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:

   We have the following:

x	1	2	3	4	5	6	7	8	9	10
$\text{ind}_6 x$	0	9	2	8	6	1	3	7	4	5

   (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:

   We have the following:

$$\begin{aligned} x^8 &\equiv 5 \mod 11 \\ 8\text{ind}_6 x &\equiv \text{ind}_6 5 \mod \phi(11) \\ 8\text{ind}_6 x &\equiv 6 \mod 10 \\ \text{ind}_6 x &\equiv 2, 7 \mod 10 \\ x &\equiv 3, 8 \mod 11 \end{aligned}$$

   (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]

   Solution:

   We have the following:

$$\begin{aligned} 3^x &\equiv 5 \mod 11 \\ x\,\text{ind}_6 3 &\equiv \text{ind}_6 5 \mod \phi(11) \\ x(2) &\equiv 6 \mod 10 \\ x &\equiv 3, 8 \mod 10 \end{aligned}$$

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:

Solution Note: These solution were autogenerated recursively in Python and may take a minute to understand.
R = Reduce numerator mod denominator,
QR = Quadratic reciprocity,
2 = 2-rule.
$\left(\frac{87676}{50431}\right) \underset{R}{=} \left(\frac{37245}{50431}\right)$
We factor the denominator as $50431 = 29^1 \cdot 37^1 \cdot 47^1$:

- ➔ $\left(\frac{37245}{29}\right) \underset{R}{=} \left(\frac{9}{29}\right)$
  We factor the numerator as $9 = 3^2$:
  - ➔ $\left(\frac{3}{29}\right)^2 \underset{QR}{=} \left(\frac{29}{3}\right)^2 \underset{R}{=} \left(\frac{2}{3}\right)^2 \underset{2}{=} (-1)^2 = 1$
- ➔ $\left(\frac{37245}{37}\right) \underset{R}{=} \left(\frac{23}{37}\right) \underset{QR}{=} \left(\frac{37}{23}\right) \underset{R}{=} \left(\frac{14}{23}\right)$
  We factor the numerator as $14 = 2^1 \cdot 7^1$:
  - ➔ $\left(\frac{2}{23}\right) \underset{2}{=} 1$
  - ➔ $\left(\frac{7}{23}\right) \underset{QR}{=} -\left(\frac{23}{7}\right) \underset{R}{=} -\left(\frac{2}{7}\right) \underset{2}{=} -1$
- ➔ $\left(\frac{37245}{47}\right) \underset{R}{=} \left(\frac{21}{47}\right)$
  We factor the numerator as $21 = 3^1 \cdot 7^1$:
  - ➔ $\left(\frac{3}{47}\right) \underset{QR}{=} -\left(\frac{47}{3}\right) \underset{R}{=} -\left(\frac{2}{3}\right) \underset{2}{=} (-(-1)) = 1$
  - ➔ $\left(\frac{7}{47}\right) \underset{QR}{=} -\left(\frac{47}{7}\right) \underset{R}{=} -\left(\frac{5}{7}\right) \underset{QR}{=} -\left(\frac{7}{5}\right) \underset{R}{=} -\left(\frac{2}{5}\right) \underset{2}{=} (-(-1)) = 1$

Final answer equals product of ± 1s: -1

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:

We factor $11639 = (103)(113)$ and so $\phi(11639) = (103-1)(113-1) = 11424$. We solve $1655d \equiv 1 \mod 11424$ and get $d \equiv 6599 \mod 11424$. We use this to decrypt:

$$\begin{aligned}
18^{6599} &\equiv 18 \mod 11639 \to \texttt{AS} \\
717^{6599} &\equiv 717 \mod 11639 \to \texttt{HR} \\
2013^{6599} &\equiv 2013 \mod 11639 \to \texttt{UN} \\
1812^{6599} &\equiv 1812 \mod 11639 \to \texttt{SM} \\
3^{6599} &\equiv 3 \mod 11639 \to \texttt{AD} \\
1124^{6599} &\equiv 1124 \mod 11639 \to \texttt{LY}
\end{aligned}$$

So the plaintext is:

`ASH RUNS MADLY`

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:

To find a we need to solve $3^a \equiv 159 \mod 2539$. This yields $a = 354$.

To decrypt then:

$(2414, 240)$ yields $2414^{2539-1-354} \cdot 240 \equiv 1500 \mod 2539$ so `PA`.

$(50, 50)$ yields $50^{2539-1-354} \cdot 50 \equiv 1818 \mod 2539$ so `SS`.

Thus the plaintext is `PASS`.

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:

   Alice chooses $p = 131$ and $q = 103$ and calculates $n = pq = 13493$. She sends this to Bob. Bob picks $\alpha = 1234$ and calculates $\alpha^2 \equiv 11540 \mod 3901$ and sends 11540 back to Alice. Alice solves $x^2 \equiv 11540 \mod 13493$ as follows:

   She solves the first system:

$$x \equiv 11540^{(131+1)/4} \equiv 55 \mod 131$$
$$x \equiv 11540^{(103+1)/4} \equiv 2 \mod 103$$

   The CRT gives us $x \equiv 8963 \mod 13493$. This is our X. Then $-X \equiv 4530 \mod 13493$.

   She solves the second system:

$$x \equiv 11540^{(131+1)/4} \equiv 55 \mod 131$$
$$x \equiv -11540^{(103+1)/4} \equiv 101 \mod 103$$

   The CRT gives us $x \equiv 1234 \mod 3901$. This is our Y. Then $-Y \equiv 12259 \mod 3901$.

   All together she has: $X = 8963$, $-X = 4530$, $Y = 1234$, $-Y = 12259$.

   She knows Bob used one of these but doesn't know which. She chooses one of them and sends it back. Observe:

   - If she sends 8963 then Bob tests $\gcd(1234 \pm 8963, 13493)$ yielding either 131 or 103 and then he can factor n and wins.
   - If she sends 4530 then Bob tests $\gcd(1234 \pm 4930, 13493)$ yielding either 131 or 103 and then he can factor n and wins.
   - If she sends 1234 then Bob cannot factor n and loses.
   - If she sends 12259 then Bob cannot factor n and loses.

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:

Observe that:

$$\begin{aligned}
\phi(5+7) = \phi(12) = \phi(2) &= (2,0) \\
\phi(5) + \phi(7) = (0,1) + (2,1) &= (2,0)
\end{aligned}$$

and

$$\begin{aligned}
\phi(5 \cdot 7) = \phi(35) = \phi(5) &= (0,1) \\
\phi(5) \cdot \phi(7) = (0,1) \cdot (2,1) &= (0,1)
\end{aligned}$$

(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:

He would calculate:

$$\begin{aligned}
\phi(8) &= (3,0) \\
\phi(2) &= (2,0) \\
\phi(3) &= (3,1) \\
\phi(4) &= (4,0)
\end{aligned}$$

He would send Alice $\{(3,0),(2,0),(3,1),(4,0)\}$ and tell her to multiply the last two, add the second, then multiply by the first.

Alice would do:

$$(3,0) \cdot ((2,0) + (3,1) \cdot (4,0)) = (3,0) \cdot ((2,0) + (2,0)) = (3,0) \cdot (4,0) = (2,0)$$

Bob would then find $\mathcal{D}(2,0) = 2$ and that would be the answer.

(Note that this is correct since $8(2 + 3(4)) = 8(2 + 12) = 8(14) = 8(4) = 2$ in $\mathbb{Z}_{10}$.)

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:

If a is a QR of p but $2a$ is a QNR of p then $\left(\frac{a}{p}\right) = 1$ and $\left(\frac{2a}{p}\right) = -1$. However $\left(\frac{2a}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{a}{p}\right)$ so then $\left(\frac{2}{p}\right) = -1$.

Since p is odd we could only have $p \equiv \pm 3 \mod 8$ or $p \equiv \pm 1 \mod 8$. Then by the 2-Theorem we know $p \equiv 3, 5 \mod 8$ which is the same as $p \equiv \pm 3 \mod 8$.

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:

We know $r^{p-1} \equiv 1 \mod p$ and so $p \mid \left(r^{(p-1)/2} - 1\right)\left(r^{(p-1)/2} + 1\right)$ which means it divides one of them. We can't have $p \mid \left(r^{(p-1)/2} - 1\right)$ since $r^{(p-1)/2} \neq 1 \mod p$ and so we must have $p \mid \left(r^{(p-1)/2} + 1\right)$, meaning $r^{(p-1)/2} \equiv -11 \mod p$.

A similar argument holds for s.

But then $(rs)^{(p-1)/2} \equiv (-1)(-1) \equiv 1 \mod p$ and so rs is not a primitive root.