Math 302 Theorem 2.3

Raiden van Bronkhorst

27 January 2020

Proof. Because $gcd(a, b) = gcd(|a|, |b|)$, let $a = |a|$ and $b = |b|$ from now on.

Suppose set $S = \{ax + by : x, y \in \mathbb{Z}, ax + by > 0\}$.

Case 1. $a = 0$ or $b = 0$

Without loss of generality, suppose $a = 0$. Then choosing $y = 1$ gives us $0 + b = b$. Because a and b cannot both be zero, $b > 0$. Therefore b is in set S.

Case 2. $a \neq 0$ and $b \neq 0$.

Then choose $x = 1$ and $y = 1$, which gives us $a + b$. Because $a \geq 0$, $b \geq 0$, and a and b cannot both be 0, $a + b > 0$. Therefore $a + b$ is in set S.

Therefore S is nonempty. By the well-ordering property, S must have some least element d, so d is the smallest positive integer that can be written as $ax + by$.

Suppose $c = gcd(a, b)$. Then $c|a$ and $c|b$, so $ck_1 = a$ and $ck_2 = b$ for some integers k_1 and k_2. Thus $d = ax + by = ck_1x + ck_2y = c(k_1x + k_2y)$. So, $c|d$. This means $c \leq d$.

By the Division Algorithm, we can write $a = m_1d + r_1$ for some integers m_1 and r_1, such that $0 \leq r_1 < m_1$. Then $r_1 = a - dm_1 = a - (ax + by)m_1 = a(1 - m_1x) + b(-m_1y)$. So, r_1 is also in the form $ax + by$. Since $0 \leq r_1 < d$ and d is the smallest positive integer of the form $ax + by$, r_1 must be 0. Therefore $a = md$, so $d|a$.

By the Division Algorithm we can also write $b = m_2d + r_2$ for some integers m_2 and r_2, such that $0 \leq r_2 < m_2$. By the same process as above, we find that $r_2 = 0$, so $d|b$.

Since $d|a$ and $d|b$, then $d \leq c$. We have $c \leq d \leq c$, so $c = d$. $\square$