Handout 4.3

DEFINITION 1

An integer p greater than 1 is called *prime* if the only positive factors of p are 1 and p. A positive integer that is greater than 1 and is not prime is called *composite*.

THEOREM 1

THE FUNDAMENTAL THEOREM OF ARITHMETIC Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of nondecreasing size.

THEOREM 2

If n is a composite integer, then n has a prime divisor less than or equal to $\sqrt{n}$.

THEOREM 3

There are infinitely many primes.

THEOREM 4

THE PRIME NUMBER THEOREM The ratio of the number of primes not exceeding x and $x/\ln x$ approaches 1 as x grows without bound. (Here $\ln x$ is the natural logarithm of x.)

DEFINITION 2

Let a and b be integers, not both zero. The largest integer d such that $d \mid a$ and $d \mid b$ is called the *greatest common divisor* of a and b. The greatest common divisor of a and b is denoted by $\gcd(a, b)$.

DEFINITION 3

The integers a and b are *relatively prime* if their greatest common divisor is 1.

DEFINITION 4

The integers $a_1, a_2, \ldots, a_n$ are *pairwise relatively prime* if $\gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.

DEFINITION 5

The *least common multiple* of the positive integers a and b is the smallest positive integer that is divisible by both a and b. The least common multiple of a and b is denoted by $\operatorname{lcm}(a, b)$.

LEMMA 1

Let $a = bq + r$, where a, b, q, and r are integers. Then $\gcd(a, b) = \gcd(b, r)$.

THEOREM 6 **BÉZOUT'S THEOREM** If a and b are positive integers, then there exist integers s and t such that $\gcd(a, b) = sa + tb$.

ALGORITHM 1 The Euclidean Algorithm.

procedure $gcd(a, b$: positive integers)
$x := a$
$y := b$
while $y \neq 0$
    $r := x$ **mod** y
    $x := y$
    $y := r$
return $x\{\gcd(a, b)$ is $x\}$

THEOREM 5 Let a and b be positive integers. Then

$$ab = \gcd(a, b) \cdot \operatorname{lcm}(a, b).$$