# Discrete Mathematics

# Exercise Sheet 2

Alistair O'Brien

November 22, 2022

## Before Attempting the Problems

The primary goal of this course is to introduce to you *formal reasoning* and various (discrete) mathematical structures such as *sets, relations, and functions* along side some niche number and automata theory. It is vitial that you master many of these topics for various other Tripos courses[1].

Please complete these exercises and submit your solutions 48 hours before our scheduled supervisions to `ajo41@cam.ac.uk` as a **PDF** attachment. Feel free to choose the format of your answers (handwritten, typed, LaTeX'd) – just ensure that they're (mostly) legible[2].

Attempt to complete at least 75% of the set exercises – if you get stuck simply make a note of it in your answer and move onto the next question. We will be able to discuss all the solutions during the supervisions.

These supervisions will focus on both examinable and *non-examinable material*, the latter being for pedigogical reasons. Each week I will provide a 'Material' section with notes/summaries of the lecture material . You are welcome to skip these sections, they are simply there for your benefit. However, some questions will (explicitly) refer to this material.

Some of the exercises are taken from Marcelo's exercise sheets which you can find here: https://www.cl.cam.ac.uk/teaching/2223/DiscMath/materials.html.

[1] In particular, Algorithms (IA), Semantics of Programming Languages (IB), Logic and Proof (IB), Computation Theory (IB), Complexity Theory (IB), Formal Models of Language (IB), Denotational Semantics (II), Types (II), Hoare Logic and Model Checking (II), and Category Theory (II)

[2] Don't worry too much about this though, I can't handwrite anything legible either

# 1 Material

## 1.1 Divisibility

**Definition 1.1.** For integers $d, n \in \mathbb{Z}$, *d divides n*, denoted $d \mid n$, iff

$$\exists k \in \mathbb{Z}.\ n = k \times d$$

**Theorem 1.1.** (**Division Theorem**) For all integers $m, n \in \mathbb{N}$ where $n \neq 0$ there exists a *unique* pair of integers $q, r \in \mathbb{Z}$ such that $0 \leq r < |n|$ and $m = q \times n + r$.

$$\forall m, n \in \mathbb{Z}.n \neq 0 \implies \exists! q, r \in \mathbb{Z}.0 \leq r < |n| \wedge m = q \times n + r$$

In the above, we say that $m$ is the *dividend*, $n$ is the *divisor*, $q$ is the *quotient*, and $r$ is the *remainder*.

A division algorithm is an algorithm that for two integers $m, n \in \mathbb{Z}$ computes the quotient and remainders $q, r$. Here is one written in OCaml:

```
let div m n =
  let rec loop q r =
    if r < n
    then q, r
    else loop (q + 1) (r - n)
  in loop 0 m
```

We write quo$(m, n)$ and rem$(m, n)$ for the quotient $q$ and remainder $r$ computed by `div m n`.

**Definition 1.2.** For natural $n \in \mathbb{N}$, the set of divisors of $n$ is defined by

$$D(n) \triangleq \{d \in \mathbb{N} : d \mid n\}$$

**Definition 1.3.** Let $S \subseteq \mathbb{N}$ be a finite set of naturals. An integer $c \in \mathbb{Z}^+$ is said to be the *common divisor* of the set $S$ if:

$$\forall n \in S.\ c \mid n$$

**Definition 1.4.** Let $m, n \in \mathbb{N}$ be two naturals. The set of common divisors of $m, n$ are

$$CD(m, n) \triangleq D(m) \cap D(n) = \{c \in \mathbb{N} : c \in D(m) \wedge c \in D(n)\}$$

The algorithm for computing the set of common divisors is as follows:

```
let divides d n = n mod d = 0

let divisors n =
  Set.range 1 n
  |> Set.filter (fun d -> divides d n)
```

```
let rec common_divisors m n =
  if divides n m
  then divisors n
  else common_divisors (rem m n) n
```

The *Key Lemma* is a theorem that is *key* to the proof of correctness of the above algorithm.

**Lemma 1.1.** (**Key Lemma**) For all $m, m', n \in \mathbb{Z}$ where $n \neq 0$,

$$m \equiv m' \pmod{n} \implies CD(m,n) = CD(m',n).$$

A corollary of this lemma is that

$$CD(m,n) = CD(\text{rem}(m,n),n)$$

**Definition 1.5.** For natural numbers $m, n \in \mathbb{N}$, the **greatest common divisor** of $m$ and $n$ is a natural number $d \in \mathbb{N}$, written as $d = \gcd(m,n)$, such that:

(i) $d \mid m \wedge d \mid n$

(ii) $\forall c \in \mathbb{N}.\ c \mid m \wedge c \mid n \implies c \mid d$

Here are some simple (but useful) lemmas that you should use (and be able to prove):

**Lemma 1.2.** For all natural $k, m, n \in \mathbb{N}$

(i) $CD(k \times n, n) = D(n)$

(ii) $CD(m,n) = CD(n,m)$

(iii) $\gcd(m,n) = \max CD(m,n)$

(iv) $\gcd(m,n) = \gcd(n,m)$

(v) $\gcd(k, \gcd(m,n)) = \gcd(\gcd(k,m),n)$

(vi) $\gcd(k \times m, k \times n) = k \times \gcd(m,n)$

(vii) $\forall c \in \mathbb{N}.\ c \mid m \wedge c \mid n \iff c \mid \gcd(m,n)$

Since the maximum of the divisors of $n$ is $n$, then by $\gcd(m,n) = \max CD(m,n)$ and the *Key Lemma* we have:

$$\gcd(m,n) = \begin{cases} n, & \text{if } n \mid m; \\ \gcd(\text{rem}(m,n),n), & \text{otherwise.} \end{cases}$$

[*hint*: You can easily see this by comparing the `common_divisors` function and Euclid's algorithm (`gcd`).]

**Euclid's algorithm** is implemented in OCaml as follows:

```
let rec gcd m n =
  let r = rem m n in
  if r = 0
    then n
    else gcd n r
```

**Theorem 1.2.** (**Euclid's Theorem**) For all $k, m, n \in \mathbb{Z}^+$,

$$k \mid m \times n \wedge \gcd(k, m) = 1 \implies k \mid n$$

## 1.2 Modular Arithmetic

**Definition 1.6.** For a pair of integers $a, b \in \mathbb{Z}$ and $m \in \mathbb{Z}^+$, $a$ is *congruent* to $b$ modulo $m$ iff $m \mid a - b$.

$$a \equiv b \pmod{m} \iff m \mid a - b$$

**Definition 1.7.** For any $m \in \mathbb{Z}^+$, the *equivalence class* of $a \in \mathbb{Z}$ is the set $[a]_m$ defined by

$$[a]_m = \{x \in \mathbb{Z} : a \equiv x \pmod{m}\}$$

The set of integers *modulo* $m$ is defined as $\mathbb{Z}_m \triangleq \{0, 1, \ldots, m-1\}$

**Definition 1.8.** Modular addition and multiplication is defined by

$$[a]_m +_m [b]_m \triangleq [a + b]_m \qquad [a]_m \times_m [b]_m \triangleq [a \times b]_m,$$

for $a, b \in \mathbb{Z}_m$ and $m \in \mathbb{Z}^+$.

## 1.3 Primes

**Definition 1.9.** The positive integer $p \geq 2$ is said to be *prime* if it's only divisors are 1 and itself, that is

$$\forall x \in \mathbb{Z}^+.\ x \mid p \implies x = 1 \vee x = p$$

The set of prime numbers is denoted $\mathbb{P}$.

**Theorem 1.3.** (**Fermat's Little Theorem**) For all $i \in \mathbb{N}$ and prime $p \in \mathbb{P}$,

$$i^p \equiv i \pmod{p}.$$

A corollary of Fermat's Little Theorem is if $p \nmid i$, then

$$i^{p-1} \equiv 1 \pmod{p}.$$

**Theorem 1.4.** (**The Freshman's Dream**) For all natural $m, n \in \mathbb{N}$ and prime $p \in \mathbb{P}$,

$$(m + n)^p \equiv m^p + n^p \pmod{p}$$

**Lemma 1.3.** (**Euclid's Lemma**) For all $m, n \in \mathbb{Z}^+$ and primes $p \in \mathbb{P}$,

$$p \mid m \times n \implies p \mid m \vee p \mid n$$

## 2 Exercises

1. Prove that for all $i, j \in \mathbb{Z}$, $m \in \mathbb{Z}^+$, and $n \in \mathbb{N}$,

$$i \equiv j \pmod{m} \implies i^n \equiv j^n \pmod{m}.$$

2. Prove that for all $k, l \in \mathbb{N}$, and $m \in \mathbb{Z}^+$,

   (a) $\text{rem}(k \times m + l, m) = \text{rem}(l, m)$

   (b) $\text{rem}(k + l, m) = \text{rem}(\text{rem}(k, m) + l, m)$

   (c) $\text{rem}(k \times l, m) = \text{rem}(k \times \text{rem}(l, m), m)$

3. Let $n \in \mathbb{N}$ be arbitrary such that:

$$n = \sum_{i=0}^{k} d_i \times 10^i,$$

   where $d_i \in [0, 9] \subseteq \mathbb{N}$ for all $1 \leq i \leq k$.

   (a) Prove that $3 \mid n \iff 3 \mid \sum_{i=0}^{k} d_i$.

   (b) Prove that $11 \mid n \iff 11 \mid \sum_{i=0}^{k} (-1)^i d_i$.

4. Calculate $\text{rem}(55^2, 79)$, $\text{rem}(23^2, 79)$, $\text{rem}(23 \times 55, 79)$, and $\text{rem}(55^{78}, 79)$.

5. Show that $2^{153} \equiv 53 \pmod{153}$.

6. Let $n \in \mathbb{Z}^+$ and $p$ be a prime. Show that

$$n \equiv 1 \pmod{p-1} \implies i^n \equiv i \pmod{p},$$

   for all $i \in \mathbb{Z}^+$ not multiple of $p$.

7. A decimal (respectively binary) repunit is a natural number whose decimal (respectively binary) representation consists solely of 1's.

   (a) What are the first three decimal repunits? And the first three binary ones?

   (b) Show that no decimal repunit strictly greater than 1 is a square, and that the same holds for binary repunits.
   Is this the case for every base?

   [*hint*: Use Lemma 27 from lectures]

8. Prove for all $m, n \in \mathbb{Z}^+$, $k, l \in \mathbb{Z}$,

$$\gcd(m, n) \mid (k \times m + l \times n).$$

9. Prove that for all positive integers $m, n \in \mathbb{Z}^+$ and integers $i, j \in \mathbb{Z}$,

$$n \times i \equiv n \times j \pmod{m} \iff i \equiv j \mod \frac{m}{\gcd(m, n)}.$$

10. (i) Prove that for all $m, n \in \mathbb{Z}^+$, there exists integers $x, y \in \mathbb{Z}$ such that

$$x \times m + y \times n = \gcd(m, n).$$

[hint: Use strong induction on the iterations of Euclid's Algorithm]

(ii) Find integers $x, y \in \mathbb{Z}$ such that $x \times 30 + y \times 22 = \gcd(30, 22)$.

(iii) Find integers $x', y' \in \mathbb{Z}$ such that $0 \leq y' < 30$ and $x' \times 30 + y' \times 22 = \gcd(30, 22)$.

11. Let $n \in \mathbb{Z}$ be an arbitrary integer.

(i) Prove that if $n$ is not divisible by 3, then $n^2 \equiv 1 \pmod 3$.

(ii) Show that if $n$ is odd, then $n^2 \equiv 1 \pmod 8$.

(iii) Conclude that if $p$ is a prime number greater than 3, then $p^2 - 1$ is divisible by 24.

12. (i) [*optional*] Let $m \in \mathbb{Z}^+$ be a positive integer. Prove that $(\mathbb{Z}_m, +_m, \times_m)$ forms a *ring*.

A structure $(S, +, \times)$ is a *ring* if $S$ is a non-empty set and $+, \times$ are binary operators:

$$+ : S \times S \to S$$
$$\times : S \times S \to S$$

satisfying the following *axioms*:

(A1) **Associativity**. For all $x, y, z \in S$, $x + (y + z) = (x + y) + z$.

(A2) **Zero element**. There exists $0 \in S$ such that $\forall x \in S.\ x + 0 = 0 + x = x$.

(A3) **Inverse**. For all $x \in S$, there exists $y \in S$ such that $x + y = y + x = 0$.

(A4) **Commutativity**. For all $x, y \in S$, $x + y = y + x$.

(M1) **Associativity**. For all $x, y, z \in S$, $(x \times y) \times z = x \times (y \times z)$

(D1) **Distributivity**. For all $x, y, z \in S$,

$$x \times (y + z) = x \times y + x \times z$$
$$(x + y) \times z = x \times z + y \times z$$

(ii) Prove that $[22^{12001}]_{175}$ has a *multiplicative inverse* in $\mathbb{Z}_{175}$.

A *multiplicative inverse* is an element $x \in \mathbb{Z}_{175}$ such that

$$[22^{12001}]_{175} \times_{175} x = x \times_{175} [22^{12001}]_{175} = [1]_{175}.$$

[hint: You are not required to find this inverse, you simply must show its *existence*]