1) [20 points] Use the *Extended Euclidean Algorithm* to write the GCD of 130 and 61 as a linear combination of themselves.

Solution. We have:

$$\begin{aligned}
130 &= 2 \cdot 61 + 8 & &\longrightarrow & 8 &= \underline{130} - 2 \cdot \underline{61} \\
61 &= 7 \cdot 8 + 5 & &\longrightarrow & 5 &= \underline{61} - 7 \cdot 8 = -7 \cdot \underline{130} + 15 \cdot \underline{61} \\
8 &= 1 \cdot 5 + 3 & &\longrightarrow & 3 &= 8 - 5 = 8 \cdot \underline{130} - 17 \cdot \underline{61} \\
5 &= 1 \cdot 3 + 2 & &\longrightarrow & 2 &= 5 - 3 = -15 \cdot \underline{130} + 32 \cdot \underline{61} \\
3 &= 1 \cdot 2 + 1 & &\longrightarrow & 1 &= 3 - 2 = 23 \cdot \underline{130} - 49 \cdot \underline{61} \\
2 &= 2 \cdot 1 + 0 & & & &
\end{aligned}$$

So,

$$1 = 23 \cdot 130 - 49 \cdot 61.$$

□

2) [20 points] Give the set of all solutions of the system

$$\begin{aligned}
2x &\equiv 3 \pmod{7} \\
12x &\equiv 5 \pmod{13}
\end{aligned}$$

Solution. We have that $(-3) \cdot 2 + 1 \cdot 7 = 1$. So, the first equation can be multiplied by -3, giving $x \equiv -9 \equiv 5 \pmod{7}$. For the second we can multiply by -1, obtaining $x \equiv -5 \equiv 8 \pmod{13}$.

Since $2 \cdot 7 + (-1) \cdot 13 = 1$, we have that a solution is $x = 8 \cdot 2 \cdot 7 + 5 \cdot (-1) \cdot 13 = 47$, and all solutions are $\{47 + 91k \;:\; k \in \mathbb{Z}\}$. □

3) [20 points] Let a, b, and n be positive integers. Show that if $a^n \mid b^n$, then $a \mid b$.

Proof. We can write $a = p_1^{e_1} \cdots p_k^{e_k}$ and $b = p_1^{f_1} \cdots p_k^{f_k}$, with the p_i's distinct primes and $e_i, f_i \geq 0$.

Then, $a^n = p_1^{e_1 n} \cdots p_k^{e_k n}$ and $b = p_1^{f_1 n} \cdots p_k^{f_k n}$, and since $a^n \mid b^n$, we have that $e_i n \leq f_i n$ for all i. Hence, $e_i \leq f_i$ for all i, which implies that $a \mid b$ [from their decompositions].

[Induction also works.] $\square$

4) [20 points] Let n and b be positive integers. Show that $(b-1) \mid n$ if, and only if, the sum of the b-adic digits of n is divisible by $b-1$.

Proof. Let

$$n = n_0 + n_1 \cdot b + \cdots + n_k \cdot b^k.$$

Then, the n_i's are the b-adic digits. Since $b \equiv 1 \pmod{b-1}$, we have that

$$\begin{aligned} n &= n_0 + n_1 \cdot b + \cdots + n_k \cdot b^k \\ &\equiv n_0 + n_1 \cdot 1 + \cdots + n_k \cdot 1^k \pmod{b-1} \\ &= n_0 + n_1 + \cdots + n_k. \end{aligned}$$

Thus, $n \equiv 0 \pmod{b-1}$ if, and only if, $n_0 + n_1 + \cdots + n_k \equiv 0 \pmod{b-1}$, i.e., $(b-1) \mid n$ if, and only if, $(b-1) \mid n_0 + n_1 + \cdots + n_k$. $\square$

5) [20 points] Show that if p and $p^2 + 2$ are both prime, then $p = 3$.

Proof. If $p = 3$, then $p^2 + 2 = 29$ is also prime.

So, suppose that $p \neq 3$. Hence, $p \equiv 1$ or $p \equiv 2 \pmod 3$ [as $3 \nmid p$]. But, in either case, we have that $p^2 + 2 \equiv 0 \pmod 3$, i.e., $3 \mid (p^2 + 2)$. Since $p^2 + 2 > 3$, $p^2 + 2$ cannot be prime. $\square$