THE JOY OF NUMBERS

1. Some more about gcd

We started class by looking at some of the homework problems.

(1.1) **Theorem.** *Let a be an integer, then $gcd(a, a+1) = 1$.*

Proof. (Matt and Eric) We use two properties of the *gcd*:

1. $gcd(a, 1) = 1$ for all integers $a \in \mathbb{Z}$ (*We proved this previously*)
2. $gcd(a, b) = gcd(a, a+b)$ (*We prove this in the next theorem*)
3. $gcd(a, b) = gcd(a, -b)$ (*This is just an easy remark*)

Let a and b two be a given integer, we first claim that $\gcd(a, b) = gcd(a, b-a)$. Infact, we have

$$\begin{aligned} gcd(a,b) &= gcd(a,-b), \quad \text{by property (3);} \\ &= gcd(a, a+(-b)), \quad \text{by property (2);} \\ &= gcd(a, a-b); \\ &= gcd(a, -(a-b)) \quad \text{by property (3);} \\ &= gcd(a, b-a). \end{aligned}$$

In particular, $gcd(a, a+1) = gcd(a, (a+1)-a) = gcd(a, 1) = 1$, where the last equality follows from 1. □

(1.2) **Theorem.** *Let a and b be two integers, then $gcd(a, b) = gcd(a, a+b)$.*

Proof. (Sara) We prove something stronger: we prove that every integer which is a common divisor of a and b is also a common divisor of a and $a+b$; viceversa, every integer which is a common divisor of a and $a+b$ is also a common divisor of a and b. In math language we show that the two sets:

$$S_1 = \{d \in \mathbb{Z} \mid d|a \quad \text{and} \quad d|b\}$$

and

$$S_2 = \{d \in \mathbb{Z} \mid d|a \quad \text{and} \quad d|a+b\}$$

are the same. To prove that the two sets are the same we will show that if we pick an element x in S_1 then x is also an element of S_2 and if we pick an element $y \in S_2$ then y is also an element of S_1: in mathematical language we prove that $S_1 \subseteq S_2$ and $S_2 \subseteq S_1$.

So we need to prove two statements:

1. If $x|a$ and $x|b$ then $x|a+b$;
2. If $x|a$ and $x|a+b$ then $x|b$.

But we proved both of these statement in old homeworks, so we don't have anything to do. □

During the proof, Sara came up with the following conjecture:

Date: September 10, 2007.

(1.3) **Conjecture.** Let $d = gcd(a, b)$ and let h and k be two integers such that $a = kd$ and $b = hd$. Then $gcd(h, k) = 1$.

(1.4) **Homework.** Prove the following

1. Sara's conjecture.
2. Let a and b two integers, with $b < a$. Write $a = bq + r$, with $0 \geq r < b$. Then $gcd(a, b) = gcd(b, r)$.

Before starting to think to new problems we warmed up our math skills with some computations:

(1.5) (Danny) Find the $gcd(41, 243)$.

$$\begin{aligned} 243 &= (41)(5) + 38 \\ 41 &= (1)(38) + 3 \\ 38 &= (12)(3) + 2 \\ 3 &= (1)(2) + 1 \\ 2 &= (2)(1) + 0 \end{aligned}$$

So $gcd(41, 243) = 1$.

(1.6) (Kevin) Find the $gcd(1721, 378)$.

$$\begin{aligned} 1721 &= (4)(378) + 209 \\ 378 &= (1)(209) + 169 \\ 209 &= (1)(169) + 40 \\ 169 &= (4)(40) + 9 \\ 40 &= (4)(9) + 4 \\ 9 &= (2)(4) + 1 \end{aligned}$$

So $gcd(1721, 378) = 1$.

In trying to get people involved in the discussion, we decided that we will postpone the proof of the *Division Theorem* and think about a new practical problem.

2. The Money Problem

Suppose you are the king of the *N0BEH-Kingdom: (Nothing Bad Ever Happens)-Kingdom*, and so you have a lot of time to come up with funny laws: you decide to change the currency of your kingdome and use just bills of \$6 and \$10.

The moms of your kingdom start complaining: they cannot buy \$ 11 T-shirts. Is this true? What is going on? The king goes to the royal Mathematician.

(2.1) (Alex) If you have just \$6 and \$11 bills, then you can exchange a-dollars if and only if a is even. (So the moms are right).

In fact, let a be an even number then $a = 2b$ for some integer b. So $6a - 10b = 6a - 10(a/2) = a$ (Yes, it is a proof). On the other hand, if a is an odd number, there is no way we can write $a = x6 + y10$ for some integers x and y. In fact $x6 + y10$ is always an even number, and we showed that a number cannot be even and odd at the same time.

(2.2) Let's use \$6 and \$11 bills. We decided very soon that we were better off because we could buy \$1 T-shirts and therefore we could exchange any ammount of money:

$$1 = (2)(6) - 11$$

(2.3) What if we use \$6 and \$9 bills. You guys are really fast: we can exchange a dollars if and only if a is a multiple of 3. In fact, any number that can be written as $x6 + y9$ is a multiple of 3, and we can write $3 = 9 - 6$. So if a is a multiple of 3 then $a = 3b$, and therefore $a = b(9 - 6) = b9 - b6$

Almost immediately we were ready for the conjecture:

(2.4) **Conjecture.** If we have $\$a$ and $\$b$ bills, we can exchange x ammount of money if and only if x is a multiple of $d = gcd(a, b)$. Notice that there are two things to prove:

(1) If x is a multiple of d then we can exchange $\$x$.
(2) If we can exchange $\$x$ then x has to be a multiple of d.

(2.5) **Homework.** Try to prove the conjecture. But before doing so, write it in mathematical language.