CSPB 2824 - Stade - Discrete Structures

Started on	Monday, 16 October 2023, 11:01 PM
State	Finished
Completed on	Monday, 16 October 2023, 11:05 PM
Time taken	4 mins 22 secs
Marks	30.00/30.00
Grade	**10.00** out of 10.00 (**100**%)

Question **1**

Correct

Mark 4.00 out of 4.00

Consider the positive integers 189 and 35. Recall that Bezout's Theorem assures us that there exist coefficients s and t ($\in \mathbb{Z}$) such that $\gcd(35, 189) = 189s + 35t$.

Do not include any spaces or decimals in your answer. Only use the digits 0-9 and the "-" sign to enter your answers.

Use the Euclidean Algorithm and Bezout's Theorem as demonstrated during the lectures to determine s and t. **Warning:** These coefficients are **not** unique! If you use guess-and-check, you may find answers which work, but **will be marked as incorrect**, because you did not follow the algorithms demonstrated during class.

What is s?

-2

What is t?

11

Solution:

Euclidean algorithm to obtain gcd(35, 189):

$189 = 35 \cdot 5 + 14$

$35 = 14 \cdot 2 + 7$

$14 = 7 \cdot 2 + 0$

So gcd(35, 189) = 7.

Now we use the Euclidean algorithm in reverse to get the Bezout's Theorem coefficients:

$$\begin{aligned}\gcd(35, 189) = 7 &= 35 - 2 \cdot 14 \\ &= 35 - 2 \cdot (189 - 5 \cdot 35) \\ &= 35 - 2 \cdot 189 + 10 \cdot 35 \\ &= 11 \cdot 35 - 2 \cdot 189\end{aligned}$$

Thus, $s = -2$ and $t = 11$

Correct

Marks for this submission: 4.00/4.00.

Question **2**

Correct

Mark 4.00 out of 4.00

Consider the positive integers 198 and 21. Recall that Bezout's Theorem assures us that there exist coefficients s and t ($\in \mathbb{Z}$) such that $\gcd(198, 21) = 21s + 198t$.

Do not include any spaces or decimals in your answer. Only use the digits 0-9 and the "-" sign to enter your answers.

Use the Euclidean Algorithm and Bezout's Theorem as demonstrated during the lectures to determine s and t. **Warning:** These coefficients are **not** unique! If you use guess-and-check, you may find answers which work, but **will be marked as incorrect**, because you did not follow the algorithms demonstrated during class.

What is s?

19

What is t?

-2

Solution:

Euclidean algorithm to obtain gcd(198, 21):

$198 = 21 \cdot 9 + 9$

$21 = 9 \cdot 2 + 3$

$9 = 3 \cdot 3 + 0$

So gcd(198, 21) = 3.

Now we use the Euclidean algorithm in reverse to get the Bezout's Theorem coefficients:

$$\begin{aligned}\gcd(198, 21) = 3 &= 21 - 2 \cdot 9 \\ &= 21 - 2 \cdot (198 - 9 \cdot 21) \\ &= 21 - 2 \cdot 198 + 18 \cdot 21 \\ &= 19 \cdot 21 - 2 \cdot 198\end{aligned}$$

Thus, $s = 19$ and $t = -2$

Correct

Marks for this submission: 4.00/4.00.

Question **3**

Correct

Mark 2.00 out of 2.00

Recall that the modular inverse of an integer $a \mod m$ is some integer $\bar{a}$ such that $\bar{a}a \equiv 1 \mod m$.

Which of the following are necessarily true?

An inverse of 7 modulo 34 exists. necessarily true

An inverse of 17 modulo 34 exists. not necessarily true

Solution:

34 and 7 are relatively prime, thus an inverse of 7 modulo 34 is guaranteed to exist (Theorem 1, p 275 of Rosen textbook).

17 and 34 are *not* relatively prime, so we cannot conclude that an inverse of 17 modulo 34 exists.

In fact, we can prove that no inverse of 17 (mod 34) exists:

Proof: (by contradiction)

S'pose there exists an integer $\bar{a}$ such that $17\bar{a} \equiv 1 \pmod{34}$ (that is, we suppose that an inverse of 17 (mod 34) exists).

$\Rightarrow 17\bar{a} - 1 = 34k$ (for some integer k)

$$\Rightarrow \bar{a} = \frac{34k+1}{17} = 2k + \frac{1}{17}$$

But then for any integer k, this $\bar{a}$ is not an integer, which contradicts our assumption (since inverses have to be integers here).

Therefore, no inverse of 17 modulo 34 exists.

Correct

Marks for this submission: 2.00/2.00.

Question **4**

Correct

Mark 2.00 out of 2.00

Recall that the modular inverse of an integer $a \mod m$ is some integer $\bar{a}$ such that $\bar{a}a \equiv 1 \mod m$.

Which of the following are necessarily true?

An inverse of 12 modulo 24 exists. not necessarily true

An inverse of 7 modulo 27 exists. necessarily true

Solution:

27 and 7 are relatively prime, thus an inverse of 7 modulo 27 is guaranteed to exist (Theorem 1, p 275 of Rosen textbook).

12 and 24 are *not* relatively prime, so we cannot conclude that an inverse of 12 modulo 24 exists.

In fact, we can prove that no inverse of 12 (mod 24) exists:

Proof: (by contradiction)

S'pose there exists an integer $\bar{a}$ such that $12\bar{a} \equiv 1 \pmod{24}$ (that is, we suppose that an inverse of 12 (mod 24) exists).

$\Rightarrow 12\bar{a} - 1 = 24k$ (for some integer k)

$$\Rightarrow \bar{a} = \frac{24k+1}{12} = 2k + \frac{1}{12}$$

But then for any integer k, this $\bar{a}$ is not an integer, which contradicts our assumption (since inverses have to be integers here).

Therefore, no inverse of 12 modulo 24 exists.

Correct

Marks for this submission: 2.00/2.00.

Question **5**

Correct

Mark 2.00 out of 2.00

For each of these congruences, select which **one** of the following is **not** a solution to the given congruence.

$7x \equiv 4 \mod 5$ 11

$6x \equiv 3 \mod 7$ 40

Solution:

3 is the inverse of 7 (mod 5), so we can solve the first congruence as:

$3 \cdot 7x \equiv 3 \cdot 4 \mod 5$

$\Rightarrow x \equiv 12 \equiv 2 \mod 5$, so anything congruent to 2 (mod 5) is a solution.

2, 7 and -3 are all congruent to 2 (mod 5), so 11 is the answer.

Also note that \(7\cdot 11 = 77 \equiv 2 \bmod{5}$, so 11 does not solve the given congruence.

Similarly, you can note that \)6\cdot 40 = 240 \equiv 2 \bmod{7}$$, so 40 does not solve the second congruence.

Correct

Marks for this submission: 2.00/2.00.

Question **6**

Correct

Mark 2.00 out of 2.00

For each of these congruences, select which **one** of the following is **not** a solution to the given congruence.

$25x \equiv 5 \mod 7$ 9

$4x \equiv 3 \mod 7$ 23

Solution:

2 is the inverse of 25 (mod 7), so we can solve the first congruence as:

$2 \cdot 25x \equiv 2 \cdot 5 \mod 7$

$\Rightarrow x \equiv 10 \equiv 3 \mod 7$, so anything congruent to 3 (mod 7) is a solution.

17, 3 and -4 are all congruent to 3 (mod 7), so 9 is the answer.

Also note that \(25\cdot 9 = 225 \equiv 1 \bmod{7}$, so 9 does not solve the given congruence.

Similarly, you can note that \)4\cdot 23 = 92 \equiv 1 \bmod{7}$$, so 23 does not solve the second congruence.

Correct

Marks for this submission: 2.00/2.00.

Question **7**

Correct

Mark 2.00 out of 2.00

Use Fermat's Little Theorem to Calculate

7^121 **mod** 13

(Could be an exam type question, be able to show your work)

Answer: 7

Correct
Marks for this submission: 2.00/2.00.

Question **8**

Correct

Mark 2.00 out of 2.00

Using Fermat's Little Theorem find

23^(1002) **mod** 41

(Could be an exam type question, be able to show your work. For this quiz question, just provide the integer solution)

Answer: 37

Correct
Marks for this submission: 2.00/2.00.

Question **9**

Correct

Mark 5.00 out of 5.00

Suppose Mehmet and Nihar want to create some RSA private and public keys so they can talk smack about Sriram and Chris without their knowledge. Use your newfound knowledge of RSA cryptosecurity to help them go about their devious task!

Let's start by helping Mehmet develop his public and private keys.

The first step in RSA is for Mehmet to pick two large primes p and q, which will give our encryption/decryption modulus $n = pq$. Suppose Mehmet picks $p = 23$ and $q = 47$, so $n = 1081$.

Next, Mehmet needs to select his public encryption key, e, so Nihar will know how to encrypt a message to send him. What do we need to be true of e? B

A. e must be relatively prime to pq
B. e must be relatively prime to $(p-1)(q-1)$
C. e must be a factor of both p and q
D. e must be prime

Mehmet selects $e = 27$. Mehmet publicly posts his RSA public key, (e, n), and now Nihar (or anyone!) can encrypt messages to send to Mehmet! Remember that to encrypt a message whose numerical value is M (where A is 00, B is 01, ... , Z is 25), Nihar would calculate the encrypted character C's numerical value as $C = M^e \bmod n$.

Now things get interesting. Nihar can encrypt messages to his heart's content, but Sriram and Chris might intercept the messages. Chris would be devastated to learn that Nihar thinks Sriram's chili recipe is superior to Chris'. Thank goodness Mehmet and Nihar are clever and kind enough to save Chris this embarrassment. Even if Siram and Chris intercept the CAs' messages, they would need to know the **decryption key** d in order to do this.

In words, what is the decryption key d? F

E. the inverse of e modulo n
F. the inverse of e modulo $(p-1)(q-1)$
G. the inverse of e modulo $n-1$
H. the inverse of e modulo $p+q$

This demonstrates the power of RSA: Mehmet can pass around the encryption key (e, n) to everyone, and everyone can encrypt and send messages to him with knowledge of n and e. But in order to *decrypt* a message, one would need to know the two primes that went into constructing n: p and q. And only Mehmet knows those! For the rest of us, if he chooses p and q large enough, it would be prohibitively computationally expensive to crack the code by brute force attacks (i.e., trying to factor n into p and q).

Finally, as a teaching tool, Mehmet pretends to have forgotten all the super cool number theory he learned in his glory days as a CSCI 2824 student himself, and asks for your help to calculate the decryption key d. Use the Euclidean Algorithm and Bezout's Theorem to calculate d.

$d =$ 75

Solution:

The encryption key \(e\) must be relatively prime to \((p-1)(q-1)\). This ensures that the inverse of \(e\) modulo \((p-1)(q-1)\) exists.

The decryption key \(d\) is the inverse of \(e\) modulo \((p-1)(q-1)\) (which we know exists because \(e\) is relatively prime to \((p-1)(q-1)\).

Calculating \(d\) using Euclidean Algorithm and "Reverse Euclidean Algorithm"/Bezout's Theorem:

\((p-1)(q-1) = 22\cdot 46 = 1012\), and want inverse of \(27\) modulo 1012. Here we go!

\(1012 = 27\cdot 37 + 13\)

\(27 = 13\cdot 2 + 1\)

\(13 = 1\cdot 13 + 0\)

So gcd(27,1012) = 1 (as expected), and we climb back out (Reverse Euclidean Algorithm) to find the Bezout Theorem coefficient on 27:

\(1 = 27 - 2\cdot 13\)

\(= 27 - 2\cdot(1012 - 37\cdot 27)\)

\(= 27 - 2\cdot 1012 + 37\cdot 27\)

\(= 75\cdot 27 - 2\cdot 1012\)

So \(d=75\)

Correct

Marks for this submission: 5.00/5.00.

Question **10**

Correct

Mark 1.00 out of 1.00

Modular inverses, and the results of running the Extended Euclidean Algorithm to find them, can be a negative integer.

Select one:

- (•) True
- ( ) False

Correct

Marks for this submission: 1.00/1.00.

Question **11**

Correct

Mark 1.00 out of 1.00

(After completing the first part of the Mastery Workbook)

If you find a negative modular inverse, how can you create positive modular inverse that works just as well?

- a. Keep adding the modulo m to the inverse you found until you until you reach a positive integer. Since Modular inverses are unique mod m (m the modulus you are using) this new integer will work just as well.
- b. Modular inverse are unique, they cannot be changed.
- c. Just put a negative sign in front of your modular inverse.
- d. Multiply the modular inverse you have found by its additive inverse.
- e. Multiply the modular inverse you have found by its multiplicative inverse.

Your answer is correct.

Correct

Marks for this submission: 1.00/1.00.

Question **12**

Correct

Mark 1.00 out of 1.00

When coding RSA, we need to use a positive modular inverse when creating the RSA keys.

Why?

(See the example 9, Rosen page 301)

- a. Positive integers are just better.
- b. In the RSA algorithm we use a modular inverse as an exponent as part of the decryption. If the modular inverse is negative this would return a non-integer result - which would not 'unlock the code.'
- c. This is not true, a negative modular inverse is just fine.
- d. Because there is only one modular inverse that works.

Your answer is correct.

Correct

Marks for this submission: 1.00/1.00.

Question **13**

Correct

Mark 1.00 out of 1.00

Hypothetically, if you were coding a large RSA Project, would you want to make sure the modular inverse you return using the Extended Euclidean Algorithm is positive?

- a. Yes! It's great to return values that will function properly.
- b. No, I love having my code only work sometimes. It's exciting to wonder if it will work or not.

Your answer is correct.

Correct

Marks for this submission: 1.00/1.00.

Question **14**

Correct

Mark 1.00 out of 1.00

A simple way to make sure your RSA EEA returns a positive value is to add a simple loop.

Select one:

- True
- False

Correct

Marks for this submission: 1.00/1.00.