of a, b, c, d is 1 and the rest are 0. so one of them is 2 and the rest are 1. Yields: $n = 2, 3, 5, 11$.

$(a+1)(b+1)(c+1)(d+1) = 4$ in which case two of a, b, c, d are 1 and the rest are 0 or else one of a, b, c, d is 3 and the rest are 0. Yields: $n = 6, 10, 22, 15, 33, 55$ and $n = 8, 27, 125, 1331$.

Then we try those values (work omitted) we find that $n = 33$ is the only one that works.

4. It's a fact that $r = 2$ is a primitive root mod 13.

   (a) Use this to construct a table of indices for this primitive root. [5 pts]

   Solution:

   We have the following:

x	1	2	3	4	5	6	7	8	9	10	11	12
$\text{ind}_2 x$	0	1	4	2	9	5	11	3	8	10	7	6

   (b) Use the table of indices to solve the equation: $4^x \equiv 12 \mod 13$. Your answer(s) should be mod 12. [5 pts]

   Solution:

   We have the following:

$$\begin{aligned} 4^x &\equiv 12 \mod 13 \\ x \,\text{ind}_2 4 &\equiv \text{ind}_2 12 \mod \phi(13) \\ x(2) &\equiv 6 \mod 12 \\ x &\equiv 3, 9 \mod 12 \end{aligned}$$

(c) Use the table of indices to solve the equation: $x^2 \equiv 12 \mod 13$. Your answer(s) should be mod 13. [5 pts]

Solution:

We have the following:

$$\begin{aligned} x^2 &\equiv 12 \mod 13 \\ 2\text{ind}_2 x &\equiv \text{ind}_2 12 \mod \phi(13) \\ 2\text{ind}_2 x &\equiv 6 \mod 12 \\ \text{ind}_2 x &\equiv 3, 9 \mod 12 \\ x &\equiv 8, 5 \mod 13 \end{aligned}$$

(d) Find the least nonnegative residues of all of the other primitive roots mod 13. [5 pts]

Solution:

The other primitive roots will be 2^k for k satisfying $\gcd(k, \phi(13)) = 1$.

This is $\gcd(k, 12) = 1$ so $k = 1, 5, 7, 11$.

Thus we have:

$2^1 \equiv 2 \mod 13$

$2^5 \equiv 6 \mod 13$

$2^7 \equiv 11 \mod 13$

$2^{11} \equiv 7 \mod 13$

5. Suppose $a, n \in \mathbb{Z}^+$. Let $m = a^n - 1$. Prove that $\text{ord}_m a = n$. [10 pts]

Solution:

First, observe that $a^n \equiv 1 \mod m$ and so $\text{ord}_m a \mid n$.

Second, suppose that $\text{ord}_m a = k < n$. Then $a^k \equiv 1 \mod m$ so then $a^k \equiv 1 \mod a^n - 1$ and then $(a^n - 1) \mid (a^k - 1)$ which is impossible since $k < n$.

6. Prove that if $a, m \in \mathbb{Z}^+$ with $\gcd(a, m) = \gcd(a-1, m) = 1$ then: [10 pts]

$$1 + a + a^2 + ... + a^{\phi(m)-1} \equiv 0 \mod m$$

Solution:

Observe that:

$$\begin{aligned} a^{\phi(m)} &\equiv 1 \mod m \\ a^{\phi(m)} - 1 &\equiv 0 \mod m \\ (a-1)\left(1 + a + a^2 + ... + a^{\phi(m)-1}\right) &\equiv 0 \mod m \end{aligned}$$

Since $\gcd(a-1, m) = 1$ we can cancel the $a - 1$, yielding the result.

7. Show that a positive integer n is composite iff $\phi(n) \leq n - \sqrt{n}$. [12 pts]

Solution:

$\Rightarrow$: Suppose n is composite. Let p be the smallest prime divisor of n which must be less than or equal to $\sqrt{n}$. Then $p \leq \sqrt{n}$ and so $p\sqrt{n} \leq n$ and so $\frac{n}{p} \geq \sqrt{n}$. Then observe that if $q_1, ..., q_k$ are the other prime divisors of n then:

$$\phi(n) = n(1 - 1/p)(1 - 1/q_1)...(1 - 1/q_k) \leq n(1 - 1/p) = n - n/p \leq n - \sqrt{n}$$

$\Leftarrow$: Suppose n satisfies $\phi(n) \leq n - \sqrt{n}$. Since $\phi(n) \neq n - 1$ we know n is not prime.

8. Define $f(n) = \gcd(n, 6)$. Prove that $f(n)$ is multiplicative. [10 pts]

Solution:

We claim that if $\gcd(n, m) = 1$ then $\gcd(nm, 6) = \gcd(n, 6)\gcd(m, 6)$. We can break this into cases:

- If $\gcd(nm, 6) = 1$ then 2 and 3 divide neither n nor m. Then $\gcd(n, 6) = \gcd(m, 6) = 1$.
- If $\gcd(nm, 6) = 2$ then 2 divides exactly one of them and 3 divides neither. Suppose WLOG $2 \mid n$ and $3 \nmid n, m$. Then $\gcd(n, 6) = 2$ and $\gcd(m, 6) = 1$.
- If $\gcd(nm, 6) = 3$ then 3 divides exactly one of them and 2 divides neither. Suppose WLOG $3 \mid n$ and $2 \nmid n, m$. Then $\gcd(n, 6) = 3$ and $\gcd(m, 6) = 1$.
- If $\gcd(nm, 6) = 6$ then 2 divides exactly one of them and 3 divides exactly one of them. Suppose WLOG $2 \mid n$ and $3 \mid m$. Then $\gcd(n, 6) = 2$ and $\gcd(m, 6) = 3$. Suppose WLOG $2 \mid n$ and $3 \mid n$ then $\gcd(n, 6) = 6$ and $\gcd(m, 6) = 1$.

9. Let p be an odd prime and t a positive integer. Show that p^t and $2p^t$ have the same number of primitive roots. You can assume that they both do actually have primitive roots. [5 pts]

Solution:

If some n has primitive roots then there are $\phi(\phi(n))$ of them. Then observe that:

$$\phi(\phi(2p^t)) = \phi(\phi(2)\phi(p^t)) = \phi(\phi(p^t))$$

10. Let n be a positive integer. Prove that the product of the divisors of n equals $n^{\tau(n)/2}$. [12 pts]

Hint: The case where n is not a perfect square is easier so do it first.

Solution:

If n is not a perfect square then for each divisor d there is another divisor n/d with $d \neq n/d$. The product of each pair is n and there are $\tau(n)/2$ such pairs. Thus the product of the divisors is $n^{\tau(n)/2}$.

If n is a perfect square then the above statement is true except for the divisor $\sqrt{n}$. If we ignore that divisor then there are $(\tau(n)-1)/2$ pairs and the product of the remaining divisors equals $n^{(\tau(n)-1)/2}$. But then including $\sqrt{n}$ tells us the product of all the divisors equals $n^{(\tau(n)-1)/2}n^{1/2} = n^{\tau(n)/2}$.