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]

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

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

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

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]

   (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]

   (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]

4. Calculate: [15 pts]

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

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.

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

Solution:

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:

(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:

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:

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:

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

Solution:

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:

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:

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:

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: