PROPOSITIONS ABOUT DIVISIBILITY

In the following propositions, the letters a, b, c, m, n, etc. always represent integers.

1. If $a|b$ and $b|c$, then $a|c$.

2. If $a|b$ and $a|c$, then $a|(mb+nc)$ for all $m, n \in \mathbf{Z}$.

3. (The Division Algorithm) Assume that $a \geq 1$ and that b is any integer. Then there exist integers q and r such that $b = aq + r$ and $0 \leq r < a$. For given a and b, the integers q and r are uniquely determined.

4. Assume that a and b are not both zero. Let $d = (a, b)$. Then there exist integers m and n such that $ma + nb = d$.

5. The integers a and b are relatively prime if and only if there exist integers m and n such that $ma + nb = 1$.

6. Assume that a and b are not both zero. Let $d = (a, b)$. Then $(a/d.\ b/d) = 1$.

7. (The SeeSaw Lemma) Suppose that $a = bq + c$, where $q \in \mathbf{Z}$. Then $(a, b) = (b, c)$.

8. Assume that a and b are not both zero. Let $d = (a, b)$. Suppose that $c|a$ and $c|b$. Then $c|d$.

9. Assume that $a \geq 1$ and $b \geq 1$. Let $d = (a, b)$. Let $m = ab/d$. Then $a|m$ and $b|m$. Furthermore, suppose that $n \in \mathbf{Z}$ and that $a|n$ and $b|n$. Then $m|n$. (Note; The integer m is called the *"least common multiple"* of a and b. It is often denoted by $m = [a, b]$.)

10. (Euclid's Lemma, first version) Suppose that p is a prime. If $p|ab$, then $p|a$ or $p|b$.

11. (Euclid's Lemma, extended version) Suppose that p is a prime and that $a_1, a_2, ..., a_t$ are integers. If $p|a_1 a_2 \cdots a_t$, then $p|a_i$ for at least one value of i, $\quad 1 \leq i \leq t$.

12. (Euclid's Lemma, alternate version) Assume that $a|bc$ and that $(a, b) = 1$. Then $a|c$.

13. (The Fundamental Theorem of Arithmetic) Suppose that $n > 1$. Then n can be expressed uniquely as a product of primes, up to order of the factors.

14. Suppose that $m \geq 1$. Let $a_1, a_2, ..., a_t$ be integers such that $(a_1, m) = (a_2, m) = ... = (a_t, m) = 1$. Then $(a_1 a_2 \cdots a_t, m) = 1$.