

THE JOY OF NUMBERS

1. DIVISIBILITY II

Before starting with what we discussed in class, let me point out the axioms that hold for the integers. We noticed that we are using them, without ever having stated them clearly. So here they are:

If a , b and c are integers, then

- (1) (Commutativity) $a + b = b + a$.
- (2) (Associativity) $a + (b + c) = (a + b) + c$.
- (3) (Distributivity) $a(b + c) = ab + ac$.
- (4) (Commutativity of the product) $ac = ca$.
- (5) (Neutral element for the addition) $a + 0 = a$.
- (6) (Neutral element for the multiplication) $1a = a$.
- (7) (Inverse element for the addition) $a + (-a) = 0$.

OK, now what we have done in class. Recall from last time, we gave the following definition,

(1.1) **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 $a = 2b + 1$.

The first task left last time was to prove that the three definitions of odd number are equivalent. We proved the following

(1.2) **Theorem.** Let a be an integer then there exists an integer b such that $a = 2b + 1$ if and only if there exists an integer c such that $a = 2c - 1$

Proof. (Sara) If $a = 2c - 1$, for some integer c , then

$$a = 2(c - 1 + 1) - 1 = 2(c - 1) + 2 - 1 = 2(c - 1) + 1.$$

If we let $b = c - 1$ then we see that $a = 2b + 1$.

If $a = 2b + 1$, for some integer b , then

$$a = 2(b + 1 - 1) + 1 = 2(b + 1) - 2 + 1 = 2(b + 1) - 1.$$

If we let $c = b + 1$ then we see that $a = 2c - 1$. □

This theorem shows that in Definition 1.1, the statements in (2) and (3) are equivalent. We also argued that if an integer $a = 2b + 1$ for some integer b , then a cannot be even. In fact if a is even, then there exists an integer c such that $a = 2c$, but then

$$a = 2b + 1 = 2c, \quad \text{which implies that } b = c - 1/2,$$

contradicting the fact that b is an integer. This shows that in Definition (1.1), (2) implies (1), we decide to leave the other implication, (1) implies (2), for later.

Date: September 10, 2007.

We then work some of the homework from last time:

(1.3) **Theorem.** *If a and b are two even integers then so is $a + b$.*

Proof. (Matt) If a and b are even then there exist two integers x and y such that $a = 2x$ and $b = 2y$. So

$$a + b = 2x + 2y = 2(x + y),$$

which shows that $a + b$ is even. \square

(1.4) **Theorem.** *If a and b are two even integers then so is ab .*

Proof. (Eric) If a and b are even then there exist two integer x and y such that $a = 2x$ and $b = 2y$. So

$$ab = 2x2y = 2(2xy),$$

which shows that ab is even. \square

In fact we can say more, ab is divisible by 4. We now looked at other questions. Recall that the symbols $d|a$ reads d divides a , or a is divisible by d .

(1.5) **Question.** Let a, b , and d be integers.

- (1) if $d|a$ and $d|b$ does $d|(a + b)$?
- (2) if $d|a$ and $d|b$ does $d|ab$?
- (3) if $d|(a + b)$ does $d|a$ and $d|b$?
- (4) if $d|ab$ does $d|a$ and $d|b$?

We worked a little and here there are the answers:

(1.6) **Theorem.** *Let a, b , and d be integers. The following hold*

- (1) *if $d|a$ and $d|b$ does $d|(a + b)$,*
- (2) *if $d|a$ and $d|b$ does $d|ab$.*

And the following do not hold

- (1) *if $d|(a + b)$ does $d|a$ and $d|b$,*
- (2) *if $d|ab$ does $d|a$ and $d|b$.*

Proof. (J) If $a/d = x$ and $b/d = y$ for some integers x and y , then $(a + b)/d = a/d + b/d = x + y$, which is an integer.

(Eric) If $d|a$ and $d|b$, then there are integers k_1 and k_2 such that $a = k_1d$ and $b = k_2d$. This implies that $ab = (k_1d)(k_2d) = (k_1k_2d)d$, which shows that $d|ab$ (in fact $d^2|ab$).

(Eric) It is not true that if $d|(a + b)$ then $d|a$ and $d|b$. For example take $d = 6$, $a = 1$ and $b = 5$

(Sara) It is not true that if $d|(ab)$ then $d|a$ and $d|b$. For example take $a = 3$, $b = 5$ and $d = 15$. \square

We notice that the examples that Eric and Sara found are also counterexamples to weaker statements:

1. if $d|(a + b)$ then $d|a$ or $d|b$

and

2. if $d|(ab)$ then $d|a$ or $d|b$,

which therefore are not true. We decide to be a little more careful about statement (2) and we came up with more examples for which statement (2) holds and more examples for which statement (2) does not hold:

d	a	b		d	a	b	
5	4	5	(Kelsey)	9	3	6	(Kevin)
3	6	5	(Emily)	12	4	6	
5	100	3	(Jessica)	10	5	12	(Matt)
2	4	8		6	3	4	(Dan)
7	15	14		20	10	2	

What is the pattern? Statement (2) does not hold when we can factor d into smaller integers, on the contrary it does hold when we cannot factor d into smaller integers (besides of course 1 and d itself).

(1.7) **Definition.** Let d be an integer. d is prime if its only factors are ± 1 and $\pm d$.

The conjecture we seem to claim is the following: if d is a prime number and $d|ab$ then $d|a$ or $d|b$.

We moved on to another definition

(1.8) **Definition.** Let a and b be two integers, the greatest common divisor between a and b is the largest integer d such that $d|a$ and $d|b$. We write

$$d = \gcd(a, b)$$

For example $\gcd(10, 15) = 5$,

(1.9) **Homework.** Prove or disprove:

- (1) If $d|a + b$ and $d|a$ then $d|b$.
- (2) If $d > 1$ is not prime then there exist two integers a and b such that $d|ab$ but d does not divide a or b . (This was actually conjecture by Jay)
- (1) What is the $\gcd(a, 0)$ for $a \neq 0$?
- (2) What is the $\gcd(a, 1)$ for $a \neq 0$?
- (3) Find $\gcd(121, 275)$ and $\gcd(1423, 10751)$.