Jan 18 Math 250: Divisibility

David Zureick-Brown

January 2022

Definition. Let a and b be integers. We say that a divides b if there exists an integer k such that $b = ak$. In this case, we write $a \mid b$. If a does not divide b we write $a \nmid b$.

In general: when we have a definition, say of blah, the definition of 'not blah' is the negation of blah.

What is the definition of 'does not divide'? I.e., what is the negation of 'there exists an integer k such that $b = ak$'?

Technically... there does not exist an integer k such that $b = ak$. Better: for all integers k, $b \neq ak$. Generally, don't just add ' it is not true that' to the beginning to negate something.

Consider the sentence 'this sentence has five words'.'It is not true that this sentence has five words."

What does it mean to prove that $a \mid b$? For example: $3 \mid 6$? I.e., can we solve the equation $6 = 3k$ (with an integer k)? Sure; $k = 2$ works.

To give a proof of a statement about existence, just give an example.

On the other hand, does $3 \mid 7$? Ask: can we solve the equation $7 = 3k$ with an integer k? No: the only solution is $k = 7/3$, which is not an integer.

Why be so so careful? Does 0 divide 3? I.e., can we solve the equation $3 = 0k$? No. $0k$ is always equal to 0. So $0 \nmid 3$

What about: does $3 \mid 0$? Well, can we solve the equation $0 = 3k$ (with an integer k)? Sure: $k = 0$ always works.

Basic properties of divisibility. Let a, b, c and d be integers. Then the following are true.

1. If $a \mid b$, then $a \mid -b$.
2. (Transitivity) If $a \mid b$ and $b \mid c$, then $a \mid c$.
3. (Additivity) If $a \mid b$ and $a \mid c$, then $a \mid b + c$.
4. (2 out of 3 rule) If a divides at least two of b, c and $b + c$, then a divides the third.
5. (2 out of 3 rule) If a divides at least two of b, c and $b - c$, then a divides the third.

Proof of 1. Suppose that $a \mid b$. Then there exists an integer k such that $b = ak$. Then multiplying by -1 gives $-b = -ak = a(-k)$. Since $-k$ is an integer, we conclude that $a \mid -b$.

Proof of 2. Suppose that $a \mid b$ and $b \mid c$. Then for some integers k and l, $b = ak$ and $c = bl$. Then $c = (ak)l = a(kl)$. Since kl is an integer, we conclude that $a \mid c$.

Prove that for any integer n, $n(n + 1)$ is even.

Proof by 'cases'. There are two cases: either n is even, or n is odd. If n is even, then $2 \mid n$. Also, $n \mid n(n+1)$. By transitivity, $2 \mid n(n+1)$. Thus $n(n+1)$ is even.

If n is odd, then $n = 2k + 1$ for some integer k. Thus $n + 1 = 2k + 1 + 1 = 2k + 2 = 2(k + 1)$. Thus $n + 1$ is even, so $2 \mid n + 1$. Also, $n + 1 \mid n(n + 1)$. Thus, by transitivity, $2 \mid n(n+1)$ and thus $n(n+1)$ is even. We conclude that, in both cases, $n(n + 1)$ is even.

Division algorithm. Let a and b be integers. Then there exist integers q and r such that $a = bq + r$ and $0 \leq r < b$.

This is something that needs to be proved. We won't prove it, and I will have you look at chapter 5 for a proof.

HW hint: for all integers n, $3 \mid n(n + 1)(n + 2)$

By the division algorithm, there exist integers q and r such that $n = 3q + r$, where $r = 0, 1$, or 2.

Prove that for any integers a, b, $2 \mid ab(a - b)$.

Proof. There are 3 cases: a is even, b is even, or a and b are both odd. If a is even, then by transitivity, $ab(a-b)$ is also even. If b is even, then by transitivity, $ab(a - b)$ is also even. Finally: if a and b are both odd, then $a - b$ is even, so again by transitivity $ab(a - b)$ is even. We conclude that in each case $ab(a - b)$ is even.