MGF 3301 : Bridge to Abstract Mathematics

Professor: Brendan Nagle

Notes by James Harbour

October 26, 2019

§1 Exam 1 Proofs

Theorem 1.1 (Bezout's Identity)
For all $a, b \in \mathbb{N}$,

$$\gcd(a,b) = \min\{as + bt : s,t \in \mathbb{Z} \text{ satisfy } as + bt > 0\}$$

Proof. Let $a, b \in \mathbb{N}$ be positive integers and let $A = \{as+bt : s,t \in \mathbb{Z} \text{ satisfy } as+bt > 0\}$. Set $D = \gcd(a,b)$. Because $A \subseteq \mathbb{N}$ and trivially $A \neq \varnothing$, by the Well Ordering Principle there is a smallest element in A. Thus, set $m = \min(A)$. We now continue by proving two claims.

Claim 1.2 (Easy Part) — $D \leq m$

Proof. Let $s_0, t_0 \in \mathbb{Z}$ satisfy $m = as_0 + bt_0$. Since $D \mid a$ and $D \mid b$, it follows that $D \mid (as_0 + bt_0)$. Thus, by our hypothesis, $D \mid m$, so by definition $D \leq m$. ■

Claim 1.3 (Hard Part) — $D \geq m$

Proof. Consider that $(m \mid a \wedge m \mid b) \implies m \mid D \implies m \leq D$. So we show that $m \mid a \wedge m \mid b$. Assume, for the sake of contradiction, that *w.l.o.g.*, $m \nmid a$.
By division with remainder, $\exists\ q = q_{m,a} \in \mathbb{Z}$ and $\exists\ r = r_{m,a} \in \mathbb{Z}$ such that

$$a = qm + r, \qquad 0 \leq r < m \tag{1}$$

In fact, because $m \nmid a$, we know that $0 \leq r < m$. Since $m = as_0 + bt_0$,

$$\begin{aligned} a &= qm + r \\ &\overset{(1)}{=} q(as_0 + bt_0) + r \\ &= (qs_0)a + (qt_0)b + r \\ r &= (1 - qs_0)a + (-qt_0)b \end{aligned}$$

So, r is an integer linear combination of a and b because $1 - qs_0 \in \mathbb{Z}$ and $-qt_0 \in \mathbb{Z}$. By division with remainder, $r > 0$ and $r < m$. So it follows that $r \in A$, however by the well ordering principle, m is the smallest element of A, thus we have reached a contradiction. ■

□

Lemma 1.4 (Euclid's Lemma)
For all $a, b, p \in \mathbb{N}$, if p is prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof. Let $a, b \in \mathbb{N}$ and let $p \in \mathbb{N}$ be prime with $p \mid ab$. If $p \mid a$ or $p \mid b$, then we are done. So, assume *w.l.o.g.* that $p \nmid a$. Because p is prime, its only divisors are p and 1, and since $p \nmid a$, it follows that $\gcd(p, a) = 1$. Thus, by Bezout's Identity, $\exists\ s, p \in \mathbb{Z}$ such that

$$\begin{aligned} as + pt &= 1 \\ abs + pbt &= b \end{aligned}$$

Because $p \mid ab \implies p \mid abs$ and $p \mid p \implies p \mid p(bt)$, we have that $p \mid (abs + pbt)$. Thus $p \mid b$. $\square$

§2 Exam 2 Proofs

Theorem 2.1 (Division with Remainder)

For all integers $a, b \in \mathbb{Z}$, where $a \neq 0$, there exist unique integers $q, r \in \mathbb{Z}$ such that

$$b = aq + r, \quad \text{where } 0 \leq r < |a|.$$

Existence Portion. Let integers $a, b \in \mathbb{Z}$ be given, where $a \neq 0$. If $a \mid b$, then there exists some integer $k \in \mathbb{Z}$ such that $b = ka$. By choosing $q = k$ and $r = 0$, we have that $b = aq + r$ with $0 \leq r = 0 < |a| \neq 0$ and are done. Thus, suppose that $a \nmid b$, with $a \neq 1$ and $b \neq 1$.

Consider the sets

$$\mathcal{R} = \{b - am : m \in \mathbb{Z}\} \quad \text{and} \quad \mathcal{R}^+ = \mathcal{R} \cap \mathbb{N}.$$

Claim 2.2 (W.O.P. Condition) — $\mathcal{R}^+ \neq \emptyset$

Proof. Choose $m = m_0 = -\dfrac{|a||b|}{a}$. Because $\dfrac{|a|}{a} = \pm 1 \in \mathbb{Z}$, we have that $m_0 = \pm|b| \in \mathbb{Z}$; thus $b - am_0 \in \mathcal{R}$. With this choice, we have that

$$\begin{aligned} b - am_0 &= b - a\left(\frac{-|a||b|}{a}\right) \\ &= b + |a||b| \\ &\geq -|b| + |a||b| \\ &= |b|\left(|a| - 1\right) \overset{\text{hyp}}{\geq} 1 \end{aligned}$$

Thus $b - am_0 \in \mathcal{R}^+$, so $\mathcal{R}^+ \neq \emptyset$. ■

Because $\emptyset \neq \mathcal{R}^+ \subseteq \mathbb{N}$, the Well-Ordering Principle guarantees that $\mathcal{R}^+$ admits a least element $r_0 = \min \mathcal{R}^+$, where we write $r_0 = b - aq_0$ for some positive integer $m = q_0 \in \mathbb{Z}$. Thus $b = aq_0 + r_0$ with $r_0 \geq 1 > 0$ because $r_0 \in \mathcal{R}$. We must now show that $r_0 < |a|$.

Claim — $r_0 < |a|$

Proof. Suppose, for the sake of contradiction, that $r_0 \geq |a|$. If $r_0 = |a|$, then

$$\begin{aligned} b &= aq_0 + r_0 \\ &= aq_0 + |a| \\ &= a\left(q_0 + \frac{|a|}{a}\right) = a\left(q_0 \pm 1\right) \end{aligned}$$

Thus $a \mid b$, which is a contradiction. If $r_0 > |a|$, i.e. $r_0 \geq |a| + 1$, then

$$\begin{aligned} b &= aq_0 + r_0 \\ &\geq aq_0 + |a| + 1 \\ &= a\left(q_0 + \frac{|a|}{a}\right) + 1 \end{aligned}$$

And so the integer

$$b - a\left(q_0 + \frac{|a|}{a}\right) \geq 1$$

belongs to $\mathcal{R}^+$. On the other hand,

$$\begin{aligned} b - a\left(q_0 + \frac{|a|}{a}\right) &= b - aq_0 - |a| \\ &< b - aq_0 = r_0 \end{aligned}$$

which is a contradiction, as r_0 is the smallest element of $\mathcal{R}^+$. Thus, $r_0 < |a|$ ■

□