1) [20 points] Compute the remainder of 2^{2839} when divided by 13. [Show work!]

Solution. We have:

$$\begin{aligned} 2839 &= 218 \cdot 13 + 5 \\ 218 &= 16 \cdot 13 + 10 \\ 16 &= 1 \cdot 13 + 3 \\ 1 &= 0 \cdot 13 + 1. \end{aligned}$$

So, $2839 = 5 + 10 \cdot 13 + 3 \cdot 13^2 + 1 \cdot 13^3$. Then, by *Fermat's Theorem*:

$$\begin{aligned} 2^{2839} = 2^{5+10 \cdot 13+3 \cdot 13^2+1 \cdot 13^3} &\equiv 2^{5+10+3+1} = 2^{19} \\ &= 2^{6+1 \cdot 13} \equiv 2^{6+1} = 2^7 = 2^4 \cdot 2^3 \equiv 3 \cdot 8 = 24 \equiv 11 \pmod{13}. \end{aligned}$$

So, the remainder is 11. □

2) [20 points] Find all integers x such that

$$\begin{aligned} 5x &\equiv 7 \pmod{8} \\ 2x &\equiv 4 \pmod{10}. \end{aligned}$$

[If there is no such integer, explain how you could tell.]

Solution. Since $2 \cdot 8 + (-3) \cdot 5 = 1$, we have that the first equation gives that $x \equiv -3 \cdot 7 = -21 \equiv 3 \pmod{8}$. So, $x = 8k + 3$, for some $k \in \mathbb{Z}$.
Substituting in the second equation, we get: $2 \cdot (8k+3) \equiv 4 \pmod{10}$, so $6k \equiv -2 \pmod{10}$. Now, $\gcd(8, 10) = 2$ and $2 \mid -2$, so we have a solution. Dividing through out [including modulus] by 2, getting $3k \equiv -1 \pmod{5}$. Now $2 \cdot 3 + (-1) \cdot 5 = 1$, so multiplying by 2, we get $k \equiv -2 \equiv 3 \pmod{5}$. So, $k = 5l + 3$ for $l \in \mathbb{Z}$.
Substituting back, we get $x = 8(5l + 3) + 3 = 40l + 27$, for $l \in \mathbb{Z}$. □

3) [20 points] Prove that there are no positive integers a and b such that

$$\gcd(a,b) = 2^5 \cdot 3^4 \cdot 7 \cdot 11^2,$$
$$\operatorname{lcm}(a,b) = 2^8 \cdot 3^2 \cdot 5^3 \cdot 7^2 \cdot 11^2.$$

[Make it *very* clear what results you are using!]

Proof. We have that $\gcd(a,b) \mid a$ and $a \mid \operatorname{lcm}(a,b)$. So, $\gcd(a,b) \mid \operatorname{lcm}(a,b)$. By Lemma 1.54, this means that the power of 3 in $\gcd(a,b)$, namely 4, must be less than or equal to the power of 3 in $\operatorname{lcm}(a,b)$, namely 2. So, clearly we have a contradiction, so no such a and b exist.

Alternative Proof: By Proposition 1.55, the power of 3 in $\gcd(a,b)$, namely 4, is the minimum between the powers of 3 in a and b, say x and y respectively. [So, $\min(x,y) = 4$.] On the other hand, the power of 3 in $\operatorname{lcm}(a,b)$, namely 2, is the maximum between the powers of 3 in a and b. [So, $\max(x,y) = 2$.]
But this means that $\max(x,y) = 2 < 4 = \min(x,y)$, a contradiction. □

4) [20 points] Show that if x, y and z are integers such that $x^4 + y^4 = z^4$, then at least one of them is divisible by 3.

Proof. Suppose none of x, y and z are divisible by 3. Then, they are congruent to either 1 or 2 modulo 3. Hence, their fourth powers are $1^4 = 1$ and $2^4 = 16 \equiv 1 \pmod 3$. [Thus, $x^4 \equiv y^4 \equiv z^4 \equiv 1 \pmod 3$.] Then,

$$x^4 + y^4 \equiv 1 + 1 = 2 \pmod 3.$$

But if $x^4 + y^4 = z^4$, then

$$x^4 + y^4 \equiv z^4 \equiv 1 \pmod 3.$$

Since $1 \not\equiv 2 \pmod 3$, we have a contradiction. Hence, at least one of x, y and z must be divisible by 3. □

5) [20 points] Let $a \in \mathbb{Z}_{\geq 2}$ with prime factorization

$$a = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k}$$

[p_i's distinct primes and $e_i \in \mathbb{Z}_{>0}$]. Prove that a is a perfect square [i.e., $a = b^2$ for some $b \in \mathbb{Z}$] if and only if e_i is even for all i.
[**Note:** This was a HW Problem.]

Proof. [$\Rightarrow$] Suppose that $a = b^2$ for some $b \in \mathbb{Z}$. Since $b^2 = (-b)^2$ we may assume that $b \geq 0$. Since $a \geq 2$, we must have that $b \geq 2$ [as $0^2 = 0 < 2$ and $1^2 = 1 < 2$]. Let

$$b = q_1^{f_1} \cdots q_l^{f_l},$$

with q_i's distinct primes and $f_i > 0$. Then,

$$p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k} = a = b^2 = (q_1^{f_1} \cdots q_l^{f_l})^2 = q_1^{2f_1} \cdots q_l^{2f_l}.$$

By the *Fundamental Theorem of Arithmetic*, the p_i's and q_i's are the same primes, up to order, and their corresponding exponents are the same. Since the exponents on the left-hand side are all even [namely $2f_i$], the exponents on the right hand side [namely, the e_i's] must also be even.

[$\Leftarrow$] Suppose that all e_i's are even, say $e_i = 2f_i$. Then:

$$a = p_1^{e_1} \cdot p_2^{e_2} \cdots p_k^{e_k} = p_1^{2f_1} \cdot p_2^{2f_2} \cdots p_k^{2f_k} = (p_1^{f_1} \cdot p_2^{f_2} \cdots p_k^{f_k})^2.$$

Since $p_1^{f_1} \cdot p_2^{f_2} \cdots p_k^{f_k} \in \mathbb{Z}$, we have that a is a perfect square.

$\square$