Problem 1
Is it possible to find $x, y \in \mathbb{Z}$ such that $5x + 11y = 4$?
Solution
Yes, because $\gcd(5, 11) = 1 \mid 4$. We will first find $m, n \in \mathbb{Z}$ such that $5m + 11n = 1$, and then multiply both sides by 4 to get the desired x and y.

To find m, n with $5m + 11n = 1$, we perform the Euclidean algorithm on 5 and 11, and then back substitute:

$$\begin{aligned} & \gcd(11, 5) & \\ =& \gcd(5, 1) & (11 = 2 \cdot 5 + 1) \\ =& \gcd(1, 0) & (5 = 5 \cdot 1 + 0) \\ =& 1. & \end{aligned}$$

$$1 = 11 - 2 \cdot 5.$$

So $m = -2$ and $n = 1$ gives us $5m + 11n = 1$. Thus $x = -8$ and $y = 4$ should give us $5x + 11y = 4$.

Problem 2
Let p be prime, and $a \in \mathbb{N}$. Show that $p \mid a^2$ if and only if $p \mid a$.
Solution

- ($\Rightarrow$) If $p \mid a^2$, then by Euclid's lemma, $p \mid a$ or $p \mid a$. Either way, $p \mid a$ as needed.
- ($\Leftarrow$) If $p \mid a$, then $p \mid ka$ for all integers $k \in \mathbb{Z}$. So of course $p \mid a \cdot a = a^2$.

Problem 3
Let $a, n \in \mathbb{N}$. Show that there is $k \in \mathbb{N}$ such that $ak \equiv 1 \bmod n$ if and only if $\gcd(a, n) = 1$.
Solution

- ($\Rightarrow$) Suppose there is $k \in \mathbb{N}$ such that $ak \equiv 1 \bmod n$. Then by definition, $n \mid ak - 1$. Let $\ell \in \mathbb{Z}$ so that $n\ell = ak - 1$. Rearranging, we have $1 = ak - n\ell$. Since $\gcd(a, n) \mid a$ and $\gcd(a, n) \mid n$, it follows $\gcd(a, n) \mid ak - n\ell$. Thus $\gcd(a, n) \mid 1$; the only natural number that divides 1 is 1 itself, so $\gcd(a, n) = 1$ as needed.
- ($\Leftarrow$) Suppsoe $\gcd(a, n) = 1$. Using Bézout's identity, find $k, \ell \in \mathbb{Z}$ such that

  $$ak + n\ell = 1.$$

  Rearranging, $ak - 1 = n\ell$, which shows $ak \equiv 1 \bmod n$.

Problem 4

1. Find an equivalence relation over $\mathbb{R}$ that satisfies the following:
   - The equivalence relation has uncountably infinitely many equivalence classes.
   - Each equivalence class has countably many members.
2. Find an equivalence relation over $\mathbb{R}$ that satisfies the following:
   - The equivalence relation has countably infinitely many equivalence classes.
   - Each equivalence class has uncountably infinitely many members.

Solution

- Consider the equivalence relation $\sim$ over $\mathbb{R}$ defined as

$$x \sim y \Leftrightarrow x - y \in \mathbb{Z}.$$

  This is an equivalence relation over $\mathbb{R}$:

  - For all $x \in \mathbb{R}$, $x - x = 0 \in \mathbb{Z}$, so $x \sim x$.
  - For all $x, y \in \mathbb{R}$, if $x \sim y$, then $x - y \in \mathbb{Z}$, so $y - x = -(x - y) \in \mathbb{Z}$ which implies $y \sim x$.
  - For all $x, y \in \mathbb{R}$, if $x \sim y$ and $y \sim z$, then $x-y, y-z \in \mathbb{Z}$. Then $x-z = (x-y)+(y-z) \in \mathbb{Z}$, so $x \sim z$.

  To show that there are uncountably many equivalence classes, notice that every number in $(0, 1)$ belongs in a distinct equivalence class (and there are uncountably many such numbers). This is because there are no $0 < x, y < 1$ such that $x-y \in \mathbb{Z}$. Given any $x \in \mathbb{R}$, the equivalence class of x is

$$[x] = \{x + n : n \in \mathbb{Z}\}$$

  which is countable.

- Consider the equivalence relation $\sim$ over $\mathbb{R}$ defined as

$$x \sim y \Leftrightarrow \lfloor x \rfloor = \lfloor y \rfloor$$

  where $\lfloor x \rfloor$ is the largest integer $\leq x$. This is an equivalence relation:

  - For all $x \in \mathbb{R}$, $\lfloor x \rfloor = \lfloor x \rfloor$, so $x \sim x$.
  - For all $x, y \in \mathbb{R}$, if $x \sim y$, then $\lfloor x \rfloor = \lfloor y \rfloor$, so $\lfloor y \rfloor = \lfloor x \rfloor$ giving us $y \sim x$.
  - For all $x, y, z \in \mathbb{R}$, if $x \sim y$ and $y \sim z$, then $\lfloor x \rfloor = \lfloor y \rfloor = \lfloor z \rfloor$, so $x \sim z$.

  There are countably many equivalence classes: $\ldots, [-2], [-1], [0], [1], [2], \ldots$. The equivalence class of any $x \in \mathbb{R}$ is the interval

$$[x] = [\lfloor x \rfloor, \lfloor x \rfloor + 1)$$

  which is uncountable.

Problem 5

Show that 7270324727853158 is not a square number without using a calculator. *Hint: There are no square numbers in the sequence* $2, 6, 10, 14, \ldots$.

Solution

We show that for any $n \in \mathbb{N}$, if n is a square number, then $n \not\equiv 2 \bmod 4$. This shows 7270324727853158 is not a square number, as the remainder of 7270324727853158 when divided by 4 is the same as the remainder of 58 divided by 4, which is 2.

Suppose $n \in \mathbb{N}$ is a square number. Let $a \in \mathbb{N}$ be such that $a^2 = n$. We have four cases:

- $a \equiv 0 \bmod 4$: Then $a^2 \equiv 0 \cdot 0 = 0 \bmod 4$.
- $a \equiv 1 \bmod 4$: Then $a^2 \equiv 1 \cdot 1 = 1 \bmod 4$.
- $a \equiv 2 \bmod 4$: Then $a^2 \equiv 2 \cdot 2 = 4 \equiv 0 \bmod 4$.
- $a \equiv 3 \bmod 4$: Then $a^2 \equiv 3 \cdot 3 = 9 \equiv 1 \bmod 4$.

In all cases, we have $a^2 \not\equiv 2 \bmod 4$ as needed.