Bi-implication

Some theorems can be written in the form

$$\boxed{P \text{ is equivalent to } Q}$$

or, in other words,

$$\boxed{P \text{ implies } Q\text{, and vice versa}}$$

or

$$\boxed{Q \text{ implies } P\text{, and vice versa}}$$

or

$$\boxed{P \text{ if, and only if, } Q} \qquad \boxed{P \text{ iff } Q}$$

or, in symbols,

$$\boxed{P \iff Q}$$

Proof pattern:

In order to prove that

$$P \iff Q$$

1. Write: $(\Longrightarrow)$ and give a proof of $P \implies Q$.
2. Write: $(\Longleftarrow)$ and give a proof of $Q \implies P$.

Proposition 12 *Suppose that n is an integer. Then, n is even iff n^2 is even.*

PROOF: Let n be an integer.

($\Rightarrow$) If n is even then so is n^2.

Assume n is even, that $n = 2i$ for an integer i. Then, $n^2 = 2(2i^2)$ and hence also an even integer.

($\Leftarrow$) If n^2 is even then n is even.

Equivalently, we prove the contrapositive statement: If n is odd then so is n^2. This is a corollary of Proposition 8. $\boxtimes$

DIVISIBILITY:

For integers d and n,

d divides n

or, in other words,

n is a multiple of d

for which we write

$$d \mid n$$

whenever

$n = k \cdot d$ for k an integer.

Example:

For n an integer, $0 \mid n \Leftrightarrow n = 0$.

Divisibility and congruence

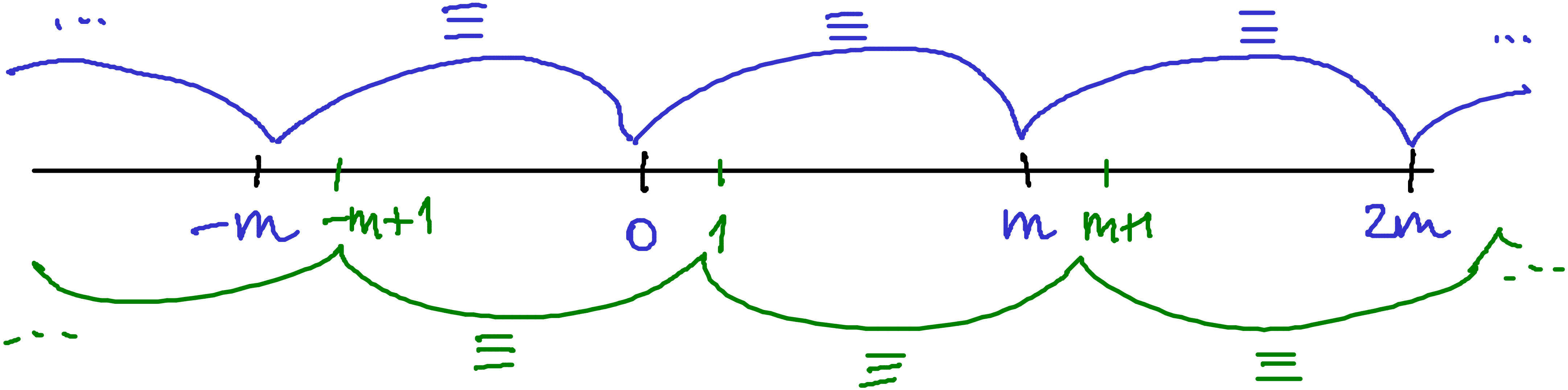
Definition 13 *Let* d *and* n *be integers. We say that* d divides n*, and write* $d \mid n$*, whenever there is an integer* k *such that* $n = k \cdot d$*.*

Example 14 *The statement* $2 \mid 4$ *is true, while* $4 \mid 2$ *is not.*

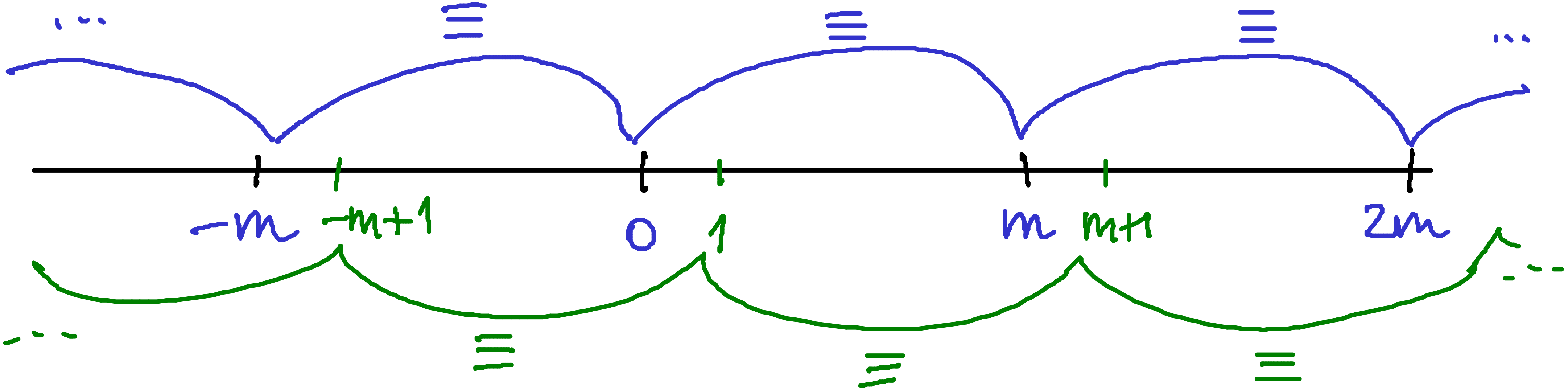
Definition 15 *Fix a positive integer* m*. For integers* a *and* b*, we say that* a *is congruent to* b *modulo* m*, and write* $\boxed{a \equiv b \pmod{m}}$*, whenever* $m \mid (a - b)$*.*

Example 16

1. $18 \equiv 2 \pmod{4}$
2. $2 \equiv -2 \pmod{4}$
3. $18 \equiv -2 \pmod{4}$



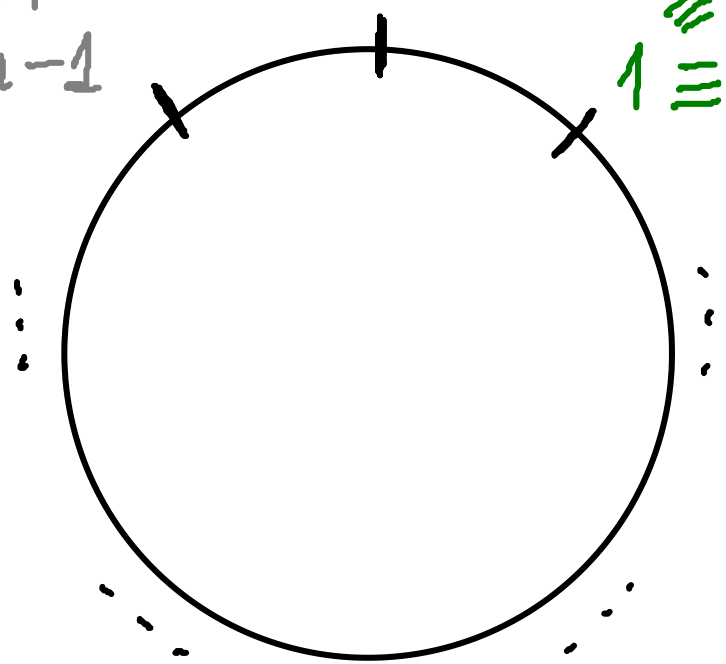
$-m$
$-m+1$
0
1
m
$m+1$
$2m$
$\equiv$
$\equiv$
$\equiv$
$\equiv$
$\equiv$
$\equiv$



$$\cdots \equiv -m-1 \equiv -1$$
$$\cdots \equiv 2m-1 \equiv m-1$$

$$\cdots \equiv -m \equiv 0 \equiv m \equiv \cdots$$

$$-m+1 \equiv -2m+1 \equiv \cdots$$
$$1 \equiv m+1 \equiv 2m+1 \equiv \cdots$$



Proposition 17 *For every integer n,*

1. *n is even if, and only if, $n \equiv 0 \pmod 2$, and*
2. *n is odd if, and only if, $n \equiv 1 \pmod 2$.*

PROOF:

The use of bi-implications:

To use an assumption of the form $P \iff Q$, use it as two separate assumptions $P \implies Q$ and $Q \implies P$.