MATH 335 Lecture 4

Chris Camano: ccamano@sfsu.edu

September 1, 2022

Continuation of division algorithm proof: Proof of uniqueness

Gernela philosophy of proving unieqeness. Suppose there exist two of something that is supposed to be unique then prove that they have to be equal to eachother by some proof techinque. Applying that here we will take a direct proof alongside the division algorithm.

Suppose there also exist integersq^*, r^*, with $r^* < b$ and $a = bq^* + r^*$

we can rearrnage into the following eequivilancy:

$$\begin{aligned} bq + r &= bq^* + r^* \\ b(q - q^*) &= r^* - r \end{aligned}$$

Since $0 \le r < b$ and $0 \le r^* < b$ the difference must also be smaller then b.

$$b|(q - q^*)| = |r^* - r|$$

The only way this equation holds is if $|(q - q^*)| = |r^* - r| = 0$ meaning that the difference of the two quotients and remainders is zero so they are the same.

Theorem 0.1. *Let a,b $\in \mathbb{Z}, a, b \neq 0$ Then $\exists t, u \in \mathbb{Z}$such that:*

$$gcd(a, b) = at + bu$$

Proof. Let :

$$S = \{am + bn : m, n \in \mathbb{Z}, am + bn > 0\}$$

$S \subset \mathbb{N}$ therefore by well ordering there is a least element denoted $S_{\min} = d$

So there exist integers t,u such that:

$$d = at + bu$$

We now show that d is the gcd of a and b: By division algorithm:

$$a = dq + r, 0 \leq r < d \quad q, r \in \mathbb{Z}$$

$$\begin{aligned} r &= a - dq \\ r &= a - (at + bu)q \\ r &= a(1 - qt) + b(-uq) \end{aligned}$$

So $r \in \S$ but by definition $r < d$ and d is the smallest element of S so r cannot exist meaning that $d|a$

Suppose that there is some other integer e such that $e|a$ and $e|b$ then:

$$e|at + bu$$

so $e|d$ □

Definition 0.2. if the gcd of two intergers is equal to one they are called relatively prime. Note that in this case if two integers are relatively ,$gcd(a, b) = 1 = at + bu, t, u \in \mathbb{Z}$

Definition 0.3. The counting function: Let $n > 1, n \in \mathbb{Z}$ Let:

$$U_n = \{a \in \mathbb{Z} : 1 \leq a \leq n, gcd(a, n) = 1\}$$

Then $\phi(n)$ is the cardinality of U_n

$$\phi(n) = |U_n|$$

$$\phi(p) = p - 1$$

when p is a prime. Because a prime number is realtively prime to all integers before it. if :

$$1 \leq a \leq a$$

and n is prime gcd(a,n)=1 unless a=n