MATH1005/MATH6005: Discrete Mathematical Models

Adam Piggott

Semester 1, 2021

Section B: Digital Information

Representing numbers (cont.)

What is a rational number?

Recall that Q is the set of **rational numbers**. A rational number is a number that can be represented as the ratio of two integers.

EXAMPLE $\frac{2}{3}$ is a rational number.

Please note that every integer is a rational number as, for example $6 = \frac{6}{1}$.

What is a rational number?

Recall that Q is the set of **rational numbers**. A rational number is a number that can be represented as the ratio of two integers.

EXAMPLE $\frac{2}{3}$ is a rational number.

Please note that every integer is a rational number as, for example $6 = \frac{6}{1}$.

Are you happy with this definition?

What is a rational number ? (again)

Let $Q = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$.

What does an element of Q look like?

What is a rational number ? (again)

Let $Q = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$.

What does an element of Q look like?

The set Q may be partitioned so that any elements (n_1, d_1) and (n_2, d_2) of Q are in the same partition setif and only if $n_1 d_2 = n_2 d_1$.

So, for example, $\{(2,3), (-2,-3), (4,6), (-4,-6), (6,9), (-6,-9), \ldots\}$ is one of the sets in the partition

The sets in the partition may themselves be considered rational numbers. We usually write $\frac{2}{3}$ instead of $\{(2,3), (-2,-3), (4,6), (-4,-6), (6,9), (-6,-9), \ldots\}$.

Representing a rational number in a computer

For computer storage of any **non-zero** rational number q we need to express it using **scientific notation** with base 2. For any base b this is

$$\boxed{q = (-1)^s \times m \times b^n}$$

where

- $q \in \mathbb{Q}$, $q \neq 0$;
- $b \in \mathbb{Z}^+$, $b \geq 2$;
- $s \in \{0, 1\}$, (s is the **sign bit**)
- $m \in \mathbb{Q}$, $1 \leq m < b$, (m is the '**mantissa**') and
- $n \in \mathbb{Z}$ (n is the **exponent**).

Given q and b, the values of of s, m and n are uniquely determined by these conditions.

Example in base 10: $13.5 = (-1)^0 \times 1.35 \times 10^1$.

A technicality and more examples

Example in base 10: $13.5 = (-1)^0 \times 1.35 \times 10^1$.

To save space, we store 135 instead of 1.35 because 1.35 is the only number between 1 and 10 with digits $1, 3, 5$.

A technicality and more examples

Example in base 10: $13.5 = (-1)^0 \times 1.35 \times 10^1$.

To save space, we store 135 instead of 1.35 because 1.35 is the only number between 1 and 10 with digits $1, 3, 5$.

Examples in base 10:

- $-154 = (-1)^1 \times 1.54 \times 10^2$. Store m as 154.
- $0.031 = (-1)^0 \times 3.1 \times 10^{-2}$. Store m as 31.

The number of digits used to store m is called the **precision**.

An example in binary

Example in base 2, precision 4, 4-bit exponent n
(As we have seen, using a 4-bit signed integer means that $-8 \leq n \leq 7$):

$$\underbrace{1}_{s} \ \underbrace{0101}_{m} \ \underbrace{0011}_{n} \quad \text{or, alternatively,} \quad \underbrace{1}_{s} \ \underbrace{1010}_{m} \ \underbrace{0011}_{n}$$

$m = 1.01_2 = 1(2^0) + 0(2^{-1}) + 1(2^{-2}) = 1 + \frac{1}{4} = \frac{5}{4}$.
$n = 3_{10}$.

So $q = -\frac{5}{4} \times 2^3 = -10_{10}$.

NOTE: In practice, when using binary, the “1.” part of the mantissa m is not stored, since it is implied. So in 4-bit precision 1.01_2 would be stored as 0100 (with *no* alternative).

A warning

WARNING: With limits on precision and exponent size, some rational numbers can only be stored inaccurately, if at all.

Of course, the same sort of thing is true for integers. But with integers we can represent ALL of the integers close enough to 0, so it is easier to understand which integers we can and cannot represent.

If you have a reason to represent rational numbers accuracy beyond the accuracy provided by some sort of standard set up, you can write dedicated software to represent numbers with greater precision.

Modular arithmetic

A Theorem

Theorem

$$\forall n \in \mathbb{Z}\, \forall d \in \mathbb{Z}^+\, \exists! q \in \mathbb{Z}\, \exists! r \in \mathbb{N} (n = qd + r) \wedge (0 \leq r < d)$$

RECALL: In the lecture slides we use the notation $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ and $\mathbb{Z}^+ = \{1, 2, 3, \ldots\}$.

A Theorem

Theorem

$$\forall n \in \mathbb{Z}\ \forall d \in \mathbb{Z}^+\ \exists! q \in \mathbb{Z}\ \exists! r \in \mathbb{N} (n = qd + r) \wedge (0 \leq r < d)$$

RECALL: In the lecture slides we use the notation $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$ and $\mathbb{Z}^+ = \{1, 2, 3, \ldots\}$.

We can say the same thing in words.

Theorem: Given any integer n and given any positive integer d, there is exactly one way to express n as an integer multiple qd of d plus a non-negative 'remainder' r less than the 'divisor' d.

This theorem is called the **Quotient-Remainder Theorem**.

A way to understand q and r

Fix a choice of $n \in \mathbb{Z}$ and $d \in \mathbb{Z}^+$.

Now picture a number line with the integers marked in some dramatic way.

Now: qd is the integer multiple of d that is closest to n but NOT to the right of n; and r is the distance between qd and n.

A picture will help...

The ‘mod’ and ‘div’ operations

We define: $q = n$ **div** d; $r = n$ **mod** d.

You may like to say that:

- n div d gives the **quotient** when n is divided by d;
- n mod d gives the **remainder** when n is divided by d.

Examples

Q: Evaluate the following expressions:

87 mod 13

-100 div 13

Examples

Q: Evaluate the following expressions:

87 mod 13

-100 div 13

A:
Since $87 = 6(13) + 9$, 87 mod 13 = 9.

Since $-100 = (-8)(13) + 4$, -100 div 13 = -8.

The division algorithm

The 'primary school' method of finding quotient and remainder is to use *repeated subtraction*. This only works for non-negative n.

Input: $n \in \mathbb{N}$ and $d \in \mathbb{Z}^+$.
Output: $q = n$ div d and $r = n$ mod d.

Method:
Set $r = n$, $q = 0$.
Loop: If $r < d$ stop.
Replace r by $r - d$.
Replace q by $q + 1$.
Repeat loop

Some small modifications to the algorithm allow it cope also with negative n.

Congruence modulo n

Let $n \in \mathbb{Z}^+$. The **congruence modulo** n relation $R_n \subseteq \mathbb{Z} \times \mathbb{Z}$ is defined by

$$aR_nb \Leftrightarrow \exists k \in \mathbb{Z}\ ;\ a = b + kn.$$

We have unusual notation for this relation. We write $a \equiv b \pmod{n}$ to mean aR_nb

Understanding the relation:

Congruence modulo n

Let $n \in \mathbb{Z}^+$. The **congruence modulo** n relation $R_n \subseteq \mathbb{Z} \times \mathbb{Z}$ is defined by

$$aR_nb \Leftrightarrow \exists k \in \mathbb{Z}\ ;\ a = b + kn.$$

We have unusual notation for this relation. We write $a \equiv b \pmod{n}$ to mean aR_nb

Understanding the relation:

Two integers are congruent modulo n when they leave the same remainder upon division by n.

Congruence modulo n

Let $n \in \mathbb{Z}^+$. The **congruence modulo** n relation $R_n \subseteq \mathbb{Z} \times \mathbb{Z}$ is defined by

$$aR_nb \Leftrightarrow \exists k \in \mathbb{Z} \; ; \; a = b + kn.$$

We have unusual notation for this relation. We write $a \equiv b \pmod{n}$ to mean aR_nb

Understanding the relation:

Two integers are congruent modulo n when they leave the same remainder upon division by n.

$$\forall a, b \in \mathbb{Z} \, \forall n \in \mathbb{Z}^+ \, [a \equiv b \pmod{n}] \Leftrightarrow [a \bmod n = b \bmod n]$$

Example: $-17 \equiv 15 \pmod{8}$ since $-17 = 15 + (-4)8$.

$\equiv$ partitions the integers

For any $n \in \mathbb{Z}^+$ and any $a \in \mathbb{Z}$ the **congruence class** $[\mathbf{a}]_\mathbf{n}$ (or ‘equivalence class’) of a modulo n is defined by

$$[a]_n = \{m \in \mathbb{Z} \mid m \equiv a \pmod{n}\}.$$

Lemma: R_n induces the partition $\{[0]_n, [1]_n, \ldots, [n-1]_n\}$ on $\mathbb{Z}$