CS111 Fall'25 ASSIGNMENT 2

Solution 1: 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!.
Let's rewrite $(p^2-1)(p^2+5p+6)$ as $(p-1)(p+1)(p+2)(p+3)$. If we multiply the last expression by p, we get the product of 5 consecutive integers: $(p-1)p(p+1)(p+2)(p+3)$. Therefore, this product is divisible by 5!. We also know that p is prime and $p > 5$, so it's not divisible by any of the factors of 120. Thus, all the prime factors of 120 are among $(p-1), (p+1), (p+2), (p+3)$, and so $(p^2-1)(p^2+5p+6)$ is divisible by $5! = 120$. That proves the original statement.

Solution 2:

1. Start by factoring $n = 6557 : n = 79 \cdot 83$. So the secret primes are $p = 61, q = 73$.
2. This gives us $\phi(n) = (p-1)(q-1) = 78 \cdot 82 = 6396$.
3. Then we can compute the secret exponent d:

$$\begin{aligned} d &\equiv e^{-1} \pmod{\phi(n)} \\ de &\equiv 1 \pmod{\phi(n)} \\ 7d &\equiv 1 \pmod{6396} \end{aligned}$$

   Then 7d = 6396b + 1 (for some int. $b \neq 0$)
   7d = 7, 14, 21,...,25585
   6396b + 1 = 6397, 12793, ... 25585

   From 7d = 25585, we find $d = 3655$

4. To decrypt 4584, we do the following:

$$\begin{aligned} 4584^{3655} \pmod{6557} &= 4584 \cdot 4584^{3654} \mod 6557 \\ &= 4584 \cdot (4584^2)^{1827} && \text{mod } 6557 \\ &= 4584 \cdot (4428)^{1827} && \text{mod } 6557 \\ &= 4584 \cdot 4428 \cdot (4428^2)^{913} && \text{mod } 6557 \\ &= 4584 \cdot 4428 \cdot 1754 \cdot (1754^2)^{456} && \text{mod } 6557 \\ &\vdots \\ &= 13 \text{ mod } 6557 \end{aligned}$$

   13 corresponds to the letter I.

   With d, we can decrypt all numbers, which gives us the original message:

```
32 13 10 31 20  9 19 20 16  9 31  8 19 31 18 19 24
31  6  9 16 13  9 26  9 31 24 12  5 24 31 17  5 24
12  9 17  5 24 13  7 23 31 13 23 31 23 13 17 20 16
 9 33 31 13 24 31 13 23 31 19 18 16 29 31  6  9  7
 5 25 23  9 31 24 12  9 29 31  8 19 31 18 19 24 31
22  9  5 16 13 30  9 31 12 19 27 31  7 19 17 20 16
13  7  5 24  9  8 31 16 13 10  9 31 13 23 34 32
```

”IF PEOPLE DO NOT BELIEVE THAT MATHEMATICS IS SIMPLE, IT IS ONLY BECAUSE THEY DO NOT REALIZE HOW COMPLICATED LIFE IS.” - John von Neumann.

Solution 3:
(a)

$$\begin{aligned} 5^{1257} &\equiv 5 \cdot (5^2)^{628} \\ &\equiv 5 \cdot (1)^{628} \equiv 5 \pmod{12} \end{aligned}$$

(b) We want to find integers a, b such that $8a = 17b + 1$.
Multiples of 8: $8, 16 \cdots, 120$
Multiples of $17b + 1$: $18, 35, 52, 69, 86, 103, 120$
So $a = 15$.
Thus, $8^{-1} \equiv 15 \pmod{17}$

(c) By Fermat's Little Theorem: $8^{16} \equiv 1 \pmod{17}$. Then:

$$\begin{aligned} 8^{-11} &\equiv 8^{-11} \cdot 8^{16} \equiv 8^5 \equiv 8 \cdot 64^2 \equiv 8 \cdot 13^2 \equiv 8 \cdot (-4)^2 \equiv 8 \cdot 16 \\ &\equiv 128 \equiv 9 \pmod{17} \end{aligned}$$

(d) By Fermat's Little Theorem: $8^{18} \equiv 1 \pmod{19}$. We have:

$$8^{721803} \equiv (8^{18})^{40100} \cdot 8^3 \equiv 8^3 \equiv 512 \equiv 18 \pmod{19}$$

(e) We have:

$$\begin{aligned} -9x + 45 &\equiv 6 \pmod{41} \\ 9x &\equiv 39 \pmod{41} \\ 9^{-1} \cdot 9x &\equiv 9^{-1} \cdot (-2) \pmod{41} \\ x &\equiv 9^{-1} \cdot (-2) \pmod{41} \end{aligned}$$

By Fermat's Little Theorem: $9^{40} \equiv 1 \pmod{41}$

$$\begin{aligned} 9^{-1} &\equiv 9^{40} \cdot 11^{-1} \\ &\equiv 9^{39} \\ &\equiv 9 \cdot 9^{38} \equiv 9 \cdot 81^{19} \\ &\equiv 9 \cdot (-1)^{19} \equiv 9 \cdot (-1) \\ &\equiv -9 \equiv 11 \cdot 32 \pmod{19} \end{aligned}$$

Finally:

$$x \equiv 32 \cdot (-2) \equiv -64 \equiv 18 \pmod{41}$$

Academic integrity declaration. The homework papers must include at the end an academic integrity declaration. In this statement all 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.

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.