DS8

On s'intéresse dans ce sujet au problème de la *double dépense* de *bitcoins* par un groupe d'individus mal intentionnés.
On rappelle que le bitcoin est une monnaie virtuelle dont l'utilisation pour des transactions est associée à une structure unique appelée *blockchain*, partagée sur le réseau des usagers de cette monnaie et ayant pour but de sécuriser ces transactions.
La modélisation étudiée ne nécessite pas de connaissances particulières sur le *bitcoin* et la *blockchain*.

Partie I - Deux résultats généraux / 40

On démontre dans cette partie deux résultats préliminaires, aux questions ***5.*** et ***6.***. Ces résultats seront utilisés dans la suite du sujet et pourront être admis.

Calcul d'une probabilité

Soient X et Y deux variables aléatoires sur un espace probabilisé, à densité et indépendantes.
On note F_X et F_Y les fonctions de répartition de X et Y.
On suppose que Y est à valeurs positives et possède une densité f_Y dont la restriction à $[0, +\infty[$ est continue sur cet intervalle.
Pour tout $x \in \mathbb{R}_+$, on pose : $H(x) = \mathbb{P}(\,[X \leqslant Y] \cap [Y \leqslant x]\,)$.

1. a) Montrer que H est une fonction croissante sur $\mathbb{R}_+$ qui admet une limite finie en $+\infty$.

- **1 pt : comprendre qu'il faut démontrer** $x \leqslant y \Rightarrow H(x) \leqslant H(y)$
- **1 pt :** $[Y \leqslant x] \subset [Y \leqslant y]$ **(même sans démo)**
- **1 pt :** $\mathbb{P}\big(\,[X \leqslant Y] \cap [Y \leqslant x]\,\big) \leqslant \mathbb{P}\big(\,[X \leqslant Y] \cap [Y \leqslant y]\,\big)$
- **1 pt : par théorème de la limite monotone,** H **admet une limite finie en** $+\infty$**.**

b) En utilisant la suite $\big(H(n)\big)_{n\in\mathbb{N}}$, démontrer : $\lim\limits_{x\to+\infty} H(x) = \mathbb{P}(\,[X \leqslant Y]\,)$.
Que vaut $H(0)$?

- **3 pts :** $\Omega = \bigcup\limits_{k=0}^{+\infty} [Y \leqslant k]$
  - × **1 pt : l'affirmer**
  - × **1 pt :** $\Omega \subset \bigcup\limits_{k=0}^{+\infty} [Y \leqslant k]$
  - × **1 pt :** $\Omega \supset \bigcup\limits_{k=0}^{+\infty} [Y \leqslant k]$ **(affirmer que c'est un événement suffit)**
- **1 pt :** $\mathbb{P}\left(\bigcup\limits_{k=0}^{+\infty}\Big([X \leqslant Y] \cap [Y \leqslant k]\Big)\right) = \lim\limits_{N\to+\infty} \mathbb{P}\left(\bigcup\limits_{k=0}^{N}\Big([X \leqslant Y] \cap [Y \leqslant k]\Big)\right)$ **par propriété de la limite monotone**
- **1 pt :** $\bigcup\limits_{k=0}^{N}\Big([X \leqslant Y] \cap [Y \leqslant k]\Big) = [X \leqslant Y] \cap [Y \leqslant N]$ **car** $\big([X \leqslant Y] \cap [Y \leqslant k]\big)_{k\in\mathbb{N}}$ **est une suite croissante d'événements (l'affirmer suffit)**
- **1 pt :** $[Y < 0] = \varnothing$ **(**$[Y \leqslant 0] = \varnothing$ **accepté) car** Y **à valeurs positives**
- **0 pt :** $H(0) = 0$

2. Soit (u, v) un couple de réels positifs tels que : $u < v$.

a) Montrer : $H(v) - H(u) = \mathbb{P}(\,[X \leqslant Y] \cap [u < Y \leqslant v]\,)$. Puis :

$$F_X(u)\,\frac{F_Y(v) - F_Y(u)}{v-u} \;\leqslant\; \frac{H(v) - H(u)}{v-u} \;\leqslant\; F_X(v)\,\frac{F_Y(v) - F_Y(u)}{v-u}$$

- **3 pts :** $[Y \leqslant v] \;=\; [Y \leqslant u] \;\cup\; [u < Y \leqslant v]$
  (ou $[X \leqslant Y] \cap [Y \leqslant v] \;=\; [X \leqslant Y] \cap [Y \leqslant u] \;\cup\; [X \leqslant Y] \cap [u < Y \leqslant v]$**)**
  - × **1 pt : l'affirmer**
  - × **1 pt :** $[Y \leqslant v] \;\subset\; [Y \leqslant u] \;\cup\; [u < Y \leqslant v]$
  - × **1 pt :** $[Y \leqslant v] \;\supset\; [Y \leqslant u] \;\cup\; [u < Y \leqslant v]$
- **0 pt : en déduire** $H(v) = H(u) + \mathbb{P}\big(\,[X \leqslant Y] \cap [u < Y \leqslant v]\,\big)$
- **2 pts :** $[X \leqslant Y] \cap [u < Y \leqslant v] \;\subset\; [X \leqslant v] \cap [u < Y \leqslant v]$
  - × **1 pt : l'affirmer**
  - × **1 pt : le démontrer (démo avec les ω attendue mais on accepte aussi démo avec les mains)**
- **1 pt :** $\mathbb{P}\big(\,[X \leqslant Y] \cap [u < Y \leqslant v]\,\big) \;\leqslant\; \mathbb{P}\big(\,[X \leqslant v] \cap [u < Y \leqslant v]\,\big)$ **par croissance et $\mathbb{P}$ puis conclusion par indépendance**
- **1 pt : par un raisonnement similaire** $F_X(u)\,\dfrac{F_Y(v) - F_Y(u)}{v-u} \;\leqslant\; \dfrac{H(v) - H(u)}{v-u}$

b) En déduire que pour tout $x \in \mathbb{R}_+$, H est dérivable en x et : $H'(x) = F_X(x)\,f_Y(x)$.

- **1 pt :** F_X **et** F_Y **sont de classe** $\mathcal{C}^1$ **sur** $\mathbb{R}_+$ **car** f_X **et** f_Y **y sont continues**
- **3 pts :** H **admet une dérivée à droite en** x_0
  - × **1 pt : l'affirmer**
  - × **1 pt :** $\displaystyle\lim_{\substack{x \to x_0 \\ x > x_0}} \frac{F_Y(x) - F_Y(x_0)}{x - x_0} = F_Y'(x_0) = f_Y(x_0)$
  - × **1 pt : conclusion par théorème d'encadrement**
- **1 pt :** H **admet une dérivée à gauche en** x_0 **et conclusion** H **est dérivable en** x_0

Seulement 2/4 si l'aspect droite / gauche n'a pas été perçu.

c) En conclure que pour tout x réel positif : $H(x) = \displaystyle\int_0^x F_X(t)\,f_Y(t)\,dt$.

- **1 pt :** H **est la primitive sur** $\mathbb{R}_+$ **et qui s'annule en** 0 **de la fonction** h

3. Démontrer : $\mathbb{P}(\,[X \leqslant Y]\,) = \displaystyle\int_0^{+\infty} F_X(t)\,f_Y(t)\,dt$.

- **1 pt : la fonction** $x \mapsto \displaystyle\int_0^x F_X(t)\,f_Y(t)\,dt$ **admet une limite finie en** $+\infty$ $\big(= \mathbb{P}\big(\,[X \leqslant Y]\,\big)\big)$ **d'après *1.***
- **1 pt :** $\mathbb{P}\big(\,[X \leqslant Y]\,\big) = \displaystyle\lim_{x \to +\infty} H(x) = \lim_{x \to +\infty} \int_0^x F_X(t)\,f_Y(t)\,dt$

4. En utilisant la fonction $K : x \mapsto \mathbb{P}(\,[X < Y] \cap [Y \leqslant x]\,)$, on montrerait de même et nous l'admettrons :

$$\mathbb{P}(\,[X < Y]\,) \;=\; \int_0^{+\infty} F_X(t)\, f_Y(t)\; dt \;=\; \mathbb{P}(\,[X \leqslant Y]\,)$$

Que peut-on en déduire pour $\mathbb{P}(\,[X = Y]\,)$?

- **1 pt :** $[X \leqslant Y] \;=\; [X < Y] \cup [X = Y]$
- **1 pt :** $\mathbb{P}\big([X = Y]\big) = \mathbb{P}\big([X \leqslant Y]\big) - \mathbb{P}\big([X < Y]\big) = 0$

5. *Application aux lois exponentielles*
On suppose que U et V sont deux variables aléatoires indépendantes suivant des lois exponentielles de paramètres respectifs λ et μ, réels strictement positifs.
Soit θ un réel positif ou nul.

a) Déterminer la fonction de répartition de la variable aléatoire $X = U - \theta$.

- **1 pt :** $X(\Omega) = [-\theta, +\infty[$
- **1 pt : si** $x < -\theta$**,** $F_X(x) = \mathbb{P}\big([X \leqslant x]\big) = \mathbb{P}(\varnothing) = 0$
- **1 pt : si** $x \geqslant \theta$**,** $F_X(x) = 1 - \exp\big(-\lambda\,(x + \theta)\big)$

b) En déduire que pour tout $\theta \geqslant 0$:

$$\mathbb{P}(\,[U - \theta \leqslant V]\,) \;=\; 1 - \frac{\mu}{\lambda + \mu}\, \mathrm{e}^{-\lambda\,\theta}$$

- **1 pt : la v.a.r.** $X = U - \theta$ **est une v.a.r. à densité en tant que transformée affine d'une v.a.r. à densité**
- **2 pts : vérifier qu'on est dans le cadre d'application du résultat de l'énoncé**
  - × **1 pt :** X **et** V **sont indépendantes par le lemme des coalitions**
  - × **1 pt :** $f_V|_{[0,+\infty[} : t \mapsto \mu\ \mathbf{e}^{-\mu\,t}$ **est une fonction continue sur** $[0, +\infty[$

  (on peut lâcher 1 pt / 2 pour une tentative honnête de vérification des hypothèses)
- **2 pts :** $\mathbb{P}\big([U - \theta \leqslant V]\big) = 1 - \dfrac{\mu}{\lambda + \mu}\ \mathbf{e}^{-\lambda\,\theta}$
  - × **1 pt : linéarité de l'intégration, les intégrales en présence étant convergentes**
  - × **1 pt : calcul, notamment** $\displaystyle\int_0^{+\infty} \mu\ \mathbf{e}^{-\mu\,t}\ dt = 1$ **et** $\displaystyle\int_0^{+\infty} (\lambda + \mu)\ \mathbf{e}^{-(\lambda+\mu)\,t}\ dt = 1$ **comme moments d'ordre** 0

Inégalité de Boole

6. On considère $(B_k)_{k\in\mathbb{N}^*}$ une famille d'événements d'un espace probabilisé.

a) Montrer par récurrence sur $n \in \mathbb{N}^*$: $\mathbb{P}\left(\bigcup_{k=1}^{n} B_k\right) \leqslant \sum_{k=1}^{n} \mathbb{P}(B_k)$.

- **1 pt : initialisation** $\mathbb{P}\,(B_1) \;\leqslant\; \mathbb{P}\,(B_1)$
- **1 pt :** $\mathbb{P}\left(\bigcup_{k=1}^{n+1} B_k\right) = \mathbb{P}\left(\left(\bigcup_{k=1}^{n} B_k\right) \;\cup\; B_{n+1}\right)$
- **1 pt : formule du crible + hypothèse de récurrence + majoration**

b) On suppose que la série $\sum_{k\geqslant 1} \mathbb{P}(B_k)$ converge. Démontrer :

$$\mathbb{P}\left(\bigcup_{k=1}^{+\infty} B_k\right) \;\leqslant\; \sum_{k=1}^{+\infty} \mathbb{P}(B_k)$$

- **1 pt : par propriété de la limite monotone** $\mathbb{P}\left(\bigcup_{k=1}^{+\infty} B_k\right) \;=\; \lim_{N\to+\infty} \mathbb{P}\left(\bigcup_{k=1}^{N} B_k\right)$
- **1 pt : conclusion par passage à la limite dans l'inégalité précédente**

Partie II - Une compétition entre deux groupes /65

7. ***a)*** Que représente la variable aléatoire $\sum_{k=1}^{n} X_k$?

- **1 pt :** $\sum_{k=1}^{n} X_k$ **reprénsent le temps passé par le groupe** A **pour résoudre les** n **premiers problèmes** P_1**,** $\ldots$**,** P_n

b) On suppose que $X_1 = 5$, $X_2 = 2$, $X_3 = 3$, $X_4 = 2$, $Y_1 = 2$, $Y_2 = 2$, $Y_3 = 4$ et $Y_4 = 2$.
Déterminer U_1, $\ldots$, U_7.
Peut-on aussi en déduire la valeur de U_8 ?

- **1 pt :** $U_1(\omega) = 0$, $U_2(\omega) = 0$, $U_3(\omega) = 1$, $U_4(\omega) = 1$, $U_5(\omega) = 0$
- **1 pt :** $U_6(\omega) = 1$ **(car en cas d'ex aequo c'est le problème résolu par le groupe** A **qui est ajouté à la liste en** 1^{er}**),** $U_7(\omega) = 0$
- **1 pt : on ne peut pas conclure pour** $U_8(\omega)$ **(si** $Y_5(\omega) = 1$**, alors** $U_8(\omega) = 0$**; mais si** $Y_5(\omega) = 4$**, alors** $U_8(\omega) = 1$**)**

c) Compléter le script **Scilab** suivant pour qu'il simule le jeu et, pour n, p donnés, affiche la liste des valeurs U_1, U_2, $\ldots$, U_n :

- **4 pts : 1 pt par ligne**

```
9          if sommeX == mini then
10             U(k) = 1
```

```
13         sommeY = sommeY + grand(1, 1, 'exp', 1/q)
```

```
17     disp(U)
```

d) Quelle(s) instruction(s) faut-il ajouter pour afficher la valeur de S_n ?

- **1 pt :** `disp(sum(U))`

8. *Loi de* U_n
Dans cette question, on démontre par récurrence sur $n \geqslant 1$: $\mathbb{P}([U_n = 1]) = p$.

a) Démontrer : $\mathbb{P}([U_1 = 1]) = \mathbb{P}([X_1 \leqslant Y_1]) = p$.

- **1 pt : explication** $[U_1 = 1] = [X_1 \leqslant Y_1]$
  0 à la moindre confusion d'objets
- **1 pt :** X_1 **et** Y_1 **vérifient les hypothèses de la question *5.* (avec** $\lambda = p$ **et** $\mu = q$**)**
- **1 pt : application de *5.b)* avec** $\theta = 0$

b) (i) Démontrer, pour tout réel $x < 0$: $\mathbb{P}_{[U_1=1]}([Y_1 - X_1 \leqslant x]) = 0$.

- **1 pt : on a bien** $\mathbb{P}([U_1 = 1]) = p \neq 0$
- **1 pt : par définition d'une probabilité conditionnelle** $\mathbb{P}_{[U_1=1]}([Y_1 - X_1 \leqslant x]) = \dfrac{\mathbb{P}([U_1 = 1] \cap [Y_1 - X_1 \leqslant x])}{\mathbb{P}([U_1 = 1])}$
- **1 pt : en utilisant la qst précédente** $\mathbb{P}([U_1 = 1] \cap [Y_1 - X_1 \leqslant x]) = \mathbb{P}([X_1 \leqslant Y_1] \cap [Y_1 - X_1 \leqslant x]) = \mathbb{P}(\varnothing) = 0$

(ii) Soit x un réel positif ou nul.
Établir : $\mathbb{P}_{[U_1=1]}([Y_1 - X_1 \leqslant x]) = \dfrac{1}{p}\,\mathbb{P}([X_1 \leqslant Y_1 \leqslant X_1 + x])$,
puis calculer $\mathbb{P}_{[U_1=1]}([Y_1 - X_1 \leqslant x])$.

- **1 pt :** $\mathbb{P}_{[U_1=1]}([Y_1 - X_1 \leqslant x]) = \dfrac{1}{p}\,\mathbb{P}([X_1 \leqslant Y_1 \leqslant X_1 + x])$
- **1 pt : par FPT sur le SCE** $\big([Y_1 \leqslant X_1 + x], [Y_1 > X_1 + x]\big)$, $\mathbb{P}([X_1 \leqslant Y_1 \leqslant X_1 + x]) = \mathbb{P}([X_1 \leqslant Y_1]) - \mathbb{P}([Y_1 > X_1 + x]) = p - \big(1 - \mathbb{P}([Y_1 - x \leqslant X_1])\big)$
- **1 pt : d'après *5.b)* avec** $\theta = x \geqslant 0$, $\lambda = q$ **et** $\mu = p$, $\mathbb{P}([X_1 \leqslant Y_1 \leqslant X_1 + x]) = p - 1 + \left(1 - \dfrac{p}{p+q}\,\mathbf{e}^{-q\,x}\right) = p\,(1 - \mathbf{e}^{-q\,x})$
- **1 pt :** $\mathbb{P}_{[U_1=1]}([Y_1 - X_1 \leqslant x]) = 1 - \mathbf{e}^{-q\,x}$

c) On peut interpréter ce résultat en disant que la *loi conditionnelle de* $Y_1 - X_1$ *sachant* $[U_1 = 1]$ est une loi exponentielle. Quelle est son paramètre ?
Par analogie, quelle est la loi conditionnelle de $X_1 - Y_1$ sachant $[U_1 = 0]$? (on n'attend pas une démonstration précise mais un argument de bon sens pour justifier le résultat proposé).

- **1 pt : d'après *8.b)*,** $\mathbb{P}_{[U_1=1]}([Y_1 - X_1 \leqslant x]) = \begin{cases} 0 & \text{si } x < 0 \\ 1 - \mathbf{e}^{-q\,x} & \text{si } x \geqslant 0 \end{cases}$
  Donc la loi de $Y_1 - X_1$ **conditionnellement à** $[U_1 = 1]$ **est la loi** $\mathcal{E}(q)$
- **1 pt : en intervertissant les rôles de** X_1 **et** Y_1**, on en déduit que la loi de** $X_1 - Y_1$ **conditionnellement à** $[U_1 = 0]$ **est la loi** $\mathcal{E}(p)$

d) On suppose que $n \in \mathbb{N}^*$ et $\mathbb{P}([U_n = 1]) = p$.
Déduire de cette hypothèse et de la question précédente :

$$\mathbb{P}_{[U_1=1]}([U_{n+1} = 1]) = p \quad \text{et} \quad \mathbb{P}_{[U_1=0]}([U_{n+1} = 1]) = p$$

- **1 pt : si** $[U_1 = 1]$ **est réalisé, on peut considérer la résolution de** P_1 **comme nouvelle origine des temps, et le problème sur** $(X_1, X_2, \ldots)$ **et** $(Y_1, Y_2, \ldots)$ **se ramène à un problème sur** $(X_2, X_3, \ldots)$ **et** $(Y_1 - X_1, Y_2, Y_3, \ldots)$
- **1 pt : par lemme des coalitions,** U_1**,** X_2**,** X_3**, …,** Y_2**,** Y_3**, … son indépendantes**
- **1 pt : par indépendance, pour tout** $i \geqslant 2$**, la loi de** X_i **(resp.** Y_i**) conditionnellement à** $[U_1 = 1]$ **est la loi** $\mathcal{E}(p)$ **(resp.** $\mathcal{E}(q)$**)**
- **1 pt : d'après *8.c)*, la loi de** $Y_1 - X_1$ **conditionnellement à** $[U_1 = 1]$ **est la loi** $\mathcal{E}(q)$
- **1 pt : on déduit des 4 points précédents,** $\mathbb{P}[U_1 = 1]([U_{n+1} = 1]) = \mathbb{P}([U_n = 1]) = p$ **(par hypothèse de récurrence)**
- **1 pt : de même,** $\mathbb{P}_{[U_1=0]}([U_{n+1} = 1]) = \mathbb{P}([U_n = 1]) = p$

e) Conclure.

- **1 pt : par FPT sur le SCE** $\big([U_1 = 0], [U_1 = 1]\big)$, $\mathbb{P}([U_{n+1} = 1]) = p$
- **1 pt : faire le lien avec la structure de raisonnement par récurrence**

9. On montrerait aussi par récurrence, et nous l'admettrons, que pour tout $n \in \mathbb{N}^*$, les variables aléatoires U_1, …, U_n sont mutuellement indépendantes.
En déduire la loi de S_n.

- **1 pt : par stabilité des lois binomiales** $S_n \hookrightarrow \mathcal{B}(n, p)$
  0 si les hypothèses de la stabilité des lois binomiales ne sont pas citées

Soit $r \in \mathbb{N}$, on s'intéresse, dans les questions qui suivent, à la probabilité a_r de l'événement :

$$A_r \quad : \quad \begin{array}{l} \text{« il existe un } n \geqslant r \text{ tel que, lorsque } n \text{ problèmes} \\ \text{en tout ont été résolus, le groupe } A \text{ en a résolu} \\ r \text{ de plus que le groupe } B \text{ »} \end{array}$$

10. a) Justifier : $a_0 = 1$.

- **1 pt :** A_0 **est réalisé si et seulement s'il existe** $n \geqslant 0$ **tel que, lorsque** n **problèmes en tout ont été résolus, le groupe** A **en a résolu autant que** B**. Ceci est toujours réalisé (un entier satisfaisant toujours la condition est** $n = 0$**)**
- **1 pt :** $a_0 = \mathbb{P}(A_0) = \mathbb{P}(\Omega) = 1$

b) Démontrer, pour tout $r \geqslant 1$:

$$\mathbb{P}_{[U_1=1]}(A_r) = \mathbb{P}(A_{r-1}) \quad \text{et} \quad \mathbb{P}_{[U_1=0]}(A_r) = \mathbb{P}(A_{r+1})$$

- **1 pt : si** $[U_1 = 1]$ **est réalisé, alors le groupe** A **résout** P_1 **(avant que le groupe** B **n'est résolu** Q_1**). Il a donc** 1 **problème d'avance sur** B **à l'instant** t **de résolution de** P_1
- **1 pt : dans ce cas, il existe un instant** n **tel que le groupe** A **ait** r **problèmes d'avance sur le groupe** B **si et seulement si il existe un instant** $m = n - t$ **tel que le groupe** A **ait** $r - 1$ **problèmes d'avance sur le groupe** B**. D'où** $\mathbb{P}_{[U_1=1]}(A_r) = \mathbb{P}(A_{r-1})$
- **1 pt : de même, si** $[U_1 = 0]$ **est réalisé, il existe un instant** n **tel que le groupe** A **ait** r **problèmes d'avance sur le groupe** B **si et seulement si il existe un instant** $m = n - t$ **tel que le groupe** A **ait** $r + 1$ **problèmes d'avance sur le groupe** B**. D'où** $\mathbb{P}_{[U_1=0]}(A_r) = \mathbb{P}(A_{r+1})$

c) En déduire, pour tout $r \geqslant 1$: $a_{r+1} = \dfrac{1}{q}\, a_r - \dfrac{p}{q}\, a_{r-1}$.

- **1 pt : par FPT sur le SCE** $\big([U_1 = 0], [U_1 = 1] \big)$**,** $\forall r \geqslant 1$**,** $a_{r+1} = \dfrac{1}{q}\, a_r - \dfrac{p}{q}\, a_{r-1}$

d) En remarquant que $1 - 4pq = (1 - 2p)^2$, donner une expression de a_r en fonction de p, q, r et de deux constantes que l'on introduira.

- **1 pt : d'après la qst précédente,** $\forall r \in \mathbb{R}$**,** $a_{r+2} = \dfrac{1}{q}\, a_{r+1} - \dfrac{p}{q}\, a_r$**. (**$(a_r)$ **est donc une suite récurrente linéaire d'ordre** 2**)**
- **1 pt : les racines de son équation caractéristiques sont** $x_1 = 1$ **et** $x_2 = \dfrac{p}{q}$ **(distinctes si et seulement si** $p \neq \dfrac{1}{2}$
- **1 pt : si** $p \neq \dfrac{1}{2}$**, il existe** $(\alpha, \beta) \in \mathbb{R}^2$ **tel que :** $\forall r \in \mathbb{N}$**,** $a_r = \alpha + \beta \left(\dfrac{p}{q}\right)^n$
- **1 pt : si** $p = \dfrac{1}{2}$**, il existe** $(\alpha', \beta') \in \mathbb{R}^2$ **tel que :** $\forall r \in \mathbb{N}$**,** $a_r = \alpha' + \beta' r$

11. Le cas $p \geqslant \dfrac{1}{2}$.

Montrer que, dans les cas $p = \dfrac{1}{2}$ et $p > \dfrac{1}{2}$, la suite $(a_r)_{r\in\mathbb{N}}$ est constante et égale à 1.

- **3 pts : cas $p > \dfrac{1}{2}$**
  - × **2 pts : démonstration par l'absurde de $\beta = 0$**
    - **1 pt : comme $p > \dfrac{1}{2}$, $\dfrac{p}{q} > 1$**
    - **1 pt : alors $\lim\limits_{r\to+\infty} a_r = +\infty$. Absurde car $\forall r \in \mathbb{N}$, $a_r \in [0,1]$**
  - × **1 pt : comme $a_0 = 1$ d'après *10.a)*, alors $\alpha = 1$**
- **2 pts : cas $p = \dfrac{1}{2}$**
  - × **1 pt : comme $a_0 = 1$, $\alpha' = 1$**
  - × **1 pt : toujours en raisonnant par l'absurde (arguments similaires au cas précédent), $\beta' = 0$**

12. Le cas $p < \dfrac{1}{2}$.

a) Soit k un entier naturel.

(i) Établir : $A_{2k} = \bigcup\limits_{i\geqslant k} [S_{2i} = i + k]$.

- **2 pts : $\bigcup\limits_{i\geqslant k} [S_{2i} = i + k] \subset A_{2k}$**
  - × **1 pt : si l'événement $[S_{2i} = i + k]$ est réalisé alors, au moment où $2i$ problèmes ont été résolus, $i + k$ l'ont été par le groupe A, et donc $i - k$ par le groupe B. Le groupe A a donc résolu $2k$ problèmes de plus que le groupe B.**
  - × **1 pt : ainsi, pour tout $i \geqslant k$, $[S_{2i} = k] \subset A_{2k}$. D'où l'inclusion voulue**
- **2 pts : $A_{2k} \subset \bigcup\limits_{i\geqslant k} [S_{2i} = i + k]$**
  - × **1 pt : si l'événement A_{2k} est réalisé, on note $n \geqslant 2k$ le nombre de problèmes résolus à l'instant où le groupe A en résolus $2k$ de plus que le groupe B. À cet instant n, le groupe A a résolu $S_n(\omega)$ problèmes et B en a résolu $S_n(\omega) - 2k$**
  - × **1 pt : on en déduit, $S_n(\omega) + (S_n(\omega) - 2k) = n$. D'où : $n = 2\,(S_n(\omega) - k)$. En posant $i = S_n(\omega) - k$, on a bien que l'événement $[S_{2i} = i + k]$ est réalisé. Donc : $A_{2k} \subset [S_{2i} = i + k]$. D'où l'inclusion voulue**

(ii) Montrer que pour tout $i \geqslant k$, on a : $\mathbb{P}(\,[S_{2i} = i + k]\,) = \dbinom{2i}{i+k} p^{i+k}\, q^{i-k}$.

- **1 pt : d'après la question *9.*, $S_{2i} \hookrightarrow \mathcal{B}\,(2i, p)$**

(iii) Après avoir donné la valeur de la somme $\sum\limits_{j=0}^{2i} \dbinom{2i}{j}$, démontrer :

$$\forall i \geqslant k,\ \binom{2i}{i+k} \leqslant 4^i$$

- **1 pt : par formule du binôme de Newton, $\sum\limits_{j=0}^{2i} \dbinom{2i}{j} = 2^{2i} = 4^i$**
- **1 pt : comme $i \leqslant k$, alors $i + k \in [\![0, 2i]\!]$. On peut donc découper la somme**
- **1 pt : $4^i = \sum\limits_{k=0}^{2i} \dbinom{2i}{j} = \sum\limits_{k=0}^{i+k-1} \dbinom{2i}{j} + \dbinom{2i}{i+k} + \sum\limits_{j=i+k+1}^{2i} \dbinom{2i}{j}$**
- **1 pt : comme $\sum\limits_{k=0}^{i+k-1} \dbinom{2i}{j} \geqslant 0$ et $\sum\limits_{j=i+k+1}^{2i} \dbinom{2i}{j} \geqslant 0$, on conclut**

(iv) En déduire l'inégalité :

$$\sum_{i=k}^{+\infty} \mathbb{P}(\,[S_{2i} = k+i]\,) \;\leqslant\; \left(\frac{p}{q}\right)^k \;\frac{(4pq)^k}{1-4pq}$$

- **1 pt : d'après les 2 qsts précédentes,** $\mathbb{P}([S_{2i} = i+k]) \leqslant 4^i\, p^{i+k}\, q^{i-k} = \left(\frac{p}{q}\right)^k\, (4pq)^i$
- **1 pt :** $\sum (4pq)^i$ **est une série géométrique de raison** $4pq \in\,]-1,1[$ **(car** $p < \frac{1}{2}$**). Elle est donc convergente**
- **1 pt : on somme les inégalités précédentes, car les séries en présence sont convergentes. On obtient :** $\sum_{i=k}^{+\infty} \mathbb{P}([S_{2i} = i+k]) \leqslant \left(\frac{p}{q}\right)^k \sum_{i=k}^{+\infty} (4pq)^i$
- **1 pt :** $\sum_{i=k}^{+\infty} (4pq)^i = \left(\frac{p}{q}\right)^k \sum_{j=0}^{+\infty} (4pq)^{i+k} = \left(\frac{p}{q}\right)^k \;\frac{(4pq)^k}{1-4pq}$

b) Montrer en utilisant l'inégalité de Boole (voir question ***6.***) que si $p < \frac{1}{2}$, alors : $\lim\limits_{k\to+\infty} a_{2k} = 0$.

- **1 pt : d'après** ***6.***, $\mathbb{P}\left(\bigcup\limits_{i\geqslant k} [S_{2i} = i+k]\right) \leqslant \sum\limits_{i=k}^{+\infty} \mathbb{P}([S_{2i} = i+k])$
- **1 pt : d'après la qst précédente, on obtient** $0 \leqslant \mathbb{P}(A_{2k}) \leqslant \left(\frac{p}{q}\right)^k \;\frac{(4pq)^k}{1-4pq}$
- **1 pt : comme** $p < \frac{1}{2}$**, alors** $\frac{p}{q} \in\,]0,1[$ **et** $4pq \in\,]0,1[$**, d'où** $\lim\limits_{k\to+\infty} \left(\frac{p}{q}\right)^k \;\frac{(4pq)^k}{1-4pq} = 0$
- **1 pt : on conclut par théorème d'encadrement**

c) Conclure en utilisant la question ***10.d)***, que si $p < \frac{1}{2}$, alors :

$$\forall r \in \mathbb{N},\; a_r = \left(\frac{p}{q}\right)^r$$

- **1 pt : d'après** ***10.d)***, $\forall r \in \mathbb{N},\; a_r = \alpha + \beta \left(\frac{p}{q}\right)^r$**. D'où :** $\lim\limits_{k\to+\infty} a_{2k} = \alpha$
- **1 pt : par unicité de la limité et la qst précédente,** $\alpha = 0$
- **1 pt : d'après** ***10.a)***, $a_0 = 1$**. D'où :** $\beta = 1$

On a ainsi établi dans les questions ***11.*** et ***12.*** :

$$\forall r \in \mathbb{N}, \quad a_r = \begin{cases} \left(\frac{p}{q}\right)^r & \text{si } p < \frac{1}{2} \\ 1 & \text{si } p \geqslant \frac{1}{2} \end{cases}$$

Ce résultat pourra être admis et utilisé dans la suite du sujet.

Partie III - La *blockchain* et la stratégie de la *double dépense* /40

13. On s'intéresse tout d'abord à la loi de la variable aléatoire T_n égale au nombre de problèmes résolus par le groupe A lorsque l'on place Q_n dans la liste des problèmes résolus.

a) Démontrer, pour tout $k \in \mathbb{N}$: $[T_n = k] = [S_{n+k-1} = k] \cap [U_{n+k} = 0]$.

- **3 pts :**
  - × **1 pt :** $\omega \in [S_{n+k-1} = k] \cap [U_{n+k} = 0]$ $\Leftrightarrow$ **dans les** $n+k-1$ **premiers problèmes résolus,** k **l'ont été par le groupe** A **et le** $(n+k)^{\text{ème}}$ **problème a été résolu par le groupe** B
  - × **1 pt :** $\Leftrightarrow$ **sur les** $n+k-1$ **premiers problèmes,** k **ont été résolus par le groupe** A **et** Q_n **est le** $(n+k)^{\text{ème}}$ **problème résolu**
  - × **1 pt :** $\Leftrightarrow$ **lorsque** Q_n **est résolu par le groupe** B**,** k **problèmes ont été résolus par le groupe** $A \Leftrightarrow \omega \in [T_n = k]$

b) En déduire : $\mathbb{P}(\,[T_n = k]\,) = \binom{n+k-1}{k} p^k\, q^n$.

- **1 pt :** $\mathbb{P}([T_n = k]) = \mathbb{P}([S_{n+k-1} = k]) \times \mathbb{P}([U_{n+k} = 0])$ **car, par lemme des coalitions** $S_{n+k-1} = \sum_{i=1}^{n+k-1} U_i$ **indépendante de** U_{n+k}
- **1 pt :** $\mathbb{P}([S_{n+k-1} = k]) \times \mathbb{P}([U_{n+k} = 0]) = \binom{n+k-1}{k} p^k\, q^{(n+k-1)-k} \times q$ **(d'après les questions *8.* et *9.*)**

14. ***a)*** En utilisant la formule des probabilités totales, établir :

$$\mathbb{P}(G_n) \;=\; \mathbb{P}(\,[T_n \geqslant n+1]\,) + \sum_{k=0}^{n} \mathbb{P}(\,[T_n = k]\,)\, a_{n+1-k}$$

- **1 pt : FPT sur le SCE** $\big(\,[T_n = k]\,\big)_{k\in\mathbb{N}}$
- **1 pt :** $\mathbb{P}(G_n) = \sum_{k=0}^{+\infty} \mathbb{P}([T_n = k])\, \mathbb{P}_{[T_n=k]}(G_n)$ **(car :** $\forall k \in \mathbb{N}$**,** $\mathbb{P}([T_n = k]) = 0$**)**
- **1 pt : si** $k \in [\![0, n]\!]$**,** $\mathbb{P}_{[T_n=k]}(G_n) = \mathbb{P}(A_{n-k+1}) = a_{n-k+1}$
- **1 pt : si** $k \in [\![n+1, +\infty[\![$**,** $\mathbb{P}_{[T_n=k]}(G_n) = 1$
- **1 pt :** $\sum_{k=n+1}^{+\infty} \mathbb{P}([T_n = k]) = \mathbb{P}([T_n \geqslant n+1])$

b) Dans le cas où $p \geqslant \dfrac{1}{2}$, en déduire : $\mathbb{P}(G_n) = 1$.

- **1 pt : pour tout** $k \in [\![0, n]\!]$**, comme** $n-k+1 \in \mathbb{N}$**, d'après le résultat établi en fin de Partie II :** $a_{n+1-k} = 1$
- **1 pt :** $\mathbb{P}(G_n) = \sum_{k=0}^{n} \mathbb{P}([T_n = k]) + \mathbb{P}([T_n \geqslant n+1]) = 1$ **car** $\big(\,[T_n = k]\,\big)_{k\in\mathbb{N}}$ **forme un SCE**

c) De même lorsque $p < \dfrac{1}{2}$, démontrer :

$$\mathbb{P}(G_n) \;=\; 1 - \sum_{k=0}^{n} \binom{n+k-1}{k} \left(p^k\, q^n - p^{n+1}\, q^{k-1}\right)$$

- **1 pt : comme** T_n **à valeurs entières,** $\mathbb{P}([T_n \geqslant n+1]) = 1 - \mathbb{P}([T_n \leqslant n]) = 1 - \sum_{k=0}^{n} \mathbb{P}([T_n = k])$

- **1 pt : d'après *14.a)* et le résultat de fin de Partie II ($n+1-k \in \mathbb{N}$),** $\mathbb{P}(G_n) = 1 - \sum_{k=0}^{n} \mathbb{P}([T_n = k]) \left(1 - \left(\frac{p}{q}\right)^{n+1-k}\right)$
- **1 pt : d'après *13.b)*,** $\mathbb{P}(G_n) = 1 - \sum_{k=0}^{n} \binom{n+k-1}{k} p^k q^n \left(1 - \frac{p^{n+1-k}}{q^{n+1-k}}\right)$

15. *Une meilleure expression de* $\mathbb{P}(G_n)$ *lorsque* $p < \frac{1}{2}$

Pour tout $x \in [0,1]$ et $n \in \mathbb{N}^*$, on pose :

$$u_n(x) \;=\; (1-x)^n \sum_{k=0}^{n} \binom{n+k-1}{k} x^k$$

a) Vérifier que pour tout $n \in \mathbb{N}^*$: $\mathbb{P}(G_n) = 1 - u_n(p) + \frac{p}{q}\, u_n(q)$.

- **1 pt : en utilisant *14.c)***

b) Pour tout $x \in [0,1]$ et $n \in \mathbb{N}^*$, établir la relation :

$$u_{n+1}(x) \;=\; u_n(x) + (1-x)^n\, x^{n+1} \left(\binom{2n}{n+1} - \binom{2n+1}{n+1} x\right)$$

- **1 pt :** $u_{n+1}(x) = (1-x)^n \sum_{k=0}^{n+1} \binom{n+k}{k} x^k - x\,(1-x)^n \sum_{k=0}^{n} \binom{n+k}{k} x^k - x^{n+1}\,(1-x)^n \binom{2n+1}{n+1} x$
- **1 pt :** $x\,(1-x)^n \sum_{k=0}^{n} \binom{n+k}{k} x^k = (1-x)^n \sum_{k=1}^{n+1} \binom{n+k-1}{k-1} x^k$
- **1 pt : par triangle de Pascal,** $(1-x)^n \sum_{k=0}^{n+1} \binom{n+k}{k} x^k - (1-x)^n \sum_{k=1}^{n+1} \binom{n+k-1}{k-1} x^k = (1-x)^n \sum_{k=0}^{n+1} \binom{n+k-1}{k} x^k$
- **1 pt :** $u_{n+1}(x) = (1-x)^n \sum_{k=0}^{n+1} \binom{n+k-1}{k} x^k - x^{n+1}\,(1-x)^n \binom{2n+1}{n+1} x = u_n(x) + x^{n+1}\,(1-x)^n \left(\binom{2n}{n+1} - \binom{2n+1}{n+1} x\right)$

c) En déduire, pour tout $n \in \mathbb{N}^*$:

$$\mathbb{P}(G_{n+1}) \;=\; \mathbb{P}(G_n) - \left(1 - \frac{p}{q}\right)\, (pq)^{n+1} \binom{2n+1}{n+1}$$

- **1 pt :** $\mathbb{P}(G_{n+1}) = 1 - u_{n+1}(p) + \frac{p}{q}\, u_{n+1}(q)$ **d'après *15.a)***
- **1 pt :** $= 1 - \left(u_n(p) + p^{n+1} q^n \left(\binom{2n}{n+1} - \binom{2n+1}{n+1} p\right)\right) + \frac{p}{q} \left(u_n(q) + q^{n+1} p^n \left(\binom{2n}{n+1} - \binom{2n+1}{n+1} q\right)\right.$ **d'après la question précédente**
- **1 pt : d'après *15.a)*,** $= \mathbb{P}(G_n) - p^{n+1} q^n \binom{2n+1}{n+1}(q-p) = \mathbb{P}(G_n) - \left(1 - \frac{p}{q}\right)\, (pq)^{n+1} \binom{2n+1}{n+1}$

d) Montrer par récurrence, pour tout $n \in \mathbb{N}^*$:

$$\mathbb{P}(G_n) \;=\; \frac{p}{q} - \left(1 - \frac{p}{q}\right) \sum_{k=1}^{n} \binom{2k-1}{k} (pq)^k$$

- **2 pts : initialisation**
  - × **1 pt :** $\mathbb{P}(G_1) = p + \dfrac{p^2}{q} - p\,q + p^2$ **et** $\dfrac{p}{q} - \left(1 - \dfrac{p}{q}\right) \displaystyle\sum_{k=1}^{1} \binom{2k-1}{k} (p\,q)^k = \dfrac{p}{q} - p\,q + p^2$
  - × **1 pt : vérification égalité (utilisation de** $p + q = 1$**)**
- **3 pts : hérédité**
  - × **1 pt : d'après *15.c)*,** $\mathbb{P}(G_{n+1}) = \mathbb{P}(G_n) - \left(1 - \dfrac{p}{q}\right) (p\,q)^{n+1} \binom{2n+1}{n+1}$
  - × **1 pt :** $= \left(\dfrac{p}{q} - \left(1 - \dfrac{p}{q}\right) \displaystyle\sum_{k=1}^{n} \binom{2k-1}{k} (p\,q)^k\right) - \left(1 - \dfrac{p}{q}\right) (p\,q)^{n+1} \binom{2n+1}{n+1}$ **par hypothèse de récurrence**
  - × **1 pt : fin du calcul**

16. *Application à la sécurisation des transactions*

Connaissant $p < \dfrac{1}{2}$, on cherche à limiter le risque que la stratégie mise en place par le groupe de mineurs A réussisse.

a) Après avoir établi la formule $\binom{n}{k} = \dfrac{n}{k} \binom{n-1}{k-1}$ lorsque $k \in [\![1, n]\!]$, écrire une fonction **Scilab** qui calcule les coefficients binomiaux.

- **2 pts :** $\forall k \in [\![1, n]\!]$, $\binom{n}{k} = \dfrac{n}{k} \binom{n-1}{k-1}$ **(peu importe la méthode : calcul direct ou dénombrement)**
- **4 pts :**
  - × **1 pt : structure de fonction**
  - × **1 pt : initialisation**
  - × **2 pts : structure itérative**

```
function c = CoeffBin(k, n)
    c = 1
    for i = 1:k
        c = c * (n - i + 1) / i
    end
endfunction
```

b) Écrire un script **Scilab** qui détermine n_p, le plus petit entier n tel que $\mathbb{P}(G_n) \leqslant \varepsilon$ pour $p < \dfrac{1}{2}$ et $\varepsilon > 0$ saisis au clavier par l'utilisateur.

- **6 pts**
  - × **1 pt : les** 2 `input`
  - × **1 pt : initialisation de** `n` **et** `ProbGn`
  - × **1 pt : structure itérative** `while` **(avec bonne condition)**
  - × **1 pt : mise à jour** `ProbGn`
  - × **1 pt : mise à jour** `n`
  - × **1 pt :** `disp(n)`

```
p = input(' Entrez la valeur de p : ')
eps = input(' Entrez la valeur de epsilon : ')
q = 1 - p
n = 1
ProbGn = p/q - (1 - p/q) * p * q
while ProbGn > eps
    ProbGn = ProbGn - (1 - p/q) * (p * q)^(n+1) * CoeffBin(n + 1, 2 * n + 1)
    n = n + 1
end
disp(n)
```