Dr. Nestler - Math 10 - Primes

Lemma. Let $a, b, c \in \mathbb{Z}$.

(1) If $a \mid b$ and $b \neq 0$, then $|a| \leq |b|$.

(2) If $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ for any $x, y \in \mathbb{Z}$.

Proof: (1) If $a \mid b$ then $b = ac$ for some $c \in \mathbb{Z}$. Since $b \neq 0$, $c \neq 0$. Then $|b| = |ac| = |a||c|$. Since $c \neq 0$, $|c| \geq 1$, and so $|b| = |a||c| \geq |a|$.

(2) If $a \mid b$ and $a \mid c$, then $b = ar$ and $c = as$ for some $r, s \in \mathbb{Z}$. Then $bx + cy = arx + asy = a(rx + sy)$ for any $x, y \in \mathbb{Z}$. Since $rx + sy \in \mathbb{Z}$, this says $a \mid (bx + cy)$. □

Let $\gcd(a, b)$ represent the greatest common divisor of integers a and b.

Theorem. Given integers a and b, not both of which are zero, there exist integers x and y such that $\gcd(a, b) = ax + by$.

Proof: Let $S = \{au + bv : u, v \in \mathbb{Z} \text{ and } au + bv > 0\}$; that is, S is the set of all positive linear combinations of a and b. S is not empty since, for example, if $a \neq 0$, then the integer $|a| = au + b \cdot 0$ is in S, where we choose u to be 1 or -1 depending on whether $a > 0$ or $a < 0$. By the Well-Ordering Principle, a nonempty set S of positive integers must have a least element d. Therefore there exist $x, y \in \mathbb{Z}$ such that $d = ax + by$. We will prove that $d = \gcd(a, b)$.

By the Division Algorithm, proved in Section 5.2 Example 5 on p. 341, $a = qd + r$ where $q, r \in \mathbb{Z}$ and $0 \leq r < d$. (In other words, given any integers a and $d \neq 0$, dividing a by d leads to a quotient q and remainder r, both integers.) Then we have $r = a - qd = a - q(ax + by) = a(1 - qx) + b(-qy)$.

If $r > 0$, then this would imply that $r \in S$. But d is the least integer in S. Thus $r = 0$, and so $a = qd$, so $d \mid a$. By a similar argument, $d \mid b$. So d is a common divisor of both a and b. If c is any positive common divisor of a and b, then by (2) of the lemma, $c \mid (ax + by)$, meaning $c \mid d$. By (1) of the lemma, $c = |c| \leq |d| = d$, so that d is larger than every positive common divisor of a and b. Thus $d = \gcd(a, b)$. □

Theorem (Euclid's Lemma). If $a \mid bc$, with $\gcd(a, b) = 1$, then $a \mid c$.

Proof: By the previous theorem, there exist integers x and y such that $1 = ax+by$. So $c = 1 \cdot c = (ax + by)c = acx + bcy$. Since $a \mid ac$ and $a \mid bc$, we have $a \mid (acx + bcy)$ by (2) of the lemma. But $acx + bcy = c$. So $a \mid c$.

Corollary: If p is prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof: If $p \mid a$, then we are done. So suppose p does not divide a. Since p is prime, $\gcd(p, a) = 1$. So by Euclid's Lemma, $p \mid b$. □