6-6-2008

Divisibility

- $a \mid b$ means that a **divides** b — that is, b is a *multiple* of a.
- An integer n is **prime** if $n > 1$ and the only positive divisors of n are 1 and n. Prime numbers are important in number theory and its applications.
- The **Division Algorithm** says that an integer can be divided by another (nonzero) integer, with a unique quotient and remainder.
- The Division Algorithm is a consequence of the Well-Ordering Axiom for the positive integers.

If a and b are integers and $a \neq 0$, a **divides** b if there is an integer c such that

$$ac = b.$$

The notation $a \mid b$ to mean that a divides b.

Be careful not to confuse "$a \mid b$" with "a/b" or "$a \div b$". The notation "$a \mid b$" is read "a divides b", which is a **statement** — a complete sentence which could be either true or false. On the other hand, "$a \div b$" is read "a divided by b". This is an expression, not a complete sentence. Compare "6 divides 18" with "18 divided by 6" and be sure you understand the difference.

Example. $3 \mid 6$, since $3 \cdot 2 = 6$. And $-2 \mid 10$, since $(-2) \cdot (-5) = 10$.

The properties in the next proposition are easy consequences of the definition of divisibility; see if you can prove them yourself.

Proposition.

(a) Every nonzero number divides 0.

(b) 1 divides everything. So does -1.

(c) Every nonzero number is divisible by itself.

Proof. (a) If $a \in \mathbb{Z}$, then $a \cdot 0 = 0$, so $a \mid 0$.

(b) To take the case of 1, note that if $a \in \mathbb{Z}$, then $1 \cdot a = a$, so $1 \mid a$.

(c) If $n \in \mathbb{Z}$, then $n \cdot 1 = n$, so $n \mid n$. $\square$

Definition. An integer $n > 1$ is **prime** if its only positive divisors are 1 and itself. An integer $n > 1$ is **composite** if it isn't prime.

The first few primes are

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, \ldots.$$

The first few composite numbers are

$$4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 22, \ldots.$$

Prime numbers play an important role in number theory.

From now on, when I write "$x \mid y$", I'll take it as understood that x must be nonzero.

Proposition. Let $a, b, c, d \in \mathbb{Z}$.

(a) If $a \mid b$ and $b \mid c$, then $a \mid c$.

(b) If $a \mid b$, $a \mid c$, and $m, n \in \mathbb{Z}$, then

$$a \mid mb + nc.$$

(c) If $a \mid b$ and $c \mid d$, then $ac \mid bd$.

(In case you were wondering, mathematicians have different names for results which are intended to indicate their relative importance. A **Theorem** is a very important result. A **Proposition** is a result of less importance. A **Lemma** is a result which is primarily a step in the proof of a theorem or a proposition. Of course, there is some subjectivity involved in judging how important a result is.)

Proof. (a) Suppose $a \mid b$ and $b \mid c$. This means that there are numbers d and e such that $ad = b$ and $be = c$. Substituting the first equation into the second, I get $(ad)e = c$, or $a(de) = c$. This implies that $a \mid c$.

(b) Suppose $a \mid b$ and $a \mid c$. This means that there are numbers d and e such that $ad = b$ and $ae = c$. Then

$$mb + nc = mad + nae = a(md + ne), \quad \text{so} \quad a \mid mb + nc. \quad \square$$

To say it in words, if an integer a divides integers b and c, then a divides any **linear combination** of b and c.

Two important special cases of (b): If $a \mid b$ and $a \mid c$, then

$$a \mid (b + c) \quad \text{and} \quad a \mid (b - c).$$

(c) $a \mid b$ means $ae = b$ for some e, and $c \mid d$ means $cf = d$ for some f. Therefore,

$$bd = (ae)(cf) = (ef)(ac), \quad \text{so} \quad ac \mid bd. \quad \square$$

Example. Prove that if x is even, then $x^2 + 2x + 4$ is divisible by 4.

x is even means that $2 \mid x$.
$2 \mid x$ and $2 \mid x$ implies that $4 = 2 \cdot 2 \mid x \cdot 2 = x^2$ by part (c) of the proposition.
$2 \mid 2$ and $2 \mid x$ implies that $4 = 2 \cdot 2 \mid 2 \cdot x = 2x$ by part (c) of the proposition.
Obviously, $4 \mid 4$.
Then $4 \mid x^2 + 2x$ by part (b) of the proposition, so $4 \mid (x^2 + 2x) + 4$, again by part (b) of the proposition.
$\square$

Example. Prove that if a divides b, then a divides any multiple of b.

First, here's a proof which uses part (c) of the Proposition.

Assume that $a \mid b$. Let bd be a multiple of b. I want to show that $a \mid bd$. I observed earlier that 1 divides everything, so $1 \mid d$. Then $a \mid b$ and $1 \mid d$ implies $a \cdot 1 \mid b \cdot d$ by the Proposition, so $a \mid bd$.

You can also use part (b) of the proposition.

Alternatively, here's a proof that uses the definition of divisibility. Assume that $a \mid b$. Let bd be a multiple of b. I want to show that $a \mid bd$.

Since $a \mid b$, I have $ac = b$ for some c. Multiplying both sides by d, I get $acd = bc$, i.e. $a(cd) = bd$. This equation implies that $a \mid bd$. $\square$

Here is an important result about division of integers. It will have a lot of uses — for example, it's the key step in the **Euclidean algorithm**, which is used to compute **greatest common divisors**.

Theorem. (**The Division Algorithm**) Let a and b be integers, with $b > 0$. There are unique integers q and r such that

$$a = b \cdot q + r, \quad \text{and} \quad 0 \le r < b.$$

Of course, this is just the "long division" of grade school, with q being the quotient and r the remainder.

Proof. The idea is to find the remainder r using Well-Ordering. What is division? Division is successive subtraction. You ought to be able to find r by subtracting b's from a till you can't subtract without going negative. That idea motivates the construction which follows.

Look at the set of integers

$$S = \{a - bn \mid n \in \mathbb{Z}\}.$$

In other words, I take a and subtract *all possible multiples* of b.

If I choose $n < \dfrac{a}{b}$ (as I can — there's always an integer less than any number), then $bn < a$, so $a - bn > 0$. This choice of n produces a positive integer $a - bn$ in S. So the subset T consisting of nonnegative integers in S is *nonempty*.

Since T is a nonempty set of nonnegative integers, I can apply Well-Ordering. It tells me that there is a smallest element $r \in T$. Thus, $r \ge 0$, and $r = a - bq$ for some q (because $r \in T$, $T \subset S$, and everything in S has this form).

Moreover, if $r \ge b$, then $r - b \ge 0$, so

$$a - bq - b \ge 0, \quad \text{or} \quad a - b(q + 1) \ge 0.$$

So $a - b(q + 1) \in T$, but $r = a - bq > a - b(q + 1)$. This contradicts my assumption that r was the smallest element of T.

All together, I now have r and q such that

$$a = b \cdot q + r, \quad \text{and} \quad 0 \le r < b.$$

To show that r and q are unique, suppose r' and q' also satisfy these conditions:

$$a = b \cdot q' + r', \quad \text{and} \quad 0 \le r' < b.$$

Then

$$b \cdot q + r = b \cdot q' + r', \quad \text{so} \quad b(q - q') = r' - r.$$

But r and r' are two nonnegative numbers less than b, so they are less than b units apart. This contradicts the last equation, which says they are $|b(q - q')|$ units apart — unless $|b(q - q')| = 0$. Since $b > 0$, this forces $q - q' = 0$, or $q = q'$. In addition, $r' - r = 0$, so $r = r'$. This proves that r and q are unique. □

Example. Applying the Division Algorithm to 59 and 7 gives

$$59 = 8 \cdot 7 + 3.$$

The quotient is 8, the remainder is 3, and $0 \le 3 < 7$.

Applying the Division Algorithm to -59 and 7 gives

$$-59 = (-9) \cdot 7 + 4.$$

The quotient is -9, the remainder is 4, and $0 \le 4 < 7$. □

Example. By the Division Algorithm, if a is an integer and I divide a by 4, there are four possible remainders: 0, 1, 2, and 3. This means that a can be written in one of the following forms:

$$a = 4q + 0, \quad a = 4q + 1, \quad a = 4q + 2, \quad a = 4q + 3.$$

This kind of idea is often the basis for proofs which consider these four cases. Even better, it's the idea behind for **modular arithmetic**, which I'll discuss shortly.

Finally, note that if n is a positive integer, then dividing a by n leaves one of the n remainders 0, 1, ..., $n - 1$. $\square$

The Division Algorithm is sometimes used in proofs, in the following way: Suppose you want to prove that m divides n and the divisibility rules don't work. Try applying the Division Algorithm to divide n by m, then use other information to show that the remainder must be 0. (Of course, in a given situation, there may be easier ways to show that m divides n.)