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 $\operatorname{lcm}(1485, 1745)$.

Solution: Using Euclidean algorithm we get:

$$\begin{aligned}
1745 &= 1 \cdot \mathbf{1485} + \mathbf{260} & \Rightarrow \gcd(1485, 1745) &= \gcd(1485, 260)\\
1485 &= 5 \cdot \mathbf{260} + \mathbf{185} & &= \gcd(185, 260)\\
260 &= 1 \cdot \mathbf{185} + \mathbf{75} & &= \gcd(185, 75)\\
185 &= 2 \cdot \mathbf{75} + \mathbf{35} & &= \gcd(35, 75)\\
75 &= 2 \cdot \mathbf{35} + \mathbf{5} & &= \gcd(35, 5)\\
35 &= 7 \cdot \mathbf{5} + \mathbf{0} & &= \gcd(0, 5) = 5.
\end{aligned}$$

Proceeding from the bottom to the top we get a required expression for 5:

$$\begin{aligned}
\mathbf{5} &= \mathbf{75} - 2 \cdot \mathbf{35}\\
&= \mathbf{75} - 2 \cdot (\mathbf{185} - 2 \cdot \mathbf{75}) = 5 \cdot \mathbf{75} - 2 \cdot \mathbf{185}\\
&= 5 \cdot (\mathbf{260} - \mathbf{185}) - 2 \cdot \mathbf{185} = 5 \cdot \mathbf{260} - 7 \cdot \mathbf{185}\\
&= 5 \cdot \mathbf{260} - 7 \cdot (\mathbf{1485} - 5 \cdot \mathbf{260}) = 40 \cdot \mathbf{260} - 7 \cdot \mathbf{1485}\\
&= 40 \cdot (\mathbf{1745} - \mathbf{1485}) - 7 \cdot \mathbf{1485} = 40 \cdot \mathbf{1745} - 47 \cdot \mathbf{1485}
\end{aligned}$$

Hence $\alpha = -47$ and $\beta = 40$ is a solution. This problem has infinitely many solutions. You can check yourself that for any solution (α, β) a pair $(\alpha - 1745, \beta + 1485)$ is a solution too.

$$\operatorname{lcm}(1485, 1745) = \frac{1485 \cdot 1745}{\gcd(1485, 1745)} = 518265.$$

$\square$

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 $\gcd(f_n, f_{n+1}) = 1$.

Solution: Induction on n. For $n = 1$ we have:

$$\gcd(f_1, f_2) = 1,$$

which is true. Assume the result holds for k:

$$\gcd(f_k, f_{k+1}) = 1,$$

and prove that $\gcd(f_{k+1}, f_{k+2}) = 1$. Note that dividing f_{k+2} by f_{k+1} gives:

$$f_{k+2} = 1 \cdot f_{k+1} + f_k,$$

and, hence, by Euclidean Lemma:

$$\gcd(f_{k+1}, f_{k+2}) = \gcd(f_{k+1}, f_k) = 1.$$

Thus, the statement holds by induction on n. $\square$

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

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

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

Solution: For $n = 1$ we have $6 \mid 7 - 1$ which is true.
Assume that statement holds for some k, i.e.

$$6 \mid 7^k - 1,$$

which means that $7^k - 1 = 6q$ for some $q \in \mathbb{N}$. We need to prove that $6 \mid 7^{k+1} - 1$. Indeed,

$$7^{k+1} - 1 = 7 \cdot 7^k - 1 = 7 \cdot (6q + 1) - 1 = 42q + 6 = 6(7q + 1),$$

which means that $7^{k+1} - 1$ is divisible by 6. □

Exercise 1.4. [5pts] Compute the remainder of division of 3^{100} by 7.

Solution: Notice that, $3^6 \equiv_7 1$. Therefore,

$$3^{100} = (3^6)^{16} 3^4 \equiv_7 1^{16} 3^4 = 81 \equiv_7 4.$$

□

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 1.5. [5pts] 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 $[n]_6$.

Solution:

- For $[n] = [0]$ we have $[0] \cdot [1] \cdot [1] = [0]$;
- For $[n] = [1]$ we have $[1] \cdot [2] \cdot [3] = [0]$;
- For $[n] = [2]$ we have $[2] \cdot [3] \cdot [5] = [0]$;
- For $[n] = [3]$ we have $[3] \cdot [4] \cdot [1] = [0]$;
- For $[n] = [4]$ we have $[4] \cdot [5] \cdot [3] = [0]$;
- For $[n] = [5]$ we have $[5] \cdot [0] \cdot [5] = [0]$.

□

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 $x \in X$ is a **multiplicative identity** in $(X, \cdot)$ if $xy = yx = y$ for every $y \in X$.

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

Exercise 1.6. [+3pts] 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) $\{-1, 0, 1\}$.

Solution:

(1) Yes.
(2) No.
(3) Yes.
(4) Yes.
(5) Yes.
(6) Yes.

□

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

$\cdot$	x_1	$\dots$	x_n
x_1	$x_1 \cdot x_1$	$\dots$	$x_1 \cdot x_n$
$\dots$	$\dots$		$\dots$
x_n	$x_n \cdot x_1$	$\dots$	$x_n \cdot x_n$

Exercise 1.7. [+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) Is there a multiplicative identity in $(X, \cdot)$?

Explain your answers!

Solution:

(1) $\cdot$ is not commutative because $a \cdot b = a \neq b = b \cdot a$.
(2) $\cdot$ is not associative because $a \cdot (b \cdot c) = a \cdot a = b \neq c = a \cdot c = (a \cdot b) \cdot c$.

(3) $\cdot$ is not closed on $\{a, b\}$ because $b \cdot b = c \notin \{a, b\}$.
(4) No, we do not have a multiplicative identity:
  - a is not an identity because $a \cdot a \neq a$;
  - b is not an identity because $a \cdot b \neq a$;
  - c is not an identity because $a \cdot c \neq b$.

$\square$