

# Lecture #5 Exercises

Distributed Lab

August 20, 2024



**Exercise 1.** Alice decided to commit to the race results, but forgot to use the blinding factor. She used a hash-based commitment and SHA256 hash function. Set of race participant numbers:  $(0x1, 0x3, 0x8, 0x15)$ . Can you break the hiding property of the commitment? Select the participant number Alice made a commitment to.

- (A)  $0x1$ .
- (B)  $0x3$ .
- (C)  $0x8$ .
- (D)  $0x15$ .

**Exercise 2.** Suppose that over  $\mathbb{R}$  we define the following equivalence relation:  $a \sim b$  iff  $a - b \in \mathbb{Z}$  ( $a, b \in \mathbb{R}$ ). What is the equivalence class of 1.4 (that is,  $[1.4]_{\sim}$ )?

- (A) A set of all real numbers.
- (B) A set of all integers.
- (C) A set of reals  $x \in \mathbb{R}$  with the fractional part of  $x$  equal to 0.4.
- (D) A set of reals  $x \in \mathbb{R}$  with the integer part of  $x$  equal to 1.
- (E) A set of reals  $x \in \mathbb{R}$  with the fractional part of  $x$  equal to 0.6.

**Exercise 3.** Which of the following pairs of points in homogeneous projective space  $\mathbb{P}^2(\mathbb{R})$  are **not** equivalent?

- (A)  $(1 : 2 : 3)$  and  $(2 : 4 : 6)$ .
- (B)  $(2 : 3 : 1)$  and  $(6 : 9 : 3)$ .
- (C)  $(5 : 5 : 5)$  and  $(2 : 2 : 2)$ .
- (D)  $(4 : 3 : 2)$  and  $(16 : 8 : 4)$ .

**Exercise 4.** The main reason for using projective coordinates in elliptic curve cryptography is:

- (A) To reduce the number of point additions in algorithms involving elliptic curves.
- (B) To make the curve more secure against attacks.
- (C) To make the curve more efficient in terms of memory usage.

- (D) To reduce the number of field multiplications when performing scalar multiplication.
- (E) To avoid making too many field inversions in complicated algorithms involving elliptic curves.

**Exercise 5.** Suppose  $k = 19$  is a scalar and we are calculating  $[k]P$  using the double-and-add algorithm. How many elliptic curve point addition operations will be performed?

- (A) 0.
- (B) 1.
- (C) 2.
- (D) 3.
- (E) 4.

**Exercise 6.** What is the minimal number of inversions needed to calculate the value of expression (over  $\mathbb{F}_p$ )

$$\frac{a-b}{(a+b)^4} + \frac{c}{a+b} + \frac{d}{a^2+c^2},$$

for the given scalars  $a, b, c, d \in \mathbb{F}_p$ ?

- (A) 1.
- (B) 2.
- (C) 3.
- (D) 4.
- (E) 5.

**Exercise 7.** Given pairing  $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$  with  $G_1$  — generator of  $\mathbb{G}_1$  and  $G_2 \in \mathbb{G}_2$  — generator of  $\mathbb{G}_2$ , which of the following is **not** equal to  $e([3]G_1, [5]G_2)$ ?

- (A)  $e([5]G_1, [3]G_2)$ .
- (B)  $e([4]G_1, [4]G_2)$ .
- (C)  $e([15]G_1, G_2)$ .
- (D)  $e([3]G_1, G_2)e(G_1, [12]G_2)$ .
- (E)  $e(G_1, G_2)^{15}$ .

**Exercise 8\*.** *Unit Circle Proof.* Suppose Alice wants to convince Bob that she knows a point on the unit circle  $x^2 + y^2 = 1$ . Suppose we are given a symmetric pairing  $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$  for  $\mathbb{G}_1 = \mathbb{G}_2 = \langle G \rangle$  and Alice computes  $P \leftarrow [x]G, Q \leftarrow [y]G$ . She then proceeds to sending  $(P, Q)$  to Bob. Which of the following checks should Bob perform to verify that Alice indeed knows a point on the unit circle?

- (A) Check if  $e(P, Q)e(Q, P) = 1$ .
- (B) Check if  $e([2]P, [2]Q) = e(G, G)$ .
- (C) Check if  $e([2]P, Q)e(Q, [2]P) = 1$ .
- (D) Check if  $e(P, P) + e(Q, Q) = 1$ .
- (E) Check if  $e(P, P)e(Q, Q) = e(G, G)$ .