Chapter 0 Exercises
Gallian's Book on Abstract Algebra

Spencer T. Parkin

January 26, 2014

Problem 12

Let a and b be positive integers and let $d = \gcd(a, b)$ and $m = \operatorname{lcm}(a, b)$. If t divides both a and b, prove that t divides d. If s is a multiple of both a and b, prove that s is a multiple of m.

By Theorem 0.2, d is a linear combination of a and b, and therefore, any common divisor of a and b, such as t, also divides d.

To see that m divides s, simply notice that all common multiples of a and b are generated by all positive multiples of m.

Problem 24

(Generalized Euclid's Lemma) If p is a prime and p divides $a_1 a_2 \dots a_n$, prove that p divides a_i from some i.

The case $n = 2$ is covered by Euclid's Lemma. Now suppose, for a fixed integer $k > 2$, that the generalized lemma holds in the case $n = k - 1$. Now consider the case $n = k$. If p does not divide a_n, then clearly p divides $a_1 a_2 \dots a_{n-1}$ by Euclid's Lemma. Then, by our inductive hypothesis, p must divide a_i for an integer $i \in [1, n-1]$. We have now proven the general lemma by the principle of mathematical induction.

Problem 25

Use the Generalized Euclid's Lemma (see Exercise 24) to establish the uniqueness portion of the Fundamental Theorem of Arithmetic.

Suppose an integer n has two different prime factorizations $p_1^{a_1} \dots p_r^{a_r}$ and $q_1^{b_1} \dots q_s^{b_s}$. By the Generalized Euclid's Lemma, if $p \in \{p_i\}_{i=1}^r$, then $p \in \{q_i\}_{i=1}^s$, because p divides n. Conversely, if $p \in \{q_i\}_{i=1}^s$, then $p \in \{p_i\}_{i=1}^r$ by the same reason. It follows that $\{p_i\}_{i=1}^r = \{q_i\}_{i=1}^s$, which is a contradiction, and therefore, no integer n has two different prime factorizations.