Euclidean Algorithm Proof

Kelin Luo

1 Preliminary

Definition 1. *For any two integers a and e, if integer a is divided by e without producing a remainder, then we have $e|a$ (read as e divides a).*

Definition 2. *An integer e is called the $gcd(a, b)$ (read as the greatest common divisor of integers a and b) if the following two conditions hold:*

- *$e|a$ and $e|b$*
- *For any common divisor d of a and b, $e \geq d$.*

2 Proof for Euclidean Algorithm

Lemma 3. *Given two integers a and b, WLOG, assume $a \geq b$. Then, for any integers c and d such that $a = bc + d$, $gcd(a, b) = gcd(b, d)$.*

Note: WLOG is a common abbreviation for "without loss of generality", which means that the assumption made (in this case, $a \geq b$) does not restrict the generality of the proof.

Proof. We prove the lemma in two directions:

- Forward Direction: if $gcd(a, b) = e$, then we show that $gcd(b, d) = e$.

  Since $gcd(a, b) = e$, according to the Definition of gcd, we know that:

  $$e|a \quad \text{and} \quad e|b.$$

  From the equation $a = bc + d$, we can rewrite it as: $a - bc = d$. Since $e|a$ and $e|b$, we have: $e|(a - bc)$, which implies that: $e|d$.

  Now, since $e|b$ and $e|d$, by the Definition of gcd, we can conclude that: $gcd(b, d) = e$. This is because any common divisor of b and d must also divide their linear combination $bc + d$, and since e is the gcd of a and b, it follows that any common divisor of b and d must be less than or equal to e. This completes the forward direction proof.

- Reverse Direction: if $gcd(b, d) = e$, then we show that $gcd(a, b) = e$.

  Please complete the proof for Reverse Direction on your own.

$\square$