Simple Example

For any integers a and b, if a and b are odd, then ab is also odd.

Proof:

Definition: integer a is odd iff $a = 2m + 1$ for some integer m Let $a, b \in \mathbb{Z}$ s.t. a and b are odd.

Then by definition of odd $a = 2m + 1.m \in \mathbb{Z}$ and $b = 2n + 1.n \in \mathbb{Z}$ So

$$\begin{aligned} ab &= (2m+1)(2n+1) \\ &= 4mn + 2m + 2n + 1 \\ &= 2(2mn + m + n) + 1 \end{aligned}$$

and since $m, n \in \mathbb{Z}$ it holds that $(2mn + m + n) \in \mathbb{Z}$, so $ab = 2k + 1$ for some $k \in \mathbb{Z}$.

Thus ab is odd by definition of odd. $\square$

Proof with divisibility

For any integers a, x, y, b, c, if $a \mid x$ and $a \mid y$, then $a \mid bx + cy$.

Proof:

Definition: Integer a divides integer b iff $b = an$ for some integer n.

Let $a, x, y, b, c \in \mathbb{Z}$ s.t. $a \mid x$ and $a \mid y$.

By the definition $x = an$ and $y = am$ for some $n, m \in \mathbb{Z}$

So $bx + cy = ban + cam = a(bn + cm)$

$bn + cm \in \mathbb{Z}$ since $b, n, c, m \in \mathbb{Z}$

Therefor, $a \mid (bc + cy)$ by definition of divides $\square$

Proof with Modulus

For any integers a, b, c, d, k with $k > 0$, if $a \equiv b \pmod{k}$ and $c \equiv d \pmod{k}$ then $(a + c) \equiv (b + d) \pmod{k}$.

Proof

Definition: $a \equiv b \pmod{k} \leftrightarrow k \mid (a - b)$

Let $a, b, c, d, k \in \mathbb{Z}$ with $k > 0$ s.t. $a \equiv b \pmod{k}$ and $c = d \pmod{k}$.

From the definition of mod we get $k \mid a - b$ and $k \mid c - d$.

Lets prove linearity of divides holds over addition which says that $a, b, k \in \mathbb{Z}$ if $k \mid a$ and $k \mid b$ then $k \mid a + b$.

Let $a, b, k \in \mathbb{Z}$ such that $k \mid a$ and $k \mid b$.

Since $k \mid a$ and $k \mid b$ by definition of divides $a = km$ and $b = kn$ for $n, m \in \mathbb{Z}$. So $a + b = km + kn = k(m + n)$ and since $m, n \in \mathbb{Z}$ then $m + n$ is also $\in \mathbb{Z}$ thus $k \mid a + b$. Thus we have shown that the linearity of division hold over addition.

From linearity of divides we get $k \mid (a-b)+(c-d)$ and then $k \mid (a+c)-(b+d)$ so $(a+c) \equiv (b+d) \pmod{k}$. $\square$

Disproving Existential Statements

Claim to disprove: There exists a real $x, x^2 - 2x + 1 < 0$.

Proof

To prove this claim false we will prove the negation which is the following.

For all x in the reals $x^2 - 2x + 1 \geq 0$

Let x be a real number. $x^2 - 2x + 1 = (x-1)^2$. $(x-1)^2 \geq 0$ since $x - 1$ is a real number and the square of a real number is non-negative. $\square$

Disproving Existential Statements

Claim to disprove: For all real $x, (x+1)^2 > 0$.

Proof

The claim is false. If $x = -1, (x+1)^2 = 0$. So since 1 is a real there then exists a real that proves the negation of the claim and thus the original claim is disproved. $\square$