1. [10]	2. [10]	3. [10]	4. [10]	5. [10]
6. [10]	7. [10]	8. [10]	9. [10]	10. [10]
Total. [100]				

MA 503 **Final** **May 12, 2021**

Name: ***Solutions***

Open book and notes.	*Answers must include supporting work.*
Calculators and wolfram alpha can be used for basic computations.	*No collaboration!*
	No Chegg or similar services!

(1) [10 pts] Suppose that G is an abelian group generated by x_1, x_2, x_3. Using a quantum algorithm we've learnt that x_1, x_2, x_3 are subject to the following relations:

$$r_1 = -2x_1 + 4x_2 - x_3 = 0$$
$$r_2 = 5x_1 + 2x_2 + 7x_3 = 0$$
$$r_3 = 4x_1 - 3x_2 + 2x_3 = 0.$$

Assuming that this set of relations is complete (all other relations follow from r_1, r_2, r_3), express G as a direct product of cyclic groups.

Solution: Compute the normal form of the relation matrix

$$\begin{bmatrix} -2 & 4 & -1 \\ 5 & 2 & 7 \\ 4 & -3 & 2 \end{bmatrix} \to \begin{bmatrix} -1 & -2 & 4 \\ 7 & 5 & 2 \\ 2 & 4 & -3 \end{bmatrix} \to \begin{bmatrix} -1 & -2 & 4 \\ 0 & -9 & 30 \\ 0 & 0 & 5 \end{bmatrix} \to \begin{bmatrix} -1 & 0 & 0 \\ 0 & -9 & 30 \\ 0 & 0 & 5 \end{bmatrix}$$

Then do the same for a submatrix

$$\begin{bmatrix} -9 & 30 \\ 0 & 5 \end{bmatrix} \to \begin{bmatrix} -9 & 0 \\ 0 & 5 \end{bmatrix} \to \begin{bmatrix} -9 & 0 \\ 10 & 5 \end{bmatrix} \to \begin{bmatrix} -9 & 0 \\ 1 & 5 \end{bmatrix} \to \begin{bmatrix} 0 & 45 \\ 1 & 5 \end{bmatrix} \to \begin{bmatrix} 0 & 45 \\ 1 & 0 \end{bmatrix} \to \begin{bmatrix} 1 & 0 \\ 0 & 45 \end{bmatrix}$$

Thus, the group is isomorphic to $\mathbb{Z}_1 \times \mathbb{Z}_1 \times \mathbb{Z}_{45}$, but, since $\mathbb{Z}_1$ is trivial, the group is isomorphic to $\mathbb{Z}_{45}$.

(2) [10 pts] Let F be a field. Show that $F[x]$ is a vector space over F.

Solution: $(F[x],+)$ is an abelian group:

- $0 \in F[x]$;
- $f(x) \in F[x] \quad \Rightarrow \quad -f(x) \in F[x]$;
- polynomial addition is commutative and associative.

For any $\alpha, \beta \in F$ and $f(x) \in F[x]$ it is easy to check that

$$\alpha(\beta f(x)) = (\alpha\beta) f(x).$$

$1 \in F[x]$ and $1 \cdot f(x) = f(x)$.

For any $\alpha, \beta \in F$ and $f(x), g(x) \in F[x]$ it is easy to check that

$$(\alpha+\beta) f(x) = \alpha f(x) + \beta f(x) \quad \text{and} \quad \alpha(f(x)+g(x)) = \alpha f(x) + \alpha g(x).$$

(3) [10 pts] Let F be a field. Let $I = \langle f(x) \rangle$ and $J = \langle g(x) \rangle$ be ideals in $F[x]$.

(a) [6pts] Prove that $K = I \cap J$ is an ideal in $F[x]$.

(b) [1pt] Every ideal in $F[x]$ is principle and, hence, $K = \langle h(x) \rangle$. Show that $h(x)$ is a common multiple for $f(x)$ and $g(x)$.

(c) [3pts] Prove that $h(x)$ divides every common multiple for $f(x)$ and $g(x)$.

Basically, it is a way to define $\operatorname{lcm}(f(x), g(x))$.

Solution: To prove that $K = I \cap J$ is an ideal in $F[x]$ we check that $(K, +)$ is a subgroup of $F[x]$. $0 \in K$ because

$$0 \in I, 0 \in J \quad \Rightarrow \quad 0 \in I \cap J = K.$$

K is closed under $+$ because

$$\begin{array}{c} x \in K \\ y \in K \end{array} \quad \Rightarrow \quad \begin{array}{c} x \in I, x \in J \\ y \in I, y \in J \end{array} \quad \Rightarrow \quad \begin{array}{c} x + y \in I \\ x + y \in J \end{array} \quad \Rightarrow \quad x + y \in K.$$

K contains additive inverses, because

$$x \in K \quad \Rightarrow \quad x \in I, x \in J \quad \Rightarrow \quad -x \in I, -x \in J \quad \Rightarrow \quad -x \in I \cap J = K.$$

Also, K is closed under R-multiplication because

$$x \in K \quad \Rightarrow \quad x \in I, x \in J \quad \Rightarrow \quad \forall r \in R, \quad rx \in I, rx \in J \quad \Rightarrow \quad \forall r \in R, \quad rx \in I \cap J = K$$

Thus, K is an ideal.

(b) is obvious because

$$\begin{array}{lcl} h(x) \in K \subseteq I = \langle f(x) \rangle & \Rightarrow & f(x) \mid h(x) \\ h(x) \in K \subseteq J = \langle g(x) \rangle & \Rightarrow & g(x) \mid h(x) \end{array}$$

To prove (c) pick any common multiple $m(x)$ for $f(x)$ and $g(x)$ and observe the following:

$$\begin{array}{c} f(x) \mid m(x) \\ g(x) \mid m(x) \end{array} \quad \Rightarrow \quad \begin{array}{c} m(x) \in I \\ m(x) \in J \end{array} \quad \Rightarrow \quad m(x) \in I \cap J = K = \langle h(x) \rangle \quad \Rightarrow \quad h(x) \mid m(x).$$

(4) [10 pts] Let $f(x) = x^3 + x^2 + 2x + 1 \in \mathbb{Z}_3[x]$.

(a) [3 pts] Show that $E = \mathbb{Z}_3[x]/\langle f(x)\rangle$ is a field.

(b) [1 pt] What is $\chi(E)$ and $|E|$?

(c) [3 pts] Is $-x$ (negative x) primitive in E?

(d) [3 pts] Find $(x+1)^{-1}$ in E. Explain!

Solution:

(a) $f(x) = x^3 + x^2 + 2x + 1 \in \mathbb{Z}_3[x]$ is cubic that has no zeros in $\mathbb{Z}_3$

$$f(0) = 1 \not\equiv_3 0 \qquad f(1) = 5 \not\equiv_3 0 \qquad f(2) = 17 \not\equiv_3 0.$$

Hence, $f(x)$ is irreducible and E is a field.

(b) Obviously, $\chi(E) = 3$ and $|E| = 3^3 = 27$.

(c) The size of the multiplicative group E^* of E is $27 - 1 = 26 = 2 \cdot 13$. So, to check if $-x$ is primitive it is sufficient to compute $(-x)^2 = x^2 \neq 1$ and $(-x)^{13} = 1$. Thus, $-x$ is not primitive.

(d) Consider a general element $ax^2 + bx + c \in E$ with unknown a, b, c. Then

$$\begin{aligned}(ax^2 + bx + c)(x+1) &= ax^3 + (a+b)x^2 + (c+b)x + c \\ &= a(2x^2 + x + 2) + (a+b)x^2 + (c+b)x + c \\ &= x^2(2a + a + b) + x(a + b + c) + (2a + c)\end{aligned}$$

which should be 1. Hence,

$$\begin{cases} 3a + b \equiv_3 0 \\ a + b + c \equiv_3 0 \\ 2a + c \equiv_3 1 \end{cases}$$

which gives $b = 0, c = 2, a = 1$. Thus, $(x+1)^{-1} = x^2 + 2$.

(5) [10 pts] Let $f(x) = x^3 + x^2 + 2x + 1 \in \mathbb{Z}_3[x]$ and $E = \mathbb{Z}_3[x]/\langle f(x) \rangle$, the field from the problem (4). Use **Pohlig–Hellman algorithm** (discussed in lecture 5) to find $\log_x(x^2 + 2x + 2)$. You can use the fact that $|x| = 26$ in E. Show computations: identify h_i, g_i, enumerate powers of g_i to compute $\log_{g_i}(h_i)$. Here you are allowed to use wolfram alpha and compute polynomials modulo $f(x)$

```
PolynomialMod[x^4,{3,x^3+x^2+2x+1}]
```

Solution: Here $|x| = 26 = 2 \cdot 13$ and, hence,

$$N_1 = 13 \qquad g_1 = x^{13} \equiv 2 \qquad h_1 = (x^2 + 2x + 2)^{13} \equiv 2 \qquad \log_2(2) = 1 = x_1$$

$$N_2 = 2 \qquad g_2 = x^2 \equiv x^2 \qquad h_2 = (x^2 + 2x + 2)^2 \equiv x + 1 \qquad \log_{x^2}(x + 1) = x_2.$$

So, the value of x_1 is obvious. To compute x_2 we enumerate powers of x^2 until we get $x + 1$:

$$(x^2)^2 \equiv 2x^2 + x + 1 \qquad (x^2)^3 \equiv x^2 + 1 \qquad (x^2)^4 \equiv x + 1.$$

Hence, $x_2 = 4$ and solving the system

$$\begin{cases} x_1 \equiv_2 1 \\ x_2 \equiv_{13} 4 \end{cases}$$

we get $x = 17$.

(6) [10 pts] For polynomials $f(x) = 2x^3 + 6x^2 + 5x + 1$ and $g(x) = 3x^4 + x^3 + 3x^2 + x + 3$ in $\mathbb{Z}_7[x]$.

(a) [5 pts] Compute $\gcd(f(x), g(x))$.

(b) [5 pts] Compute $\alpha(x), \beta(x) \in \mathbb{Z}_7[x]$ such that $\gcd(f(x), g(x)) = \alpha(x)f(x) + \beta(x)g(x)$. Show ALL supporting work.

Solution: Using the Euclidean algorithm we obtain

$$\begin{aligned} g(x) &= (5x+3)f(x) + (2x^2+2x) & \Rightarrow\quad \gcd(f,g) &= \gcd(f, 2x^2+2x) \\ f(x) &= (x+2)(2x^2+2x) + (x+1) & &= \gcd(x+1, 2x^2+2x) \\ 2x^2+2x &= 2x(x+1) + 0 & &= \gcd(x+1, 0) = x+1. \end{aligned}$$

For instance, for $f(x) = x^5 + 2x^3 + x + 1$ and $g(x) = x^4 + x + 2$ in $\mathbb{Z}_3[x]$.

$$\begin{aligned} x+1 &= \mathbf{f(x)} - (x+2)(\mathbf{2x^2+2x}) \\ &= \mathbf{f(x)} - (x+2)(\mathbf{g(x)} - (5x+3)\mathbf{f(x)}) \\ &= (5x^2+6x)\mathbf{f(x)} - (x+2)\mathbf{g(x)} \end{aligned}$$

Thus, $\alpha(x) = 5x^2 + 6x$ and $\beta(x) = -(x+2)$.

(7) [10 pts] Consider $f(x) = x^3 + 1 \in \mathbb{Z}_2[x]$ and the quotient ring $E = \mathbb{Z}_2[x]/\langle f(x)\rangle$.

(a) [5pts] Construct the multiplication table for E.

(b) [1pt] Find all zero divisors in E. [Hint. Recall that $g \neq 0$ is a zero divisor in E if $g \cdot h = 0$ for some $h \neq 0$.]

(c) [1pt] Find the set U of all units in E. For each unit find its multiplicative inverse.

(d) [1pt] Is U closed under $\cdot$?

(e) [1pt] Is $(U, \cdot)$ a group?

(f) [1pt] How many primitive element does $(U, \cdot)$ have?

Solution: Elements from E are the quadratic polynomials over $\mathbb{Z}_2$ and, hence, $E = \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}$.

	0	1	x	$1+x$	x^2	$1+x^2$	$x+x^2$	$1+x+x^2$
0	0	0	0	0	0	0	0	0
1	0	1	x	$1+x$	x^2	$1+x^2$	$x+x^2$	$1+x+x^2$
x	0	x	x^2	$x+x^2$	1	$1+x$	$1+x^2$	$1+x+x^2$
$1+x$	0	$1+x$	$x+x^2$	$1+x^2$	$1+x^2$	$x+x^2$	$1+x$	0
x^2	0	x^2	1	$1+x^2$	x	$x+x^2$	$1+x$	$1+x+x^2$
$1+x^2$	0	$1+x^2$	$1+x$	$x+x^2$	$x+x^2$	$1+x$	$1+x^2$	0
$x+x^2$	0	$x+x^2$	$1+x^2$	$1+x$	$1+x$	$1+x^2$	$x+x^2$	0
$1+x+x^2$	0	$1+x+x^2$	$1+x+x^2$	0	$1+x+x^2$	0	0	$1+x+x^2$

Now, it is easy to find zero divisors

$$\{x+1, x^2+1, x^2+x, x^2+x+1\}$$

and the units

$$U = \{1, x, x^2\}$$

$x^{-1} = x^2$ and $(x^2)^{-1} = x$. U is clearly a cyclic group with two primitive elements x and x^2.

(8) [10 pts] Consider an instance of Shamir's $(2, 4)$-threshold scheme over $\mathbb{Z}_{17}$. Suppose that all four participants decide to compute the secret and contribute their shares

#1 $(12, 2)$,
#2 $(3, 14)$,
#3 $(9, 11)$,
#4 $(7, 12)$.

Unfortunately, one (exactly one!) dishonest participant provided a fake (modified) share. Identify the dishonest participant.

Solution: In a $(2, n)$-scheme, the function $f(x)$ used to construct shares is linear $mx + b$ and every two participants can reconstruct it. We can use Lagrange interpolation formula to find $f(x)$ for each pair of participants. Or we can reconstruct $m = \frac{y_2 - y_1}{x_2 - x_1}$ for all pairs of participants:

	#1	#2	#3	#4
#1		10	14	15
#2			8	8
#3				8

Here we see that $m = 8$ is consistent for participants #2, #3, and #4. And the share of the participant #1 gives different values of m. Hence, #1 must be dishonest.

(9) [10 pts] Consider the elliptic curve $\mathcal{E}$ defined by the equation $y^2 = x^3 + 2x + 6$ over $\mathbb{Z}_{13}$. Its addition table is shown below

	$\mathcal{O}$	(1,3)	(1,10)	(3,0)	(4,0)	(6,0)	(7,5)	(7,8)	(8,1)	(8,12)	(9,5)	(9,8)	(10,5)	(10,8)	(12,4)	(12,9)
$\mathcal{O}$	$\mathcal{O}$	(1,3)	(1,10)	(3,0)	(4,0)	(6,0)	(7,5)	(7,8)	(8,1)	(8,12)	(9,5)	(9,8)	(10,5)	(10,8)	(12,4)	(12,9)
(1,3)	(1,3)	(7,5)	$\mathcal{O}$	(8,1)	(9,5)	(10,5)	(8,12)	(1,10)	(7,8)	(3,0)	(12,4)	(4,0)	(12,9)	(6,0)	(10,8)	(9,8)
(1,10)	(1,10)	$\mathcal{O}$	(7,8)	(8,12)	(9,8)	(10,8)	(1,3)	(8,1)	(3,0)	(7,5)	(4,0)	(12,9)	(6,0)	(12,4)	(9,5)	(10,5)
(3,0)	(3,0)	(8,1)	(8,12)	$\mathcal{O}$	(6,0)	(4,0)	(7,8)	(7,5)	(1,3)	(1,10)	(10,5)	(10,8)	(9,5)	(9,8)	(12,9)	(12,4)
(4,0)	(4,0)	(9,5)	(9,8)	(6,0)	$\mathcal{O}$	(3,0)	(12,4)	(12,9)	(10,5)	(10,8)	(1,3)	(1,10)	(8,1)	(8,12)	(7,5)	(7,8)
(6,0)	(6,0)	(10,5)	(10,8)	(4,0)	(3,0)	$\mathcal{O}$	(12,9)	(12,4)	(9,5)	(9,8)	(8,1)	(8,12)	(1,3)	(1,10)	(7,8)	(7,5)
(7,5)	(7,5)	(8,12)	(1,3)	(7,8)	(12,4)	(12,9)	(3,0)	$\mathcal{O}$	(1,10)	(8,1)	(10,8)	(9,5)	(9,8)	(10,5)	(6,0)	(4,0)
(7,8)	(7,8)	(1,10)	(8,1)	(7,5)	(12,9)	(12,4)	$\mathcal{O}$	(3,0)	(8,12)	(1,3)	(9,8)	(10,5)	(10,8)	(9,5)	(4,0)	(6,0)
(8,1)	(8,1)	(7,8)	(3,0)	(1,3)	(10,5)	(9,5)	(1,10)	(8,12)	(7,5)	$\mathcal{O}$	(12,9)	(6,0)	(12,4)	(4,0)	(9,8)	(10,8)
(8,12)	(8,12)	(3,0)	(7,5)	(1,10)	(10,8)	(9,8)	(8,1)	(1,3)	$\mathcal{O}$	(7,8)	(6,0)	(12,4)	(4,0)	(12,9)	(10,5)	(9,5)
(9,5)	(9,5)	(12,4)	(4,0)	(10,5)	(1,3)	(8,1)	(10,8)	(9,8)	(12,9)	(6,0)	(7,5)	$\mathcal{O}$	(7,8)	(3,0)	(8,12)	(1,10)
(9,8)	(9,8)	(4,0)	(12,9)	(10,8)	(1,10)	(8,12)	(9,5)	(10,5)	(6,0)	(12,4)	$\mathcal{O}$	(7,8)	(3,0)	(7,5)	(1,3)	(8,1)
(10,5)	(10,5)	(12,9)	(6,0)	(9,5)	(8,1)	(1,3)	(9,8)	(10,8)	(12,4)	(4,0)	(7,8)	(3,0)	(7,5)	$\mathcal{O}$	(1,10)	(8,12)
(10,8)	(10,8)	(6,0)	(12,4)	(9,8)	(8,12)	(1,10)	(10,5)	(9,5)	(4,0)	(12,9)	(3,0)	(7,5)	$\mathcal{O}$	(7,8)	(8,1)	(1,3)
(12,4)	(12,4)	(10,8)	(9,5)	(12,9)	(7,5)	(7,8)	(6,0)	(4,0)	(9,8)	(10,5)	(8,12)	(1,3)	(1,10)	(8,1)	(3,0)	$\mathcal{O}$
(12,9)	(12,9)	(9,8)	(10,5)	(12,4)	(7,8)	(7,5)	(4,0)	(6,0)	(10,8)	(9,5)	(1,10)	(8,1)	(8,12)	(1,3)	$\mathcal{O}$	(3,0)

(a) [1pt] Is it singular?

(b) [3pts] Find the order of $(1,3)$.

(c) [3pts] If $\mathcal{E}$ is cyclic, then find ALL primitive points on $\mathcal{E}$. If $\mathcal{E}$ is not cyclic, then show that $\mathcal{E}$ has no primitive points.

(d) [3pts] Solve an instance $((1,3),(8,12),(7,8))$ of an ECCDH, or prove that it has no solutions. (Formally speaking, ECCDH always has a solution. ECCDH is a **promise problem** and, by definition, the arguments must be properly chosen. If the solution does not exist, then we say that a given triple does not define an instance of ECCDH).

Solution:

(a) $\mathcal{E}$ is not singular because $4a^3 + 27b^2 = 4 \cdot 2^3 + 27 \cdot 6^2 \equiv_{13} 3$.

(b) It is easy to find multiples of $(1,3)$ using the table

$2 \cdot (1,3) = (7,5)$ $\quad 3 \cdot (1,3) = (8,12)$ $\quad 4 \cdot (1,3) = (3,0)$ $\quad 5 \cdot (1,3) = (8,1)$

$6 \cdot (1,3) = (7,8)$ $\quad 7 \cdot (1,3) = (1,10)$ $\quad 8 \cdot (1,3) = \mathcal{O}$.

Hence, $|(1,3)| = 8$.

(c) If $\mathcal{E}$ is not cyclic because it has no element of order 16. We've seen above that $(1,3)$ is not primitive. Obviously the multiples of $(1,3)$ are not primitive too. Consider the remaining elements of $\mathcal{E}$.

$$2 \cdot (4,0) = \mathcal{O}$$

So, $(4,0)$ is not primitive.

$$2 \cdot (6,0) = \mathcal{O}$$

So, $(6,0)$ is not primitive.

$2 \cdot (9,5) = (7,5)$ $\quad 3 \cdot (9,5) = (10,8)$ $\quad 4 \cdot (9,5) = (3,0)$ $\quad 5 \cdot (9,5) = (10,5)$

$6 \cdot (9,5) = (7,8)$ $\quad 7 \cdot (9,5) = (9,8)$ $\quad 8 \cdot (9,5) = \mathcal{O}$.

So, $(9,5)$ is not primitive. Hence, $(9,8),(10,8),(10,5)$ are not primitive. In a similar way we can show that $(12,4),(12,9)$ are not primitive.

(d) Using the table it is easy to compute

$$\log_{(1,3)}(8,12) = 3 \quad \text{and} \quad \log_{(1,3)}(7,8) = 6.$$

Since $3 \cdot 6 = 18 \equiv_{|(1,3)|} 2$, we have

$$18 \cdot (1,3) = 2 \cdot (1,3) = (7,5).$$

(10) [10 pts] Suppose that Bob uses an elliptic curve ElGamal protocol to send a message m to Alice using

- the elliptic curve $\mathcal{E}$ defined by the equation $y^2 = x^3 + 3x + 4$ over $\mathbb{Z}_{11}$,
- the primitive (base) element $g = (5, 1)$,
- the Alice's private key $(9, 10)$.

If Bob's ciphertext is the pair (c_1, c_2), where $c_1 = (7, 7), c_2 = (9, 1)$, then what is m?
Show all computations!

Solution: $\mathcal{E}$ has the following addition table:

	$\mathcal{O}$	$(0,2)$	$(0,9)$	$(4,5)$	$(4,6)$	$(5,1)$	$(5,10)$	$(7,4)$	$(7,7)$	$(8,1)$	$(8,10)$	$(9,1)$	$(9,10)$	$(10,0)$
$\mathcal{O}$	$\mathcal{O}$	$(0,2)$	$(0,9)$	$(4,5)$	$(4,6)$	$(5,1)$	$(5,10)$	$(7,4)$	$(7,7)$	$(8,1)$	$(8,10)$	$(9,1)$	$(9,10)$	$(10,0)$
$(0,2)$	$(0,2)$	$(4,6)$	$\mathcal{O}$	$(0,9)$	$(8,1)$	$(10,0)$	$(9,10)$	$(7,7)$	$(9,1)$	$(8,10)$	$(4,5)$	$(5,1)$	$(7,4)$	$(5,10)$
$(0,9)$	$(0,9)$	$\mathcal{O}$	$(4,5)$	$(8,10)$	$(0,2)$	$(9,1)$	$(10,0)$	$(9,10)$	$(7,4)$	$(4,6)$	$(8,1)$	$(7,7)$	$(5,10)$	$(5,1)$
$(4,5)$	$(4,5)$	$(0,9)$	$(8,10)$	$(8,1)$	$\mathcal{O}$	$(7,7)$	$(5,1)$	$(5,10)$	$(9,10)$	$(0,2)$	$(4,6)$	$(7,4)$	$(10,0)$	$(9,1)$
$(4,6)$	$(4,6)$	$(8,1)$	$(0,2)$	$\mathcal{O}$	$(8,10)$	$(5,10)$	$(7,4)$	$(9,1)$	$(5,1)$	$(4,5)$	$(0,9)$	$(10,0)$	$(7,7)$	$(9,10)$
$(5,1)$	$(5,1)$	$(10,0)$	$(9,1)$	$(7,7)$	$(5,10)$	$(4,5)$	$\mathcal{O}$	$(4,6)$	$(8,1)$	$(9,10)$	$(7,4)$	$(8,10)$	$(0,2)$	$(0,9)$
$(5,10)$	$(5,10)$	$(9,10)$	$(10,0)$	$(5,1)$	$(7,4)$	$\mathcal{O}$	$(4,6)$	$(8,10)$	$(4,5)$	$(7,7)$	$(9,1)$	$(0,9)$	$(8,1)$	$(0,2)$
$(7,4)$	$(7,4)$	$(7,7)$	$(9,10)$	$(5,10)$	$(9,1)$	$(4,6)$	$(8,10)$	$(0,9)$	$\mathcal{O}$	$(5,1)$	$(10,0)$	$(0,2)$	$(4,5)$	$(8,1)$
$(7,7)$	$(7,7)$	$(9,1)$	$(7,4)$	$(9,10)$	$(5,1)$	$(8,1)$	$(4,5)$	$\mathcal{O}$	$(0,2)$	$(10,0)$	$(5,10)$	$(4,6)$	$(0,9)$	$(8,10)$
$(8,1)$	$(8,1)$	$(8,10)$	$(4,6)$	$(0,2)$	$(4,5)$	$(9,10)$	$(7,7)$	$(5,1)$	$(10,0)$	$(0,9)$	$\mathcal{O}$	$(5,10)$	$(9,1)$	$(7,4)$
$(8,10)$	$(8,10)$	$(4,5)$	$(8,1)$	$(4,6)$	$(0,9)$	$(7,4)$	$(9,1)$	$(10,0)$	$(5,10)$	$\mathcal{O}$	$(0,2)$	$(9,10)$	$(5,1)$	$(7,7)$
$(9,1)$	$(9,1)$	$(5,1)$	$(7,7)$	$(7,4)$	$(10,0)$	$(8,10)$	$(0,9)$	$(0,2)$	$(4,6)$	$(5,10)$	$(9,10)$	$(8,1)$	$\mathcal{O}$	$(4,5)$
$(9,10)$	$(9,10)$	$(7,4)$	$(5,10)$	$(10,0)$	$(7,7)$	$(0,2)$	$(8,1)$	$(4,5)$	$(0,9)$	$(9,1)$	$(5,1)$	$\mathcal{O}$	$(8,10)$	$(4,6)$
$(10,0)$	$(10,0)$	$(5,10)$	$(5,1)$	$(9,1)$	$(9,10)$	$(0,9)$	$(0,2)$	$(8,1)$	$(8,10)$	$(7,4)$	$(7,7)$	$(4,5)$	$(4,6)$	$\mathcal{O}$

- Find the Alice's private key $a = \log_{(5,1)}(9, 10)$ directly by computing multiples of $(5, 1)$. It is not much computation (even without the table).
  - $2 \cdot (5, 1) = (4, 5)$,
  - $3 \cdot (5, 1) = (7, 7)$,
  - $4 \cdot (5, 1) = (8, 1)$,
  - $5 \cdot (5, 1) = (9, 10)$.

  Hence, $a = 5$.
- Compute m as

$$c_2 - a \cdot c_1 = (9, 1) - 5 \cdot (7, 7) = (9, 1) - (5, 1) = (9, 1) + (5, 10) = (0, 9).$$