Introduction to Proofs - Divisibility

Prof Mike Pawliuk

UTM

May 7, 2020

Slides available at: mikepawliuk.ca

Learning Objectives (for this video)

By the end of this video, participants should be able to:

1. State the definitions for integer divisibility, primes, and composite numbers.
2. Make a conjecture about divisibility and then prove it by definition unwinding, or provide a counterexample.

Divisibility

Definition (divisibility)

Let d, n be integers. We say that $\underline{d \text{ divides } n}$ if there is an integer k such that $n = dk$.

We also say $\underline{d \text{ is a divisor of } n}$, or that $\underline{n \text{ is a multiple of } d}$. We represent this as $d|n$.

Examples

- $3|12$ since $12 = 3 \cdot 4$ and 4 is an integer.
- $5| - 30$ since $-30 = 5 \cdot (-6)$, and -6 is an integer.
- a is even if and only if $2|a$. (Prove it!)

Non examples

We use $\not|$ to mean "does not divide".

- $12 \not| 3$ since $3 = 12 \cdot k$ has no integer solution.
- 5 is not a multiple of 10.

Conjectures

Goal: Discover what is true about divisibility.

1. **Play**. Create 5 examples and 5 non-examples of divisibility.

Goal: Discover what is true about divisibility.

1. **Play**. Create 5 examples and 5 non-examples of divisibility.
2. **Conjecture**. Make a conjecture (guess) about how divisibility works for <u>all</u> integers.

Conjectures

Goal: Discover what is true about divisibility.

1. **Play**. Create 5 examples and 5 non-examples of divisibility.
2. **Conjecture**. Make a conjecture (guess) about how divisibility works for all integers.
3. **Test**. Try to break your conjecture by finding integers that make your conjecture false.

Conjectures

Goal: Discover what is true about divisibility.

1. **Play**. Create 5 examples and 5 non-examples of divisibility.
2. **Conjecture**. Make a conjecture (guess) about how divisibility works for all integers.
3. **Test**. Try to break your conjecture by finding integers that make your conjecture false.
4. **Modify**. Play/conjecture/test again as needed.

Conjectures

Goal: Discover what is true about divisibility.

1. **Play**. Create 5 examples and 5 non-examples of divisibility.
2. **Conjecture**. Make a conjecture (guess) about how divisibility works for <u>all</u> integers.
3. **Test**. Try to break your conjecture by finding integers that make your conjecture false.
4. **Modify**. Play/conjecture/test again as needed.
5. **Prove**. Prove your conjecture by definition unwinding.

Example 1

After coming up with many examples, you notice the following pattern, and make a conjecture.

Conjecture

Suppose a, b, n are integers and $a|n$ and $b|n$, then $(a+b)|n$.

Test. Now you should attempt to break your conjecture.

Example 1

After coming up with many examples, you notice the following pattern, and make a conjecture.

Conjecture

Suppose a, b, n are integers and $a|n$ and $b|n$, then $(a+b)|n$.

Test. Now you should attempt to break your conjecture.
After playing for a while you discover: $1|4$ and $2|4$, but $3 \nmid 4$.

Example 1

After coming up with many examples, you notice the following pattern, and make a conjecture.

Conjecture

Suppose a, b, n are integers and $a|n$ and $b|n$, then $(a+b)|n$.

Test. Now you should attempt to break your conjecture.
After playing for a while you discover: $1|4$ and $2|4$, but $3 \not| 4$.
Modify. One option for adjusting your conjecture is

Conjecture

Suppose d, a, b are integers and $d|a$ and $d|b$, then $d|(a+b)$.

Example 2

After coming up with many examples, you notice the following pattern, and make a conjecture.

Conjecture

Suppose a, b are integers and $a|b$ and $b|a$, then $a = b$.

Proof.

Suppose that a, b are integers and that $a|b$ and $b|a$.

Example 2

After coming up with many examples, you notice the following pattern, and make a conjecture.

Conjecture

Suppose a, b are integers and $a|b$ and $b|a$, then $a = b$.

Proof.

Suppose that a, b are integers and that $a|b$ and $b|a$.
By definition (of divisibility) there are integers k, m such that $b = ak$ and $a = bm$.

Example 2

After coming up with many examples, you notice the following pattern, and make a conjecture.

Conjecture

Suppose a, b are integers and $a|b$ and $b|a$, then $a = b$.

Proof.

Suppose that a, b are integers and that $a|b$ and $b|a$.
By definition (of divisibility) there are integers k, m such that $b = ak$ and $a = bm$.
Putting these together, $b = ak = (bm)k$.

$$b = b(mk)$$

Example 2

After coming up with many examples, you notice the following pattern, and make a conjecture.

Conjecture

Suppose a, b are integers and $a|b$ and $b|a$, then $a = b$.

Proof.

Suppose that a, b are integers and that $a|b$ and $b|a$.
By definition (of divisibility) there are integers k, m such that $b = ak$ and $a = bm$.
Putting these together, $b = ak = (bm)k$.

$$b = b(mk)$$

So then $1 = mk$.

Example 2

After coming up with many examples, you notice the following pattern, and make a conjecture.

Conjecture

Suppose a, b are integers and $a|b$ and $b|a$, then $a = b$.

Proof.

Suppose that a, b are integers and that $a|b$ and $b|a$.
By definition (of divisibility) there are integers k, m such that $b = ak$ and $a = bm$.
Putting these together, $b = ak = (bm)k$.

$$b = b(mk)$$

So then $1 = mk$.
So then $m = k = 1$ ( ), . □

Example 2

After coming up with many examples, you notice the following pattern, and make a conjecture.

Conjecture

Suppose a, b are integers and $a|b$ and $b|a$, then $a = b$.

Proof.

Suppose that a, b are integers and that $a|b$ and $b|a$.
By definition (of divisibility) there are integers k, m such that $b = ak$ and $a = bm$.
Putting these together, $b = ak = (bm)k$.

$$b = b(mk)$$

So then $1 = mk$.
So then $m = k = 1$ (so $a = b$), . □

Example 2

After coming up with many examples, you notice the following pattern, and make a conjecture.

Conjecture

Suppose a, b are integers and $a|b$ and $b|a$, then $a = b$.

Proof.

Suppose that a, b are integers and that $a|b$ and $b|a$.
By definition (of divisibility) there are integers k, m such that $b = ak$ and $a = bm$.
Putting these together, $b = ak = (bm)k$.

$$b = b(mk)$$

So then $1 = mk$.
So then $m = k = 1$ (so $a = b$), or $m = k = -1$ ( ). □

Example 2

After coming up with many examples, you notice the following pattern, and make a conjecture.

Conjecture

Suppose a, b are integers and $a|b$ and $b|a$, then $a = b$.

Proof.

Suppose that a, b are integers and that $a|b$ and $b|a$.
By definition (of divisibility) there are integers k, m such that $b = ak$ and $a = bm$.
Putting these together, $b = ak = (bm)k$.

$$b = b(mk)$$

So then $1 = mk$.
So then $m = k = 1$ (so $a = b$), or $m = k = -1$ ($a = -b$). □

Example 2

After coming up with many examples, you notice the following pattern, and make a conjecture.

Conjecture

Suppose a, b are integers and $a|b$ and $b|a$, then $a = b$ or $a = -b$.

Proof.

Suppose that a, b are integers and that $a|b$ and $b|a$.
By definition (of divisibility) there are integers k, m such that $b = ak$ and $a = bm$.
Putting these together, $b = ak = (bm)k$.

$$b = b(mk)$$

So then $1 = mk$.
So then $m = k = 1$ (so $a = b$), or $m = k = -1$ ($a = -b$). □

Reflection

- What are the main steps in making and proving a conjecture?
- Do these steps apply to only divisibility, or can they apply to other definitions?
- Is it okay to make false conjectures?
- What is the role of play and creativity in math?