## 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, $p \in \mathbf{Z}^{+} \cap \overline{\{1\}}$ is called composite. (Note that by this definition, 1 and 0 are neither prime nor composite.)
2. "The Fundamental Theorem of Arithmetic": Every $n \in \mathbf{Z}^{+}$has a (unique) factorization into primes:

$$
n=p_{1}^{s_{1}} p_{2}^{s_{2}} \cdots p_{t}^{s_{t}}
$$

Examples: $8=2^{3}, 65536=2^{16}, 30=2 \cdot 3 \cdot 5,12=2^{2} 3,180=2^{2} 3^{2} 5,105=$ $3 \cdot 5 \cdot 7,37=37$.
3. $a \mid b$ means that $a$ divides $b$ (i.e., $b=n a$ for some $n \in \mathbf{Z}^{+}$).
4. The greatest common divisor, $\operatorname{gcd}(a, b)$, is the largest number that divides both $a$ and $b$. Example: $\operatorname{gcd}(6,9)=3$.
5. $a$ and $b$ are relatively prime (or coprime) if $\operatorname{gcd}(a, b)=1$. 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, $\operatorname{lcm}(a, b)$, 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

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

Example: $\operatorname{lcm}(6,9)=18$.
7. Division algorithm: Given $a \in \mathbf{Z}$ and $b \in \mathbf{Z}^{+}$, there exist (unique) integers $q$ and $r$ ("quotient and remainder") such that $a=q b+r$ and $0 \leq r<b$. In $\mathbf{C}$ (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, $b \mid\left(a_{1}-a_{2}\right)$ ), then $a_{1}$ and $a_{2}$ are said to be congruent modulo $b$, or $a_{1} \equiv a_{2}(\bmod b)$ (see Grimaldi Sec. 14.3). Example: ; $36 \% 7=1=29 \% 7 ; 36 \equiv 29(\bmod 7)($ but $36 \neq 29 \% 7$ and $36 \neq 29 \bmod 7$, 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).
(c) S. A. Fulling 2002

