Homework Help

Section 1.1, Problem 5

February 2, 2006

Exercise 1.1-5

Prove the equality $\gcd(m, n) = gcd(n, mmodn)$ for every pair of positive integers m and n.

Help

The hint in the back of the book is very helpful for this problem. In addition, I will help by making a few basic observations about basic facts of which we are aware, as well as comments about the hint provided by the book. Some facts that may help us here are as follows:

(i) An integer added to, or subtracted from, another integer always results in an integer

(ii) An integer multiplied by another integer always results in an integer

The following are some observations about the hint:

(iii) The "Why?" question in the last line of the hint can be answered simply by application of the commutative rule and (i) from above.

(iv) The formula given in the hint is pulled directly from the definition of the division of natural numbers: if m and n are natural numbers and n is non-zero, there exist two unique integers q (quotient) and r (remainder) such that $m = qn + r$ and $r \in [0, n)$

(v) Observe that q must be a natural number by definition and consider the formula from (iv) and facts (i) & (ii) from above. Suppose m and n are evenly divisible by some integer d, what does that tell as about r? Suppose n and r and evenly divisible by d, what does that tell us about m? What is r?

One more thing remains:

(vi) The above hints will get the the **cd** (common divisor) part of $\gcd$, but there's one last bit of logic to get the **g** part ...