CS111 Fall'24 ASSIGNMENT 2

Problem 1:

Prove the following statement:
If $p > 5$ is a prime integer, then $(p^2 + 59)(p^2 - 4) \equiv 0 \pmod{60}$.

To receive full credit, you must use the method based on the following property of integers:
The product of any k consecutive integers is divisible by k.

For small extra credit, you can also show how this statement can be proved using the method of arguing by cases.

In order to prove the statement above using the property of integers, we must do the following:

- Express 60 in terms of Prime Factors: $60 = 2^2 * 3 * 5$

- Show that $(p^2 + 59)(p^2 - 4)$ is divisible by 2, 3, and 5:

  - Since p is an odd prime because 2 is the only even prime and $p > 5$, we have $p^2 \equiv 1 \pmod 2$. Now, $p^2 + 59 \equiv 1 + 1 \equiv 0 \pmod 2$ and $p^2 - 4 \equiv 1 - 1 \equiv 0 \pmod 2$. Since we see that both terms are divisible by 2, their product is also divisible by $2^2 = 4$.

  - Next, for any $p > 3$, p must be congruent to either 1 or 2 $\pmod 3$ since 3 is prime and isn't divisible by 3. Since $p^2 \equiv 1 \pmod 3$, $p^2 + 59 \equiv 1 + 2 \equiv 0 \pmod 3$ and $p^2 - 4 \equiv 1 - 1 \equiv 0 \pmod 3$. If $p \equiv 2 \pmod 3$ then $p^2 \equiv 4 \equiv 1 \pmod 3$, proving that both equations hold true.

  - Lastly, for any $p > 5$, p is congruent to 1,2,3, or 4 $\pmod 5$. Since $p^2 \equiv 1 \pmod 5$, it leads for $p^2 + 59 \equiv 1 + 59 \equiv 0 \pmod 5$ and $p^2 - 4 \equiv 4 - 4 \equiv 0 \pmod 5$, leading to the product being $0 \pmod 5$. For $p \equiv 2 \pmod 5$, we have $p^2 \equiv 4 \pmod 5$ which allows for $p^2+59 \equiv 4+59 \equiv 3 \pmod 5$ and $p^2-4 \equiv 4-4 \equiv 0 \pmod 5$, leading to a product of $0 \pmod 5$. For $p \equiv 3 \pmod 5$, we have $p^2 \equiv 9 \equiv 4 \pmod 5$, which actually reduces to to our previous case. And, for $p \equiv 4 \pmod 5$, we have $p^2 \equiv 16 \equiv 1$, which also reduces to our $p \equiv 1 \pmod 5$ case, leading to conclude that one of our factors is divisible by 5.

- Since we have proven that $(p^2 + 59)(p^2 - 4)$ is divisible by 4,3, and 5, it is divisible by $60 = 2^2 * 3 * 5$, which also proves that $(p^2 + 59)(p^2 - 4) \equiv 0 \pmod{60}$.

Problem 2:

Alice's RSA public key is $P = (e, n) = (7, 4453)$. Bob sends Alice the message by encoding it as follows. First he assigns numbers to characters: A is 7, B is 8, ..., Z is 32, a blank is 33, quotation marks: 34, a coma: 35, a period: 36, an apostrophe: 37. Then he uses RSA to encode each number separately.

Bob's encoded message is:

1400	2218	99	2088	4191	84	843	99	4191	3780	764	4191	2979	2269	99	764
2218	2269	2088	843	3015	99	2970	1443	1655	99	3237	2979	99	447	1443	3237
1032	2382	871	843	1655	99	871	1443	99	4242	843	99	4191	2269	99	843
4191	2269	2979	99	871	1443	99	2382	2269	843	99	4191	2269	99	3237	2979
99	871	843	3780	843	1032	2088	1443	2962	843	2916	99	3237	2979	99	764
2218	2269	2088	99	2088	4191	2269	99	447	1443	3237	843	99	871	1655	2382
843	99	4242	843	447	4191	2382	2269	843	99	2218	99	447	4191	2962	99
2962	1443	99	3780	1443	2962	1294	843	1655	99	2970	2218	1294	2382	1655	843
99	1443	2382	871	99	2088	1443	764	99	871	1443	99	2382	2269	843	99
3237	2979	99	871	843	3780	843	1032	2088	1443	2962	843	2916	1400		

Decode Bob's message. Notice that you only know Alice's public key, but don't know the private key. So you need to "break" RSA to decrypt Bob's message. For the solution, you need to provide the following:

(a) Describe step by step how you arrived at the solution: show how to find p and q, $\phi(n)$ and d.

(b) Show your work for one integer in the message (C = 2218): the expression, the decrypted integer, the character that it is mapped to.

(c) To decode the remaining numbers, you need to write a program in C++ (see below) and test it in Gradescope.

(d) Give the decoded message (in integers).

(e) Give Bob's message in plaintext. What does it mean and who said it?

For part (c). Your program should :

(i) Take three integers, e, n (the public key for RSA), and m (the number of characters in the message) as input to your program. Next, input the ciphertext.

(ii) Test whether the public key is valid. If not, output a single line "Public key is not valid!" and quit the program.

(iv) If the public key is valid, decode the message.

(v) Output p and q, $\phi(n)$ and d.

(vi) On a new line, output the decoded message in integers.

(vii) On a new line, output the decoded message in English. The characters should be all uppercase. You can assume that the numbers will be assigned to characters according to the mapping above.

More information and specifications will be provided separately.

Upload your code to Gradescope to test. There will be 15-16 (open and hidden) test cases. Your score for the RSA code will be based on the score that you received in Gradescope. If you have any questions, post them on Slack.

Problem 3:

(a) Compute $5^{1257} \pmod{12}$. Show your work.

- Using modular exponentiation, we find that $5^{1257} \equiv 5^1 \equiv 5 \pmod{12}$. This is true because the power of $5 \pmod{12}$ cycles as shown and it repeats every 2 powers. Computing for 1257, this proves true.

(b) Compute $8^{-1} \pmod{17}$ by listing the multiples. Show your work.

- We solve this by rewriting the equation to $8x \equiv 1 \pmod{17}$ finding that $x = 15$ since $8 * 5 = 120 \equiv 1 \pmod{17}$

(c) Compute $8^{-1} \pmod{17}$ using Fermat's Little Theorem. Show your work.

- By Fermat's Little Theorem, we compute $8^{15} \equiv 15 \pmod{17}$, leading to prove that $x = 15$.

(d) Compute $8^{-11} \pmod{17}$ using Fermat's Little Theorem. Show your work.

- By Fermat's Little Theorem, we find that $8^6 = 262144 \equiv 2 \pmod{17}$, leading to $8^{-11} \equiv 2 \pmod{17}$.

(e) Find an integer x, $0 \leq x \leq 40$, that satisfies the following congruence: $-9x + 14 \equiv 16 \pmod{41}$. Show your work. You should not use brute force approach.

- After rearranging the equation, we find $-9x \equiv 2 \pmod{41}$ and finding the modular inverse of $-9 \pmod{41}$ which is 29, leading to $x \equiv 2 * 29 \equiv 58 \equiv 34 \pmod{41}$

Academic integrity declaration. The homework papers must include at the end an academic integrity declaration. This should be a brief paragraph where you state *in your own words* (1) whether you did the homework individually or in collaboration with a partner student (if so, provide the name), and (2) whether you used any external help or resources.

Submission. To submit the homework, you need to upload the pdf and cpp files to Gradescope. If you submit with a partner, you need to put two names on the assignment and submit it as a group assignment.

Reminders. Remember that only LaTeX papers are accepted.