Geoffrey Parker - grp352
HW 9: 2.25-2.31
M328K
February 16th, 2012

2.25 Theorem. *Let a, b, and n be integers. If $a \mid n$, $b \mid n$, and $(a,b) = 1$, then $ab \mid n$.*

Proof. Let a, b, and n be integers where $a \mid n$, $b \mid n$, and $(a,b) = 1$. We will show that $ab \mid n$. Let $p_1^{r_1} p_2^{r_2} \cdots p_m^{r_m}$ be the unique prime factorization of a, $q_1^{r_1} q_2^{r_2} \cdots q_s^{t_s}$ be the unique prime factorization of b, and $x_1^{y_1} x_2^{y_2} \cdots x_z^{y_z}$ be the unique prime factorization of n. Now, since a and b are coprime, there cannot be any i and j such that $p_i = q_j$, because if there were, (a,b) would be p_i. This means that the unique prime factorization of ab is $p_1^{r_1} q_1^{r_1} p_2^{r_2} q_2^{r_2} \cdots p_m^{r_m} q_s^{t_s}$, with s and m possibly being different and none of these terms combining. However, by theorem 2.12, we have that for all integers $i \leq m$ there exists a $u \leq y$ such that $p_i = x_u$ and $r_i \leq y_u$, and for all integers $j \leq s$ there exists an integer $v \leq z$ such that $q_j = x_v$ and $t_j \leq y_v$. Therefore given the unique prime factorization of ab and theorem 2.12, this means that $ab \mid n$.

OR

This is just theorem 1.42, restated exactly. $\square$

2.26 Theorem. *Let p be prime and let a be an integer. Then p does not divide a if and only if $(a,p) = 1$.*

Proof. Let p be prime and let a be an integer.
First, assume that $p \nmid a$. Since p is prime, the only divisors that p has are 1 and itself. And since $p \nmid a$, the only divisor p and a could possibly share is 1. Therefore $(a,p) = 1$.
Now, assume that $(a,p) = 1$. Since all numbers divide them selves, if $p \mid a$, then (a,p) would be p. Therefore $p \nmid a$. $\square$

2.27 Theorem. *Let p be prime and let a and b be integers. If $p \mid ab$, then $p \mid a$ or $p \mid b$.*

Proof. Let p be prime and let a and b be integers with $p \mid ab$. We will show that $p \mid a$ or $p \mid b$. Assume by way of contradiction that $p \nmid a$ and $p \nmid b$. Since p is prime, the unique prime factorization of p is just p. By theorem 2.12 and our assumption, this means that p is not a member of the unique prime factorizations of either a or b. This means in turn that p is not a member of the unique prime factorization of ab. And by theorem 2.12, this implies that $p \nmid ab$, so we have our contradiction. Therefore $p \mid a$ or $p \mid b$. □

2.28 Theorem. *Let a, b, and c be integers. If $(b, c) = 1$, then $(a, bc) = (a, b) \cdot (a, c)$.*

Solution. Let a, b, and c be integers with $(b, c) = 1$. By definition, $(a, b) \mid a$, and by theorem 1.6 $(a, b) \mid bc$. Similarly, $(a, c) \mid a$ and $(a, c) \mid bc$. Now by definition of gcd, $((a, b), (a, c))$ will be the greatest of all the divisors common to a, b, and c, which since $(b, c) = 1$, is 1. So $(a, b) \cdot (a, c) \mid (a, bc)$. //TODO □

2.29 Theorem. *Let a, b and c be integers. If $(a, b) = 1$ and $(a, c) = 1$, then $(a, bc) = 1$.*

Solution. Let a, b and c be integers with $(a, b) = 1$ and $(a, c) = 1$. We will show that $(a, bc) = 1$. Let A be the set of primes in the unique prime factorization of a, B for b and C for c. So we can say that there is no prime p which is a common element of either the sets A and B or the sets A and C, because if there was, we would have $(a, b) = p$ or $(a, c) = p$. Therefore $A \cap (B \cup C)$ is empty. Now consider any integer k which is a common divisor of a and bc. Let K be the set of primes in the unique prime factorization of k. By theorem 2.12, since $k \mid a$ and $k \mid bc$, every element of K must be an element of both A and $(B \cup C)$. That is K is a subset of $A \cap (B \cup C)$. However, $A \cap (B \cup C)$ is empty, so K must also be empty. Therefore k must be 1, that is the only common divisor of a and bc is 1, so $(a, bc) = 1$. □

2.30 Theorem. *Let a and b be integers. If $(a, b) = d$, then $(\frac{a}{d}, \frac{b}{d}) = 1$.*

Proof. Let a and b be integers, with $(a, b) = d$. We will show that $(\frac{a}{d}, \frac{b}{d}) = 1$. //TODO □

2.31 Theorem. *Let a, b, u, and v be integers. If $(a, b) = 1$ and $u \mid a$ and $v \mid b$, then $(u, v) = 1$.*

Proof. Type your proof here! □