Exercise 1.1. [20pt] Let $a = 90$ and $b = 218$

(1) [7pt] Use Euclidean algorithm to find $\gcd(90, 218)$
(2) [7pt] Find $\alpha, \beta \in \mathbb{Z}$ satisfying $90 \cdot \alpha + 218 \cdot \beta = \gcd(90, 218)$.
(3) [2pt] Find a particular solution for the linear Diophantine equation $90x + 218y = 6$.
(4) [2pt] Write down a general solution of the equation $90x + 218y = 6$.
(5) [2pt] Compute $\mathrm{lcm}(90, 218)$.

Solution: Using Euclidean algorithm we get:

$$\begin{aligned}
218 &= 2 \cdot 90 + 38 & \Rightarrow \gcd(90,218) &= \gcd(38,90)\\
90 &= 2 \cdot 38 + 14 & &= \gcd(14,38)\\
38 &= 2 \cdot 14 + 10 & &= \gcd(10,14)\\
14 &= 1 \cdot 10 + 4 & &= \gcd(4,10)\\
10 &= 2 \cdot 4 + 2 & &= \gcd(2,4)\\
4 &= 2 \cdot 2 + 0 & &= \gcd(0,2) = 2
\end{aligned}$$

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

$$\begin{aligned}
2 &= -2 \cdot 4 + 1 \cdot 10\\
&= -2 \cdot (14 - 1 \cdot 10) + 1 \cdot 10 = 3 \cdot 10 - 2 \cdot 14\\
&= 3 \cdot (38 - 2 \cdot 14) + -2 \cdot 14 = -8 \cdot 14 + 3 \cdot 38\\
&= -8 \cdot (90 - 2 \cdot 38) + 3 \cdot 38 = 19 \cdot 38 - 8 \cdot 90\\
&= 19 \cdot (218 - 2 \cdot 90) + -8 \cdot 90 = -46 \cdot 90 + 19 \cdot 218
\end{aligned}$$

Hence $\alpha = -46$ and $\beta = 19$. Multiply the coefficients in the identity from above

$$-46 \cdot 90 + 19 \cdot 218 = 2$$

by 3 to get

$$-138 \cdot 90 + 57 \cdot 218 = 6$$

which gives a particular solution $x_0 = -138, y_0 = 57$ for $90x + 218y = 6$. Now, we can immediately form a general solution for $90x + 218y = 6$:

$$\begin{cases} x = -138 + \frac{218}{2} n \\ y = 57 - \frac{90}{2} n \end{cases}$$

which gives

$$\begin{cases} x = -138 + 109n \\ y = 57 - 45n \end{cases}$$

$$\mathrm{lcm}(90, 218) = \frac{90 \cdot 218}{\gcd(90, 218)} = 9810.$$

□

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 prove that $\gcd(f_n, f_{n+1}) = 1$ for every $n \in \mathbb{N}$.

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. $\square$

Exercise 1.4. [5pts] Use modulo-7 arithmetic to compute the remainder of division of 3^{100} by 7.

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

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

$\square$

Exercise 1.5. [5pts] Suppose that $\gcd(n_1, n_2) = 1$.

(a) Use Bezout's identity to prove that for any $c \in \mathbb{Z}$

$$\begin{cases} n_1 \mid c \\ n_2 \mid c \end{cases} \Leftrightarrow \quad n_1 n_2 \mid c.$$

(b) Use item (a) to prove that for any $x, y \in \mathbb{Z}$

$$\begin{cases} x \equiv_{n_1} y \\ x \equiv_{n_2} y \end{cases} \Leftrightarrow \quad x \equiv_{n_1 n_2} y.$$

(This is very useful when you deal with with a congruence modulo a large composite number – it allows to lower the modulus.)

Solution:

(a) $\gcd(n_1, n_2) = 1 \overset{Bezout}{\Rightarrow} 1 = \alpha n_1 + \beta n_2 \quad \Rightarrow \quad c = \alpha n_1 c + \beta n_2 c$. Therefore,

$$\begin{aligned} \begin{cases} n_1 \mid c \\ n_2 \mid c \end{cases} &\Rightarrow \begin{cases} c = n_1 q_1 \\ c = n_2 q_2 \end{cases} \\ &\Rightarrow \quad c = \alpha n_1 c + \beta n_2 c = \alpha n_1 n_2 q_2 + \beta n_2 n_1 q_1 = (n_1 n_2)(\alpha q_2 + \beta q_1) \\ &\Rightarrow \quad n_1 n_2 \mid c. \end{aligned}$$

Conversely,

$$n_1 n_2 \mid c \quad \Rightarrow \quad c = q(n_1 n_2) \quad \Rightarrow \quad c = n_1 \cdot q n_2 \quad \Rightarrow \quad n_1 \mid c.$$

Same can be done to n_2.

(b) Indeed,

$$\begin{cases} x \equiv_{n_1} y \\ x \equiv_{n_2} y \end{cases} \Leftrightarrow \begin{cases} n_1 \mid (x - y) \\ n_2 \mid (x - y) \end{cases} \Leftrightarrow \quad n_1 n_2 \mid (x - y) \quad \Leftrightarrow \quad x \equiv_{n_1 n_2} y.$$

$\square$

Exercise 1.6. [+3pts] 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 $ab = ba$.

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) $\left\{ a + b\sqrt{2}i \mid a, b \in \mathbb{Q} \right\}$.
(6) $\{-1, 0, 1\}$.

Solution:

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

$\square$

Exercise 1.7. [+4pts] 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	$x_n \cdot x_1$	$\ldots$	$x_n \cdot x_n$

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 $a \cdot c \neq b$.

$\square$