# MA503: Homework 1

**Exercise 1.1.** [10pt] Let $a = 1485$ and $b = 1745$

(1) [4pt] Use Euclidean algorithm to find $\gcd(1485, 1745)$
(2) [4pt] Find $\alpha, \beta \in \mathbb{Z}$ satisfying $1485 \cdot \alpha + 1745 \cdot \beta = \gcd(1485, 1745)$.
(3) [2pt] Compute $\operatorname{lcm}(1485, 1745)$.

**Exercise 1.2.** [5pts] The Fibonacci numbers $\{f_i\}$ are defined recurrently by

$$\begin{cases} f_1 = 1; \\ f_2 = 1; \\ f_3 = f_1 + f_2; \\ \dots \\ f_n = f_{n-1} + f_{n-2}. \end{cases}$$

Use Euclidean lemma to show that $\gcd(f_n, f_{n+1}) = 1$.

**Exercise 1.3.** [5pt] Use mathematical induction to prove that

$$6 \mid 7^n - 1$$

for every $n \in \mathbb{N}$.

Perhaps you are familiar with some divisibility tests, e.g., divisibility by 3, by 9, by 2, by 5. For instance:

- It is easy to see that 342 is divisible by 3 because the sum of digits $3+4+2 = 6$ is divisible by 3
- It is easy to see that 344 is divisible by 2 because its last digit 4 is divisible by 2.
- It is easy to see that 344 is not divisible by 5 because its last digit 4 is not divisible by 5.

There is a very simple idea behind each of these tests. Consider divisibility by 3 test. A given decimal $abcde$ (where $a, b, c, d, e$ are digits) defines a number

$$a \cdot 10^4 + b \cdot 10^3 + c \cdot 10^2 + d \cdot 10^1 + e.$$

Note that $10^n \equiv_3 1$ for any $n \in \mathbb{N}$. Hence,

$$abcde \equiv_3 a + b + c + d + e.$$

In particular, $abcde$ is divisible by 3 if and only if $a + b + c + d + e$ is.

**Exercise 1.4.** [5pts] Prove that a decimal number $a_n a_{n-1} \dots a_1 a_0$ is divisible by 11 if and only if the alternating sum of the digits:

$$a_n - a_{n-1} + a_{n-2} - a_{n-3} + a_{n-4} - \dots$$

is divisible by 11.

**Exercise 1.5.** [5pts] Compute the remainder of division of $3^{100}$ by 7.

We can use induction to prove that $6 \mid n(n+1)(2n+1)$ for every $n \in \mathbb{N}$. But a much easier approach is to notice that

$$\begin{aligned} 6 \mid n(n+1)(2n+1) \quad &\Leftrightarrow \quad n(n+1)(2n+1) \equiv_6 0 \\ &\Leftrightarrow \quad [n(n+1)(2n+1)]_6 = [0]_6 \\ &\Leftrightarrow \quad [n] \cdot [n+1] \cdot [2n+1]_6 = [0]_6. \end{aligned}$$

The last equality is easy to check for every $n$, because there are just 6 congruence classes modulo 6.

**Exercise 1.6.** [+2pts] Prove that $6 \mid n(n+1)(2n+1)$ for every $n \in \mathbb{N}$ by checking that $[n]_6 \cdot [n+1]_6 \cdot [2n+1]_6 = [0]$ for each congruence class $[n]_6$.

Let $X$ be a set. A function $f : X \times X \to X$ is called a **binary function** on $X$. If there is no ambiguity ($f$ is the only binary function) instead of writing $f(a, b)$ we write $a \cdot b$ or simply $ab$.

**Definition 1.1.** A binary function $\cdot$ on a set $X$ is

- **commutative** if $ab = ba$ for every $a, b \in X$;
- **associative** if $(ab)c = a(bc)$ for every $a, b, c \in X$;
- **closed on a subset** $S \subset X$ if $ab \in S$ for every $a, b \in S$; in this event we also say that $S$ is **closed under** $\cdot$. A restriction of $\cdot$ of $S \times S$ is a binary operation too.

We say that $a$ and $b$ **commute** in $G$ if $ab = ba$.

**Exercise 1.7.** [2pts] Consider the set of all complex numbers $\mathbb{C}$ equipped with the standard multiplication $\cdot$. Which of the following subsets of $\mathbb{C}$ are closed under $\cdot$? Just circle appropriate sets, no explanation is required in this problem.

(1) $\mathbb{R}$.
(2) The set of purely imaginary numbers $\mathbb{R}i = \{ ai \mid a \in \mathbb{R} \}$.
(3) $\{1, -1, i, -i\}$.
(4) $\mathbb{N}$.
(5) $\left\{ a + b\sqrt{2}i \;\middle|\; a, b \in \mathbb{Q} \right\}$.
(6) $\{-1, 0, 1\}$.

A binary function $\cdot$ on a small set $X = \{x_1, \ldots, x_n\}$ can be defined by a table, called a composition (or multiplication) table

| $\cdot$ | $x_1$ | $\ldots$ | $x_n$ |
|---|---|---|---|
| $x_1$ | $x_1 \cdot x_1$ | $\ldots$ | $x_1 \cdot x_n$ |
| $\ldots$ | $\ldots$ | | $\ldots$ |
| $x_n$ | $x_n \cdot x_1$ | $\ldots$ | $x_n \cdot x_n$ |

**Exercise 1.8.** [4pts] Define $\cdot$ on $X = \{a, b, c\}$ using the table

| $\cdot$ | $a$ | $b$ | $c$ |
|---|---|---|---|
| $a$ | $b$ | $a$ | $c$ |
| $b$ | $b$ | $c$ | $a$ |
| $c$ | $c$ | $c$ | $c$ |

(1) Is $\cdot$ commutative?
(2) Is $\cdot$ associative?
(3) Is $\cdot$ closed on $\{a, b\}$?
(4) We say that $x \in X$ is the multiplicative identity if $xy = yx = y$ for every $y \in X$? Do we have a multiplicative identity for our operation?

EXPLAIN!