CS111 Spring'25 ASSIGNMENT 2

Problem 1:
Prove the following statement:
If $p > 5$ is a prime number, then $(p^2 - 1)(p^2 + 5p + 126) \equiv 0 \pmod{120}$.

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 $k!$.

Highest Degree = 4, since we need 5 consecutive integers, we can insert an extra p in this case in order for the proof to be true after factoring out.

Solution 1: We need to show that $(p^2 - 1)(p^2 + 5p + 126) \equiv 0 \pmod{120}$.
Given that

$$(p^2 - 1)(p^2 + 5p + 126) \equiv (p^2 - 1)(p^2 + 5p + 6) \pmod{120},$$

it suffices to prove that $(p^2 - 1)(p^2 + 5p + 6)$ is divisible by 120.

Since $120 = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 = 5!$, we will show that the product above is divisible by 5!.

Key observation: Rewrite $(p^2 - 1)(p^2 + 5p + 6)$ by factoring:

$$\begin{aligned}(p^2 - 1)(p^2 + 5p + 6) &= (p - 1)(p + 1) \cdot (p + 2)(p + 3) \\ &= (p - 1)(p + 1)(p + 2)(p + 3)\end{aligned}$$

Inserting the extra p: If we multiply the expression $(p - 1)(p + 1)(p + 2)(p + 3)$ by p, we get:

$$(p - 1)p(p + 1)(p + 2)(p + 3)$$

which is the product of 5 consecutive integers.

By the given property, the product of any 5 consecutive integers is divisible by $5! = 120$. Therefore:

$$(p - 1)p(p + 1)(p + 2)(p + 3) \equiv 0 \pmod{120}$$

Removing the factor of p: Since $p > 5$ is prime, p is not divisible by any of the prime factors of $120 = 2^3 \cdot 3 \cdot 5$.

This means that $\gcd(p, 120) = 1$, so all the prime factors of 120 must be distributed among the remaining factors: $(p - 1), (p + 1), (p + 2), (p + 3)$.

Therefore, $(p - 1)(p + 1)(p + 2)(p + 3)$ is divisible by 120.

Conclusion: Since $(p^2 - 1)(p^2 + 5p + 6) = (p - 1)(p + 1)(p + 2)(p + 3)$ is divisible by 120, and

$$(p^2 - 1)(p^2 + 5p + 126) \equiv (p^2 - 1)(p^2 + 5p + 6) \pmod{120},$$

we conclude that:

$$(p^2 - 1)(p^2 + 5p + 126) \equiv 0 \pmod{120}$$

Problem 2:

Alice's RSA public key is $P = (e, n) = (7, 6557)$. Bob sends Alice the message by encoding it as follows. First he assigns numbers to characters: A is 5, B is 6, ..., Z is 30, a blank is 31, quotation marks: 32, a coma: 33, a period: 34, an apostrophe: 35. Then he uses RSA to encode each number separately. Bob's encoded message is:

```
2691 4584  575 6013 1473 2916 1828 1473 4990 2916 6013
5469 1828 6013 6056 1828  735 6013 4542 2916 4990 4584
2916 3179 2916 6013  735 4360 5998  735 6013 1613 5998
 735 4360 2916 1613 5998  735 4584 3918 4842 6013 4584
4842 6013 4842 4584 1613 1473 4990 2916 1875 6013 4584
 735 6013 4584 4842 6013 1828 6056 4990 2660 6013 4542
2916 3918 5998 4302 4842 2916 6013  735 4360 2916 2660
6013 5469 1828 6013 6056 1828  735 6013 2961 2916 5998
4990 4584 5138 2916 6013 4360
1828 3888 6013 3918 1828
1613 1473 4990 4584 3918 5998  735 2916 5469 6013 4990
4584  575 2916 6013 4584 4842 3197 2691
```

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 = 4584): the expression, the calculations, 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 16-18 (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.

Solution 2: The public key is $P = (e, n) = (7, 6557)$. We must find the private key d by factoring n.
(a) 1. Factor n to find p and q: We test prime divisors starting from 2 up to $\sqrt{6557} \approx 80.97$.

- 6557 is not divisible by 2, 3, or 5.
- $6557/7 \approx 936.7$
- $6557/11 \approx 596.09$
- ...
- Testing prime 79: $6557/79 = 83$ exactly.
- We verify that both 79 and 83 are prime.
- Therefore, $\mathbf{p = 79}$ and $\mathbf{q = 83}$.

2. Calculate $\phi(n)$: The Euler's totient function is $\phi(n) = (p-1)(q-1)$.

$$\phi(n) = (79-1)(83-1) = 78 \times 82 = \mathbf{6396}$$

3. Find Private Key d: d is the modular inverse of $e = 7$ modulo $\phi(n) = 6396$. We need $d \equiv 7^{-1} \pmod{6396}$. Using the Extended Euclidean Algorithm:

$$\begin{aligned} 6396 &= 913 \times 7 + 5 \\ 7 &= 1 \times 5 + 2 \\ 5 &= 2 \times 2 + 1 \\ 2 &= 2 \times 1 + 0 \end{aligned}$$

Working backwards to express 1 as a linear combination:

$$\begin{aligned} 1 &= 5 - 2 \times 2 \\ 1 &= 5 - 2 \times (7 - 1 \times 5) \\ 1 &= 5 - 2 \times 7 + 2 \times 5 \\ 1 &= 3 \times 5 - 2 \times 7 \\ 1 &= 3 \times (6396 - 913 \times 7) - 2 \times 7 \\ 1 &= 3 \times 6396 - 2739 \times 7 - 2 \times 7 \\ 1 &= 3 \times 6396 - 2741 \times 7 \end{aligned}$$

Therefore, $-2741 \times 7 \equiv 1 \pmod{6396}$, which means:

$$d \equiv -2741 \equiv 6396 - 2741 = 3655 \pmod{6396}$$

$$\mathbf{d = 3655}$$

(b) We decrypt $C = 4584$ using the formula $M \equiv C^d \pmod{n}$.

$$\text{Expression:} \quad M \equiv 4584^{3655} \pmod{6557}$$

We use the Exponentiation by Squaring method.

$$\text{Calculations:} \quad M = 4584^{3655} \text{ rem } 6557$$

$$\text{Decrypted Integer:} \quad M = \mathbf{13}$$

$$\text{Mapped Character:} \quad \text{Since A=5, the character is } 'A' + (13-5) =' A' + 8 = \mathbf{I}$$

Problem 3:

(a) Compute $5^{1257} \pmod{12}$ using the exponentiation by squaring method. Show your work.

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

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

(d) Compute $8^{721803} \pmod{19}$ using Fermat's Little Theorem. Show your work.

(e) Find an integer x, $0 \leq x \leq 40$, that satisfies the following congruence: $-9x + 45 \equiv 6 \pmod{41}$. Show your work. You should not use brute force approach.

Solution 3:

(a)

We note that $5^2 = 25 \equiv 1 \pmod{12}$. The exponent 1257 in binary is 10011101001_2.

$$1257 = 1024 + 128 + 64 + 32 + 8 + 1$$

$$\begin{aligned} 5^{1257} &\equiv 5^{1024} \cdot 5^{128} \cdot 5^{64} \cdot 5^{32} \cdot 5^{8} \cdot 5^{1} \pmod{12} \\ &\equiv 1 \cdot 1 \cdot 1 \cdot 1 \cdot 1 \cdot 5 \pmod{12} \quad (\text{since } 5^{2^k} \equiv 1 \text{ for } k \geq 1) \\ &\equiv 5 \pmod{12} \end{aligned}$$

Result: $5^{1257} \equiv \mathbf{5} \pmod{12}$.

(b)

We seek x such that $8x \equiv 1 \pmod{17}$. We list multiples of 8 mod 17:

- $8 \times 1 = 8$
- $8 \times 2 = 16 \equiv -1$
- $8 \times 3 \equiv -1 + 8 = 7$
- ...
- Since $8 \times 2 \equiv -1 \pmod{17}$, multiplying by -1 will give 1: $(-1) \cdot (-1) \equiv 1 \pmod{17}$. The inverse of 2 is $-1 \equiv 16 \pmod{17}$. Thus, we need $x \equiv 2 \cdot 16 = 32 \equiv 15 \pmod{17}$. Check: $8 \times 15 = 120$. $120 = 7 \cdot 17 + 1$. $120 \equiv 1 \pmod{17}$.

Result: $8^{-1} \equiv \mathbf{15} \pmod{17}$.

(c)

By Fermat's Little Theorem (FLT), since 17 is prime and $\gcd(8, 17) = 1$, we have $8^{17-1} \equiv 8^{16} \equiv 1 \pmod{17}$. We simplify the negative exponent using the identity $a^k \equiv a^{k+\phi(p)} \pmod{p}$:

$$8^{-11} \equiv 8^{-11+16} \equiv 8^5 \pmod{17}$$

Now we compute $8^5 \pmod{17}$:

- $8^2 \equiv 64 \equiv 13 \equiv -4 \pmod{17}$
- $8^4 \equiv (-4)^2 = 16 \equiv -1 \pmod{17}$

- $8^5 = 8^4 \cdot 8^1 \equiv (-1) \cdot 8 = -8 \pmod{17}$

Since $-8 \equiv 17 - 8 = 9 \pmod{17}$.
Result: $8^{-11} \equiv \mathbf{9} \pmod{17}$.

(d)
By FLT, since 19 is prime and $\gcd(8, 19) = 1$, we have $8^{19-1} \equiv 8^{18} \equiv 1 \pmod{19}$. We first reduce the exponent 721803 modulo 18:

$$721803 \pmod{18}$$

Since 721800 is divisible by 18 ($721800/18 = 40100$), we have:

$$721803 = 721800 + 3 \equiv 0 + 3 \equiv 3 \pmod{18}$$

Now we simplify the expression:

$$8^{721803} \equiv 8^{18k+3} \equiv (8^{18})^k \cdot 8^3 \equiv 1^k \cdot 8^3 \equiv 8^3 \pmod{19}$$

Finally, we compute $8^3 \pmod{19}$:

- $8^2 = 64$. $64 = 3 \cdot 19 + 7$, so $8^2 \equiv 7 \pmod{19}$.
- $8^3 = 8^2 \cdot 8 \equiv 7 \cdot 8 = 56 \pmod{19}$.
- $56 = 2 \cdot 19 + 18$, so $56 \equiv 18 \pmod{19}$.

Since $18 \equiv -1 \pmod{19}$.
Result: $8^{721803} \equiv \mathbf{18} \pmod{19}$.

(e)
Simplify the congruence:

$$\begin{aligned} -9x + 45 &\equiv 6 \pmod{41} \\ -9x &\equiv 6 - 45 \pmod{41} \\ -9x &\equiv -39 \pmod{41} \end{aligned}$$

Substitute the positive equivalents for coefficients modulo 41:

$$(-9 \equiv 32) \quad \text{and} \quad (-39 \equiv 2)$$

$$32x \equiv 2 \pmod{41}$$

Find the inverse of 32 modulo 41 using the Extended Euclidean Algorithm:

$$\begin{aligned} 41 &= 1 \cdot 32 + 9 \\ 32 &= 3 \cdot 9 + 5 \\ 9 &= 1 \cdot 5 + 4 \\ 5 &= 1 \cdot 4 + 1 \end{aligned}$$

Working backwards yields $9 \cdot 32 - 7 \cdot 41 = 1$, so $32^{-1} \equiv 9 \pmod{41}$. Multiply the congruence by 9:

$$9 \cdot 32x \equiv 9 \cdot 2 \pmod{41}$$

$$1x \equiv 18 \pmod{41}$$

The solution is $x = 18$.
Result: $x = \mathbf{18}$.

Academic integrity declaration. The homework papers must include at the end an academic integrity declaration. In this statement each group member must summarize briefly, in their own words, their contributions to the homework. (This will not affect the grades.) Each group member must also state that he/she verified and has full understanding of all solutions in the submission. In addition, you need to state whether and how you used any external help or resources.

For this assignment, I used a couple of resources in order to answer the questions above which include the following:

- The lecture notes specifically on number theory and RSA
- GeeksforGeeks articles on modular arithmetic and RSA algorithm
- Khan Academy videos on modular arithmetic and Fermat's Little Theorem
- https://www.youtube.com/watch?v=OoQ16YCYksw and https://www.youtube.com/watch?v=2tpSU7BJFMI
- Google Gemini to help with formatting of the document and debugging code snippets

Submission. To submit the homework, you need to upload the pdf file to Gradescope. If you submit for a group, you need to put all member names on the assignment and submit it as a group assignment.

Reminders. Remember that only LaTeX papers are accepted.