LIST OF THEOREMS

Theorem 1: If a and b are nonzero integers, then their gcd is a linear combination of a and b, that is there exist integer numbers s and t such that

$$sa + tb = (a, b).$$

Theorem 2 (Euclid's Lemma): If p is a prime and $p \mid ab$, then $p \mid a$ or $p \mid b$. More generally, if a prime p divides a product $a_1 a_2 \dots a_n$, then it must divide at least one of the factors a_i.

Theorem 3 (Fundamental Theorem of Arithmetic): Assume that an integer $a \geq 2$ has factorizations

$$a = p_1 \dots p_m \quad \text{and} \quad a = q_1 \dots q_n,$$

where the p's and q's are primes. Then $n = m$ and the $q's$ may be reindexed so that $q_i = p_i$ for all i.

Theorem 4 (Fermat's Little Theorem): Let p be a prime. Then $p \mid n^p - n$ for any integer $n \geq 1$.

Theorem 5:

Let G be a group.

(i) If $x * a = x * b$ or $a * x = b * x$, then $a = b$.

(ii) The identity element e is unique.

(iii) For all $x \in G$, the inverse element x^{-1} is unique.

(iv) For all $x \in G$ we have $(x^{-1})^{-1} = x$.

(v) For all $a, b \in G$ we have $(a * b)^{-1} = b^{-1} * a^{-1}$.

Theorem 6:

A subset H of a group G is a subgroup $\iff$ H is nonempty and, whenever $x, y \in H$, then $xy^{-1} \in H$.

Theorem 7:

A nonempty subset H of a finite group G is a subgroup $\iff$ H is closed.

Theorem 8:

Let G be a finite group and let $a \in G$. Then the order of a is $|\langle a \rangle|$.

Theorem 9:

Let H be a subgroup of a group G, and let $a, b \in G$. Then

(i) $aH = bH \iff b^{-1}a \in H$.

(ii) If $aH \cap bH \neq \varnothing$, then $aH = bH$.

(iii) $|aH| = |H|$ for all $a \in G$.

Theorem 10 (Lagrange):
If H is a subgroup of a finite group G, then $|H|$ divides $|G|$.

Theorem 11:

Let $f : G \longrightarrow H$ be a homomorphism of groups. Then

(i) $f(e) = e$;

(ii) $f(x^{-1}) = f(x)^{-1}$;

(iii) $f(x^n) = [f(x)]^n$ for all $n \in \mathbb{Z}$.

Theorem 12:

Let $f : G \longrightarrow H$ be a homomorphism. Then $\ker f$ is a subgroup of G.

Theorem 13:

Let R be a commutative ring. Then:

(i) $0 \cdot a = 0$ for any $a \in R$.

(ii) If $-a$ is that number which, when added to a, gives 0, then $(-1)(-a) = a$ for any $a \in R$.

(iii) $(-1)a = -a$ for any $a \in R$.

Theorem 14:

A commutative ring R is a domain if and only if the product of any two nonzero elements of R is nonzero.

Theorem 15:

$\mathbb{Z}_m$ is a domain if and only if m is a prime.

Theorem 16:

Every field F is a domain.

Theorem 17:

The commutative ring $\mathbb{Z}_m$ is a field if and only if m is a prime.

Theorem 18:

Let k be a field and let $f(x) \in k[x]$. Let $f(x)$ have degree n. Then $f(x)$ has at most n roots in k.