

THE JOY OF NUMBERS

1. THE DIVISION THEOREM AND THE EUCLIDIAN ALGORITHM

We first answer some homework problems.

(1.1) **Theorem.** *Let a, b and d be integers. If $d|(a + b)$ and $d|a$, then $d|b$.*

Proof. (Chris) If $d|(a + b)$, then $a + b = k_1d$ for some integer k_1 ; also if $d|a$, then $a = k_2d$. Then $b = (a + b) - a = k_1d - k_2d = (k_1 - k_2)d$, showing that b is a multiple of d . □

(1.2) **Theorem.** *If $d > 1$ is an integer which is not prime then there exist two integers a and b such that $d|ab$ but d does not divide a and d does not divide b .*

Proof. If d is not prime then we can write $d = ab$ such that $a > 1$ and $b > 1$. This implies that $1 < a < d$ and $1 < b < d$, showing that d cannot be a factor of either a or b . □

(1.3) **Theorem.** *Let a be any integer. Then $gcd(a, 0) = |a|$.*

Proof. (Jay) Notice that n divides 0, for all integers n . Therefore $gcd(a, 0)$ is just the greatest factor of a which is $|a|$. □

We discussed a little bit the other homeworks. In particular Jay had a nice way to show that the $gcd(1423, 10751) = 1$. If we write the difference, we have $10751 - 1423 = 9328 = 2^4(11)(53)$ but neither 2, or 53, or 11 divides 10751. And we know from previous theorems that if $d|a$ and $d|b$ then $d|(a + (-b))$.

But as soon as we moved to bigger numbers then we were in trouble, we needed to get smarter and smarter. The goal of today lecture is to realize that there is actually an algorithm that allows us to compute the greatest common divisor.

b	c	$a=b+c$	$gcd(b,c)$	$gcd(a,b)$
5	3	8	1	1
25	10	35	5	5
96	64	160	32	32
78	36	114	6	6

(1.4) **Conjecture.** Let a and b be any two integers then $gcd(a, b) = gcd(b, a + b)$.

(1.5) **Homework.** Prove Conjecture (1.4).

The next is the first big theorem we presented in class

(1.6) **Theorem.** *(The division Theorem) Let a and b be any two integers such that $b > 0$. There exist unique integers q and r such that $a = qb + r$ and $0 \leq r < b$.*

Date: September 10, 2007.

For example if $a = 5$ and $b = 2$ then we can write uniquely $5 = (2)(2) + 1$. Uniquely means that if we write $5 = 2q + r$ with $0 \leq r < 2$ then $q = 2$ and $r = 1$. There are infinitely many other ways to write 5 as a sum, for example $5 = (-1)2 + 7$.

So Matt asked why do we put that condition on r : because it is useful and we will see an application just at the end of class. He also asked if there is a uniqueness statement, if we replace $b > 0$ by $b < 0$. Is there such a statement? Think about it for next time.

We decided to look to another set of experiments

ba	b	r^1	$gcd(a,b)$	$gcd(b,r)$
73	5	3	1	1
36	67	36	1	1
-15	4	1	1	1
-33	22	11	11	11
96	64	32	32	32
78	42	36	6	6
364	28	0	28	28

(1.7) **Conjecture.** (Alex) Let a and $b > 0$ be two integers. Write $a = bq + r$ as in Theorem (1.6). Then $gcd(a, b) = gcd(b, r)$.

(1.8) **Homework.** Prove Conjecture (1.7).

So we have an idea for the algorithm:

(1.9) **Example.** Compute the $gcd(83154, 252)$:

$$83154 = (329)(252) + 246$$

$$252 = (1)(246) + 6$$

$$246 = (6)(41) + 0$$

So $gcd(83154, 252) = gcd(252, 246) = gcd(246, 6) = gcd(6, 0) = 6$.

We put our algorithm in a theorem:

(1.10) **Theorem.** (The Euclidian Algorithm) Let a and b two integers such that $b > 0$. Denote $gcd(a, b) = d$. There exists an n such that

$$a = bq + r_1$$

$$b = (q_2)(r_1) + r_2$$

$$r_1 = q_3 r_2 + r_3$$

.....

$$r_{n-1} = q_{n+1} r_n + r_{n+1}$$

with $r_{n+1} = 0$, where in each line we apply Theorem 1.6. For such an n we have $d = r_n$.

We noticed that this is an algorithm: At each step we are computing a remainder r_i which is strictly less than r_{i-1} , but also all the r_i are bounded below by zero. This is an application of the property of the remainder: we can write $a = bq + r$ with r bigger or equal than zero and strictly less than b .

We ended class with the last

(1.11) **Homework.** Let a be an integer, show that $gcd(a, a + 1) = 1$.