MATH1005/MATH6005: Discrete Mathematical Models

Adam Piggott

Semester 1, 2021

An annoucement/correction

Earlier in the course, we adopted the notation

$$\mathbb{Z}^+ = \{1, 2, 3, \dots\} \text{ and } \mathbb{N} = \{0, 1, 2, 3, \dots\}$$

In previous versions of the course, the notation

$$\mathbb{N} = \{1, 2, 3, \dots\} \text{ and } \mathbb{N}^* = \{0, 1, 2, 3, \dots\}$$

has been used.

It seems that I grossly underestimated the amount of work involved in changing all of the optional problems, worksheets, and assignments (5 variations per week) to account for my preferred notation...

Our new convention

From now on, in all conversations we have (lectures, worksheets, assignments, etc) we will adopt the notation

$$\mathbb{N} = \{1, 2, 3, \dots\} \text{ and } \mathbb{N}^* = \{0, 1, 2, 3, \dots\}.$$

Modular arithmetic

Another way to say the Q-R Theorem

Theorem: Given any integer n and given any positive integer d, there exist unique integers q and r such that

$$n = dq + r \text{ and } 0 \leq r < d.$$

We say that q is the quotient, and r the remainder, when n is divided by d.

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

Please note that the remainder is ALWAYS non-negative and less than d.

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.

WARNING: Please pay careful attention to the second example. Using the Q-R Theorem when n is negative is often a source of confusion. Note that, even when n is negative, r is non-negative.

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 $d \in \mathbb{N}$.
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 d

Let $d \in \mathbb{N}$. The **congruence modulo** d relation $R_d \subseteq \mathbb{Z} \times \mathbb{Z}$ is defined by

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

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

Two ways to understand the relation

Lemma 1: Two integers are congruent modulo d if and only if they leave the same remainder upon division by d. That is

$$\forall a, b \in \mathbb{Z}\, \forall d \in \mathbb{N}\, [a \equiv b \pmod{d}] \Leftrightarrow [a \bmod d = b \bmod d]$$

Lemma 2: Two integers are congruent modulo d if and only if their difference is a multiple of d

$$\forall a, b \in \mathbb{Z}\, \forall d \in \mathbb{N}\, [a \equiv b \pmod{d}] \Leftrightarrow [\exists k \in \mathbb{Z}\, b - a = kd]$$

Examples

Example: $-17 \equiv 15 \pmod 8$ since

$$-17 - 15 = -32 = (-4)8$$

Example: $-17 \equiv 15 \pmod 8$ since

$$-17 = (-3) \times 8 + 7$$

and

$$15 = 1 \times 8 + 7,$$

so -17 and 15 leave the same remainder upon division by 8.

$\equiv$ partitions the integers

For any $d \in \mathbb{N}$ and any $a \in \mathbb{Z}$ the **congruence class** $[\mathrm{a}]_{\mathrm{d}}$ (or 'equivalence class') of a modulo d is defined by

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

EXAMPLE: The elements of $[2]_7$, for example, are all the integers that leave remainder 2 upon division by 7.

Lemma: R_d induces the partition $\{[0]_d, [1]_d, \ldots, [d-1]_d\}$ on $\mathbb{Z}$

Modular arithmetic: Something amazing

Lemma: Let $d \in \mathbb{N}$ and let $a_1, b_1, a_2, b_2 \in \mathbb{Z}$. If

$$a_1 \equiv a_2 \pmod{d} \text{ and } b_1 \equiv b_2 \pmod{d},$$

then the following are all true:

1. $a_1 + b_1 \equiv a_2 + b_2 \pmod{d}$
2. $a_1 - b_1 \equiv a_2 - b_2 \pmod{d}$
3. $a_1 \times b_1 \equiv a_2 \times b_2 \pmod{d}$

We wil prove the first assertion together. The second and the third are left as an exercise for the reader.

Proof of the first assertion

Suppose that $a_1 \equiv a_2 \pmod{d}$ and $b_1 \equiv b_2 \pmod{d}$. By definition, there exist integers j, k such that

$$a_1 = a_2 + dj \text{ and } b_1 = b_2 + dk.$$

Now

$$\begin{aligned}(a_1 + b_1) - (a_2 + b_2) &= (a_2 + dj + b_2 + dk) - (a_2 + b_2) \\ &= dj + dk \\ &= d(j + k).\end{aligned}$$

It follows by Lemma 2 that

$$(a_1 + b_1) \equiv (a_2 + b_2) \pmod{d}. \qquad \square$$

The upshot

When working with arithmetic expressions modulo d, we may at any moment replace a number by another number that is equivalent to it, modulo d. This allows a number of fast calculations in modular arithmetic.

EXAMPLE:

$$\begin{aligned} 24 + 71 \times 13 &\equiv 2 + 5 \times 2 \pmod{11} \\ &\equiv 12 \pmod{11} \\ &\equiv 1 \pmod{11}. \end{aligned}$$

WARNING: Division is not as easy when working in modular arithmetic. Which is great!

Applications

Modular arithmetic is often used in cyrptography, to generate pseudo-random numbers (necessary for running simulations), for error-detecting codes (used in credit card numbers, for example) and many other applications.

An example

A 10-digit string $d_1 d_2 \ldots d_{10}$ (where the last digit may be X, which is considered to have the value 10) is a **valid ISBN-10** if

$$1 \times d_1 + 2 \times d_2 + \ldots 10 \times d_{10} \equiv 0 \pmod{11}$$

For example, the ISBN-10 for our optional text is 0357114086 and

$$1(0) + 2(3) + 3(5) + 4(7) + 5(1) + 6(1) + 7(4) + 8(0) + 9(8) + 10(6) = 220 \equiv 0 \pmod{11}.$$

Why is it worth making sure book identifiers have this property?

A flavour of number theory: Two statements about primes and modular arithmetic

The **greatest common divisor** of $a, b \in \mathbb{N}$, written **gcd**(a, b), is the largest $n \in \mathbb{N}$ such that a mod $n = 0$ and b mod $n = 0$.
If gcd$(a, b) = 1$, a, b are called **relatively prime**.

Examples: gcd$(30, 75) = 15$; gcd$(30, 77) = 1$; so 30,77 are relatively prime.

Fermat's little theorem, (proof omitted):
If p is prime and $a \in \mathbb{N}$ satisfies gcd$(a, p) = 1$ then $a^{p-1} \bmod p = 1$.

Example: gcd$(6, 11) = 1$, so $6^{10} \bmod 11 = 1$.
Check: $6^{10} = 60\,466\,176 = 5\,496\,925 \times 11 + 1$.

B2: Sequences

Text Reference (Epp)

3ed: Sections	4.1-4, 8.1-3 (Sequences and induction), 9.3,5 (Sorting)
4ed: Sections	5.1-4,6-8, (Sequences and induction), 11.3,5 (Sorting)
5ed: Sections	5.1-4,6-7, (Sequences and induction), 11.3,5 (Sorting)

Sequences

Let S be a set and $I \subseteq \mathbb{N}^\star$. A function $a : I \to S$ is called a **sequence in** S. Special **sequence notation** is often used:

Function notation	Sequence notation
$a : I \to S$ $n \mapsto a(n).$	$(a_n)_{n \in I} \subseteq S$

The notation $(a_n)_{n \in I}$ indicates that the function can be represented as an *ordered -tuple* or, more simply, as a *list*.

(Unlike a *set*, a list has an order, and can have repeated entries.)

Examples

- $I = \{1, 2, 3\} : \ (a_n)_{n \in I} = (a_1, a_2, a_3)$.
- $I = \mathbb{N}^\star : \ (a_n)_{n \in I} = (a_0, a_1, a_2, \ldots\ldots)$.

In practice we usually leave out the parentheses and speak of "the sequence a_1, a_2, a_3" or "the sequence $a_0, a_1, a_2, \ldots\ldots$."

Examples of Sequences

The "$\subseteq S$" part of the sequence notation $(a_n)_{n \in I} \subseteq S$ indicates that the sequence members belong to S; *i.e.* that the range of the sequence function $a : I \to S$ is a subset of its codomain S.

The sequence *itself* is **not** a subset of S, since it is not a *set*.

Examples

1. $(a_n)_{n\in\mathbb{N}} \subseteq \mathbb{Q}$ sequence of interests rates. a_n is an interest rate at time n.

2. $(p_n)_{n\in\mathbb{N}} \subseteq \mathbb{N}^\star \times \mathbb{N}^\star \times \mathbb{N}^\star$ sequence of states of an ecosystem. $p_n = (r_n, s_n, t_n)$: population of species r, s, t at time n.

3. $(a_n)_{n\in\mathbb{N}} \subseteq \mathbb{N}^\star$ sequence of amplitudes. a_n: amplitude of the harmonic of frequency $n \times f$ (f fundamental frequency).

4. U set of users. $(u_n)_{n\in\{1,2,3,4,5\}} \subseteq U$: a list of 5 users.

Describing sequences: explicit definitions

An **explicit definition** of a sequence is a formula for a_n.

Examples:

1. $\forall n \in \mathbb{N} \;\; a_n = 2^n$. $\quad (a_n)_{n\in\mathbb{N}} = 2, 4, 8, 16, \ldots,$

2. a_1 = Pierre, a_2 = Julie, a_3 = Paul.
   $(a_n)_{n\in\{1,2,3\}}$ = Pierre, Julie, Paul.

Describing sequences: Implicit definitions

An **implicit definition** of a sequence comprises starting value(s) and a relationship between the a_n's.

Examples:

$$\begin{cases} a_{n+1} = 2a_n, \\ a_1 = 2. \end{cases}$$

Defines the sequence

$$(a_n)_{n\in\mathbb{N}} = 2, 4, 8, 16, \ldots,$$

Another example

$$\begin{cases} a_{n+1} = -a_n + a_{n-1}, \\ a_2 = 1, \\ a_1 = 0. \end{cases}$$

Defines the sequence

$$\begin{aligned} a_1 &= 0 \\ a_2 &= 1 \\ a_3 &= -1+0=-1 \\ a_4 &= -(-1)+1=2 \\ a_5 &= -2+(-1)=-3 \\ \vdots &\quad \vdots \end{aligned}$$