1) [20 points] Find the remainder of

$$a = 1977 \cdot 2000^{2023} + 2046$$

when divided by 11.

Solution. We have

$$\begin{aligned} 1977 &\equiv 7 - 7 + 9 - 1 = 8 \pmod{11}, \\ 2000 &\equiv 0 - 0 + 0 - 2 = -2 \pmod{11}, \\ 2046 &\equiv 6 - 4 + 0 - 2 = 0 \pmod{11}. \end{aligned}$$

So,

$$a \equiv 8 \cdot (-2)^{2023} + 0 \pmod{11}.$$

Now,

$$2023 \equiv 3 \pmod{10},$$

and by *Fermat's Little Theorem* we have

$$a \equiv 8 \cdot (-2)^3 = -64 \equiv 2 \pmod{11}.$$

$\square$

2) [20 points] Find all integers x satisfying

$$\begin{aligned} 3x &\equiv 6 \pmod{14}, \\ 5x &\equiv 3 \pmod{21}. \end{aligned}$$

Solution. First note that since $\gcd(3, 14) = \gcd(5, 21) = 1$, both congruences have solutions, so we can attempt to solve the system.

Starting with the first: We have that $5 \cdot 3 \equiv 1 \pmod{14}$, so multiplying the first congruence by 5 we have

$$x \equiv 30 \equiv 2 \pmod{14}.$$

So, $x = 2 + 14k$ from some $k \in \mathbb{Z}$. Substituting in the second, we get

$$\begin{aligned} 5 \cdot (2 + 14k) \equiv 3 \pmod{21} \quad &\Longrightarrow \quad 10 + 70k \equiv 3 \pmod{21} \quad \Longrightarrow \\ &70k \equiv -7 \pmod{21} \quad \Longrightarrow \quad 7k \equiv 14 \pmod{21}. \end{aligned}$$

We have that $\gcd(7, 21) = 7$ and $7 \mid 14$, so we get

$$k \equiv 2 \pmod{3}.$$

We then have $k \equiv 2 \pmod{3}$, i.e., $k = 2 + 3l$ for $l \in \mathbb{Z}$. Substituting back, we get $x = 2 + 14k = 2 + 14 \cdot (2 + 3l) = 30 + 42l$ for $l \in \mathbb{Z}$.

Starting with the second: We have that $-4 \cdot 5 = -20 \equiv 1 \pmod{21}$. So, multiplying the second congruence by -4, we get

$$x \equiv -12 \equiv 9 \pmod{21}.$$

So, $x = 9 + 21k$ from some $k \in \mathbb{Z}$. Substituting in the second, we get

$$\begin{aligned} 3 \cdot (9 + 21k) \equiv 6 \pmod{14} \quad &\Longrightarrow \quad 27 + 63k \equiv 6 \pmod{14} \quad \Longrightarrow \\ &63k \equiv -21 \pmod{14} \quad \Longrightarrow \quad 7k \equiv 7 \pmod{14}. \end{aligned}$$

We have that $\gcd(7, 14) = 7$ and $7 \mid 7$, so we get

$$k \equiv 1 \pmod{2}.$$

We then have $k = 1 + 2l$ for $l \in \mathbb{Z}$. Substituting back, we get $x = 9 + 21k = 9 + 21 \cdot (1 + 2l) = 30 + 42l$ for $l \in \mathbb{Z}$. $\square$

3) [20 points] Prove that there are no integers x, y, such that $x^2 + y^4 = 2023$.

Proof. Consider the equation modulo 4. Since

$$\begin{aligned} x^2 &\equiv 0 \text{ or } 1 \pmod 4, \\ y^4 &\equiv 0 \text{ or } 1 \pmod 4, \end{aligned}$$

we have that

$$x^2 + y^4 \equiv 0, 1, \text{or } 2 \not\equiv 3 \equiv 2023 \pmod 4.$$

Hence, there can't be $x, y \in \mathbb{Z}$ satisfying the equation. $\square$

4) [20 points] Prove that $m \in \mathbb{Z}_{\geq 2}$ is a perfect square if and only if each of its prime factors appears an even number of times in its decomposition.

[**Note:** This was a HW problem.]

Proof. [$\Rightarrow$]: If m is a perfect square, then $m = n^2$ for some $n \in \mathbb{Z}_{\geq 0}$. Since $m \geq 2$, we can assume that $n \geq 2$. Then, by the *Fundamental Theorem of Arithmetic*, we have

$$n = p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n},$$

where the p_i's are distinct primes and $e_i \in \mathbb{Z}_{\geq 1}$. Then, the decomposition of $m = n^2$ is

$$m = (p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n})^2 = p_1^{2e_1} p_2^{2e_2} \cdots p_n^{2e_n},$$

so each prime factor p_i appears an even number of times, namely $2e_i$.

[$\Leftarrow$]: Now assume that the decomposition of m is

$$m = p_1^{f_1} p_2^{f_2} \cdots p_n^{f_n}$$

with $f_i \geq 1$ even. Then, we have that $f_i = 2_i$ for some $e_i \in \mathbb{Z}_{>1}$. Then,

$$m = p_1^{2e_1} p_2^{2e_2} \cdots p_n^{2e_n} = (p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n})^2.$$

Since $p_1^{e_1} p_2^{e_2} \cdots p_n^{e_n} \in \mathbb{Z}$, we have that m is a perfect square. $\square$

5) [20 points] Prove that if $\gcd(a, m) \nmid b$, then there is no $x \in \mathbb{Z}$ such that

$$ax \equiv b \pmod{m}.$$

[**Hint:** This was done in class. Start by converting the congruence into an *equality* of integers.]

Proof. Suppose there is such an x. Then, the congruence means that

$$ax = b + km, \text{ for some } k \in \mathbb{Z}.$$

So,

$$b = ax - km$$

Since $\gcd(a, m)$ is a common divisor of a and m, by the Basic Lemma, it must also divide b, proving the contrapositive (and hence, the original statement). $\square$