Basic number sets

Natural numbers $\mathbb{N} = \{0, 1, 2, 3, 4, 5, \ldots\}$, infinite set, ordering $a < b$, Well-Ordering Axiom

Integers $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ with operations $+, -, \times$

Rational numbers $\mathbb{Q} = \{\frac{a}{b} \mid a \in \mathbb{Z}, b \in \mathbb{N}\}$ with operations $+, -, \times, \div$

Division with remainder

THEOREM 1.1 For $a, b \in \mathbb{Z}$, $b > 0$, there exist unique $q, r \in \mathbb{Z}$ such that $a = qb + r$ and $0 \leq r < b$.

Proof of Existence.

$$\begin{aligned}\mathbb{Z} \;=\; & \cdots \cup \{-b, -b{+}1, \ldots, -1\} \cup \{0, 1, \ldots, b{-}1\} \\ & \cup \{b, b{+}1, \ldots, 2b{-}1\} \cup \{2b, 2b{+}1, \ldots, 3b{-}1\} \cup \cdots\end{aligned}$$

Then a lies in one of the above intervals, $a \in \{nb, nb{+}1, \ldots, nb{+}i, \ldots, nb{+}b{-}1\}$ for some $n \in \mathbb{Z}$, which means $a = nb + i$ with $0 \leq i < b$. Thus $q = n$, $r = i$ satisfies the required properties.

Proof of Uniqueness. Suppose $a = qb + r = q'b + r'$ with $0 \leq r, r' < b$. Then:

$$r - r' \;=\; (a{-}qb) - (a{-}q'b) \;=\; (q - q')b,$$

which is a multiple of $b > 0$. But:

$$-b \;<\; -r' \;\leq\; r - r' \;\leq\; r \;<\; b,$$

and the only multiple of b in this interval is zero, so $r - r' = (q - q')b = 0$. Thus $r - r' = 0$ and $q - q' = 0$, so $r = r'$ and $q = q'$. ■

Long division algorithm $b\overline{)\,a}$ gives method for computing q, r.

Euclidean Algorithm.

For $a, b \in \mathbb{N}$, their *greatest common divisor* $d = \gcd(a, b) = (a, b)$ is the largest integer dividing both a and b (with no remainder).

EXAMPLE: The divisors of 12 are 1,2,3,4,6,12; divisors of 8 are 1,2,4,8. Thus $\gcd(12, 8) = 4$.

The Euclidean Algorithm is an efficient method to find $\gcd(a, b)$ for $a \geq b > 0$ by repeated division with remainder:

$$\begin{aligned} a &= q_1 b &&+ r_1 \\ b &= q_2 r_1 &&+ r_2 \\ r_1 &= q_3 r_2 &&+ r_3 \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} &&+ r_n \\ r_{n-1} &= q_{n+1} r_n &&+ 0. \end{aligned}$$

This process must terminate since $a \geq b > r_1 > r_2 > \cdots \geq 0$, and we cannot keep decreasing infinitely by Well-Ordering.

Formally, if we start with $r_{-1} = a$, $r_0 = b$, and we have already computed $r_1, \ldots, r_{i-1}$ for some $i \geq 1$, then q_i, r_i are computed recursively by the formula:

$$r_{i-2} = q_i r_{i-1} + r_i,$$

stopping when $r_i = 0$. Next time, we will prove that the gcd is the last non-zero remainder:

$$r_n \overset{!!}{=} \gcd(a, b).$$

Example. Find $\gcd(57, 21)$.

$$\begin{aligned} 57 &= 2 \cdot 21 + 15 \\ 21 &= 1 \cdot 15 + 6 \\ 15 &= 2 \cdot 6 + 3 \\ 6 &= 2 \cdot 3 + 0. \end{aligned}$$

Here $a = 57 > b = 21 > r_1 = 15 > r_2 = 6 > r_3 = 3 > r_4 = 0$.

The gcd is the last non-zero remainder: $\gcd(57, 21) = r_3 = 3$.

Extended Euclidean Algorithm

For $\gcd(a, b) = d$, we can find integers $s, t \in \mathbb{Z}$ such that

$$d = sa + tb,$$

by starting with $d = r_n = r_{n-2} - q_n r_{n-1}$ and successively substituting $r_i = r_{i-2} - q_i r_{i-1}$ for $i = n-1, n-2, \ldots, 1$.

In our example:

$$\begin{aligned} d = 3 &= 15 - 2 \cdot 6 \\ 6 &= 21 - 1 \cdot 15 \\ 15 &= 57 - 2 \cdot 21. \end{aligned}$$

Successively substituting:

$$\begin{aligned} d = 3 &= 15 - 2 \cdot 6 \\ &= 15 - 2(21 - 1 \cdot 15) &&= -2 \cdot 21 + 3 \cdot 15 \\ &= -2 \cdot 21 + 3 \cdot (57 - 2 \cdot 21) &&= 3 \cdot 57 - 8 \cdot 21, \end{aligned}$$

so we can take $s = 3$, $t = -8$ to satisfy $3 = s \cdot 57 + t \cdot 21$.