CHIFR_Test 2

Statut	Terminée
Commencé	lundi 26 mai 2025, 11:46
Terminé	lundi 26 mai 2025, 12:45
Durée	59 min 4 s

Description

Marquer la question

Le téléphone portable est strictement interdit ainsi que l'utilisation d'internet.

Vous pouvez utiliser Python comme calculatrice .
Pour rappel x^y s'écrit $x**y$ sur Python

Pour les puissances modulaires il est conseillé d'utiliser la fonction pow(a,i,n) qui calcule $a^i \mod n$ (si vous écrivez un script vérifier s'il ne faut pas rajouter import math en début). L'inverse modulo n de a peut être calculer par pow(a,-1,n).

Pour l'exercice sur la feuille je vous invite à écrire votre prénom et nom en majuscules ainsi que l'UID de façon lisible .

Bon travail !
==

Internet and phones are forbiden.

You can use Python as a calculator.

Recall that x^y is written as $x**y$ in Python. It is advisable to use pow(a,i,n) to calculate $a^i \mod n$ (if you write a script check whether you need to add import math at the begging).
The modular inverse of a modulo n can be calculated by pow(a,-1,n).

Please try to write your name and UID on the paper as readable as you can.

Have a nice work!

Question 1

Terminé

Noté sur 2,00

Marquer la question

La matrice génératrice d'un code correcteur est :

$$G=\begin{pmatrix} 1&0&0&0&0&1&0&0&0\\ 0&1&0&0&0&1&1&0&0\\ 0&0&1&0&0&0&1&1&0\\ 0&0&0&1&0&0&0&1&1\\ 0&0&0&0&1&0&1&0&1 \end{pmatrix}$$

Combien de codes contient l'espace des codes?

==================================
How many codes has the space of codes given by the above generating matrix?

Réponse : 8

Question 2

Terminé

Noté sur 2,00

Marquer la question

Jean pense que le code correcteur de matrice génératrice G donné ci-dessous peut corriger 2 erreurs. A-t-il raison?

===
Jean thinks that the error-correcting code with generator matrix G can correct 2 errors. Is he right?"

$$G=\begin{pmatrix} 1&0&0&0&0&1&0&0&0\\ 0&1&0&0&0&1&1&0&0\\ 0&0&1&0&0&0&1&1&0\\ 0&0&0&1&0&0&0&1&1\\ 0&0&0&0&1&0&1&0&1 \end{pmatrix}$$

● Vrai

○ Faux

Description

Marquer la question

Alice et Bob utilisent El Gamal avec la courbe elliptique $y^2 = x^3 + 2x + 5 \mod 11$ et générateur $G = (0, 4)$.

1. Alice veut envoyer le message $m = 8$. Elle choisi le point sur la courbe elliptique d'abscisse 8 avec la plus grande ordonnée. Quel est le point qui correspond au message d'Alice ?
2. Bob a choisi $b = 2$ pour sa clé privé. Quelle est sa clé publique?
3. Alice a renvoyé le meme message à Bob cette fois ci en prenant le double de sa clé privé a. Eve qui surveille leur communication est au courant de cela. Peux-elle déchiffrer le message ?

Les cryptosysteme est donné en fin de la version anglaise

==

Alice and Bob invent their own cryptosystem, which uses the elliptic curve $y^2 = x^3 + 2x + 5 \mod 11$ and generator $G = (0, 4)$.

1. Alice wants to send the message m=8. She chooses the point on the elliptic curve with x-coordinate 8 that has the largest y-coordinate. **What is the point corresponding to Alice's message?**

2. Bob has chosen b=2 as his private key.
What is his public key?

3. Alice sent the same message to Bob again, but this time using double her previous private key a. Eve, who is monitoring their communication, is aware of this. **Can she decrypt the message?**

Alice	Bob
KeyGen: Diffie-Hellman	
Choisir p premier, E et $G \in E(\mathbb{F}_p)$ $\mathscr{M} = E(\mathbb{F}_p)$, $\mathscr{C} = E(\mathbb{F}_p)^2$	
	Choisir $b < \mathrm{Card}\ E(\mathbb{F}_p)$, $K_b = bG$ Clé privée de Bob : $\mathrm{sk} = b$
clé publique: $\mathrm{pk} = (\mathscr{M}, p, E, G, K_b)$	
Chiffrement	
Choisir $a < \mathrm{Card}\ E(\mathbb{F}_p)$ $c_1 = aG$, $c_2 = M + aK_b$ $c = \mathrm{Enc}(m,\ \mathrm{pk}) = (c_1, c_2)$	
Dechiffrement	
	$\mathrm{Dec}(c,\ \mathrm{sk}) = (c_2 - bc_1)$

Let P be a point on $E : y^2 = x^3 + ax + b \mod p$ then

- $P + \mathcal{O} = \mathcal{O} + P = P$

If P and Q are different from $\mathcal{O}$

- $P + Q = \mathcal{O}$ if $x_P = x_Q$ and $y_P \neq y_Q$ then
- $P + Q = 2P = \mathcal{O}$ if $P = Q$ and $y_P = y_Q = 0$ then
- else $P + Q = (x, y)$ calculated as follows :

$$\begin{array}{rcl} m &=& \begin{cases} (y_Q - y_P)(x_Q - x_P)^{-1} \mod p & P \neq Q \\ (3x_P^2 + a)(2y_P)^{-1} \mod p & P = Q,\ y_P \neq 0 \end{cases} \\ x &=& m^2 - x_P - x_Q \mod p \\ y &=& m(x_P - x) - y_P \mod p \end{array}$$

Description

Marquer la question

Cette exercice est à rédiger sur la partie Exercice 2 de votre feuille.

Vous êtes un ingénieur travaillant pour une agence météorologique. Vous êtes responsable de la transmission de données critiques provenant de capteurs distants (température, pression atmosphérique, humidité). Ces données sont transmises via un canal de communication sans fil qui est sujet au bruit, ce qui peut entraîner des erreurs de transmission. Pour garantir l'intégrité des données, vous avez décidé d'implémenter un code correcteur d'erreurs.

Vous utilisez un code linéaire défini par la matrice de vérification H.

$$H=\begin{pmatrix} 1&1&1&0&1&0&0&0\\ 1&1&0&1&0&1&0&0\\ 1&0&1&1&0&0&1&0\\ 0&1&1&1&0&0&0&1 \end{pmatrix}$$

1. Donner la matrice génératrice G de ce code et les paramètres [n,k,d] en justifiant la distance. Donner les caractéristiques de ce code : nombre de codes, d'erreurs qu'on peut détecter et corriger.
2. Le message de code c est transmis à travers le canal. Le vecteur reçu y est le suivant : y=(1 0 1 0 0 1 0 0). A-t-il eu une erreur et si oui corriger la?
3. Vous avez reçu le vecteur y_2 avec syndrôme $s(y_2) = (1111)$. Ce vecteur contient-t-il des erreurs et si oui peut-t-on les corriger? Justifier.

===

This exercise should be written in the Exercise 2 section of your sheet.

You are an engineer working for a meteorological agency. You are responsible for transmitting critical data from remote sensors (temperature, atmospheric pressure, humidity). These data are transmitted via a wireless communication channel that is subject to noise, which can lead to transmission errors. To ensure data integrity, you have decided to implement an error-correcting code.

You are using a **linear code** defined by the **parity-check matrix H**.

Tasks:

1. Determine the **generator matrix G** of this code and the parameters **[n, k, d]**, justifying the value of the distance *d*. Give the characteristics of this code: number of codewords, number of detectable errors, and number of correctable errors.

2. The codeword **c** is transmitted through the channel. The received vector is: **y = (1 0 1 0 0 1 0 0)**. Was there an error, and if so, correct it?

3. You have received the vector y_2 with syndrom s(y_2) =(1111) . Does this vector contain errors, and if so, can they be corrected? Justify your answer.

Question 3

Terminé

Noté sur 3,00

Marquer la question

Alice a crée sa clé privée avec openssl et la courbe prime256v1 et à partir de cela extrait sa clé publique.

Quelles sont les 4 premiers lettres de sa **clé publique** si sa clé privée est

```
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIMhV/T9TAsY+RxPUDbxmC/C2CKSg6jjQ4ZvU4h8ZR87QoAoGCCqGSM49
AwEHoUQDQgAELQi1BEB4509oNap3AuSNb0VJPBBYSwJ+C+w6hA6DinfuLyQInkdm
UBOPhQL0yYn/eGhw9spPxgXjV78rIv6/LA==
-----END EC PRIVATE KEY-----
```

(par exemple les 4 premières lettres de sa clé privé sont MHcC)

============================

Alice creates her private key with openssl and the curve prime256v1 and then extracts the public key.

What are the first 4 letters of her public key if her private key is

```
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIMhV/T9TAsY+RxPUDbxmC/C2CKSg6jjQ4ZvU4h8ZR87QoAoGCCqGSM49
AwEHoUQDQgAELQi1BEB4509oNap3AuSNb0VJPBBYSwJ+C+w6hA6DinfuLyQInkdm
UBOPhQL0yYn/eGhw9spPxgXjV78rIv6/LA==
-----END EC PRIVATE KEY-----
```

For example, the first for letters of her private key are MHcC

Réponse : MFkw

Question 4

Terminé

Noté sur 2,00

Marquer la question

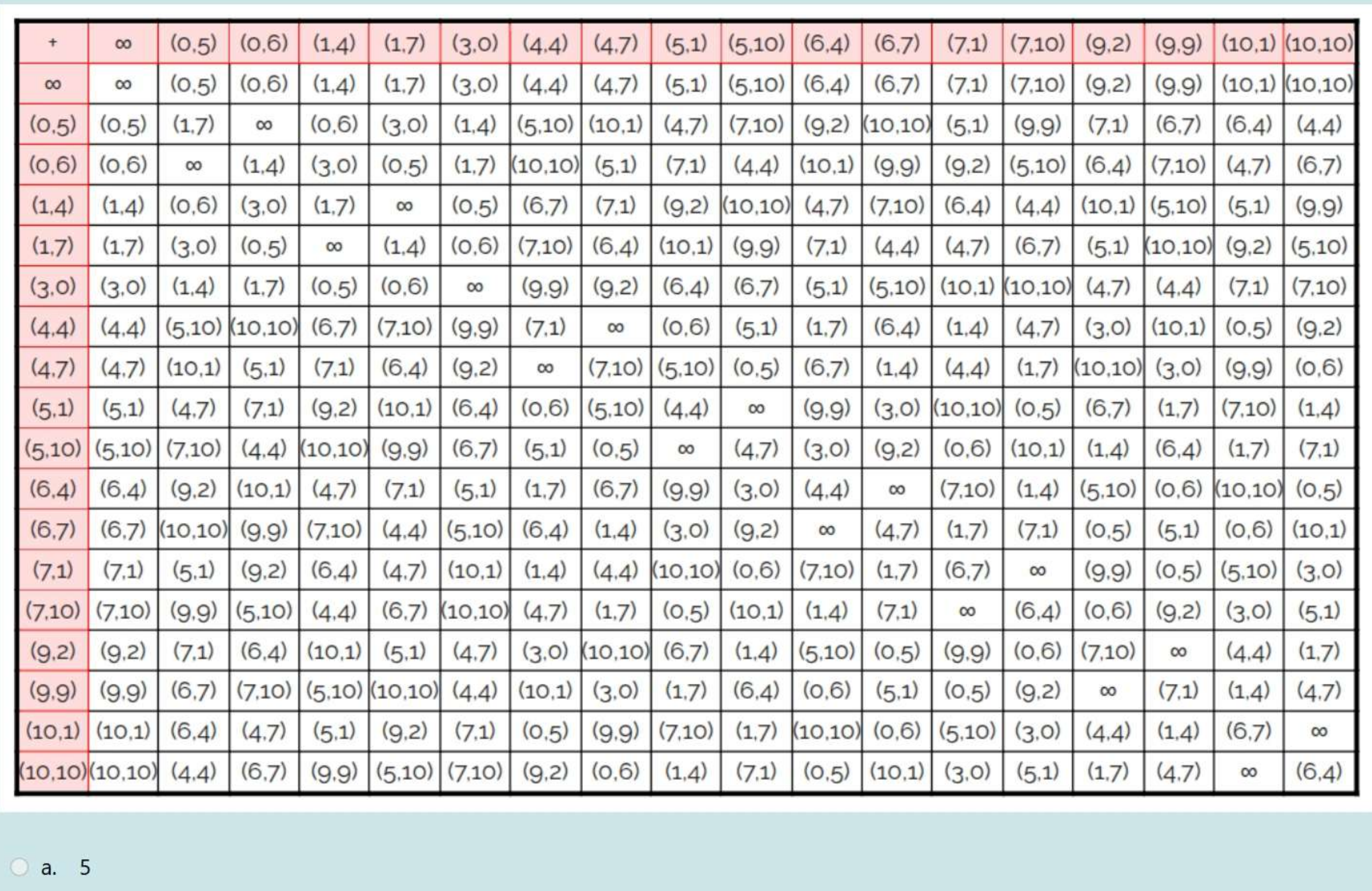
Bob a perdu sa clé privée pour le cryptosystème ElGamal pour la courbe elliptique $y^2 = x^3 + x + 3 \mod 11$ et générateur $G = (5, 1)$. Sa clé publique est $K_b = (7, 1)$. Qiuelle est sa clé privée ?

La tableau d'addition des points de la courbe elliptique est donnée ci-dessous.

===

Bob lost hist ElGamal private key for the elliptic curve $y^2 = x^3 + x + 3 \mod 11$ and generator $G = (5, 1)$. his public key is$K_b = (7, 1)$.
What is his private key?
The addition table of the points of the groupe is given bellow

Alice	Bob
KeyGen: Diffie-Hellman	
Choisir p premier, E et $G \in E(\mathbb{F}_p)$ $\mathscr{M} = E(\mathbb{F}_p)$, $\mathscr{C} = E(\mathbb{F}_p)^2$	
	Choisir $b < \mathrm{Card}\ E(\mathbb{F}_p)$, $K_b = bG$ Clé privée de Bob : $\mathrm{sk} = b$
clé publique: $\mathrm{pk} = (\mathscr{M}, p, E, G, K_b)$	
Chiffrement	
Choisir $a < \mathrm{Card}\ E(\mathbb{F}_p)$ $c_1 = aG$, $c_2 = M + aK_b$ $c = \mathrm{Enc}(m,\ \mathrm{pk}) = (c_1, c_2)$	
Dechiffrement	
	$\mathrm{Dec}(c,\ \mathrm{sk}) = (c_2 - bc_1)$



+	∞	(0,5)	(0,6)	(1,4)	(1,7)	(3,0)	(4,4)	(4,7)	(5,1)	(5,10)	(6,4)	(6,7)	(7,1)	(7,10)	(9,2)	(9,9)	(10,1)	(10,10)
∞	∞	(0,5)	(0,6)	(1,4)	(1,7)	(3,0)	(4,4)	(4,7)	(5,1)	(5,10)	(6,4)	(6,7)	(7,1)	(7,10)	(9,2)	(9,9)	(10,1)	(10,10)
(0,5)	(0,5)	(1,7)	∞	(0,6)	(3,0)	(1,4)	(5,10)	(10,1)	(4,7)	(7,10)	(9,2)	(10,10)	(5,1)	(9,9)	(7,1)	(6,7)	(6,4)	(4,4)
(0,6)	(0,6)	∞	(1,4)	(3,0)	(0,5)	(1,7)	(10,10)	(5,1)	(7,1)	(4,4)	(10,1)	(9,9)	(9,2)	(5,10)	(6,4)	(7,10)	(4,7)	(6,7)
(1,4)	(1,4)	(0,6)	(3,0)	(1,7)	∞	(0,5)	(6,7)	(7,1)	(9,2)	(10,10)	(4,7)	(7,10)	(6,4)	(4,4)	(10,1)	(5,10)	(5,1)	(9,9)
(1,7)	(1,7)	(3,0)	(0,5)	∞	(1,4)	(0,6)	(7,10)	(6,4)	(10,1)	(9,9)	(7,1)	(4,4)	(4,7)	(6,7)	(5,1)	(10,10)	(9,2)	(5,10)
(3,0)	(3,0)	(1,4)	(1,7)	(0,5)	(0,6)	∞	(9,9)	(9,2)	(6,4)	(6,7)	(5,1)	(5,10)	(10,1)	(10,10)	(4,7)	(4,4)	(7,1)	(7,10)
(4,4)	(4,4)	(5,10)	(10,10)	(6,7)	(7,10)	(9,9)	(7,1)	∞	(0,6)	(5,1)	(1,7)	(6,4)	(1,4)	(4,7)	(3,0)	(10,1)	(0,5)	(9,2)
(4,7)	(4,7)	(10,1)	(5,1)	(7,1)	(6,4)	(9,2)	∞	(7,10)	(5,10)	(0,5)	(6,7)	(1,4)	(4,4)	(1,7)	(10,10)	(3,0)	(9,9)	(0,6)
(5,1)	(5,1)	(4,7)	(7,1)	(9,2)	(10,1)	(6,4)	(0,6)	(5,10)	(4,4)	∞	(9,9)	(3,0)	(10,10)	(0,5)	(6,7)	(1,7)	(7,10)	(1,4)
(5,10)	(5,10)	(7,10)	(4,4)	(10,10)	(9,9)	(6,7)	(5,1)	(0,5)	∞	(4,7)	(3,0)	(9,2)	(0,6)	(10,1)	(1,4)	(6,4)	(1,7)	(7,1)
(6,4)	(6,4)	(9,2)	(10,1)	(4,7)	(7,1)	(5,1)	(1,7)	(6,7)	(9,9)	(3,0)	(4,4)	∞	(7,10)	(1,4)	(5,10)	(0,6)	(10,10)	(0,5)
(6,7)	(6,7)	(10,10)	(9,9)	(7,10)	(4,4)	(5,10)	(6,4)	(1,4)	(3,0)	(9,2)	∞	(4,7)	(1,7)	(7,1)	(0,5)	(5,1)	(0,6)	(10,1)
(7,1)	(7,1)	(5,1)	(9,2)	(6,4)	(4,7)	(10,1)	(1,4)	(4,4)	(10,10)	(0,6)	(7,10)	(1,7)	(6,7)	∞	(9,9)	(0,5)	(5,10)	(3,0)
(7,10)	(7,10)	(9,9)	(5,10)	(4,4)	(6,7)	(10,10)	(4,7)	(1,7)	(0,5)	(10,1)	(1,4)	(7,1)	∞	(6,4)	(0,6)	(9,2)	(3,0)	(5,1)
(9,2)	(9,2)	(7,1)	(6,4)	(10,1)	(5,1)	(4,7)	(3,0)	(10,10)	(6,7)	(1,4)	(5,10)	(0,5)	(9,9)	(0,6)	(7,10)	∞	(4,4)	(1,7)
(9,9)	(9,9)	(6,7)	(7,10)	(5,10)	(10,10)	(4,4)	(10,1)	(3,0)	(1,7)	(6,4)	(0,6)	(5,1)	(0,5)	(9,2)	∞	(7,1)	(1,4)	(4,7)
(10,1)	(10,1)	(6,4)	(4,7)	(5,1)	(9,2)	(7,1)	(0,5)	(9,9)	(7,10)	(1,7)	(10,10)	(0,6)	(5,10)	(3,0)	(4,4)	(1,4)	(6,7)	∞
(10,10)	(10,10)	(4,4)	(6,7)	(9,9)	(5,10)	(7,10)	(9,2)	(0,6)	(1,4)	(7,1)	(0,5)	(10,1)	(3,0)	(5,1)	(1,7)	(4,7)	∞	(6,4)

○ a. 5

○ b. 2

● c. 4

○ d. 3

Terminer la relecture