Division algorithm and base-\(b\) representation

1 Division algorithm

1.1 An algorithm that was a theorem

Another application of the well-ordering property is the division algorithm.

**Theorem** (The Division Algorithm). Let \(a, b \in \mathbb{Z}\), with \(b > 0\). There are unique integers \(q\) and \(r\) satisfying

\((i.)\) \(a = bq + r\), where

\((ii.)\) \(r\) satisfies \(0 \leq r < b\).

**Comment.** Important details:

- Condition \(0 \leq r < b\) is crucial. Without, there would be no uniqueness.
- The pair \((q, r)\) is *unique* in the sense that if can also write \(a = bq' + r'\) with \(0 \leq r' < b\), then \(q' = q\) and \(r' = r\).

**Example.**

- Take \(a = 17\) and \(b = 5\). Then \(17 = 5 \cdot 3 + 2\) is an instance of the division algorithm. Here \(q = 3\) and \(r = 2\). Note that the equation \(17 = 5 \cdot 2 + 7\) is not an instance, since \(7 \not< 5\).
- Take \(a = -37\) and \(b = 6\). Then \(-37 = 6 \cdot (-7) + 5\) is an instance of the division algorithm. Here \(q = (-7)\) and \(r = 5\). Note that the equation \(-37 = 6 \cdot (-6) + (-1)\) is not an instance, since \(0 \not\leq -1\).

Some terminology: When we say ‘Divide integer \(a\) by \(b\)’, we mean ‘Write \(a = bq + r\) as in the division algorithm’. We call \(a\) the **dividend** and \(b\) the **divisor**; and we call \(q\) the **quotient** and \(r\) the **remainder**.

**Definition.** Let \(a\) and \(b\) be integers. We say that \(b\) **divides** \(a\), written \(b \mid a\), if there is a \(q \in \mathbb{Z}\) such that \(a = bq\).

**Comment.** When \(b > 0\) we see that \(b \mid a\) iff the remainder is 0 when we divide \(a\) by \(b\).

Once again, our embedding \(\mathbb{Z} \subset \mathbb{R}\) allows us to visualize why the division algorithm is true.

**Figure 1:** Division \(a = bq + r\) illustrated in the real line

\[
\begin{align*}
\text{Figure 1: Division } a &= bq + r \text{ illustrated in the real line} \\
\text{Figure 1: Division } a &= bq + r \text{ illustrated in the real line} \\
\text{Figure 1: Division } a &= bq + r \text{ illustrated in the real line} \\
\text{Figure 1: Division } a &= bq + r \text{ illustrated in the real line} \\
\text{Figure 1: Division } a &= bq + r \text{ illustrated in the real line} \\
\text{Figure 1: Division } a &= bq + r \text{ illustrated in the real line} \\
\end{align*}
\]

And once again, it is the well-ordering property that will allow us to prove this is indeed true.
**Theorem (The Division Algorithm).** Let \( a, b \in \mathbb{Z} \), with \( b > 0 \). There are unique integers \( q \) and \( r \) satisfying \( a = bq + r \) and \( 0 \leq r < b \).

**Proof (Existence).** Let \( A = \{ t \in \mathbb{Z}_{\geq 0} : \exists s \in \mathbb{Z} \ a = bs + t \} \). We claim that \( A \) has a least element. We can use the well-ordering property as long as \( A \neq \emptyset \). Take any \( s \leq \frac{a}{b} \). Then \(-bs \geq -a\), in which case \( t = a - bs \geq a - a = 0 \) is an element of \( A \). Since \( A \subset \mathbb{Z}_{\geq 0} \) is nonempty, the well-ordering principle implies it has a least element \( r \). Then there is a \( q \in \mathbb{Z} \) such that \( a = bq + r \), by definition of \( A \). Suppose \( r \geq b \). Then \( 0 \leq r - b < r \), and since \( a = b(q + 1) + (r - b) \), we have \( r - b \in A \), contradicting the minimality of \( r \). Thus \( 0 \leq r < b \), and we have \( a = bq + r \) as specified.

**Proof (Uniqueness).** To prove the pair is unique, suppose we also have \( a = bq' + r' \) with \( 0 \leq r' < b \). Then we have \( a = bq' + r' = bq + r \), in which case \( b(q' - q) = (r - r') \), and we see that \( r - r' \) is a multiple of \( b \). But since \( 0 \leq r, r' < b \), we must have \( -b < (r - r') < b \). There is only one multiple of \( b \) in this range–namely, \( 0 \). Thus \( r - r' = 0 \). This means \( r = r' \), from which it follows that \( q = q' \). We have shown uniqueness.

1.2 Formulas for \( q \) and \( r \)

Recall the least integer function \( \lfloor x \rfloor : \mathbb{R} \to \mathbb{Z} \) defined by

\[
\lfloor x \rfloor := \text{the unique } n \in \mathbb{Z} \text{ such that } n \leq x < n + 1.
\]

\[
:= \text{the “closest integer to the left of } x\text{”}
\]

**Example.** We have \( \lfloor \pi \rfloor = 3 \) (since \( 3 \leq \pi < 4 \)), and \( \lfloor -\pi \rfloor = -4 \) (since \(-4 \leq -\pi < -3\)).

**Theorem.** If \( a = bq + r \) is an instance of the division algorithm, then we have

(i.) \( q = \lfloor \frac{a}{b} \rfloor \), and thus

(ii.) \( r = a - bq = a - b \cdot \lfloor \frac{a}{b} \rfloor \).

**Proof.** We need only show that \( q \) is the closest integer to the left of \( \frac{a}{b} \); i.e., that \( q \leq \frac{a}{b} < (q + 1) \). This is indeed the case, as \( \frac{a}{b} = q + \frac{r}{b} \) and \( 0 \leq \frac{r}{b} < 1 \).

**Example.** Take \( a = -37 \) and \( b = 6 \), as in our first example. Then \( q = \lfloor \frac{-37}{6} \rfloor = \lfloor -6.16 \rfloor = -7 \), and thus \( r = a - bq = -37 + 42 = 5 \).

2 Base-b representation

An excellent first application of the division algorithm is the representation of integers base-\( b \).

**Definition.** Let \( b, n \in \mathbb{Z} \) with \( b \geq 2 \) and \( n \geq 1 \). A **base-\( b \) representation** of \( n \) is an equation

\[
n = \sum_{i=0}^{r} a_i b^i = a_r b^r + a_{r-1} b^{r-1} + \cdots + a_1 b + a_0,
\]

where each \( a_i \) is an integer satisfying \( 0 \leq a_i < b \). Given such an equation, we write \( n = (a_r a_{r-1} \cdots a_1 a_0)_b \) and call the \( a_i \)'s the **base-\( b \) digits** of \( n \).
Example. Let $b = 10$; $n = 3217 = 3 \cdot 10^3 + 2 \cdot 10^2 + 1 \cdot 10 + 7 = (3217)_{10}$

$$b = 3; \quad n = 3217 = 3^7 + 3^6 + 3^5 + 0 \cdot 3^4 + 2 \cdot 3^3 + 0 \cdot 3^2 + 3 + 1 = (11102011)_3$$

Example. Let’s make a list of all the nonnegative 5-digit base-2 numbers.

|   | 1 = (00001)_2 | 2 = (00010)_2 | 3 = (00011)_2 | 4 = (00100)_2 | 5 = (00101)_2 | 6 = (00110)_2 | 7 = (00111)_2 | 8 = (01000)_2 | 9 = (01001)_2 | 10 = (01010)_2 | 11 = (01011)_2 | 12 = (01100)_2 | 13 = (01101)_2 | 14 = (01110)_2 | 15 = (01111)_2 | 16 = (10000)_2 | 17 = (10001)_2 | 18 = (10010)_2 | 19 = (10011)_2 | 20 = (10100)_2 | 21 = (10101)_2 | 22 = (10110)_2 | 23 = (10111)_2 | 24 = (11000)_2 | 25 = (11001)_2 | 26 = (11010)_2 | 27 = (11011)_2 | 28 = (11100)_2 | 29 = (11101)_2 | 30 = (11110)_2 | 31 = (11111)_2 |

You can count base-2 on your hands. Each finger corresponds to a base-2 place in the expansion; if a finger is extended, the corresponding digit is 1; if it is not extended the corresponding digit is 0. Thus we can count to 31 on one hand if we represent things base-2! How high can you count on two hands, working base-2? Note: base-2 representation is often referred to as binary representation, and a base-2 digit, or binary digit, is often referred to as a bit: a contraction of ‘binary’ and ‘digit’.

**Theorem.** Let $b \geq 2$ be an integer. Then every positive integer $n$ has a unique base-$b$ expansion; i.e.,

(i) We can write $n = \sum_{i=0}^{r} a_i b^i$, where $0 \leq a_i < b$.

(ii) If $n = \sum_{i=0}^{s} a_i' b^i$ is another such representation, then $r = s$ and $a_i = a_i'$ for all $i$.

**Proof (Existence).** Write $n = qb + r$ as in the division algorithm. If $q < b$, then we are done; we have $n = (q,r)_b$. If not, we can write $q = q'b + r'$. We have $q' < q$ and $a = qb + r = (q'b + r')b + r = q'b^2 + r'b + r$, where $r' < b$ and $q' < q$. We can continue, yielding

$$n = q_0 b + a_0$$
$$q_0 = q_1 b + a_1$$
$$\vdots$$
$$q_{r-2} = q_{r-1} b + a_{r-1}$$
$$q_{r-1} = q_0 b + a_r.$$

At each stage $q_{k-1} = q_k b + a_k$, we can write $n = q_k b^{k+1} + \sum_{i=0}^{k} a_i b^i$, where $0 \leq a_i < b$. Thus at the last stage we have $n = 0b^{r+1} + \sum_{i=0}^{r} a_i b^i = \sum_{i=0}^{r} a_i b^i$ with $0 \leq a_i < b$. This is a base-$b$ representation at last! □

Let’s compute the base-6 expansion of 2661

$$2661 = 443 \cdot 6 + 3$$
$$443 = 73 \cdot 6 + 5 \quad (2661 = 73 \cdot 6^2 + 5 \cdot 6 + 3)$$
$$73 = 12 \cdot 6 + 1 \quad (2661 = 12 \cdot 6^3 + 1 \cdot 6^2 + 5 \cdot 6 + 3)$$
$$12 = 2 \cdot 6 + 0$$
$$2 = 0 \cdot 6 + 2$$

Thus $2661 = 2 \cdot 6^4 + 0 \cdot 6^3 + 1 \cdot 6^2 + 5 \cdot 6 + 3 = (20153)_6$. The operations $n \mapsto b \cdot n$ and $n \mapsto \lfloor \frac{n}{b} \rfloor$ can be nicely visualized when viewing $n$ in its base-$b$ representation. Namely, we have
Theorem. Let \( n = \sum_{i=0}^{r} a_i b^i = (a_r a_{r-1} \cdots a_1 a_0)_b \) be a base-\( b \) representation of \( a \). Then

(i) \( b \cdot n \) has base-\( b \) representation \( (a_r a_{r-1} \cdots a_1 a_0)_b \), and

(ii) \( \lfloor \frac{n}{b} \rfloor \) has base-\( b \) expansion \( (a_r a_{r-1} \cdots a_1)_b \).

Example. Let \( n = (4321)_5 \). Then \( 5n = (43210)_5 \) and \( \lfloor \frac{n}{5} \rfloor = (432)_5 \).