2 Divisibility and the Euclidean algorithm

Divisors and divisibility. Given integers a and b, we say that a *divides* b (or "b is *divisible* by a") and we write $a|b$ if there exists an integer d such that $b = ad$. In that case we call a a *divisor* of b. Every integer $b > 1$ has at least two positive divisors: 1 and b. By a *proper divisor* of b we mean a positive divisor not equal to b itself, and by a *nontrivial divisor* of b we mean a positive divisor not equal to 1 or b. A *prime* number, by definition, is an integer greater than one which has no positive divisors other than 1 and itself; a number is called *composite* if it has at least one nontrivial divisor. The following properties of divisibility are easy to verify directly from the definition:

1. If $a|b$ and c is any integer, then $a|bc$.
2. If $a|b$ and $b|c$, then $a|c$.
3. If $a|b$ and $a|c$, then $a|b \pm c$.

If p is a prime number and α is a nonnegative integer, then we use the notation $p^\alpha||b$ to mean that p^α is the highest power of p dividing b, i.e., that $p^\alpha|b$ and $p^{\alpha+1}\nmid b$. In that case we say that p^α *exactly divides* b.

The *Fundamental Theorem of Arithmetic* states that any natural number n can be written uniquely (except for the order of factors) as a product of prime numbers. It is customary to write this factorization as a product of distinct primes to the appropriate powers, listing the primes in increasing order. For example, $4200 = 2^3 \cdot 3 \cdot 5^2 \cdot 7$.

Two consequences of the Fundamental Theorem (actually, equivalent assertions) are the following properties of divisibility:

4. If a prime number p divides ab, then either $p|a$ or $p|b$.
5. If $m|a$ and $n|a$, and if m and n have no divisors greater than 1 in common, then $mn|a$.

Another consequence of unique factorization is that it gives a systematic method for finding all divisors of n once n is written as a product of prime powers. Namely, any divisor d of n must be a product of the same primes raised to powers not exceeding the power that exactly divides n. That is, if $p^\alpha||n$, then $p^\beta||d$ for some β satisfying $0 \leq \beta \leq \alpha$. To find the divisors of 4200, for example, one takes 2 to the 0-, 1-, 2- or 3-power, multiplied by 3 to the 0- or 1-power, times 5 to the 0-, 1- or 2-power, times 7 to the 0- or 1- power. The number of possible divisors is thus the product of the number of possibilities for each prime power, which, in turn, is $\alpha+1$. That is, a number $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_r^{\alpha_r}$ has $(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_r+1)$ different divisors. For example, there are 48 divisors of 4200.

Given two integers a and b, not both zero, the *greatest common divisor* of a and b, denoted $g.c.d.(a, b)$ (or sometimes simply (a, b)) is the largest integer d dividing both a and b. It is not hard to show that another equivalent definition of $g.c.d.(a, b)$ is the following: it is the only positive integer d which divides a and b and is divisible by any other number which divides both a and b.