Problem 1. Prove the following statement:
For \( n \in \mathbb{Z} \), the integer \((n + 1)^2 - 1\) is even if and only if \( n \) is even.

A remark in the light of §5.3: I could have written "For \( n \in \mathbb{Z} \), \((n + 1)^2 - 1\) is even if and only if \( n \) is even" but this would have been breaking rule number 3.

For \( a \in \mathbb{Z} \), we denote by \( a\mathbb{Z} \) the following set:
\[
 a\mathbb{Z} = \{ax : x \in \mathbb{Z}\}.
\]

For \( a \in \mathbb{Z} \) and \( b \in \mathbb{Z} \setminus \{0\} \), we denote by \( a\mathbb{Z} + b\mathbb{Z} \) the following set:
\[
 a\mathbb{Z} + b\mathbb{Z} = \{ax + by : x, y \in \mathbb{Z}\}.
\]
For \( a \in \mathbb{Z} \) and \( b \in \mathbb{Z} \setminus \{0\} \), we say that \( b \) divides \( a \) if there is \( k \in \mathbb{Z} \) such that \( a = bk \). It is equivalent to saying that the remained of the Euclidean division of \( a \) by \( |b| \) is zero.

Problem 2. Let \( a \in \mathbb{Z} \) and \( b \in \mathbb{Z} \setminus \{0\} \). Prove that
\[
 a\mathbb{Z} \subseteq b\mathbb{Z} \text{ if and only if } b \text{ divides } a.
\]

Problem 3. Let \( a \in \mathbb{Z} \) and \( b \in \mathbb{Z} \) such that \((a, b) \neq (0, 0)\).

1. Prove that if \( n \in a\mathbb{Z} + b\mathbb{Z} \) and \( m \in a\mathbb{Z} + b\mathbb{Z} \) then we have \( n + m \in a\mathbb{Z} + b\mathbb{Z} \) and \( n - m \in a\mathbb{Z} + b\mathbb{Z} \).

2. Let \( d' \in \mathbb{N} \) with \( d' \geq 1 \) be a common divisor of \( a \) and \( b \). Show that \( a\mathbb{Z} + b\mathbb{Z} \subseteq d'\mathbb{Z} \).

3. (a) Prove that the set
\[
 (a\mathbb{Z} + b\mathbb{Z}) \cap \{n \in \mathbb{N} : n \geq 1\}
\]
is not empty. Deduce by the well ordering principle that it has a smallest element which we denote by \( d \) (there isn’t much to say here, just check that you understand why we can apply this principle here). It obviously lies in \( \mathbb{N} \) and \( d \geq 1 \).

(b) Prove that \( d\mathbb{Z} \subseteq a\mathbb{Z} + b\mathbb{Z} \) (this should follow easily from the fact that \( d \in a\mathbb{Z} + b\mathbb{Z} \))

(c) Prove that the remainder of the Euclidean division of \( a \) by \( d \) lies in \((a\mathbb{Z}+b\mathbb{Z})\cap\mathbb{N}\) (use Question (1)).

(d) Deduce that \( r = 0 \) namely \( d \) divides \( a \). (You can do a proof by contradiction: if \( r \) was not zero, it would be in \((a\mathbb{Z}+b\mathbb{Z})\cap\{n \in \mathbb{N} : n \geq 1\}\) but this contradicts the fact that...)

Likewise, we would prove that \( d \) divides \( b \) (since \( a \) and \( b \) play a symmetric role).

(e) Conclude that \( a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z} \). (Use (2) and (3)(b)).

(f) Let \( d' \in \mathbb{N} \), \( d' \geq 1 \) be a common divisor of \( a \) and \( b \). Show that \( d' \) divides \( d \) and in particular \( d \geq d' \). (Use Problem 2).

4. We have almost all the ingredients to prove:

**Theorem.** For \((a, b) \in \mathbb{Z} \setminus (0, 0)\), there is a unique element \( d \in \mathbb{N} \setminus \{0\} \) such that
\[
 a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}.
\]

This element is the greatest common divisor ("gcd") of \( a \) and \( b \) and in fact, more precisely, we have
any common divisor $d' \in \mathbb{N} \setminus \{0\}$ of $a$ and $b$ divides $d$.

Which part of the theorem haven’t we proved yet? (Feel free to think of how to prove the missing part!..)

(5) Show the following

**Theorem.** Let $a \in \mathbb{Z}$ and $n \in \mathbb{N}$ with $n \geq 1$. There is $x \in \mathbb{Z}$ such that $ax \equiv 1 \pmod{n}$ if and only if $\gcd(a,n) = 1$ (namely $a$ and $n$ are coprime).

(6) Write the multiplication table of the integers mod 10 and check that the above theorem is satisfied.

**Problem 4.** Using the Euclidean algorithm, find the gcd of 315 and 1497.