1) [12 points] Use the *Extended Euclidean Algorithm* to write the GCD of 87 and 51 as a linear combination of themselves. *Show the computations explicitly!* [**Hint:** You should get 3 for the GCD!]

Solution. We have

$$\begin{aligned} 87 &= 1 \cdot 51 + 36 \\ 51 &= 1 \cdot 36 + 15 \\ 36 &= 2 \cdot 15 + 6 \\ 15 &= 2 \cdot 6 + \boxed{3} \\ 6 &= 2 \cdot 3 + 0 \end{aligned}$$

So,

$$\begin{aligned} 3 &= 15 - 2 \cdot 6 \\ &= 15 - 2 \cdot (36 - 2 \cdot 15) \\ &= (-2) \cdot 36 + 5 \cdot 15 \\ &= (-2) \cdot 36 + 5 \cdot (51 - 36) \\ &= 5 \cdot 51 + (-7) \cdot 36 \\ &= 5 \cdot 51 + (-7) \cdot (87 - 51) \\ &= \boxed{(-7)} \cdot 87 + \boxed{12} \cdot 51. \end{aligned}$$

□

2) [12 points] Find the remainder of the division of 3^{222} when divided by 7 [i.e., what is 3^{222} congruent to modulo 7]. *Show your computations explicitly!*

Solution. We have:

$$\begin{aligned} 222 &= 31 \cdot 7 + \boxed{5} \\ 31 &= 4 \cdot 7 + \boxed{3} \\ 4 &= 0 \cdot 7 + \boxed{4}. \end{aligned}$$

So, $222 = 5 + 3 \cdot 7 + 4 \cdot 7^2$. Hence,

$$3^{222} \equiv 3^{5+3+4} = 3^{12} \pmod 7.$$

Now, $12 = 5 + 1 \cdot 7$, so

$$3^{222} \equiv 3^{12} \equiv 3^{5+1} = 3^6 = (3^2)^3 = (9)^3 = 2^3 = 8 \equiv 1 \pmod 7.$$

□

3) [12 points] Give the set of all solutions of the system

$$\begin{aligned} 2x &\equiv 4 \pmod{5} \\ x &\equiv 3 \pmod{13} \end{aligned}$$

Solution. We first solve for x in first equation. Note that $3 \cdot 2 \equiv 1 \pmod{5}$, so, multiplying the first equation by 3, we get

$$x \equiv 12 \equiv 2 \pmod{5}.$$

Hence, we get the system:

$$\begin{aligned} x &\equiv 2 \pmod{5} \\ x &\equiv 3 \pmod{13} \end{aligned}$$

Now, since $(5, 13) = 1$, we can apply the *Chinese Remainder Theorem*: we have $1 = 2 \cdot 13 + (-5) \cdot 5$. So, $x = 2 \cdot 13 \cdot 2 + (-5) \cdot 5 \cdot 3 = -23$ is a common solution. Hence, all solutions are of the form $-23 + 65k$, for $k \in \mathbb{Z}$.

□

4) [12 points] If we have that

$$7^{12} \equiv 1 \pmod{720}$$

then, what is the remainder of the division of 7^{122} when divided by 720?

Solution. We have

$$7^{122} = 7^{12 \cdot 10 + 2} = (7^{12})^{10} \cdot 7^2 \equiv 1^{10} \cdot 49 \equiv 49 \pmod{720}.$$

So, the remainder is 49. □

5) LCM and GCD:

(a) [6 points] Let $a = 2^3 \cdot 5^4 \cdot 11$ and $b = 3^2 \cdot 5^2 \cdot 7 \cdot 11$. Find (a, b) [the GCD] and $[a, b]$ [the LCM]. [You can leave powers and products indicated.]

Solution. We have:

$$(a, b) = 2^0 \cdot 3^0 \cdot 5^2 \cdot 7^0 \cdot 11,$$
$$[a, b] = 2^3 \cdot 3^2 \cdot 5^4 \cdot 7 \cdot 11.$$

□

(b) [6 points] If $a = 14$, $(a, b) = 7$ and $[a, b] = 42$, then what is b? [Justify!]

Solution. We have that

$$ab = (a, b) \cdot [a, b].$$

So,

$$b = \frac{(a, b) \cdot [a, b]}{a} = \frac{7 \cdot 42}{14} = 21.$$

□

6) [12 points] Prove that for all integers a and b, we have $(a, b) = (a, a - b)$.

Proof. Suffices to show that a and b have exactly the same common divisors as a and $a - b$, as then their greatest common divisors must coincide. So, we prove that $d \mid a$ and $d \mid b$ if and only if $d \mid a$ and $d \mid (a - b)$.
So, suppose that $d \mid a$ and $d \mid b$. By our old lemma, we have that $d \mid (a - b)$. Since also $d \mid a$ [by assumption], we are done [with this part].
Now, assume that $d \mid a$ and $d \mid (a - b)$. Then, by our old lemma [again], we have that $d \mid (a - (a - b)) = b$, so $d \mid b$. Since also $d \mid a$ [by assumption], we are done [with this part too]. □