Math 341 Homework 5

Theo Koss

September 2020

1 Practice problems

1.1 Problem 2

Suppose $a \vdots b$. Show that $\gcd(a, b) = b$.

Proof. If $a \vdots b$, then by definition, $a = bn$, for some $n \in \mathbb{Z}$. This also, by definition, implies that b is a *factor* of a. The common denominators, $\mathrm{cd}(a, b) = \{1, \ldots, b\}$, at the very least, includes 1 and b. Also, b must be the largest element, because the factors of b are $b = \{1, ..., b\}$, meaning the largest factor is b itself. And the factors of a are $a = \{1, ..., b, ..., a\}$. The largest element that both of these share is b, since b is the largest factor of b and is also included in a. Therefore $\gcd(a, b) = b$ if $a \vdots b$. QED

1.2 Problem 3

Suppose $a \not\vdots b$, divide a by b with remainder r. Show that $\gcd(a, b) = \gcd(b, r)$.

Proof. If $a \not\vdots b$, then by definition, $\exists q, r \in \mathbb{Z},$ such that $a = bq + r,$ and $0 \leq r < b$. Denote $X = \gcd(a, b)$ and $Y = \gcd(b, r)$. By definition, $a \vdots X$ must be true, as must $b \vdots X$. And, by example 2.2, since $a \vdots X$, $b \vdots X$, and $(a - bq) \vdots X$. Then $r \vdots X$. Also since both $b, r \vdots X$, then $X \leq \gcd(b, r)$. This means that X is in Y, or $X \subset Y$. Similarly, since $b \vdots Y$, $r \vdots Y$, and $(bq + r) \vdots Y$, that means $a \vdots Y$. And, since $a \vdots Y$ and $b \vdots Y$, $Y \leq \gcd(a, b)$. This means that $Y \subset X$. Since $X \subset Y$ and $Y \subset X$, $Y = X$, and therefore if $a \not\vdots b, \gcd(a, b) = \gcd(b, r)$. QED

1.3 Problem 7

Prove that Euclid's algorithm works, i.e. it always stops and produces $\gcd(a, b)$.

Proof. By definition of division, for any $a, b \in \mathbb{N}$, such that $a > b$, $\exists q, r \in \mathbb{N}$, s.t. $a = bq + r$. Due to the iterative nature of Euclid's algorithm, I'll denote the first "step" as $a = bq_1 + r_1$, second, $b = r_1q_2 + r_2$, all of the form $r_{n-1} = r_nq_{n+1} + r_{n+1}$. Since you take a smaller value every time, it follows that $0 \leq r_n < r_{n-1} < ... < r_1 < b$. And, due to the fact that it is a strictly decreasing sequence of positive integers, you can't keep getting smaller indefinitely, and so eventually $r_{n+1} = 0$. In other words, it always terminates. As for why Euclid's Alg. always produces $\gcd(a, b)$, by problem 5.3, $\gcd(a, b) = \gcd(b, r_1) = \gcd(r_1, r_2) = ... = \gcd(r_{n-1}, r_n)$, and since $r_{n+1} = 0$, then $\gcd(a, b) = \gcd(r_n, 0) = r_n$. So Euclid's algorithm always terminates, and always produces $\gcd(a, b)$. QED