MATH 406 Exam 2 Summer 2021

Due by Saturday August 7 at 3:00pm

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 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. Consider the linear congruence:

$$20x \equiv 15 \mod 75$$

(a) Use the Euclidean Algorithm and its follow-up to find one solution. Find the least nonnegative residue mod 75 of this solution. [10 pts]

Solution:

We have:

$$\begin{aligned} 75 &= 3(20) + 15 \\ 20 &= 1(15) + 5 \end{aligned}$$

Thus we have:

$$\begin{aligned} 5 &= 20 - 1(15) \\ 5 &= 20 - 1(75 - 3(20)) \\ 5 &= 4(20) - 1(75) \end{aligned}$$

Therefore we have:

$$\begin{aligned} 4(20) - 1(75) &= 5 \\ 20(4) &\equiv 5 \mod 75 \\ 20(12) &\equiv 15 \mod 75 \end{aligned}$$

Thus we have a solution $x_0 \equiv 12 \mod 75$.

(b) Find a formula for all incongruent solutions mod 75. [5 pts]

Solution:

The set of all solutions mod 75 is:

$$\begin{aligned} x &\equiv 12 + \frac{75}{\gcd(75,20)}k \mod 75 \qquad k = 0, 1, ..., \gcd(75,20) - 1 \\ x &\equiv 12 + 15k \mod 75 \qquad k = 0, 1, ..., 5 - 1 \end{aligned}$$

(c) Find the set of least nonnegative residues of all the incongruent solutions mod 75. [5 pts]

Solution:

We have:

$$x \in \{12, 27, 42, 57, 72\}$$

2. Suppose the linear congruence $40x \equiv 12 \mod m$ does not have any solutions. What must the prime factorization of m look like? [10 pts]

   Solution:

   There are solutions iff $\gcd(40, m) \mid 12$ and therefore no solutions if $\gcd(40, m) \nmid 12$.

   Since $\gcd(40, m) = 2^a 5^b$ for $0 \leq a \leq 3$ and $0 \leq b \leq 1$ and since $2^a 5^b \nmid 12$ when $a \geq 3$ or $b = 1$, this will happen precisely when $a = 3$ or $b = 1$, meaning m must either be divisible by 8 or by 5 (or both).

   Thus $m = 2^\alpha 5^\beta Q$ where $\alpha \geq 3$ or $\beta \geq 1$.

3. Calculate each of the following:

   (a) $\phi(6 \cdot 10 \cdot 20)$ [5 pts]

   Solution:

   We have:

$$\phi(6 \cdot 10 \cdot 20) = \phi(2^4 \cdot 3 \cdot 5^2) = 2^4 \cdot 3 \cdot 5^2 \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right)\left(1 - \frac{1}{5}\right)$$

   (b) $\tau(5!)$ [5 pts]

   Solution:

   We have $5! = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 = 2^3 \cdot 3 \cdot 5$ and so:

$$\tau(5!) = (3 + 1)(1 + 1)(1 + 1)$$

4. Use the Chinese Remainder Theorem to find the three smallest nonnegative solutions to the system: [10 pts]

$$\begin{aligned} x &\equiv 3 \mod 5 \\ x &\equiv 1 \mod 6 \\ x &\equiv 4 \mod 7 \end{aligned}$$

Solution:

Let $M = (5)(6)(7) = 210$ and then $m_1 = 42$, $m_2 = 35$ and $m_3 = 30$. We then solve:

- $42y_1 \equiv 1 \mod 5$ so $2y_1 \equiv 1 \mod 5$ so $y_1 = 3$.
- $35y_2 \equiv 1 \mod 6$ so $5y_2 \equiv 1 \mod 6$ so $y_2 = 5$.
- $30y_3 \equiv 1 \mod 7$ so $2y_3 \equiv 1 \mod 7$ so $y_3 = 4$.

Thus there is a unique solution mod 210 which is:

$$\begin{aligned} x &\equiv (3)(3)(42) + (1)(5)(35) + (4)(4)(30) \mod 210 \\ &\equiv 193 \mod 210 \end{aligned}$$

Thus the three smallest nonnegative solutions are 193, $193 + 210$, and $193 + 420$.

5. Use Wilson's Theorem and Fermat's Little Theorem to find to the least nonnegative residue: [10 pts]

$$25! \cdot 8^{86} \mod 29$$

Solution:

First observe that by Wilson's Theorem:

$$\begin{aligned} 28! &\equiv -1 \mod 29 \\ (28)(27)(26)25! &\equiv -1 \mod 29 \\ (-1)(-2)(-3)25! &\equiv -1 \mod 29 \\ (-6)25! &\equiv -1 \mod 29 \\ (6)25! &\equiv 1 \mod 29 \\ (5)(6)25! &\equiv 5 \mod 29 \\ 25! &\equiv 5 \mod 29 \end{aligned}$$

Then observe by Fermat's Little Theorem since 29 is prime that $8^{28} \equiv 1 \mod 29$ and so:

$$8^{86} = 8^{28(3)+2} = \left(8^{28}\right)^3 8^2 \equiv (1)^3 8^2 \equiv 64 \equiv 6 \mod 29$$

Together then:

$$25! \cdot 8^{86} \equiv 5 \cdot 6 \equiv 30 \equiv 1 \mod 29$$

6. Find, with evidence, all n with $\phi(n) = 10$. [10 pts]

Note: If you're getting loads of things to check then you're doing something wrong. This is quite manageable!

Solution:

If p^k appears in the PF of n then $(p-1) \mid \phi(n) = 10$ so $p-1 = 1, 2, 5, 10$ and so $p = 2, 3, 6, 11$, but p must be prime so that $p = 2, 3, 11$. Thus so far we have $n = 2^a \cdot 3^b \cdot 11^c$ with $a, b, c \geq 0$.

(a) If $a > 0$ then $2^{a-1} \mid \phi(n) = 10$ so $2^{a-1} = 1, 2$ so $a - 1 = 0, 1, 2$ so $a = 1, 2$. Thus we could have $a = 0, 1, 2$.

(b) If $b > 0$ then $3^{b-1} \mid \phi(n) = 10$ so $3^{b-1} = 1$ so $b - 1 = 0$ so $b = 1$. Thus we could have $b = 0, 1$.

(c) If $c > 0$ then $11^{c-1} \mid \phi(n) = 10$ so $11^{c-1} = 1$ so $c - 1 = 0$ so $c = 1$. Thus we could have $c = 0, 1$.

Thus there are 12 to check:

$$\begin{aligned}
\phi(2^0 \cdot 3^0 \cdot 11^0) &= 1 \\
\phi(2^0 \cdot 3^0 \cdot 11^1) &= 10 \\
\phi(2^0 \cdot 3^1 \cdot 11^0) &= 2 \\
\phi(2^0 \cdot 3^1 \cdot 11^1) &= 20 \\
\phi(2^1 \cdot 3^0 \cdot 11^0) &= 1 \\
\phi(2^1 \cdot 3^0 \cdot 11^1) &= 10 \\
\phi(2^1 \cdot 3^1 \cdot 11^0) &= 2 \\
\phi(2^1 \cdot 3^1 \cdot 11^1) &= 20 \\
\phi(2^2 \cdot 3^0 \cdot 11^0) &= 2 \\
\phi(2^2 \cdot 3^0 \cdot 11^1) &= 20 \\
\phi(2^2 \cdot 3^1 \cdot 11^0) &= 4 \\
\phi(2^2 \cdot 3^1 \cdot 11^1) &= 40
\end{aligned}$$

The only possibilities are then 11 and 22.

7. Suppose $a \in \mathbb{Z}^+$ and $n = 2^a$. If $2^{a+1} - 1$ is prime, prove that $\sigma(\sigma(n)) = 2^{\tau(n)}$. [10 pts]

Note: Don't overcomplicate, just calculate!

Solution:

Observe that:

$$\sigma(n) = \sigma(2^a) = \frac{2^{a+1} - 1}{2 - 1} = 2^{a+1} - 1$$

Then since $2^{a+1} - 1$ is prime we have:

$$\sigma(\sigma(n)) = \sigma(2^{a+1} - 1) = 1 + 2^{a+1} - 1 = 2^{a+1}$$

Also then consider that:

$$\tau(n) = a + 1$$

The result follows.

8. Prove that there are infinitely many even abundant numbers by finding one abundant number and by proving that if n is abundant and a prime p satisfies $p \nmid n$ then pn is also abundant. [10 pts]

Solution:

For example 12 is abundant since $\sigma(12) = 1 + 2 + 3 + 4 + 6 + 12 = 28 > 2(12)$.

If $p \nmid n$ then $\gcd(p, n) = 1$ and so

$$\sigma(pn) = \sigma(p)\sigma(n) = (p + 1)\sigma(n) > (p + 1)2n = 2np + 2n > 2pn$$

thus pn is abundant.

9. Prove that if p is an odd prime then: [10 pts]

$$1^2 \cdot 3^2 \cdot 5^2 \cdot ... \cdot (p-2)^2 \equiv (-1)^{(p+1)/2} \mod p$$

Note: This is not obvious, so definitely do this problem last!

Solution:

By Wilson's Theorem we have:

$$(p-1)! \equiv -1 \mod p$$

W write this out:

$$1 \cdot 2 \cdot 3 \cdot 4 ... \cdot (p-3) \cdot (p-2) \cdot (p-1) \equiv -1 \mod p$$

Note that there are $p-1$ values total. If we rewrite the $(p-1)/2$ even values (every other value):

$$\begin{aligned} 2 &\equiv -(p-2) \\ 4 &\equiv -(p-4) \\ \vdots & \quad \vdots \\ p-3 &\equiv -(p-(p-3)) \equiv -3 \\ p-1 &\equiv -(p-(p-1)) \equiv -1 \end{aligned}$$

We get:

$$1 \cdot (-(p-2)) \cdot 3 \cdot (-(p-4)) ... \cdot (-3) \cdot (p-2) \cdot (-1) \equiv -1 \mod p$$

Then we collect all the negatives and construct squares:

$$(-1)^{(p-1)/2} 1^2 \cdot 2^2 \cdot 3^2 \cdot ... \cdot (p-2)^2 \equiv -1 \mod p$$

Then collect the $-1s$ on the right:

$$1^2 \cdot 3^2 \cdot 5^2 \cdot ... \cdot (p-2)^2 \equiv (-1)^{(p+1)/2} \mod p$$