The Greatest Common Divisor

Given numbers \( m \) and \( n \) let
\[
(m, n) = \{d \mid d \mid m \text{ and } d \mid n\}
\]
be the set of common divisors of \( m \) and \( n \). Because 1 divides any number, this set is never empty. Because any number divides 0 we have that
\[
(n, 0) = \{q \mid q \mid n\}
\]
The following is a crucial observation. Let \( m > n \geq 0 \) and \( m = q \cdot n + r, 0 \leq r < n \) according to the division algorithm. Then
\[
(m, n) = (n, r)
\]
Clearly, if \( d \mid m \) and \( d \mid n \) then \( d \mid m - q \cdot n \) that is \( d \mid r \). Also, if \( d \mid n \) and \( d \mid r \) then \( d \mid m \).

This observation leads to an algorithm for the \( \gcd(m, n) \) :
\[
m = q_0 n + r_0, n = q_1 r_0 + r_1, r_0 = q_2 r_1 + r_2, r_1 = q_3 r_2 + r_3, r_2 = q_4 r_3 + r_4, \ldots
\]
where \( m > n > r_0 > r_1 > r_2 > \ldots > r_k > 0 \) where \( r_k \) is the last remainder different from 0. Because \( (m, n) = (n, r_0) = (r_0, r_1) = (r_1, r_2) = \ldots = (r_k, 0) \) we get
\[
(m, n) = (r_k, 0)
\]
and the divisors of \( m \) and \( n \) are the divisors of \( r_k \). That is, \( m \) and \( n \) have a greatest common divisor which is \( d = r_k \). We now use the common notation \( (m, n) \) for the \( \gcd(m, n) \).

**Theorem.** \( \gcd(m, n) = a \cdot m + b \cdot n \) for integers \( a \) and \( b \).

This is true for \( r_0 \) and then for all further remainders.

Numbers \( m \) and \( n \) are relatively prime if their greatest common divisor is 1. We now have the following important fact:
\[
\text{If } (m, n) = 1 \text{ then } a \cdot m + b \cdot n = 1 \text{ for integers } a \text{ and } b
\]
Actually, the converse is also true. If \( a \cdot m + b \cdot n = 1 \) then 1 is the only common divisor of \( m \) and \( n \).

**Corollary** If \( e \) is a common divisor of \( m \) and \( n \) then \( e \mid d = (m, n) \).
This follows from the Theorem.

An important application of the division algorithm is that every number \( n > 0 \) admits a unique expansion to base \( b > 0 \):

\[
n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0
\]

where each \( a_i \) is non-negative and \( a_k > 0 \).

\( b = 10 \) is all-too familiar: \( 923 = 9 \cdot 10^2 + 2 \cdot 10 + 3 \).

For the general case, let \( n = q \cdot b + a_0 \). If we assume that \( q = a_k b^{k-1} + a_{k-1} b^{k-2} + \cdots + a_1 \) then

\[
n = q \cdot b + a_0 = (a_k b^{k-1} + a_{k-1} b^{k-2} + \cdots + a_1) \cdot b + a_0 = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0.
\]

Let us explain the algorithm for \( b = 2 \). We wish to expand 9 in base 2. We first divide 9 by 2 with remainder and continue dividing the quotients by 2 until we get quotient 0:

\[
9 = 4 \cdot 2 + 1, 4 = 2 \cdot 2 + 0, 2 = 1 \cdot 2 + 0, 1 = 0 \cdot 2 + 1.
\]

This gives

\[
9 = 1 + 0 \cdot 2^1 + 0 \cdot 2^2 + 1 \cdot 2^3
\]

A number \( q > 0 \) which is divisible only by 1 and by itself is called prime. Prime numbers are \( 2, 3, 5, 7, 11, \ldots \). It is known that there are infinitely many prime numbers. Assume that there are only finitely many prime numbers. Let \( n_0 \) be their product. But \( n_0 + 1 \) is not divisible by any any prime smaller then \( n_0 \) because \( (n, n_0 + 1) = 1 \). Thus \( n_0 + 1 \) would be prime.

Prime numbers have the following property which makes them "prime".

If \( q \mid a \cdot b \) then \( q \mid a \) or \( q \mid b \)

Assume that \( q \not\mid a \). Then \( q \) and \( a \) are relatively prime, that is \( (q, a) = 1 \) and we have integers \( s \) and \( t \) such that \( s \cdot q + t \cdot a = 1 \). We multiply this relation by \( b \) and we get \( b = s \cdot q \cdot b + t \cdot a \cdot b \). Because of \( q \mid a \cdot b \) and \( q \mid s \cdot q \cdot b \) we get \( q \mid b \).

It is common to call a number \( p \) which has only its trivial divisors 1 and itself irreducible (and not prime). What we proved is that irreducible numbers are prime. The converse is also true and easy to see. That is a number is irreducible iff it is prime.

**Theorem.** Any number \( n > 0 \) is a unique product of prime numbers.

Proof. Assume that \( n \) is not prime. Then \( n = a \cdot b \) with smaller numbers \( a \) and \( b \). If we assume that \( a \) and \( b \) are products of primes then \( n \) is a product of primes. Now let

\[
n = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_l
\]

be two factorizations of \( n \) into primes \( p_i, q_i > 1 \). We have \( p_1 \mid q_1 \cdot (q_2 \cdots q_l) \). Thus \( p_1 \mid q_1 \) or \( p_1 \mid q_2 \cdots q_l \). If \( p_1 \mid q_1 \) then because \( q_1 \) is prime we get \( p_1 = q_1 \). Otherwise \( p_1 \mid q_2 \cdots q_l \) which yields \( p_1 \mid q_2 \) or \( p_1 \mid q_3 \cdots q_l \). At any rate, because the \( q_i \) are prime, \( p_1 = q_j \) for some \( j \). This shows \( k \leq l \) and by symmetry \( l \leq k \). Thus \( k = l \) and by an enumeration we get \( p_i = q_i \).