1) [20 points] Use the *Extended Euclidean Algorithm* to write the GCD of 210 and 77 as a linear combination of themselves. *Show the computations explicitly!* [**Hint:** You should get 7 for the GCD!]

Solution. We have:

$$\begin{aligned} 210 &= 77 \cdot 2 + 56 \\ 77 &= 56 \cdot 1 + 21 \\ 56 &= 21 \cdot 2 + 14 \\ 21 &= 14 \cdot 1 + 7 \\ 14 &= \boxed{7} \cdot 2 + 0 \end{aligned}$$

Now:

$$\begin{aligned} 7 &= 21 - 14 = 21 - (56 - 2 \cdot 21) \\ &= 3 \cdot 21 - 56 = 3 \cdot (77 - 56) - 56 \\ &= 3 \cdot 77 - 4 \cdot 56 = 3 \cdot 77 - 4 \cdot (210 - 2 \cdot 77) \\ &= 11 \cdot 77 - 4 \cdot 210. \end{aligned}$$

□

2) [10 points] Let

$$\begin{aligned} m &= 2^a \cdot 3^5 \cdot 5^b \cdot 7, \\ n &= 3^c \cdot 5 \cdot 7^d, \end{aligned}$$

where $a, b, c, d \in \mathbb{Z}_{\geq 0}$. If $(m, n) = 3^2 \cdot 7$ and $[m, n] = 2 \cdot 3^5 \cdot 5 \cdot 7^3$, then find a, b, c and d. [Justify!]

Solution. We have:

$$(m, n) = 2^{\min\{a,0\}} \cdot 3^{\min\{5,c\}} \cdot 5^{\min\{b,1\}} \cdot 7^{\min\{1,d\}} = 2^0 \cdot 3^2 \cdot 5^0 \cdot 7^1.$$

By unique factorization, we get:

$$\begin{aligned} &\min\{a, 0\} = 0, \\ &\min\{5, c\} = 2, \text{ and hence } c = 2, \\ &\min\{b, 1\} = 0, \text{ and hence } b = 0, \\ &\min\{1, d\} = 1. \end{aligned}$$

Similarly, We have:

$$[m, n] = 2^{\max\{a,0\}} \cdot 3^{\max\{5,c\}} \cdot 5^{\max\{b,1\}} \cdot 7^{\max\{1,d\}} = 2^1 \cdot 3^5 \cdot 5^1 \cdot 7^3.$$

By unique factorization, we get:

$$\begin{aligned}\max\{a,0\} &= 1, \text{ and hence } a=1,\\ \max\{5,c\} &= 5, \text{ [OK, since } c=2],\\ \max\{b,1\} &= 1, \text{ [OK, since } b=0],\\ \max\{1,d\} &= 3, \text{ and hence } d=3.\end{aligned}$$

So, $a = 1$, $b = 0$, $c = 2$, $d = 3$.

□

3) [10 points] Express 327 in base 5. *Show the computations explicitly!*

Solution. We have:

$$\begin{aligned}327 &= 65\cdot 5+2\\ 65 &= 13\cdot 5+0\\ 13 &= 2\cdot 5+3\\ 2 &= 0\cdot 5+2.\end{aligned}$$

Hence,

$$327 = 2 + 0\cdot 5 + 3\cdot 5^2 + 2\cdot 5^3.$$

□

4) [20 points] If

$$n \stackrel{\text{def}}{=} 3601292\cdot(126517)^{5784683745} - 72342003,$$

then what is its remainder when divided by 3? [Justify! Correct answer with no explanation is worth 0.]

Solution. We have:

$$\begin{aligned}3601292 &\equiv 3+6+0+1+2+9+2 \equiv 1+2+2 \equiv 2 \pmod 3\\ 126517 &\equiv 1+2+6+5+1+7 \equiv 22 \equiv 1 \pmod 3\\ 72342003 &\equiv 7+2+3+4+2+0+0+3 \equiv 21 \equiv 0 \pmod 3.\end{aligned}$$

So,

$$n \equiv 2\cdot 1^{5784683745} - 0 = 2 \pmod 3.$$

Hence, the remainder is 2. □

5) [20 points] Let

$$n \overset{\text{def}}{=} 13004385024102127.$$

Find the remainders of n when divided by 2, 4, 5, 9 and 10,000. [Justify! Correct answer with no explanation is worth 0.]

Solution. By 2: since it is odd [last digit odd], the remainder is 1.

By 4: we can look at the last two digits, so $n \equiv 27 \equiv 3 \pmod 4$, and hence the remainder is 3.

By 5: it is congruent to the last digit modulo 5, so $n \equiv 7 \equiv 2 \pmod 5$, and hence the remainder is 2.

By 9: we have $n \equiv 1+3+0+0+4+3+8+5+0+2+4+1+0+2+1+2+7 = 43 \equiv 4+3 = 7 \pmod 9$. So, the remainder is 7.

By 10,000: it's just the last 4 digits, so the remainder is 2127. □

6) [20 points] For both parts below, let $a \in \mathbb{Z}$ and $m \in \mathbb{Z}_{\geq 2}$ with $(a, m) = 1$.

(a) Prove that there is $r \in \mathbb{Z}$ such that $a \cdot r \equiv 1 \pmod m$. [**Hint:** You *have* to use the fact that $(a, m) = 1$.]

Proof. By Bezout's Theorem, there are $r, s \in \mathbb{Z}$ such that

$$ar + ms = 1, \quad \text{i.e., } ar - 1 = m(-s).$$

Thus, $m \mid (ar - 1)$ and hence, by definition, $ar \equiv 1 \pmod m$. □

(b) Given $b \in \mathbb{Z}$, prove that there is $x \in \mathbb{Z}$ such that $a \cdot x \equiv b \pmod m$. [You can use the previous part here, even if you could not do it!]

Proof. Let r as in part (a), so that $ar \equiv 1 \pmod m$, and let $x \overset{\text{def}}{=} br$. Then, we have:

$$ax = a \cdot (br) = b \cdot (ar) \equiv b \cdot 1 \equiv b \pmod m.$$

Hence, we can take $x = br$. □