MM Quiz 4

Due Nov 16 at 10pm **Points** 10 **Questions** 5
Available Nov 16 at 9am - Nov 16 at 10pm about 13 hours **Time Limit** 45 Minutes

Instructions

This is your mid-module quiz. Unlike the old quiz you did for homework, it is not collaborative. Once you start the quiz you will have a limited amount of time to complete it.

Be careful with formatting. If I specify a formatting method and you do not follow it, you will lose some credit.

The quiz is open notes. You may use your own notes and any of the resources on the course webpages. You are not allowed to use the internet for any other purpose unless a question directs you to do so.

On the day of the quiz, do not use any public forum to ask any quiz-related questions. Once you see the quiz, do not discuss it with anyone until the quiz closes for everyone.

Good luck!

This quiz was locked Nov 16 at 10pm.

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	36 minutes	8.5 out of 10

ⓘ Correct answers are hidden.

Score for this quiz: **8.5** out of 10
Submitted Nov 16 at 5:43pm
This attempt took 36 minutes.

Question 1	**3.5 / 3.5 pts**
The extended GCD algorithm learned in class calculates a sequence of	

remainders, and each remainder can be expressed as a linear combination of the original two inputs. Fill in the blanks with the sequence of remainders that are computed when calculating egcd(40,15) and the linear combination of 40's and 15's that gives you each remainder. To help, I've filled in the last row for you.

Double check your work because an error in any row will propagate to the next and cause additional incorrect answers.

Remainder	40's	15's
10	1	-2
5	-1	3
0	3	-8

Answer 1:

10

Answer 2:

1

Answer 3:

-2

Answer 4:

5

Answer 5:

-1

Answer 6:

3

Question 2

1.5 / 1.5 pts

Let's say you are generating RSA keys and you choose p=63 and q=67. What is the smallest value of e that qualifies as an encryption exponent?

You may use https://www.wolframalpha.com (https://www.wolframalpha.com) to aid with this problem. Some useful queries might be things like "gcd(50,35)" or "inverse of 7 mod 13".

5

Question 3

1.5 / 1.5 pts

Let's say you are generating RSA keys and you choose p=19, q=29 and encryption exponent e=11. What value d do you choose for the decryption exponent?

You may use https://www.wolframalpha.com (https://www.wolframalpha.com) to aid with this problem. Some useful queries might be things like "gcd(50,35)" or "inverse of 7 mod 13".

275

Incorrect

Question 4

0 / 1.5 pts

On the homework you saw that 3^5 could be expressed as a sequence of squaring and multiplying: `(((1^2*3)^2)^2*3)`

Using this same notation write the sequence of squaring and multiplying

for 7^{29}. Begin with 1^2 as your first squaring operation, and include a close-parenthesis after each step (SQ or SQ-MULT), as demonstrated in the example. Do not include any spaces. Note: 7 in binary is 111 and 29 in binary is 11101. Your answer should have 5 open-parenthesis and 5 close-parenthesis.

You may paste your text into **https://www.wolframalpha.com (https://www.wolframalpha.com)** and it should give you the correct answer (321990575581317972683760 7).

(((((1^2*7))^2*7)^2*7)^2)^2*7

Question 5

2 / 2 pts

In lecture you saw an algorithm for testing if p is prime. In it, x is chosen at random so that 1 < x < p. Some x's are compatible with p being prime and some immediately indicate that p is not prime. When p = 2465, what is the smallest x that indicates p is not prime? In other words, what is the smallest x that, if randomly chosen, would cause the algorithm immediately to report p not prime?

You may use **https://www.wolframalpha.com (https://www.wolframalpha.com)** to aid with these problems. Some useful queries might be things like "11^3 mod 11", "gcd(50,35)" or "inverse of 7 mod 13".

5

Quiz Score: **8.5** out of 10