MATH 406 (JWG) Final Exam Spring 2021

Due by Tuesday May 11 at 10:00pm

Exam Logistics:

1. From the moment you download this exam you have four 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. Exception: Problems that say "Tech Okay" mean you can use calculators, Wolfram Alpha and your own coding skills.
5. 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. Given $A = 32219517869$ and $B = 163950325$.

   (a) Find the prime factorizations of A and B and use them to find $\gcd(A, B)$. Tech okay. [5 pts]

   Solution:
   We have $A = 7^2 \cdot 11 \cdot 17^3 \cdot 23^3$ and $B = 5^2 \cdot 7^2 \cdot 11 \cdot 23^3$.
   Thus $\gcd(32219517869, 163950325) = 7^2 \cdot 11 \cdot 23^3$.

   (b) Find $\gcd(A, B)$ using the Euclidean Algorithm. Tech okay. [5 pts]

   Solution:
   We have:

$$\begin{aligned} 32219517869 &= 196(163950325) + 85254169 \\ 163950325 &= 1(85254169) + 78696156 \\ 85254169 &= 1(78696156) + 6558013 \\ 78696156 &= 12(6558013) + 0 \end{aligned}$$

   Thus $\gcd(32219517869, 163950325) = 6558013$.

2. Use the Chinese Remainder Theorem to find the smallest and second smallest nonnegative solutions to the system: [10 pts]

$$\begin{aligned} x &\equiv 7 \mod 17 \\ x &\equiv 11 \mod 12 \\ x &\equiv 6 \mod 7 \end{aligned}$$

Solution:
First we solve the three congruences:

- First:

$$\begin{aligned} (12)(7)y_1 &\equiv 1 \mod 17 \\ 16y_1 &\equiv 1 \mod 17 \\ y_1 &\equiv 16 \mod 17 \end{aligned}$$

- Second:

$$\begin{aligned} (17)(7)y_2 &\equiv 1 \mod 12 \\ 11y_2 &\equiv 1 \mod 12 \\ y_2 &\equiv 11 \mod 12 \end{aligned}$$

- Third:

$$\begin{aligned} (17)(12)y_3 &\equiv 1 \mod 7 \\ 1y_3 &\equiv 1 \mod 7 \\ y_3 &\equiv 1 \mod 7 \end{aligned}$$

We then have:

$$x \equiv (7)(12)(7)(16) + (11)(17)(7)(11) + (6)(17)(12)(1) \equiv 25031 \equiv 755 \mod 1428$$

for the smallest, and the second smallest would be 2183.

3. It's a fact that $r = 2$ is a primitive root mod 11.

(a) Use this to construct a table of indices for this primitive root. Tech okay. [10 pts]

Solution:
We have the following:

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

(b) Use the table of indices to solve the equation: $x^2 \equiv 9 \mod 11$. Your answer(s) should be mod 11. [10 pts]

Solution:
We have the following:

$$\begin{aligned} x^2 &\equiv 9 \mod 11 \\ 2\text{ind}_2 x &\equiv \text{ind}_2 9 \mod \phi(11) \\ 2\text{ind}_2 x &\equiv 6 \mod 10 \\ \text{ind}_2 x &\equiv 3, 8 \mod 10 \\ x &\equiv 8, 3 \mod 11 \end{aligned}$$

(c) Use the table of indices to solve the equation: $3^x \equiv 9 \mod 11$. Your answer(s) should be mod 10. [10 pts]

Solution:
We have the following:

$$\begin{aligned} 3^x &\equiv 9 \mod 11 \\ x\,\text{ind}_2 3 &\equiv \text{ind}_2 9 \mod \phi(11) \\ x(8) &\equiv 6 \mod 10 \\ x &\equiv 2, 7 \mod 10 \end{aligned}$$

4. Calculate: [15 pts]

$$\left(\frac{2304}{47027}\right)$$

Solution:

I didn't mean this to be so easy but 2304 is a perfect square so the answer is 1.

Or, a longer way: $\left(\frac{87910}{47027}\right) \underset{R}{=} \left(\frac{40883}{47027}\right)$ We factor the denominator as $47027 = 31^1 37^1 41^1$:

- ➔ $\left(\frac{40883}{31}\right) \underset{R}{=} \left(\frac{25}{31}\right)$ We factor the numerator as $25 = 5^2$:
  - ➔ $\left(\frac{5}{31}\right)^2 \underset{QR}{=} \left(\frac{31}{5}\right)^2 \underset{R}{=} \left(\frac{1}{5}\right)^2 = 1^2 = 1$
- ➔ $\left(\frac{40883}{37}\right) \underset{R}{=} \left(\frac{35}{37}\right)$ We factor the numerator as $35 = 5^1 7^1$:
  - ➔ $\left(\frac{5}{37}\right) \underset{QR}{=} \left(\frac{37}{5}\right) \underset{R}{=} \left(\frac{2}{5}\right) \underset{2}{=} -1$
  - ➔ $\left(\frac{7}{37}\right) \underset{QR}{=} \left(\frac{37}{7}\right) \underset{R}{=} \left(\frac{2}{7}\right) \underset{2}{=} 1$
- ➔ $\left(\frac{40883}{41}\right) \underset{R}{=} \left(\frac{6}{41}\right)$ We factor the numerator as $6 = 2^1 3^1$:
  - ➔ $\left(\frac{2}{41}\right) \underset{2}{=} 1$
  - ➔ $\left(\frac{3}{41}\right) \underset{QR}{=} \left(\frac{41}{3}\right) \underset{R}{=} \left(\frac{2}{3}\right) \underset{2}{=} -1$

Final answer equals product of ± 1s: 1

5. Suppose you intercept the following ciphertext from Alice to Bob: [15 pts]

```
4990 11344 6226 4521 5015 5848 11689
```

You know that Bob's public key is $(e, n) = (1289, 12317)$. Bob thinks this is secure because he doesn't believe that his n can be factored easily. Factor $n = 12317$, find $\phi(n)$, find d and then decrypt the message. Be clear about the steps you take. Tech okay.

Solution:
We factor $12317 = (109)(113)$ and so $\phi(12317) = (109-1)(113-1) = 12096$. We solve $1289d \equiv 1 \mod 12096$ and get $d \equiv 3641 \mod 12096$. We use this to decrypt: First we append an `X` and then:

$$\begin{aligned}
4990^{3641} &\equiv 18 \mod 12317 \to \texttt{AS} \\
11344^{3641} &\equiv 722 \mod 12317 \to \texttt{HW} \\
6226^{3641} &\equiv 11 \mod 12317 \to \texttt{AL} \\
4521^{3641} &\equiv 1018 \mod 12317 \to \texttt{KS} \\
5015^{3641} &\equiv 1200 \mod 12317 \to \texttt{MA} \\
5848^{3641} &\equiv 311 \mod 12317 \to \texttt{DL} \\
11689^{3641} &\equiv 2423 \mod 12317 \to \texttt{YX}
\end{aligned}$$

So the plaintext is:

```
ASHWALKSMADLY
```

6. Apply Pollard's Rho method to find a factor of 437. Show your steps. Tech okay. [10 pts]

Solution:

We have:
$x_1 = 5$
$x_2 = 26$ so $\gcd(26 - 5, 437) = 1$
$x_3 = 240$
$x_4 = 354$ so $\gcd(354 - 26, 437) = 1$
$x_5 = 335$
$x_6 = 354$ so $\gcd(354 - 240, 437) = 19$

Thus a factor is 19.

7. Consider from class our: $\mathcal{E}(x) = R(\lg x, d)$ and $\mathcal{D}(x) = R(2^x, 0)$.

(a) We saw in class that $d = 2$ was insufficient for correcting for the noise in the calculation $3^2 \cdot 5 \cdot 7$. What is the smallest value of d which would suffice? Justify. Tech okay. [10 pts]

Solution:

If Bob sends $d = 3$ digits then

$$\mathcal{E}(3) = R(\lg 3, 3) = 1.585$$
$$\mathcal{E}(5) = R(\lg 5, 3) = 2.322$$
$$\mathcal{E}(7) = R(\lg 7, 3) = 2.808$$

He then sends $(1.585, 1.585, 2.322, 2.808)$ to Alice with instructions to add. She does so and gets 8.3 which she sends back to Bob. Bob then calculates:

$$\mathcal{D}(2^{8.3}) = R(2^{8.3}, 0) = 315$$

which is correct.

(b) Suppose 2^k for $k \in \mathbb{Z}^+$ (positive powers) is being calculated. Do some experimentation to figure out how the number of digits needed to compensate for the noise changes as k increases. Summarize your findings. Tech okay. [10 pts]

Solution:

I intended this to be 3^k. It turns out that because the encryption takes $\log_2$ it's a perfect representation and there's no noise.

8. Suppose Bob uses the ring isomorphism $\phi : \mathbb{Z}_6 \to \mathbb{Z}_2 \times \mathbb{Z}_3$ given in class and in the notes as his encryption $\mathcal{E}$. Walk through the full process by which Bob would have Alice calculate $4(2+3)+1$ for him. [10 pts]

Solution:

Bob calculates and sends:

$$\{\mathcal{E}(4), \mathcal{E}(2), \mathcal{E}(3), \mathcal{E}(1)\} = \{(0,1), (0,2), (1,0), (1,1)\}$$

He tells Alice something like:

Add the second and third, multiply by the first, add the fourth.

She does:

$$(0,1)((0,2)+(1,0))+(1,1) = (0,1)(1,2)+(1,1) = (0,2)+(1,1) = (1,0)$$

She sends $(1,0)$ back. Bob gets back $\mathcal{E}^{-1}(1,0) = 3$.

9. Emulate/rewrite the final coin-flip example from class with $p = 53$, $q = 97$, and $b = 42$. Describe Alice's choices, Bob's choice, who sends what to whom, the equation Alice solves, what those solutions are, and what possibilities might emerge. [20 pts]

   For the equation Alice solves write down the details as in the example of Theorem 3 in the notes but you can use technology to do the gritty calculations. Tech okay.

   Solution:

   Alice chooses $p = 53$ and $q = 97$ and calculates $n = pq = 5141$. She sends this to Bob. Bob picks $b = 42$ and calculates $b^2 \equiv 1764 \mod 5141$ and sends 1764 back to Alice. Alice solves $x^2 \equiv 1764 \mod 5141$:

   She solves the first system:

$$x \equiv 1764^{(53+1)/4} \equiv 42 \mod 53$$
$$x \equiv 1764^{(97+1)/4} \equiv 55 \mod 97$$

   The CRT gives us $x \equiv 2480 \mod 5141$. This is our X. We know that $-X \equiv 2661 \mod 5141$ would solve the system with $-7, -14$.

   She solves the second system:

$$x \equiv 1764^{(53+1)/4} \equiv 42 \mod 53$$
$$x \equiv -1764^{(97+1)/4} \equiv 42 \mod 97$$

   The CRT gives us $x \equiv 42 \mod 5141$. This is our Y. We know that $-Y \equiv 5099 \mod 5141$ would solve the system with $-7, 14$.

   All together she has: $X = 2480$, $-X = 2661$, $Y = 42$, $-Y = 5099$.

   She knows Bob used one of these but doesn't know which. She chooses one of them and sends it back. If she sends back 42 or 5099 then Bob cannot factor n. However if she sends back 2480 or 2661 then he can. Observe:

   - If she sends 42 then Bob tests $\gcd(\pm 42 \pm 42, 5141)$ and they all equal 1 or 5141.
   - If she sends 5099 then Bob tests $\gcd(\pm 42 \pm 5099, 5141)$ and they all equal 1 or 5141.
   - If she sends 2480 then Bob tests $\gcd(\pm 42 \pm 2480, 5141)$ and notes that the results are 97 or 53.
   - If she sends 2661 then Bob tests $\gcd(\pm 42 \pm 2661, 5141)$ and notes that the results are 97 or 53.

10. Use prime factorizations to prove that $\log_{\sqrt{3}} \sqrt{10}$ is irrational. [10 pts]

Solution:

Assume it's rational, so then $\log_{\sqrt{3}} \sqrt{10} = \frac{a}{b}$ where a and b are integers. Then we have $(\sqrt{3})^{\frac{a}{b}} = \sqrt{10}$. Raising both sides to the b power yields $(\sqrt{3})^a = (\sqrt{10})^b$. Squaring both sides then yields $3^a = 10^b$ so $3^a = 2^b \cdot 5^b$. Since both sides are different prime factorizations, and both are equal, this contradicts the uniqueness of prime factorizations.

11. Prove by induction that for all positive integers n we have: [10 pts]

$$\sum_{i=1}^{n}(-1)^i i^2 = (-1)^n \frac{1}{2}(n)(n+1)$$

Solution:

The base case $n = 1$ asks if the following is true, which it clearly is:

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

Assume the statement is true for some k and then observe:

$$\begin{aligned}
\sum_{i=1}^{k+1}(-1)^i i^2 &= (-1)^{k+1}(k+1)^2 + \sum_{i=1}^{k}(-1)^i i^2 \\
&= (-1)^{k+1}(k+1)^2 + (-1)^k \frac{1}{2}(k)(k+1) \\
&= (-1)^k(-k^2 - 2k - 1) + (-1)^k \frac{1}{2}(k^2 + k) \\
&= (-1)^k \left(-\frac{1}{2}k^2 - k - 1\right) + (-1)^k \frac{1}{2}(k^2 + k) \\
&= (-1)^k \left(-\frac{1}{2}k^2 - \frac{3}{2}k - 1\right) \\
&= (-1)^{k+1} \frac{1}{2}(k^2 + 3k + 2) \\
&= (-1)^{k+1} \frac{1}{2}(k+1)(k+2)
\end{aligned}$$

This is as desired.

12. Suppose $a, b, d \in \mathbb{Z}$ are nonzero and d is odd. Prove that if $d|(a+b)$ and $d|(a-b)$ then $d|\gcd(a,b)$. [10 pts]

Solution:

We have $d|(a+b)+(a-b)$ so $d|2a$. Since d is odd we must have $d|a$.

We have $d|(a+b)-(a-b)$ so $d|2b$. Since d is odd we must have $d|b$.

We know that all other common divisors divide the gcd and we are done.

13. For a positive integer $n > 1$ if $n = p_1^{a_1}...p_k^{a_k}$ is the prime factorization of n then define: [15 pts]

$$\lambda(n) = (-1)^{a_1+...+a_k}$$

Prove that λ is multiplicative.

Solution:

Suppose $\gcd(n, m) = 1$. Then we have:

$$n = p_1^{a_1}...p_k^{a_k}$$

and

$$m = q_1^{b_1}...q_j^{b_j}$$

where none of the p_i and q_i are equal.

Then:

$$\begin{aligned}\lambda(nm) &= \lambda(p_1^{a_1}...p_k^{a_k}q_1^{b_1}...q_j^{b_j}) \\ &= a_1 + ... + a_k + b_1 + ... + b_j \\ &= \lambda(p_1^{a_1}...p_k^{a_k})\lambda(q_1^{b_1}...q_j^{b_j}) \\ &= \lambda(n)\lambda(m)\end{aligned}$$

14. Suppose $k > 1$ is an integer and $p = 1 + 2^k$ is prime. Prove that if $\left(\frac{a}{p}\right) = -1$ then a is a primitive root of p. [15 pts]

Solution:

We claim $\text{ord}_p a = p - 1 = 2^k$. Since $\text{ord}_p a \mid p - 1 = 2^k$ we know that the order is a power of 2 less than or equal to 2^k.

Suppose by way of contradicton that $\text{ord}_p a = 2^j$ for $j < k$ and so $a^{2^j} \equiv 1 \mod p$ and observe that:

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} = a^{2^{k-1}} \mod p$$

However then we have:

$$\begin{aligned} a^{(2^j)} &\equiv 1 \mod p \\ \left(a^{(2^j)}\right)^{(2^{k-j-1})} &\equiv 1 \mod p \\ a^{(2^{k-1})} &\equiv 1 \mod p \\ \left(\frac{a}{p}\right) &\equiv 1 \mod p \end{aligned}$$

This is a contradiction.