MATH 406 Exam 3 Summer 2021

Due by Friday August 20 at 6:00pm

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. Problems which state "Tech Okay" are exceptions to this and will state which tech resources and methods are permissible.
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. It's a fact that $r = 6$ is a primitive root mod 11.

   (a) Construct a table of indices for this primitive root. [5 pts]
   Tech Okay: You can use Wolfram Alpha to do calculations.
   Solution:

   (b) Use the table of indices to solve the equation $x^8 \equiv 5 \mod 11$. Your answer(s) should be mod 11. [10 pts]
   Solution:

   (c) Use the table of indices to solve the equation $3^x \equiv 5 \mod 11$. Your answer(s) should be mod 10. [10 pts]

2. Calculate the following Jacobi symbol using the various formulas from the class. [10 pts]

$$\left(\frac{87676}{50431}\right)$$

Tech Okay: You can use Wolfram Alpha for factoring.

Solution:

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

```
2982 2237 3239 11364 8541 7043
```

You know that this was encrypted using RSA and that Bob's public key is $(e, n) = (1655, 11639)$. Bob thinks this is secure because he doesn't believe that his n can be factored easily. Factor $n = 11639$, find $\phi(n)$, find d and then decrypt the message. Be clear about the steps you take.

Tech Okay: You can use Wolfram Alpha to do calculations but make sure you write down the calculations you are using it for.

Solution:

4. The following message: [10 pts]

(2414,240),(50,50)

was encrypted using the ElGamal Cryptosystem with $(p, r, b) = (2539, 3, 159)$. Crack the encryption and decrypt the message. Make sure your steps are clear.

Tech Okay: You can use Wolfram Alpha to do calculations but make sure you write down the calculations you are using it for.

Solution:

5. Emulate/rewrite the final coin-flip example from class with $p = 131$, $q = 103$, and $\alpha = 1234$. 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. [10 pts]

   For the equation Alice solves write down the details as we did in class but you can use technology to do the gritty calculations.

   Tech Okay: You can use Wolfram Alpha to do calculations but make sure you write down the calculations you are using it for.

   Solution:

6. Consider the following invertible function $\phi : \mathbb{Z}_{10} \to \mathbb{Z}_5 \times \mathbb{Z}_2$:

$$\begin{aligned}
\phi(0) &= (0,0) & \phi^{-1}(0,0) &= 0 \\
\phi(1) &= (1,1) & \phi^{-1}(1,1) &= 1 \\
\phi(2) &= (2,0) & \phi^{-1}(2,0) &= 2 \\
\phi(3) &= (3,1) & \phi^{-1}(3,1) &= 3 \\
\phi(4) &= (4,0) & \phi^{-1}(4,0) &= 4 \\
\phi(5) &= (0,1) & \phi^{-1}(0,1) &= 5 \\
\phi(6) &= (1,0) & \phi^{-1}(1,0) &= 6 \\
\phi(7) &= (2,1) & \phi^{-1}(2,1) &= 7 \\
\phi(8) &= (3,0) & \phi^{-1}(3,0) &= 8 \\
\phi(9) &= (4,1) & \phi^{-1}(4,1) &= 9
\end{aligned}$$

(a) This is in fact a ring isomorphism. Show that the two homomorphism rules apply to the values 5 and 7. [5 pts]

Solution:

(b) If Bob sets $\mathcal{E} = \phi$ and $\mathcal{D} = \phi^{-1}$ explain how he could ask Alice to calculate $8(2 + 3(4))$ and how he would interpret the result. [5 pts]

Solution:

7. Suppose p is an odd prime such that there is some a so that a is a quadratic residue of p but $2a$ is a quadratic non-residue of p. Prove that $p \equiv \pm 3 \mod 8$. [10 pts]

Solution:

8. Suppose p is an odd prime and both r, s are primitive roots. Prove that rs cannot be a primitive root. [10 pts]

Solution: