2. Induction and the division algorithm

The main method to prove results about the natural numbers is to use induction. We recall some of the details and at the same time present the material in a different fashion to the way it is normally presented in a first course.

Principle 2.1 (Well-ordering principle)**.** *The natural numbers are well-ordered, that is, every non-empty subset S of $\mathbb{N}$ contains a least element; that is, there is an element $a \in S$ such that $a \leq b$ for every $b \in S$.*

Note that it is not possible to prove the well-ordering principle (unless one assumes something equivalent such as the principle of mathematical induction). It is something that seems intuitevely clear that we accept is a property of the natural numbers.

Proposition 2.2 (Archimedean principle)**.** *If a and b are any positive integers, then there is a natural number n such that $na \geq b$.*

Proof. Suppose not, suppose that $na < b$ for every natural number n.

Then the set

$$S = \{\, b - na \,|\, n \in \mathbb{N} \,\}$$

is a subset of the natural numbers. As S is non-empty, it contains a smallest element, $b - ma$, say.

However, $b - (m+1)a \in S$ and

$$\begin{aligned} b - (m+1)a &= (b - ma) - a \\ &< b - ma, \end{aligned}$$

which contradicts the fact that $b - ma$ is the smallest element of S.

Thus the Archimedean principle does hold. □

Axiom 2.3 (Induction Principle)**.** *Let S be a set of natural numbers with the properties:*

(1) $1 \in S$
(2) if $k \in S$ *then* $k + 1 \in S$.

Then $S = \mathbb{N}$.

Theorem 2.4. (2.1) *and* (2.3) *are equivalent.*

Proof. Assume that (2.1) holds. Let $S \subset \mathbb{N}$ be a subset of the natural numbers with the properties

(1) $1 \in S$
(2) if $k \in S$ then $k + 1 \in S$.

Let $T = \mathbb{N} \setminus S$ be the set of natural numbers not in S.

Suppose that T is non-empty. As we are assuming (2.1) T has a smallest element a. As $a \neq 1$ as $1 \in S$. As a is the smallest element of T and $a-1$ is a natural number smaller than a, it follows that $a-1 \notin T$, that is, $a-1 \in S$. As $a-1 \in S$ it follows that $a = (a-1)+1 \in S$. Thus $a \notin T$, a contradiction.

Thus T is empty so that $S = \mathbb{N}$. Thus (2.1) implies (2.3). (2.3).

Now suppose that (2.3) holds. Let S be the set of all natural numbers n such that if $T \subset \mathbb{N}$ contains a number no bigger than n then T contains a smallest element.

Note that if $1 \in T$ then 1 is the smallest element of T. Thus $1 \in S$. Suppose that $k \in S$ and that T is a subset of the natural numbers which contains $k+1$. There are two cases. Either $k+1$ is the smallest element of T, in which case there is nothing to prove, or T contains a smaller element a. Then T contains a number no bigger than k, so that T contains a smallest element, as $k \in S$. Either way, T contains a smallest element. Thus (2.3) implies (2.1). □

Theorem 2.5 (Division Algorithm)**.** *If a and b are integers and $b \neq 0$ then there are unique integers q and r, called the* ***quotient*** *and* ***remainder*** *such that*

$$a = qb + r \qquad \textit{where} \qquad 0 \leq r < |b|.$$

Proof. We first prove this result under the additional assumption that $b > 0$ is a natural number.

Let

$$S = \{\, a - xb \mid x \in \mathbb{Z}, a - xb \geq 0 \,\}.$$

If we put $x = -|a|$ then

$$\begin{aligned} a - xb &= a + |a|b \\ &|a| + a \\ &\geq |a| - |a| \\ &= 0. \end{aligned}$$

Thus S is non-empty. By the well-ordering principle S has a smallest element $r = a - qb$.

Suppose that $r \geq b$. Then

$$r - (q+1)b = r - b \geq 0$$

is a smaller element of S, a contradiction. Thus $0 \leq r < b$. This establishes existence in the case $b > 0$.

Now suppose that

$$a = q_1 b + r_1 = q_2 b + r_2,$$

where q_1, q_2, r_1 and r_2 are all integers and $0 \leq r_i < b$. Then

$$(q_1 - q_2)b = r_1 - r_2.$$

Note that

$$-b < r_1 - r_2 < b.$$

Since $r_1 - r_2$ is a multiple of b, it follows that $r_1 - r_2 = 0$, that is, $r_1 = r_2$. But then $(q_1 - q_2)b = 0$, so that $q_1 - q_2 = 0$ as $b \neq 0$. It follows that $q_1 = q_2$. This establishes uniqueness, when $b > 0$.

It remains to deal with the case $b < 0$. In this case $-b > 0$ and there are integers q and r such that

$$-a = q(-b) + r \qquad \text{where} \qquad 0 \leq r < -b = |b|.$$

Multiplying through by -1 in the first equation we get

$$a = qb + r \qquad \text{where} \qquad 0 \leq r < |b|.$$

Finally suppose

$$a = q_i b + r_i \qquad \text{where} \qquad 0 \leq r_i < |b|,$$

for $i = 1$ and 2. In this case

$$-a = q_i(-b) + r_i \qquad \text{where} \qquad 0 \leq r_i < -b = |b|,$$

As $-b > 0$ it follows that $q_1 = q_2$ and $r_1 = r_2$. □

Definition 2.6. *Let a and b be two integers, not both zero. The* ***greatest common divisor*** *of a and b is the unique integer d with the following properties*

(1) $d|a$ and $d|b$.
(2) If $d'|a$ and $d'|b$ then $d'|d$.
(3) $d > 0$.

Theorem 2.7 (Euclid)**.** *If a and b are two integers, not both zero, then there is a unique greatest common divisor d.*

Proof. We check uniqueness. Suppose that d_1 and d_2 are both the greatest common divisor of a and b. As d_1 is a common divisor and d_2 is the greatest common divisor, we have $d_2|d_1$. Similarly, as d_2 is a common divisor and d_1 is the greatest common divisor, we have $d_1|d_2$. Thus, we may find k_1 and k_2 such that $d_1 = k_1 d_2$ and $d_2 = k_2 d_1$. It follows that

$$\begin{aligned} d_2 &= k_2 d_1 \\ &= k_1 k_2 d_2. \end{aligned}$$

Thus $k_1 k_2 = 1$ so that $d_1 = \pm d_2$. As both $d_1 > 0$ and $d_2 > 0$ we must have $d_1 = d_2$. Thus the greatest common divisor is unique.

Now we turn to existence. If $a = 0$ then we take $d = |b| > 0$. Then $d|0$ and $d|b$, so that d is common divisor. If $d'|a$ and $d'|b$ then surely d' divides $d = |b|$. Thus d is the greatest common divisor. The case $b = 0$ can be handled by symmetry.

So we may assume that both a and b are non-zero. It is easy to see that if d is the greatest common divisor of $|a|$ and $|b|$ then it is also the greatest common divisor of a and b, so that we may assume that a and b are positive. Possibly switching a and b we may assume that $a \geq b$. We may find q and r such that

$$a = qb + r.$$

Note that if d divides b and r then it divides a. Conversely, if d divides a and b then it divides r. Thus the pair $\{ a, b \}$ have the same common divisors as the pair $\{ b, r \}$. It follows that they have the same greatest common divisors, as well. Therefore it suffices to show that b and r have a greatest common divisor. But $r < b \leq a$ and so we are done by induction on the maximum a of a and b. □

It is intereting to note that (2.7) gives an algorithm to find the greatest common divisor of a pair of integers, known as the Euclidean algorithm. It is easiest just to give an example.

Question 2.8. *What is the greatest common divisor of* 45 *and* 210*?*

We first divide 45 into 210,

$$210 = 4 \cdot 45 + 30.$$

The quotient is 4 and the remainder is 30.

So it suffices to find the greatest common divisor of 45 and 30. We divide 30 into 45,

$$45 = 1 \cdot 30 + 15.$$

The quotient is 1 and the remainder is 15.

So it suffices to find the greatest common divisor of 15 and 30. We divide 15 into 30,

$$30 = 2 \cdot 15 + 0$$

The quotient is 2 and the remainder is 0.

So it suffices to find the greatest common divisor of 0 and 15, which is 15. The greatest common divisor of 45 and 210 is 15.

Euclid's algorithm has one very important consequence:

Corollary 2.9. *Let d be the greatest common divisor of integers a and b, not both zero.*

Then there are integers λ and μ such that $d = \lambda a + \mu b$.

Proof. If $a = 0$ then $d = b$ and we make take $\lambda = \mu = 1$. Similarly if $b = 0$. Thus we may assume that a and b are non-zero. Note that d is greatest common divisor of $|a|$ and $|b|$. If $d = \lambda|a| + \mu|b|$ then $d = (\pm\lambda)a + (\pm\mu)b$, where we choose the negative sign if a or b is negative.

Thus we may assume that both a and b are positive. We may assume that $a \geq b$. We may write

$$a = qb + r,$$

where $0 \leq r < b$. d is the greatest common divisor of a and r, so that by induction we may find x and y so that $d = xb + yr$. In this case

$$\begin{aligned} d &= xb + yr \\ &= xb + y(a - qb) \\ &= (q + x)b + ya. \end{aligned}$$

This completes the induction and the proof. □

Let us go back to the example above. As

$$45 = 1 \cdot 30 + 15.$$

we have

$$15 = 45 - 1 \cdot 30.$$

As

$$210 = 4 \cdot 45 + 30,$$

we have

$$30 = 210 - 4 \cdot 45.$$

Thus

$$\begin{aligned} 15 &= 45 - 1 \cdot 30 \\ &= 45 - 1 \cdot (210 - 4 \cdot 45) \\ &= 3 \cdot 45 - 1 \cdot 210. \end{aligned}$$