Proof: Let $n \in \mathbb{N}$ be large enough that $n(y-x) > 1$. Thus $(y-x)$ added to itself n times is larger than 1. Therefore,

$$n(y-x) = ny + n(-x) = ny - nx > 1.$$

It follows from Theorem 2.7.8 there exists $m \in \mathbb{Z}$ such that $nx < m < ny$ and so take $r = m/n$. ■

Definition 2.7.10 *A set $S \subseteq \mathbb{R}$ is dense in $\mathbb{R}$ if whenever $a < b$, $S \cap (a,b) \neq \emptyset$.*

Thus the above theorem says $\mathbb{Q}$ is "dense" in $\mathbb{R}$.

You probably saw the process of division in elementary school. Even though you saw it at a young age it is very profound and quite difficult to understand. Suppose you want to do the following problem $\frac{79}{22}$. What did you do? You likely did a process of long division which gave the following result. $\frac{79}{22} = 3$ with remainder 13. This meant $79 = 3(22) + 13$.You were given two numbers, 79 and 22 and you wrote the first as some multiple of the second added to a third number which was smaller than the second number. Can this always be done? The answer is in the next theorem and depends here on the Archimedean property of the real numbers.

Theorem 2.7.11 *Suppose $0 < a$ and let $b \geq 0$. Then there exists a unique integer p and real number r such that $0 \leq r < a$ and $b = pa + r$.*

Proof: Let $S \equiv \{n \in \mathbb{N} : an > b\}$. By the Archimedean property this set is nonempty. Let $p+1$ be the smallest element of S. Then $pa \leq b$ because $p+1$ is the smallest in S. Therefore, $r \equiv b - pa \geq 0$. If $r \geq a$ then $b - pa \geq a$ and so $b \geq (p+1)a$ contradicting $p+1 \in S$. Therefore, $r < a$ as desired.

To verify uniqueness of p and r, suppose p_i and r_i, $i = 1, 2$, both work and $r_2 > r_1$. Then a little algebra shows $p_1 - p_2 = \frac{r_2 - r_1}{a} \in (0,1)$. Thus $p_1 - p_2$ is an integer between 0 and 1, contradicting Theorem 2.7.8. The case that $r_1 > r_2$ cannot occur either by similar reasoning. Thus $r_1 = r_2$ and it follows that $p_1 = p_2$. ■

This theorem is called the Euclidean algorithm when a and b are integers. In this case, you would have r is an integer because it equals an integer.

2.8 Arithmetic of Integers

Here we consider some very important algebraic notions including the Euclidean algorithm just mentioned and issues related to whether two numbers are relatively prime, prime numbers and so forth. The following definition describes what is meant by a prime number and also what is meant by the word "divides".

Definition 2.8.1 *The number a divides the number b if, in Theorem 2.7.11, $r = 0$. That is, there is zero remainder. The notation for this is $a|b$, read a divides b and a is called a factor of b. A prime number is one which has the property that the only numbers which divide it are itself and 1 and it is at least 2. The greatest common divisor of two positive integers m, n is that number p which has the property that p divides both m and n and also if q divides both m and n, then q divides p. Two integers are relatively prime if their greatest common divisor is one. The greatest common divisor of m and n is denoted as (m,n).*

There is a phenomenal and amazing theorem which relates the greatest common divisor to the smallest number in a certain set. Suppose m, n are two positive integers. Then if x, y are integers, so is $xm + yn$. Consider all integers which are of this form. Some are positive such as $1m + 1n$ and some are not. The set S in the following theorem consists of exactly those integers of this form which are positive. Then the greatest common divisor of m and n will be the smallest number in S. This is what the following theorem says.