Number Theory: Summary of Definitions and Theorems

Divisibility:
Given arbitrary integers $a, b$, with $a \neq 0$, we say that “$a$ divides $b$” if there exists $k \in \mathbb{Z}$ such that $b = ka$. If $a$ divides $b$, we say $b$ is divisible by $a$, and we call $a$ a divisor (or factor) of $b$, and $b$ a multiple of $a$.
We write $a \mid b$ for “$a$ divides $b$”, and $a \nmid b$ for its negation, “$a$ does not divide $b$”.
Note: The “divisor” $a$ in this definition can be negative, but must be nonzero; divisibility by 0 is not defined.

Congruences:
Given arbitrary (positive, zero, or negative) integers $a, b$, and a modulus $m$, we say (“$a$ is congruent to $b$ modulo $m$”), and write $[a \equiv b \mod m]$ if $a = b + km$ for some integer $k$, or equivalently, if $m \mid a - b$.
Note: The modulus $m$ is an essential part of the definition. Make sure to always specify the modulus; saying “$a$ is congruent to $b$”, or writing “$a \equiv b$”, without specifying a modulus makes no sense.

Properties of congruences:
What makes congruences so useful is that, to a large extent, they can be manipulated like ordinary equations. Congruences to the same modulus can be added, multiplied, and taken to a fixed positive integral power; i.e., for any $a, b, c, d \in \mathbb{Z}$ and $m \in \mathbb{N}$ we have:

- **Sums:** If $a \equiv b \mod m$ and $c \equiv d \mod m$, then $a + c \equiv b + d \mod m$.
- **Products:** If $a \equiv b \mod m$ and $c \equiv d \mod m$, then $ac \equiv bd \mod m$.
- **Powers:** If $a \equiv b \mod m$ and $k \in \mathbb{N}$, then $a^k \equiv b^k \mod m$.
- **Polynomial values:** If $a \equiv b \mod m$ and $P(x)$ is a polynomial with integer coefficients, then $P(a) \equiv P(b) \mod m$.

Primes and composite numbers:
An integer $n$ with $n \geq 2$ is called a prime if its only positive divisors are 1 and $n$, and composite otherwise. Equivalently, $n$ is composite if it be factored in the form $n = ab$ with integers $a, b$ satisfying $1 < a, b < n$.
Note: The natural number 1 is considered neither prime nor composite. Negative numbers and 0 are not classified as prime or composite either.

Fundamental Theorem of Arithmetic:

| Every integer $n \geq 2$ has a unique factorization into primes. |

That is, every integer $n \geq 2$ can be represented in the form $n = p_1p_2\ldots p_r$, where the $p_i$ are primes (not necessarily distinct). Moreover, this representation is unique except for the ordering of the primes $p_i$.

Euclid’s Theorem:

| There are infinitely many prime numbers. |

This is perhaps the most famous theorem in Number Theory. Euclid’s proof, given below, is a classic, one of the most memorable proofs in all of mathematics, and a wonderful illustration of the method of contradiction. This is a proof that is worth remembering for the rest of your life!

**Proof of Euclid’s Theorem:** We use contradiction. Assume there are only finitely many prime numbers, say $p_1, p_2, \ldots, p_n$.
Let $N = p_1p_2\ldots p_n + 1$. Then $N$ is an integer $\geq 2$, so by the Fundamental Theorem of Arithmetic it can be written as a product of one or more prime numbers. Since, by our assumption, $p_1, \ldots, p_n$ are all the primes, at least one of these, say $p_n$, must appear in the factorization of $N$, and so $p_n \mid N$. On the other hand, $p_n \mid p_1p_2\ldots p_n = N - 1$. Since $d \mid a$ and $d \mid b$ implies $d \mid a - b$, it follows that $p_1 \mid N - (N - 1) = 1$, which is impossible, since $p_1 \geq 2$. This contradiction proves the claim.

Further Resources:
In the text this material can be found in Chapters 6 and 7. A fantastic resource on everything about primes is the Prime Pages website, http://primes.utm.edu.