CSE 311: Foundations of Computing I

GCD Annotated Proofs

Relevant Definitions

GCD (Greatest Common Divisor)	Definition
The *gcd* of two integers, a and b, is the largest integer d such that $d \mid a$ and $d \mid b$.	

Euclidean Algorithm	Algorithm

```
gcd(a, b) {
   if (b == 0) {
      return a;
   }
   else {
      return gcd(b, a mod b);
   }
}
```

Useful GCD Identity

Prove that for $a, b \in \mathbb{Z}^+$, $\gcd(a, b) = \gcd(b, a \text{ mod } b)$.

Proof	Commentary & Scratch Work
We show that the factors shared by a and b are identical to the factors shared by b and a mod b.	*The idea is to treat the left and right as sets. If the sets are equal, then the largest elements in the sets must also be equal.*
Note that, by the division theorem, there is some integer q such that a mod $b = a - qb$.	*Get rid of the mod notation.*
Now, define the following: • $F_{a,b} = \{d : (d \mid a) \land (d \mid b)\}$, and • $F_{b,m} = \{d : (d \mid b) \land (d \mid a \text{ mod } b)\}$ We show $F_{a,b} = F_{b,m}$.	*Re-state the claim in terms of sets to make it easier to think about. We'll now prove both subset inclusions.*
Suppose $d \in F_{a,b}$.	*We're proving an implication, right?*
Then, by definition of $F_{a,b}$, we have $d \mid a$ and $d \mid b$. So, by definition of divides, we have $a = dk_a$ and $b = dk_b$.	*Unroll the definition of d.*
Note that, as above, a mod $b = a - qb = dk_a - q(dk_b) = d(k_a - qk_b)$. So, $d \mid a$ mod b by definition.	*Use the definitions of a mod b, a, and d.*
Since $d \mid b$ and $d \mid a$ mod b, $d \in F_{b,m}$.	*Conclude that $d \in F_{b,m}$.*
Now, suppose $d \in F_{b,m}$.	*Prove the other implication...*

Then, by definition of $F_{b,m}$, we have $d \mid b$ and $d \mid a$ mod b. So, by definition of divides, we have $b = dk_b$ and a mod $b = dk_m$.	*Unroll the definition of d.*
Note that $a = a$ mod $b + qb = dk_m + q(dk_b) = d(k_m + qk_b)$. So, $d \mid a$ by definition.	*Use the definitions of a mod b, a, and d.*
Since $d \mid a$ and $d \mid b$, $d \in F_{b,m}$.	*Conclude that $d \in F_{b,m}$.*
It follows that $F_{a,b} = F_{b,m}$. Furthermore, $\max(F_{a,b}) = \max(F_{b,m})$. That is, the *largest* factor shared between a and b is the same as the *largest* factor shared between b and a mod b. That's just another way of saying $\gcd(a, b) = \gcd(a, a$ mod $b)$.	*Use our conclusion to show the conclusion we actually wanted.*