Divisibility - Intuition

Questions about divisibility are important in mathematics, especially Number Theory.

The intuitive way to think about divisiblity is that a divides b if $\frac{b}{a}$ is an integer.

This definition has two main problems:

- Depending on a and b the expression "$\frac{b}{a}$" may not even be a thing.
- Even if it is a thing, how can I determine if $\frac{b}{a}$ is an intenger?

Our intuition can be translated as follows:

$$\frac{b}{a} \text{ is an integer} \quad \text{“} \iff \text{”} \quad \exists k \in \mathbb{Z}, k = \frac{b}{a} \quad \text{“} \iff \text{”} \quad \exists k \in \mathbb{Z}, ak = b$$

The expression on the right gives us something concrete to work with, and always makes sense regardless of which integers a and b we have.

Divisibility - Formal

If a and b are integers, we say that a **divides** b if and only if there exists an integer k such that $ak = b$.

$$a \mid b \Leftrightarrow \exists k \in \mathbb{Z}, ak = b$$

Having a precise definition of a concept often makes proving things about it much easier. The definition of divisibility tells you exactly what you need to prove, and exactly how to use it as a hypothesis.

Example Theorems About Divisiblity

We will need the definition while we do some examples:

If a and b are integers, we say that a **divides** b if and only if there exists an integer k such that $ak = b$.

$$a \mid b \Leftrightarrow \exists k \in \mathbb{Z}, ak = b$$

Notice that the definition has exactly one quantifier, this should tell us about a couple of the lines we expect to appear in our theorems!

- $3|3111$.
- $a|b_1$, $a|b_2$, $\therefore a|(b_1 + b_2)$
- $(4a)|b$, $\therefore a|bc$.
- $a|b_1$, $a \not|(b_1 + b_2)$, $\therefore a \not|b_2$.

Useful facts about divisibility

- $a|b \iff a|(-b)$.
- $1|a$.
- $a|0$.
- $0|0$.
- $(0|a) \Rightarrow (a = 0)$.
- $(a|1) \Rightarrow ((a = 1) \vee (a = -1))$.
- $(a|b) \Rightarrow (a|bc)$
- $(a|b) \Rightarrow (ac|bc)$
- $(ab|c) \Rightarrow (a|c)$.
- $(a|b \,\&\, a|c) \Rightarrow (a|(b + c))$.

(some of these you prove on the assignment, all are good exercises)
You can't use any of these without proof, but they are nice to know!

Congruence

The idea of congruence generalizes the notion of

two numbers, a and b, have the same parity if $a - b$ is even

even (and *odd*) say something about divisibility by 2, congruence generalizes this to other numbers n.

Definition

If a, b, and n are integers, we say that a is **congruent** to b modulo n if and only if $n \mid (b - a)$

$$a \cong b \pmod{n} \Leftrightarrow n \mid (b - a)$$

You will often find it is useful to expand out the definition of divisibility that appears in the definition of congruence.

$$a \cong b \pmod{n} \Leftrightarrow n \mid (b - a) \Leftrightarrow \exists k \in \mathbb{Z}, nk = (b - a)$$

Example Theorems About Congruence

We will need the definition(s) while we do some examples:

If a, b, and n are integers, we say that a is congruent to b modulo n if and only if $(b-a) \mid n$

$$a \cong b \pmod{n} \Leftrightarrow n \mid (b-a)$$

If a and b are integers, we say that a divides b if and only if there exists an integer k such that $ak = b$.

$$a \mid b \Leftrightarrow \exists k \in \mathbb{Z}, ak = b$$

- $64 \cong 20 \pmod{11}$
- $(3a)|(b-2c), \quad c \cong 2d \pmod{2a}, \quad \therefore a+b \cong 4d \pmod{a}$.
- $nq_1 + r \cong nq_2 + r \pmod{n}$

Congruence (Intution)

Another way to think about congruence is the concept of a remainder:

Theorem (division algorithm)

Given any integer a and any positive integer n (so $n > 0$) there exist numbers q and r such that

$$a = nq + r \qquad \text{equivalently} \qquad \frac{a}{n} = q + \frac{r}{n}$$

and $0 \leq r < n$.
We call q the **quotient** of a by n and r the **remainder**.

We may prove this theorem later, in the mean time you may however just 'know' it because you know how to use long division to find q and r.

Theorem
Two integers a and b are congruent modulo n if and only if they have the same remainder when we divide by n.
We proved one direction on previous slide!
The $\Rightarrow$ direction (which we will not prove) requires
none of $1, 2, \ldots, n-1$ are divisible by n

Facts about Congruence

For any a, b and n:

- $a \cong b \pmod{n} \iff b \cong a \pmod{n}$.

This is very helpful, because it means we can check either:

$$n|(b-a) \qquad \text{or} \qquad n|(a-b)$$

to check either!

If $a_1 \cong a_2 \pmod{n}$ then

- $-a_1 \cong -a_2 \pmod{n}$,

If $a_1 \cong a_2 \pmod{n}$ and $b_1 \cong b_2 \pmod{n}$ then

- $a_1 + b_1 \cong a_2 + b_2 \pmod{n}$, and
- $a_1 b_1 \cong a_2 b_2 \pmod{n}$.

These are good exercises, hint for the last one

$$a_1 b_1 - a_2 b_2 = a_1(b_1 - b_2) + b_2(a_1 - a_2)$$

Many more facts

As with divisibility, there are many neat facts

- $(a \cong b \pmod 0) \Rightarrow (a = b)$
- $(a \cong b \pmod{nm}) \Rightarrow (a \cong b \pmod n)$
- $(a \cong b \pmod n) \Rightarrow (am \cong bm \pmod{nm})$
- $(a \cong b \pmod n) \Rightarrow (-a \cong -b \pmod n)$
- $(a \cong b \pmod n) \Rightarrow (a + c \cong b + c \pmod n)$
- $(a \cong b \pmod n) \Rightarrow (ca \cong cb \pmod n)$
- $(a \cong b \pmod n) \Rightarrow (a^c \cong b^c \pmod n)$
- $((a \cong b \pmod n) \,\&\, (c \cong d \pmod n)) \Rightarrow (a + c \cong b + d \pmod n)$
- $((a \cong b \pmod n) \,\&\, (c \cong d \pmod n)) \Rightarrow (ac \cong bd \pmod n)$

(some of these you might prove on the assignment, all are good exercises)
You can't use any of these without proof, but they are nice to know!