## Synopsis of Elementary Number Theory

This is a quick summary of Secs. 4.3–5 of Grimaldi's book. These concepts and facts are sometimes used later in the book.

- 1. An integer  $p \in \mathbf{Z}^+ \cap \overline{\{1\}}$  is prime if no other integer (except p and 1) divides it. Otherwise,  $p \in \mathbf{Z}^+ \cap \{1\}$  is called *composite*. (Note that by this definition, 1 and 0 are neither prime nor composite.)
- 2. "The Fundamental Theorem of Arithmetic": Every  $n \in \mathbb{Z}^+$  has a (unique) factorization into primes:

$$n = p_1^{s_1} p_2^{s_2} \cdots p_t^{s_t}.$$

Examples:  $8 = 2^3$ ,  $65536 = 2^{16}$ ,  $30 = 2 \cdot 3 \cdot 5$ ,  $12 = 2^23$ ,  $180 = 2^23^25$ ,  $105 = 3 \cdot 5 \cdot 7$ , 37 = 37.

- 3. a|b means that a divides b (i.e., b = na for some  $n \in \mathbb{Z}^+$ ).
- 4. The greatest common divisor, gcd(a, b), is the largest number that divides both a and b. Example: gcd(6, 9) = 3.
- 5. *a* and *b* are relatively prime (or coprime) if gcd(a, b) = 1. Example:  $a = 65536 = 2^{16}$ ,  $b = 105 = 3 \cdot 5 \cdot 7$  (each of which is definitely not prime by itself).
- 6. The least common multiple, lcm(a, b), is the smallest number that is divided by both a and b. (This is well known to fifth-graders as the "least common denominator" of fractions.) From the fundamental theorem (2) it is easy to see that

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

Example: lcm(6,9) = 18.

- 7. Division algorithm: Given  $a \in \mathbb{Z}$  and  $b \in \mathbb{Z}^+$ , there exist (unique) integers q and r ("quotient and remainder") such that a = qb + r and  $0 \le r < b$ . In C (and probably other programming languages), r = a % b and (if a and b have been declared as integer variables and are positive) q = a/b. Grimaldi uses "**mod**" for "%". More generally, for a fixed b, if  $a_1$  and  $a_2$  correspond to the same r (in other words,  $b|(a_1 a_2))$ , then  $a_1$  and  $a_2$  are said to be congruent modulo b, or  $a_1 \equiv a_2 \pmod{b}$  (see Grimaldi Sec. 14.3). Example: ; 36 % 7 = 1 = 29 % 7;  $36 \equiv 29 \pmod{7}$  (but  $36 \neq 29 \% 7$  and  $36 \neq 29 \mod{7}$ , because 29 is not less than 7).
- 8. Euclidean algorithm: To find the greatest common divisor of two large numbers, apply the division algorithm recursively. See Grimaldi Theorem 4.7, or the opening pages of Knuth's *The Art of Computer Programming* (and many later sections of Vols. 1 and 2 of Knuth).

© S. A. Fulling 2002