MATH 370 Lecture 3

Chris Camano: ccamano@sfsu.edu

August 30, 2022

Opening notes

The following is a recap of a short lecture on how to compute the greatest common denominator and least common multiple of two very large integers.

Theorem 0.1. *Division Algorithm: Let* $a, b \in \mathbb{Z}, b > 0$ *then:*

$$\exists! \quad q, r \in \mathbb{Z} : a = qb + r \quad 0 \leq r < b$$

Proof. Let S be the following nonempty set:

$$S = \{a - bk : k \in \mathbb{Z} \wedge a - bk \geq 0\}$$

First show that s is nonempty: If $a \geq 0$ then for k=0$a - bk = a$ which means a is in the set.

If $a < 0$ then let k=2a therefore $a - b(2a) = a(1 - 2b)$ so for all b since a is negative we get a product of two negative numbers which is postiive.

If $0 \in S$ then $\exists q \in \mathbb{Z}$ such that $a - bq = 0$. This means that $a = bq + 0$ or $a = bq$

If $0 \notin S$ since S is a nonempty set of positive integers by the well ordering principle there exists a smallest element of that set since the set S is then a subset of the natural number . let this smallest element be r. $r \in S, r \in \mathbb{Z}^+, r = \min(S)$

So there exists an integer q such that $r = a - bq$ this implies that $a = bq + r$

We now need to show that r is smaller than b: Suppose that r is not smaller then b, this would imply that r which means that $a = bq + r$ but since r is greater than b we can right the expression as $b(q + 1) + (r - b)$ but since r is greater than b $r - b$ is non negative. $r - b \geq 0$ Hence r-b should be in s however r-b is smaller r but r is supposed to be the smallest element in S by the well ordering principle. $\square$