Elementary results about divisibility

1. The division algorithm

Suppose $n \geq 0$, $m > 0$. There exist unique q and r with $0 \leq r < m$ such that

$$n = qm + r \ .$$

Proof by mathematical induction.

2. Greatest common divisors

If m and n are two non-negative integers not both 0, the largest integer d dividing them both is called their **greatest common divisor**. The numbers are called **relatively prime** if this is 1.

There is an algorithm for finding d due to Euclid (the beginning of book VII of the *Elements*):

(1) If $m = 0$, stop. The gcd is n.
(2) Divide n by m to get $n = qm + r$. Set $n := m$, $m := r$. Go to (1).
Two numbers are called **relatively prime** if their gcd is 1.

3. The extended Euclidean algorithm

There exist integers k and ℓ such that

$$km + \ell n = d \ .$$

They can be found by an extended version of the Euclidean algorithm. Let n_0, m_0 be the original values of m and n. The algorithm keeps track of a matrix M such that

$$\begin{bmatrix} n \\ m \end{bmatrix} = M \begin{bmatrix} n_0 \\ m_0 \end{bmatrix}$$

at all times. It starts with $M = I$, and at each step of the Euclidean algorithm sets

$$M := \begin{bmatrix} 0 & 1 \\ 1 & -q \end{bmatrix} M$$

At the end we get a matrix with

$$\begin{bmatrix} d \\ 0 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} n_0 \\ m_0 \end{bmatrix}$$

which means that $an_0 + bm_0 = d$.

4. Prime numbers

A positive integer $n > 1$ is called **prime** if it has no divisors other than itself and 1.

Every positive integer > 1 is divisible by at least one prime number.

Proof by mathematical induction.

Directly from the definition:

If p is a prime number and q is not a multiple of p then it is relatively prime to p.

Exercise 1. *Prove that if n is any positive integer greater than 1, then either (1) it is a prime number; or (2) it is a power of a prime number but not prime; or (3) it can be written as the product of two relatively prime numbers, each greater than 1.*

5. Divisibility

If a divides pq and is relatively prime to p then it divides q.

Write

$$ka + \ell p = 1$$

and multiply through by q.

An immediate corollary:

If a prime number p divides q^2 then it divides q.

Proof. If not, then p is relatively prime to q. But since it divides $q \cdot q$ and is relatively prime to q, it divides q! Contradiction.