Number Theory I: Divisibility

Divisibility is one of the most fundamental concepts in number theory. A *precise* definition of what it means for a number to be divisible by another number is essential for defining other number-theoretic concepts such as that of prime numbers. In this handout, and the accompanying worksheet, you'll find the basic definitions and key results about divisibility, primes and composite numbers, examples that illustrate these definitions, and problems to practice proof-writing skills by establishing various properties using nothing more than the definition of divisibility. Proofs of this type tend to be particularly simple, much like the proofs involving properties of even/odd numbers that you may have seen earlier in the course (and which in fact deal with a special case of divisibility, namely, divisibility by 2).

Divisibility

Definition: Let $a, b \in \mathbb{Z}$, with $a \neq 0$. We say **"a divides b"** if there exists $m \in \mathbb{Z}$ such that $b = ma$.

- **Notation and terminology:** We write $a \mid b$ for "a divides b", and $a \nmid b$ for its negation, "a does *not* divide b". If a divides b, we say **"a is a divisor of b"**, **"b is divisible by a"**, **"a is a factor of b"**, **"b is a multiple of a"**.
- **Note:** The "divisor" a in this definition can be negative, but must be nonzero; divisibility by 0 is not defined.
- **Examples:** We have $1 \mid 6$, $2 \mid 6$, $-2 \mid 6$, $6 \mid 6$, $6 \nmid 3$, $6 \mid 0$. However, neither $0 \mid 6$ nor $0 \nmid 6$ make sense since divisibility by 0 is not defined.
- **Properties:** Here are some useful properties of divisibility. (See the worksheets and homework assignments for proofs.)
  - **Transitivity:** If $a \mid b$ and $b \mid c$, then $a \mid c$.
  - **Sums/differences:** If $d \mid a$ and $d \mid b$, then $d \mid a + b$ and $d \mid a - b$.
  - **Linear combinations:** If $d \mid a$ and $d \mid b$, then, for any $x, y \in \mathbb{Z}$, $d \mid ax + by$.

Primes and composite numbers

Definition: Let $n \in \mathbb{N}$ with $n \geq 2$. Then n is called a **prime** if its only *positive* divisors are 1 and n, and n is called **composite** otherwise.

Here is an equivalent form of this definition that is particularly useful for proofs:

Definition: An integer $n \geq 2$ is **composite** if it can be written in the form $n = ab$ with $a, b \in \mathbb{Z}$ and $1 < a, b < n$; and n is **prime** if it cannot be written in this form.

- **Note: Only integers ≥ 2 are classified as prime or composite.** In particular, the natural number 1 is neither prime nor composite, and the same goes for the number 0 and all negative integers.
- **Examples:** The primes ≤ 20 are $2, 3, 5, 7, 11, 13, 17, 19$. All other integers n with $2 \leq n \leq 20$ can be written as $n = ab$ with $2 \leq a, b \leq n-1$ and hence are composite. For example, $4 = 2 \cdot 2$, $6 = 2 \cdot 3$, $8 = 2 \cdot 4$, etc.

- **Prime factorization.** A representation of an integer as a product of powers of distinct primes, i.e., a representation of the form $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$, where the p_i are distinct primes, and the exponents α_i are positive integers.
  Examples: $12 = 2^2 \cdot 3^1$, $13 = 13^1$, $60 = 2^2 \cdot 3^1 \cdot 5^1$.

Fundamental Theorem of Arithmetic

Fundamental Theorem of Arithmetic (FTA): Every integer $n \geq 2$ has a prime factorization. Moreover, this factorization is unique up to the ordering of the factors.

The FTA breaks into two separate assertions, both equally important:

- **Existence:** Any integer $n \geq 2$ *has* a prime factorization.
- **Uniqueness:** An integer $n \geq 2$ has *only one* such factorization, apart from the ordering of the factors.

The proof of the *uniqueness* of the factorization is a bit tricky and requires an auxiliary result. (See Theorem 6.9, p. 125, of the text for details; but you are not expected to know this proof.)

However, the *existence* of a prime factorization can be proved by strong induction on n; see the worksheet problem about this. The proof serves as an instructive exercise in strong induction.

Euclid's Theorem on the Infinitude of Primes

Euclid's Theorem: There are infinitely many prime numbers.

The proof of this result, given below, is one of the all-time classic proofs in mathematics, and a great illustration of the method of contradiction. It is a proof that you need to know for this class, and hopefully you'll remember for the rest of your life!

Proof of Euclid's Theorem. We use contradiction. Assume there are only finitely many prime numbers, say $p_1, p_2, \dots, p_n$. Let $N = p_1 p_2 \dots p_n + 1$. Then N is an integer ≥ 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, $p_1, \dots, p_n$ are *all* the primes, at least one of these, say p_i, must appear in the factorization of N, and hence must divide N. On the other hand, p_i also divides the product $p_1 p_2 \dots p_n$, which is equal to $N - 1$. Since $d \mid a$ and $d \mid b$ implies $d \mid a - b$ (by one of the properties of divisibility), it follows that p_i divides $N - (N - 1) = 1$, which is impossible, since $p_i \geq 2$. This contradiction proves the claim.

Further Resources and References to the Text

A fantastic resource on primes is the Prime Pages website, `http://primes.utm.edu`. Check it out!
In the text the above definitions and theorems can be found in Chapter 6:
Divisibility and primes: Definition 6.1, p. 123.
Fundamental Theorem of Arithmetic: Theorem 6.9, p. 125.
Euclid's Theorem: Exercise 6.34, p. 136.
Note: Chapters 6 and 7 contain a number of other topics (e.g., Euclidean algorithm) that we will not cover in class, and that you will not need to know for homework assignments or exams.