Worksheet 1: Euclidean Algorithm

1. In your group, remind each other about tests for divisibility by 2, 3, and 5. Prove that these tests work.

   Proof for the divisibility of three statement: Let $n \in \mathbb{Z}$ be expressed in its base 10 representation:

$$n = a_k 10^k + a_{k-1}10^{k-1} + \cdots + a_1 10 + a_0 10^0 = \sum_{i=0}^{k} a_i 10^i$$

   Argument:

$$if 3 | \sum_{i=0}^{k} a_i \rightarrow 3 | \sum_{i=0}^{k} a_i 10^i$$

$$\sum_{i=0}^{k} a_i 10^i = \sum_{i=0}^{k} a_i (1 + 10^i - 1)$$

$$\sum_{i=0}^{k} a_i 10^i = \sum_{i=0}^{k} a_i + \sum_{i=0}^{k} a_i (10^i - 1)$$

   Since $3| \sum_{i=0}^{k} a_i$ this implies $3| \sum_{i=0}^{k} a_i = 3m, m \in \mathbb{Z}$
   Also note that:

$$\forall i \in \mathbb{Z} \quad 3|(10^i - 1)$$

   Since

$$(10^i - 1) = \sum_{k=0}^{i-1} 9(10^k) = 3(\sum_{k=0}^{i-1} 3(10^k)) = 3n, n \in \mathbb{Z}$$

   Using these s we can now express the $(10^i - 1)$ as a multiple of 3 in the following way and subsitute the sum of the coeffients by the original argument:

$$\sum_{i=0}^{k} a_i 10^i = 3m + \sum_{i=0}^{k} a_i 3n$$

$$\sum_{i=0}^{k} a_i 10^i = 3(m + \sum_{i=0}^{k} a_i n)$$

   Thus we have shown that $\sum_{i=0}^{k} a_i 10^i$ must also be divisible by three.

2. Let $a, b, c \in \mathbb{Z}$ with $c \neq 0$. Prove that if $c \mid a$ and $c \mid b$ then $c \mid (ax + by)$ for any $x, y \in \mathbb{Z}$.

   Since c|a this implies that $a = ck, k \in \mathbb{Z}$ likewise since c|b this implies $b = cm, m \in \mathbb{Z}$. Using these new definitions we can re express the term $(ax + by)$ as

$$(ck(x) + cm(y)) = c(kx + my)$$

Since k, x, m, y are integers this means that $c|(ax + by)$ as $(ax + by)$ can be expressed as a multiple of c.

3. (a) Why is the fraction $\frac{a}{0}$ "undefined" for $a \neq 0$?

Since the product of any number and zero is zero there is no defined solution for the inverse of multiplication which is division. Assigning a value α to $\frac{a}{0}$ would be akin to making the argument that α*0 = 0 Which contradicts the original notion that a does not equal zero

Consider the following:

$$f : \mathbb{R} \mapsto \{0\} \quad f(x) = 0 * x$$

f is not bijective therefore there does not exist an inverse. In this case division by zero.

(b) Why is $\frac{0}{0}$ "indeterminate?"

$\frac{0}{0}$ is indeterminate because it can represent infinite different answers. For example consider the case in which $\frac{0}{0}$ assumes a finite value β. This implies that

$$0(\beta) = 0$$

this statement is true but due to the nature of multiplying by zero the selection of beta is arbitrary which implies that the solution to $\frac{0}{0}$ is also arbitary and can assume any value.

4. The *division algorithm* says that every division problem has a unique quotient and remainder. Come up with a precise mathematical statement for the division algorithm and prove it.

Assuming that the divison problem this question is concerned with is dealing with integers then the argument of the divison algorithm states that there exists two unique integers q, and r representing the quotient and remainder of the divison.
Some notes:
- The integer divisor cannot be equal to zero as explained in problem 3.
- The remainder must be greater than or equal to zero.
- It does not make sense to have the remainder be greater than or equal to the divisor of the division operation occuring since it would be divided into a smaller remainder so it must be less than
- The resulting quotient and remainder can be used to re-express the dividend.

Expressed symbolically: Given two integers n and m $\in \mathbb{N}, m \neq 0$

$$\exists! \quad q, r \in \mathbb{N} : n = qm + r, 0 \leq r < b$$

To prove this statement we will have to prove both existence and uniqueness. **Existence**: Let $a \in \mathbb{N}$ and define a set A as :

$$A = \{x \in \mathbb{N} : t(b) > a\}$$

A is a nonempty subset of the natural numbers, thus by the well ordering principle there is a smallest element in A. Let x_0 be this smallest element. Let r=a-qb
a=qb+a-qb
We now consider the case where

Uniqueness

5. Come up with a definition of the *greatest common divisor* of two integers. There are various ways to define the gcd; discuss advantages and disadvantages in your group. Eucldian algorithm 294=193(1)+101
193=101(1)+92
101=92(1)+9
92=9(10)+2
9=2(4)+1
2=1(2)+0
gcd(294,193)=1

6. Pick two 3-digit positive integers $a > b$ and run the division algorithm when b is divided into a. Run the algorithm again when the remainder is divided into b; repeat until you get remainder 0. What are you computing? Why?

7. Let $a, b \in \mathbb{Z}$, not both zero. Prove that there exist $x, y \in \mathbb{Z}$ such that

$$ax + by = \gcd(a, b)\,.$$

More generally, prove that

$$ax + by = c$$

has a solution $(x, y) \in \mathbb{Z}^2$ if and only if $\gcd(a, b) \mid c$.

8. Andrews 2.3.1.

9. Experiment with the `sage` command `divmod`. Use it with two arguments, say a 6-digit and a 3-digit number, and check that `sage` gives the correct answer.

10. Experiment with the `sage` command `xgcd`. Use it with two 5-digit arguments and check that `sage` gives the correct answer.

11. Write down a precise statement for each definition we have given this week. For each definition, give an example and a non-example.