DIVISIBILITY I

The symbol $\mathbb{Z}$ denotes the set of integers:

$$\mathbb{Z} = \{\cdots, -2, -1, 0, 1, 2, \cdots\}$$

We write $a \in \mathbb{Z}$ to say a is an integer. We first noticed some *closure operations*:

(1) If $a \in \mathbb{Z}$ and $b \in \mathbb{Z}$, then $a + b \in \mathbb{Z}$. (If a and b are integers, so is the sum);
(2) If $a \in \mathbb{Z}$ and $b \in \mathbb{Z}$, then $a - b \in \mathbb{Z}$. (If a and b are integers, so is the difference);
(3) If $a \in \mathbb{Z}$ and $b \in \mathbb{Z}$, then $ab \in \mathbb{Z}$. (If a and b are integers, so is the product);

On the other hand we noticed that the division does not work so well: if $a \in \mathbb{Z}$ and $b \in \mathbb{Z}$, then $\frac{a}{b}$ does not need to be an integer; sometimes it is an integer and sometimes it is not (for example take $a = 1$ and $b = 2$).

We wanted to single out the property that the quotient of two integers is an integer and we wrote the following

(0.1) **Definition.** Let a and b be two integers, then we say that a *divides* b, or b is a *multiple* of a, or a is a *factor* of b, if

(1) $b = ca$, for some integer c;
(2) $b = ca$, for exactly one integer c.

We showed that the two definitions are equivalent in the following

(0.2) **Theorem.** *The two definitions (1) and (2) are equivalent.*

Proof. (Alex) Let a and b be two integers, if b is a multiple of a according to the definition as in (2) then we know that there exists exactly one integer c such that $b = ca$. That c plays the role of *some integer* in the definition (1).

If b is a multiple of a according to the definition as in (1), then we know that there exists some integer c such that $b = ac$, and we want to show that c is unique. Well, we assume that there exists another integer d such that $b = ad$. It follows that

$$b = ac = ad$$

and $ac = ad$, and $c = d$. □

It seems that nobody had any problem at listing and recognizing *even* integers: $-3, 6, 4, \cdots$. Is 0 an even integer? There was a little bit of disagreement, so we decided to give first a definition and then check whether 0 would satisfy the definition or not.

(0.3) **Definition.** An integer a is *even* if there exists an integer b such that $a = 2b$.

0 is then an even integer since $0 = (2)(0)$.

We were also pretty good to recognize an *odd* integer $1, 3, 9, \ldots$, but we came up with more then one definition:

Date: September 5, 2007.

(0.4) **Definition.** An integer a is *odd* if

(1) (Alex) a is not even;
(2) (Sara) there exists an integer b such that $a = 2b - 1$;
(3) (Eric) there exists an integer b such that $a = 2b + 1$.

(0.5) **Homework.** Check that the three definitions are equivalent: an integer a is odd in the sense of Alex, *if and only if* it is odd in the sense of Sara, *if and only if* it is odd in the sense of Eric.

We finished (earlier and I did not realize it) with a list of properties to check:

(0.6) **Homework.** Give a proof or find a counterexample of the following statements:

(1) the sum of two even integers is even;
(2) the product of two even integers is even;
(3) the difference of two even integers is even.

(0.7) **Homework.** Same as in (0.6) but replacing the word *even* with the word *odd*.

(0.8) **Homework.** What is the product of an even integer and an odd integer? What is the sum of an even integer and an odd integer?