Alae KHIDOUR 24203 avec:

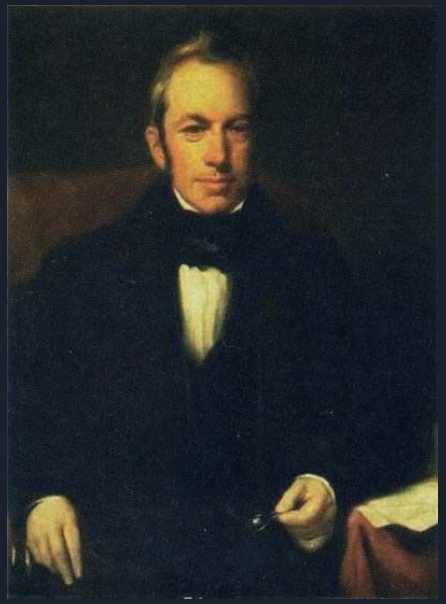
Erwan DZIK 7606
Damien LE VASSEUR 18003

Génération de nombre aléatoire à partir d'un phénomène chaotique

Plan

Introduction

- Nécessité de la génération de nombre aléatoires
- Des générateurs existants mais vulnérables
- Évaluation de cette vulnérabilité par des tests statistiques
- Génération à partir d'un phénomène chaotique
- Objectif: Lier phénomène chaotique et générateur pseudo-aléatoire
- Choix du phénomène chaotique : Mouvement Brownien



Robert Brown
(1773-1858)

Peinture de Henry William Pickersgill:https://fr.wikipedia.org/wiki/Robert_Brown_(botaniste)

Problématique:

Dans quelle mesure un phénomène chaotique peut il être un bon générateur aléatoire ?

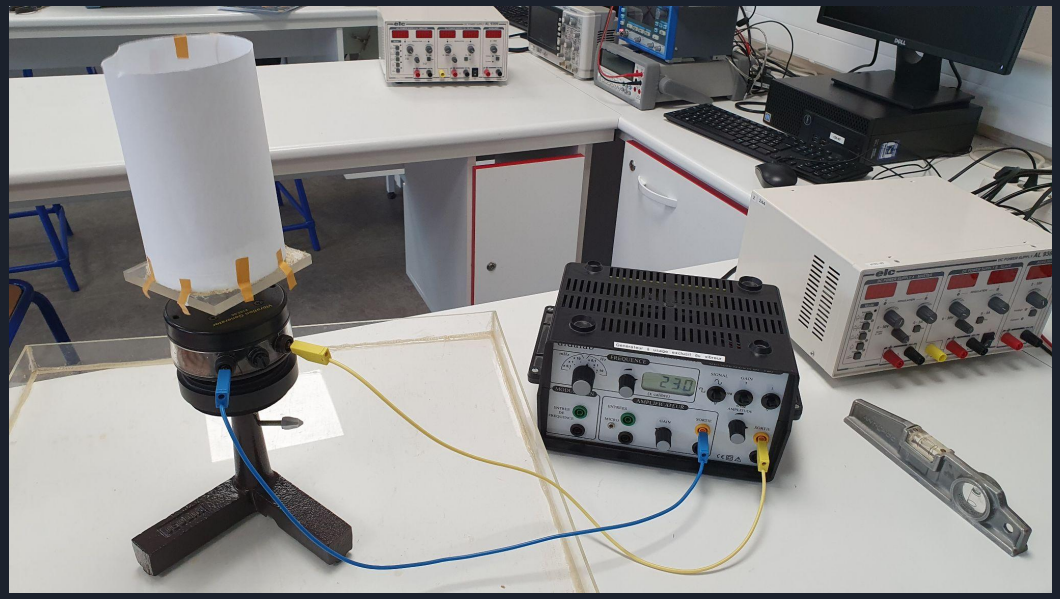
L’Expérience : Mouvement Brownien

Définition

- Le mouvement est irrégulier et imprévisible.
- La direction d’une particule change de façon erratique, et ce, quelque soit l'échelle d'observation.
- Le caractère erratique du mouvement est d'autant plus prononcé que la particule est petite.
- Le mouvement ne s'arrête jamais et est non borné.
- Déplacement moyen nul.

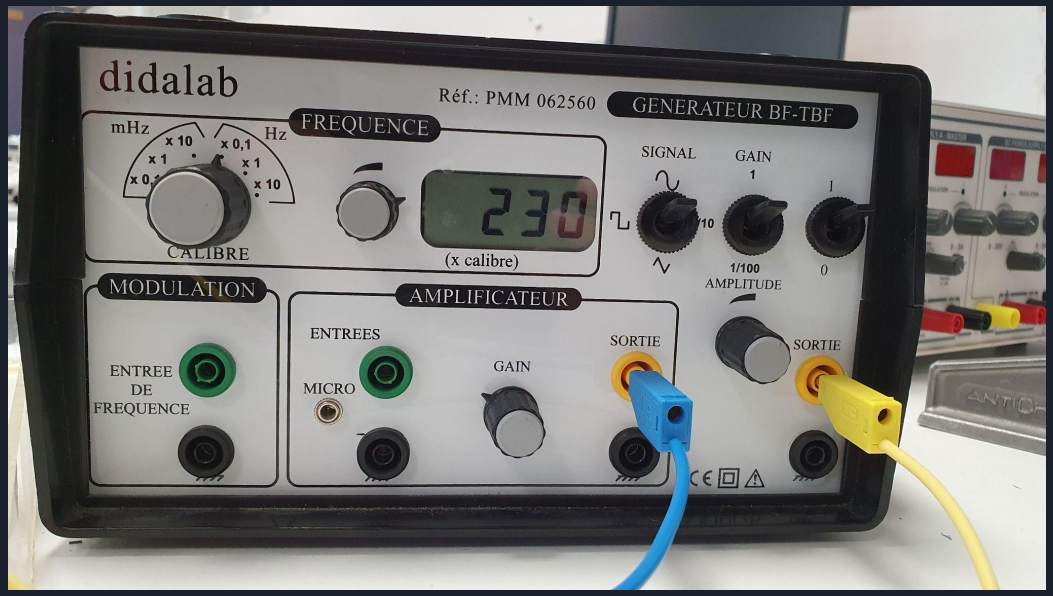
L’Expérience : Mouvement Brownien

Dispositif



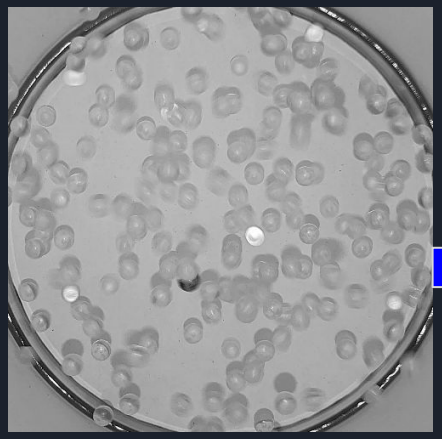
L’Expérience : Mouvement Brownien

Dispositif



L'Expérience : Mouvement Brownien

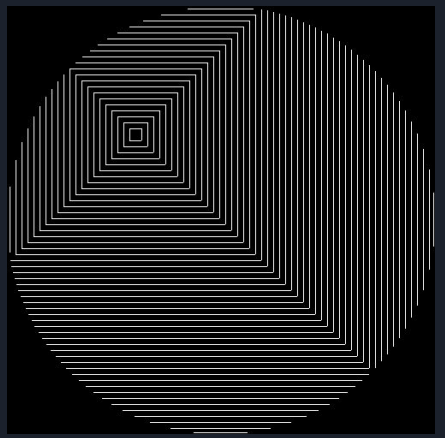
Extraction des données



- Traitement de l'image puis extraction
- Quelques chiffres:
  - 55 min de vidéo
  - 175 610 frames dont 133 969 exploitables
  - 5 090 822 chiffres générés

Ci dessus le traitement de l'image.

Ci contre le parcours pour la recherche de la bille.



L’Expérience : Mouvement Brownien

Extraction des données

X	Y
4.4171737660581472 66e-01	7.2033631079558257 12e-01
2.4643045903885679 73e-01	7.5357450132132726 94e-01
1.7682747994071650 33e-01	7.9721163182910004 25e-01
2.1894197788107069 76e-01	9.2001923385157879 93e-01

→ 417203464535768972189200...

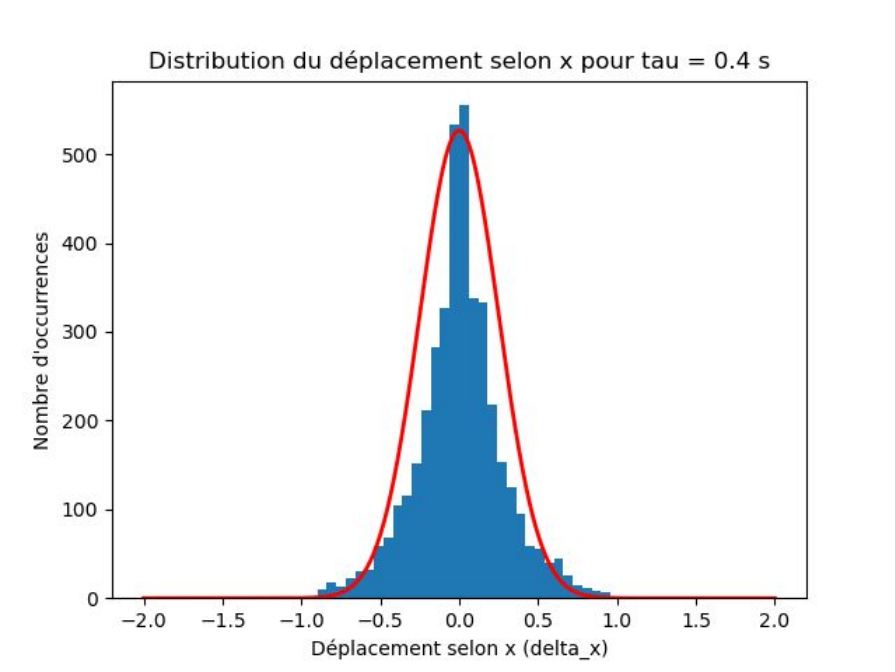
Etude statistique : Quelques propriétés

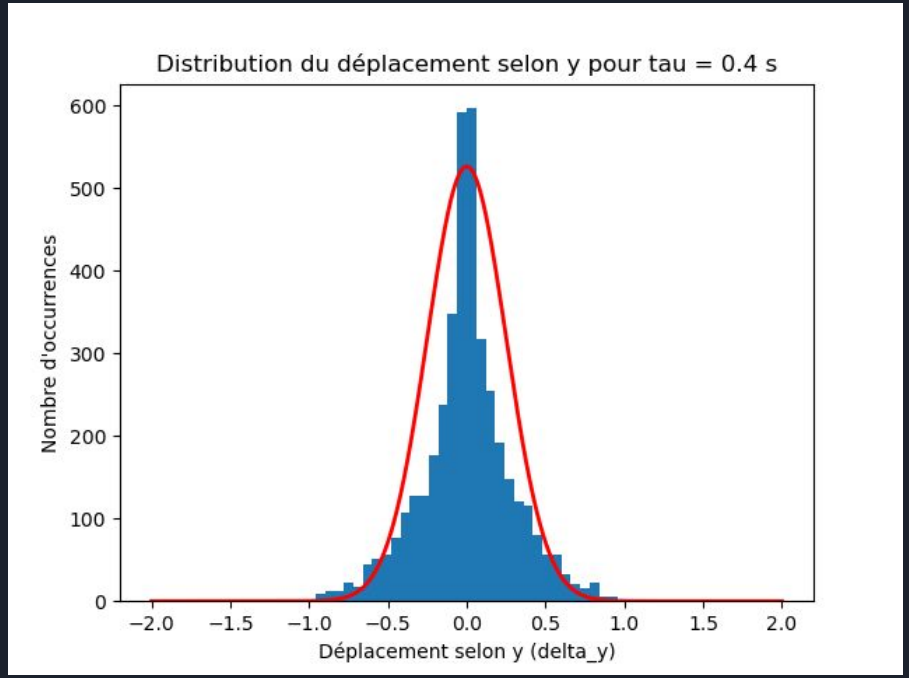
Répartition des chiffres quasi-uniforme (pour 5 090 822 chiffres généré)					
chiffre	0	1	2	3	4
	509226 (10.003%)	502846 (9.878%)	503921 (9.899%)	508556 (9.990%)	508721 (9.992%)
chiffre	5	6	7	8	9
	508582 (9.991%)	513633 (10.089%)	514109 (10.098%)	510635 (10.031%)	510593 (10.029%)

L’Expérience : Mouvement Brownien

Vérification du mouvement brownien

Distribution gaussienne du déplacement



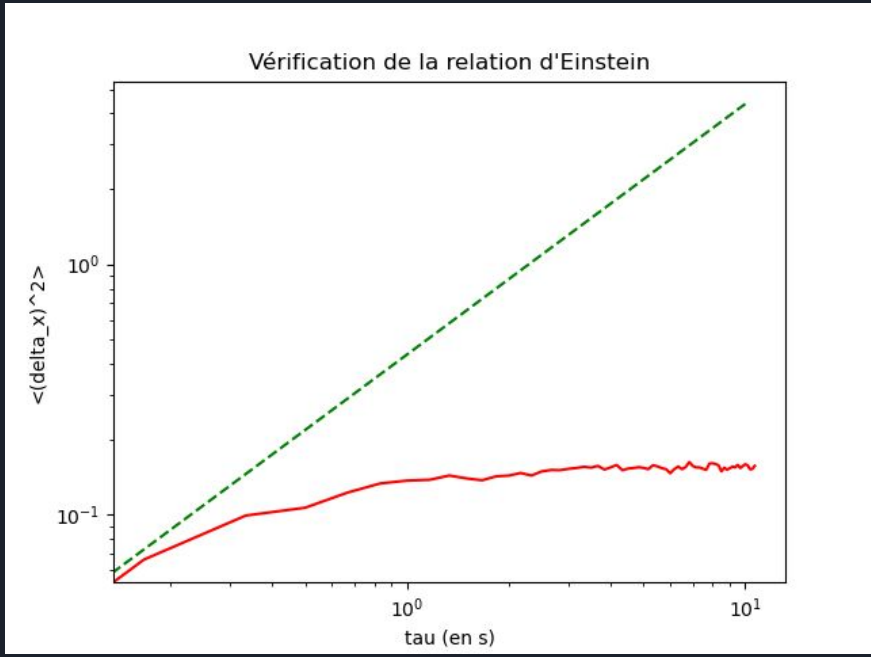


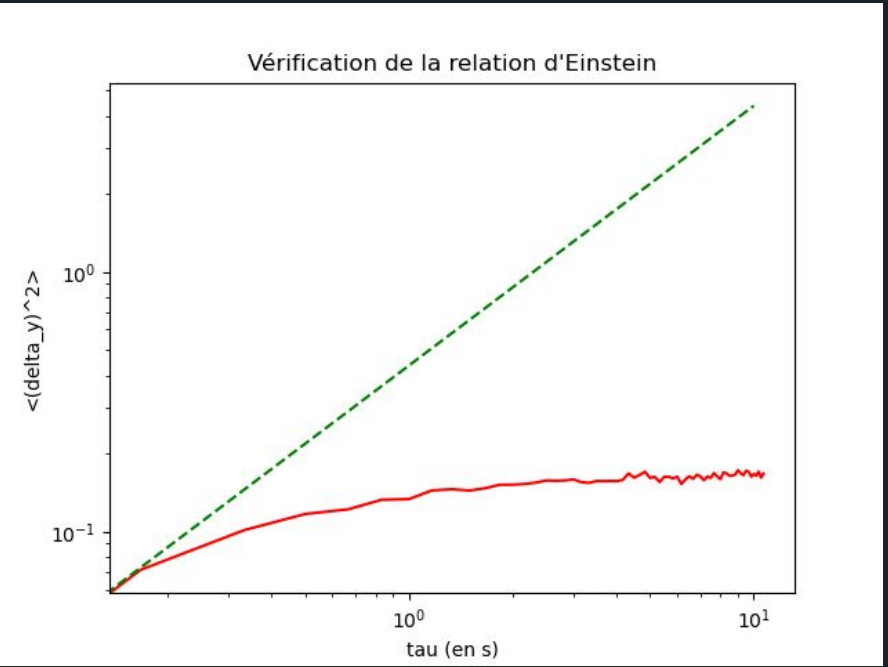
L'Expérience : Mouvement Brownien

Vérification du mouvement brownien

Relation D'Einstein (1905):

$$\overline{(\Delta x)^2} \propto \tau$$





Etude statistique: Le test du X^2 d'adéquation

-Permet de vérifier l'adéquation d'une distribution empirique à une distribution théorique.
-La valeur du X^2 est calculé ainsi:

$$\chi^2 = \sum_{i=1}^{n} \frac{(O_i - E_i)^2}{E_i}$$

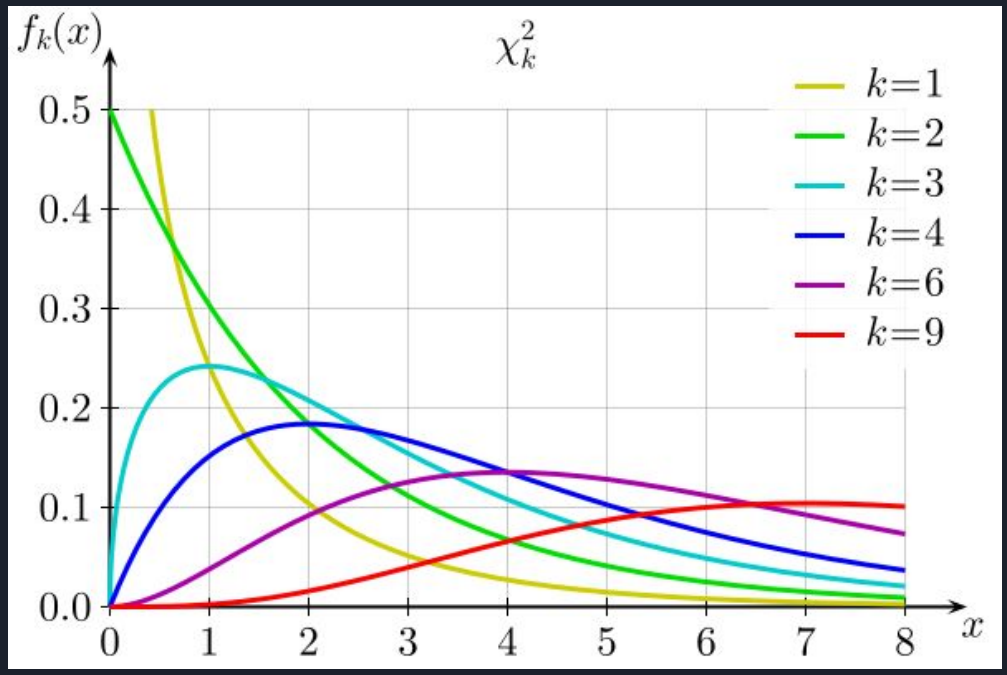
Oi: Fréquences observées
Ei: Fréquences théoriques

Etude statistique: Le test du χ^2 d'adéquation

Principe du Test:

-Hypothèse nulle: "Les valeurs obtenues empiriquement suivent la loi donnée"

-On calcule la valeur du χ^2 et on note le degré k de liberté de l'expérience.



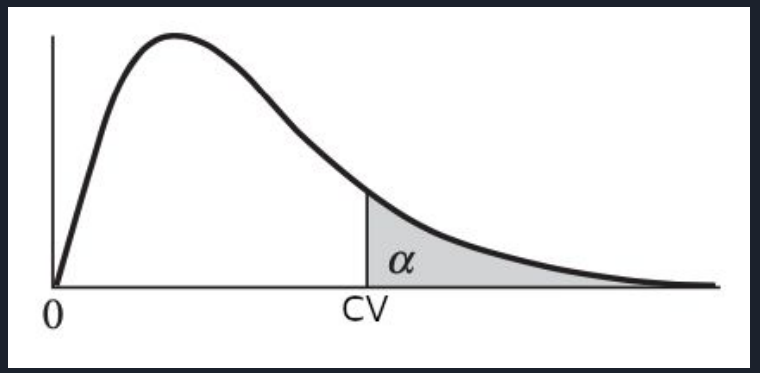
Loi du χ^2 :https://fr.wikipedia.org/wiki/Loi_du_%CF%87%C2%B2

Etude statistique: Le test du X^2 d'adéquation

- On considère CV la valeur critique telle que l'aire sous la courbe vaut α (Usuellement α=0.01 ou α=0.05)

-Pour chaque valeur de α et de k il existe des tables qui donnent la valeur de CV selon la loi du χ^2.

-Si χ^2 > CV, et si n est suffisamment grand, alors l'hypothèse nulle est à rejeter avec une probabilité d'erreur d'au plus α.



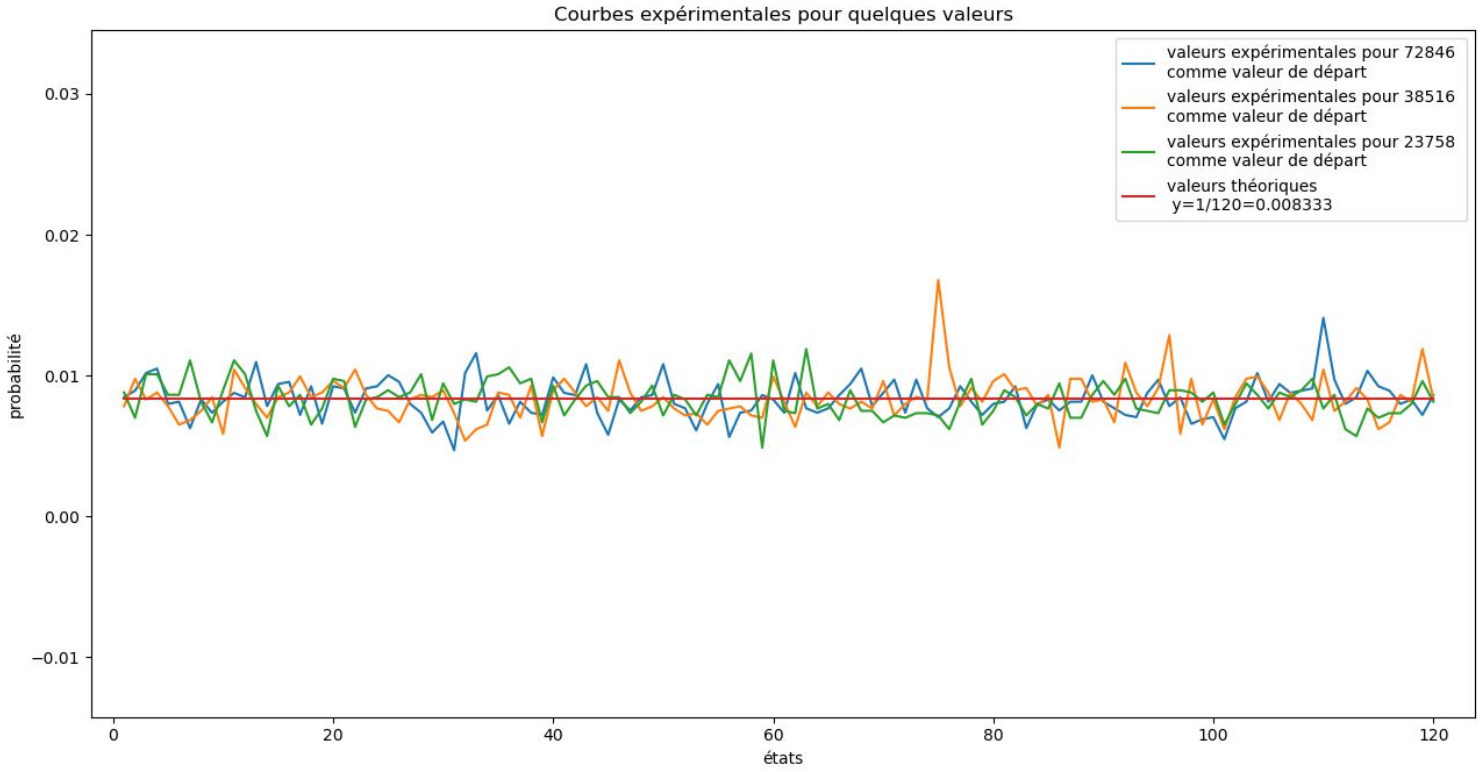
Courbe:https://statsandr.com/blog/chi-square-test-of-independence-by-hand_files/Screenshot%202020-01-28%20at%2000.56.28.png

Test OPERM5

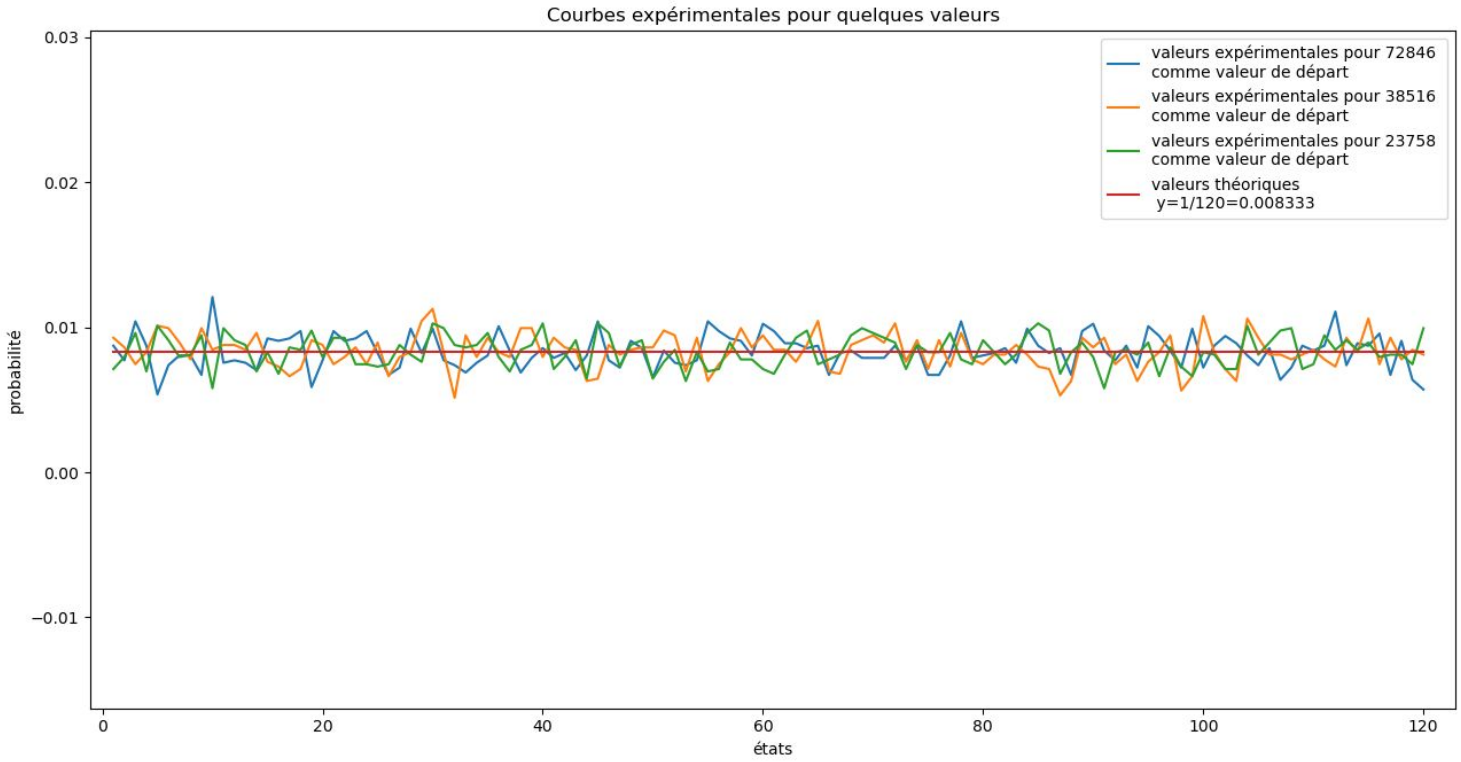
Principe du test:

1) 5 chiffres
2) Au plus 120 arrangements
3) Tableau occurrence des arrangements
4) La théorie prédit que les différents arrangements doivent être équitablement réparti et donc la probabilité d'apparition d'un des états doit suivre une loi uniforme de paramètre (1/nombre d'états).
5) Test du χ^2
6)Finalement nous répétons ce même procédé plusieurs fois pour différentes valeurs de départs et nous effectuons une moyenne des valeurs de χ^2.

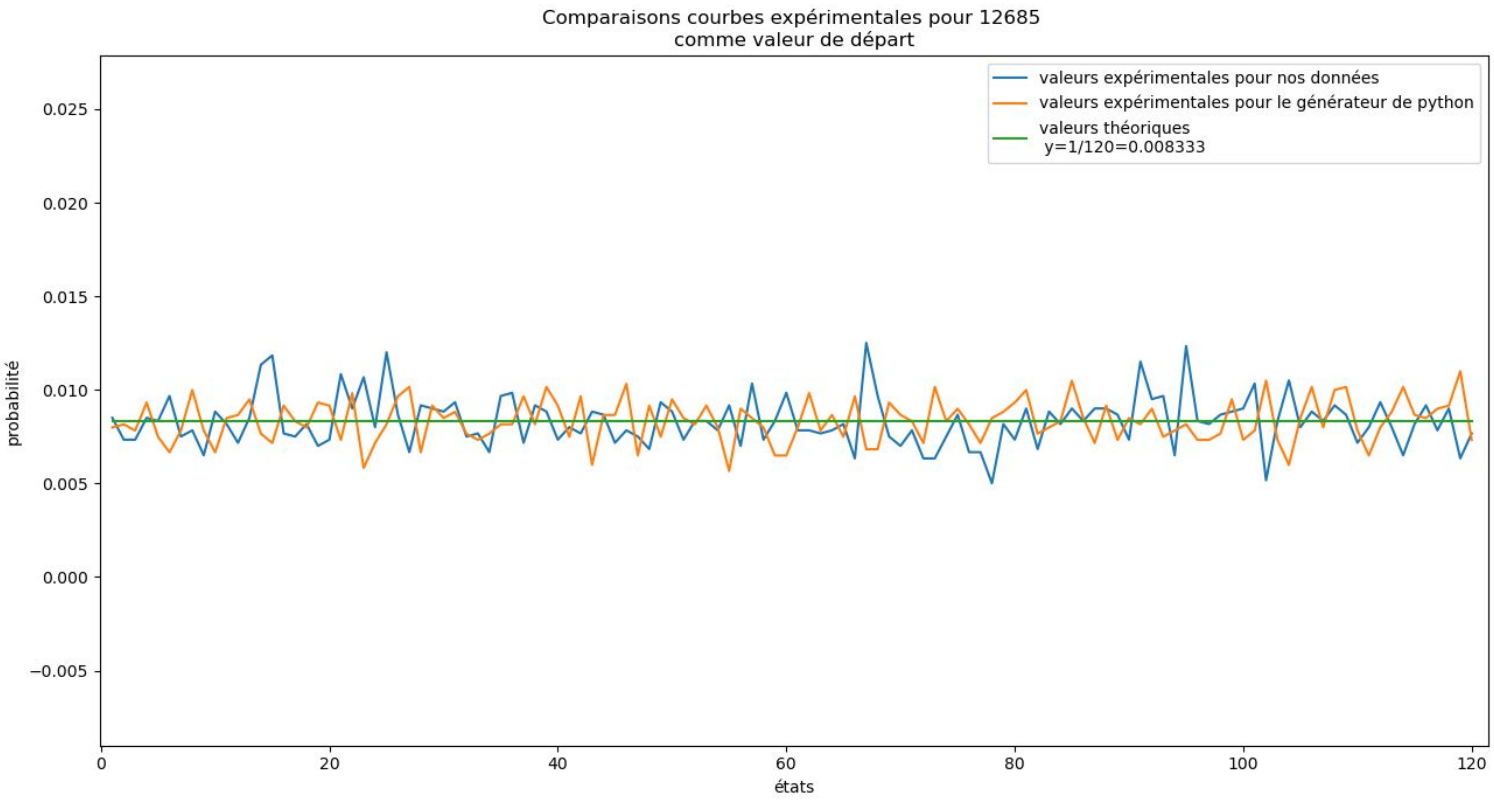
Test OPERM5


Courbes expérimentales pour quelques valeurs
valeurs expérimentales pour 72846 comme valeur de départ
valeurs expérimentales pour 38516 comme valeur de départ
valeurs expérimentales pour 23758 comme valeur de départ
valeurs théoriques y=1/120=0.008333
probabilité
0.03
0.02
0.01
0.00
−0.01
0
20
40
60
80
100
120
états

Test OPERM5
Courbe pour Python



Test OPERM5


Comparaisons courbes expérimentales pour 12685
comme valeur de départ
valeurs expérimentales pour nos données
valeurs expérimentales pour le générateur de python
valeurs théoriques
y=1/120=0.008333
probabilité
0.025
0.020
0.015
0.010
0.005
0.000
−0.005
0
20
40
60
80
100
120
états

Test OPERM5

-Le degré k de liberté de l'expérience pour un nombre de départ composé de 5 chiffres différents deux à deux est 120-1=119.

-La table du χ^2 donne CV= 157.80 pour α=0.01 et CV= 145.46 pour α=0.05

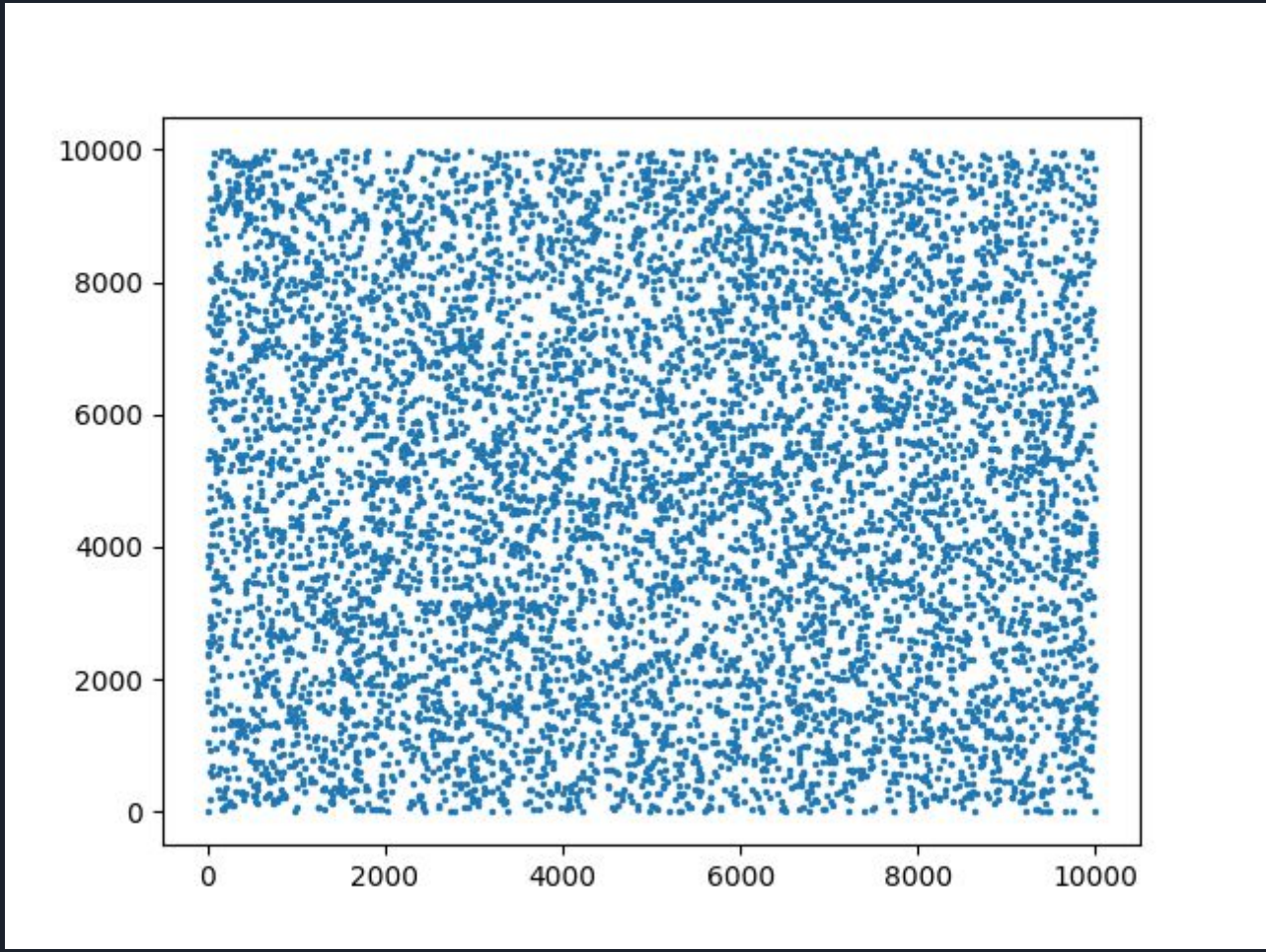
-Test effectué pour 50 valeurs de départ différentes, la moyenne donne: 132.646

-On en déduit que nos valeur passent le test puisque l'hypothèse nulle n'est pas rejetée par le test du χ^2.

Etude Statistique : Minimum Distance test

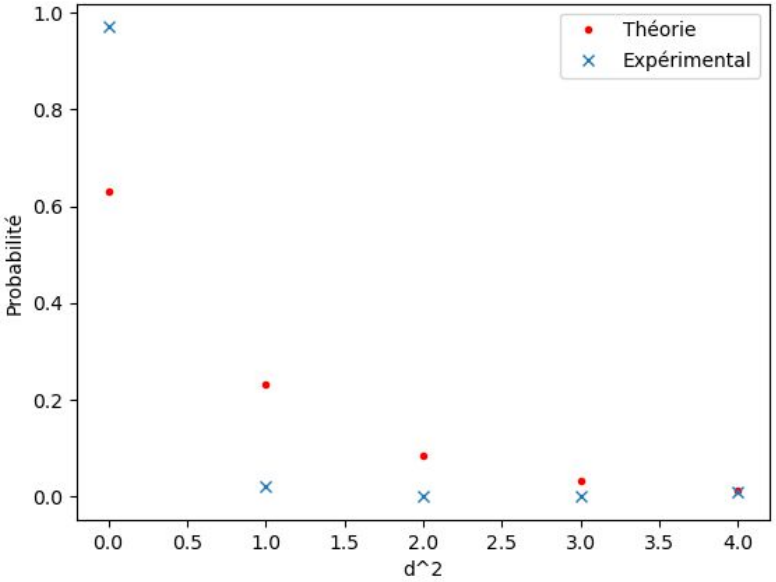
- 8000 points choisis aléatoirement dans un carré de 10000 par 10000
- d distance minimale
- On réitère 100 fois
- d^2 suit presque une loi exponentielle d'espérance 0.995
- Test du χ^2

Etude Statistique : Minimum Distance test

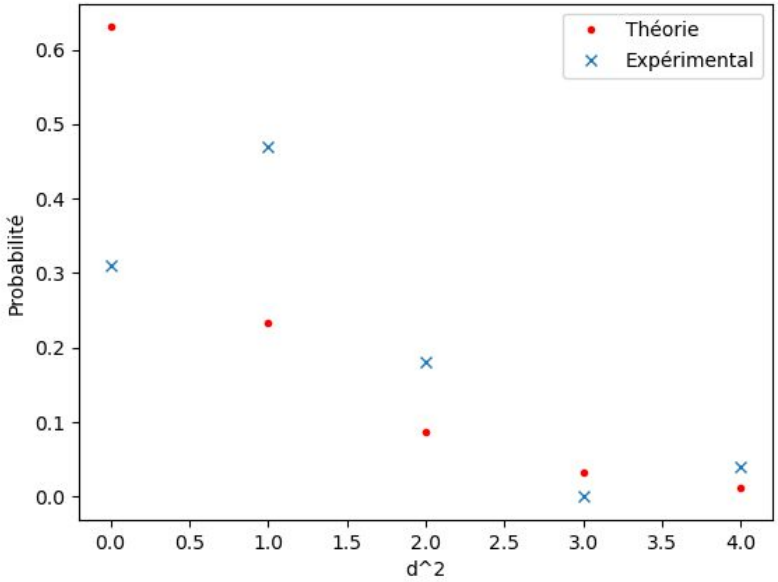


Etude Statistique : Minimum Distance test

Nos valeurs



Python



Etude Statistique : Minimum Distance test

Occurrence de d^2

d^2	0	1	2	3	4
Expérience	97	2	0	0	1
Python	31	47	18	0	4
Théorie	63.02	23.30	8.61	3.18	1.17

$$100 \times \int_{k}^{k+1} 0{,}995 e^{0{,}995t}\, dt$$

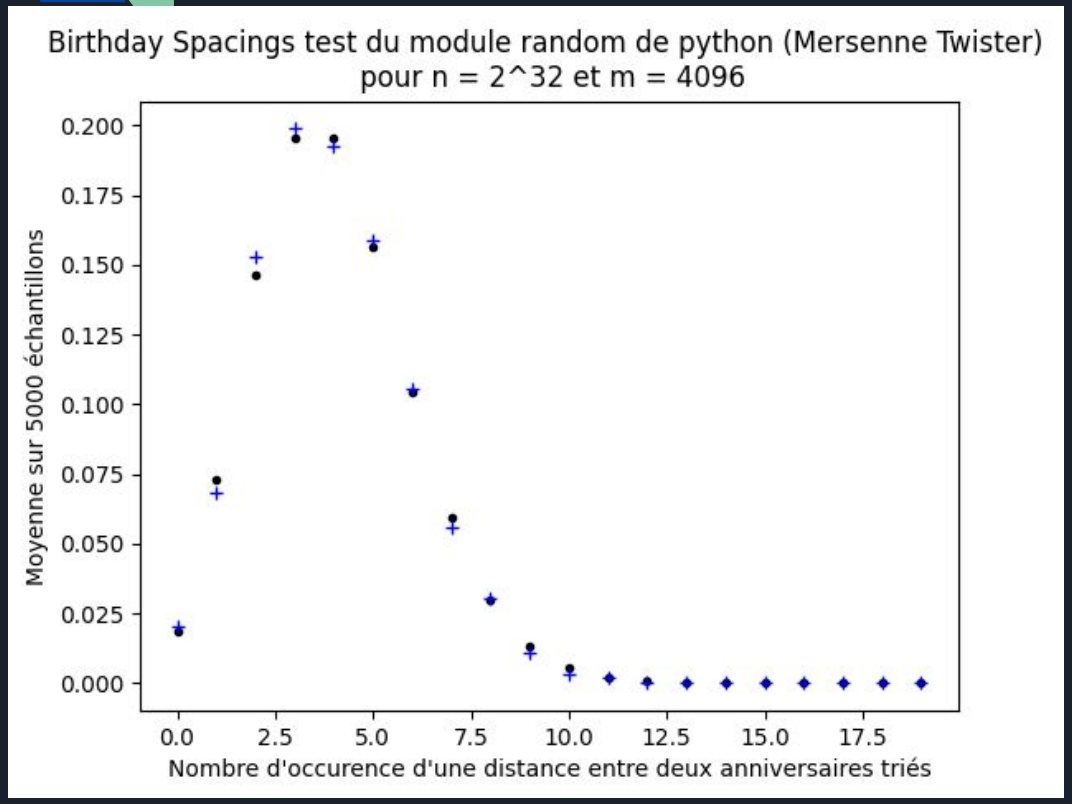
	Python	Notre générateur
χ^2	60.543	49.613

Avec Degré de liberté = 4 et $\alpha = 0.01$, on a CV = 13.28

Etude Statistique : Birthday test

- m anniversaires parmi n jours
- Tri des m anniversaires dans l'ordre croissant
- On note tous les espacements entre 2 anniversaires successifs
- On compte j le nombre d'espacements qui apparaissent plus d'une fois
- j suit asymptotiquement la loi de Poisson avec une espérance de $m^3 / 4n$

Etude Statistique : Birthday test



Loi de poisson de paramètre :

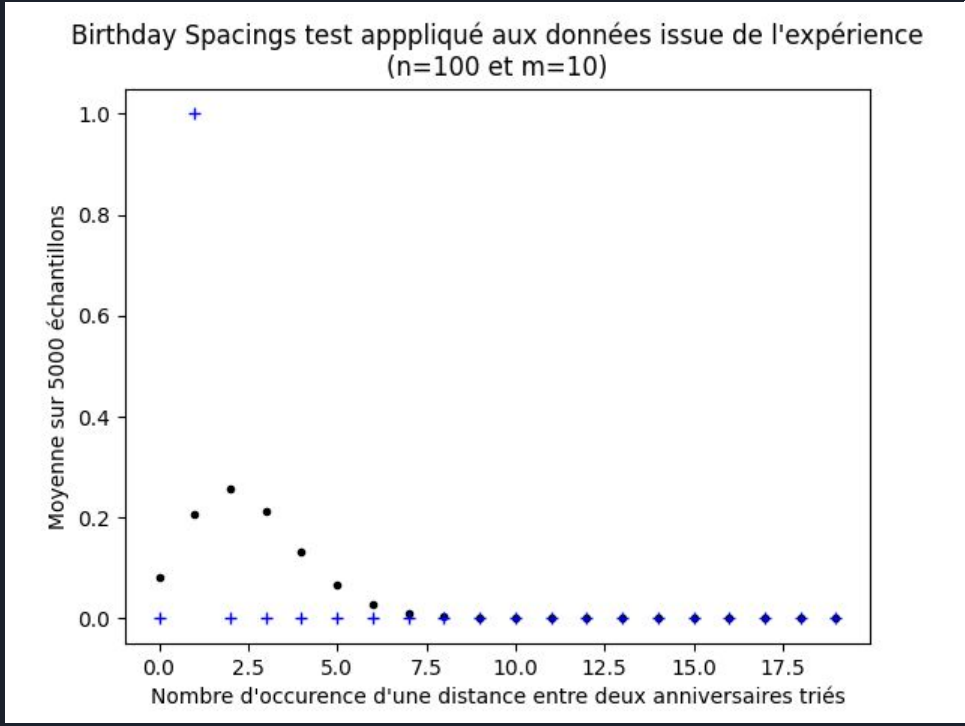
$$\frac{m^3}{4n}$$

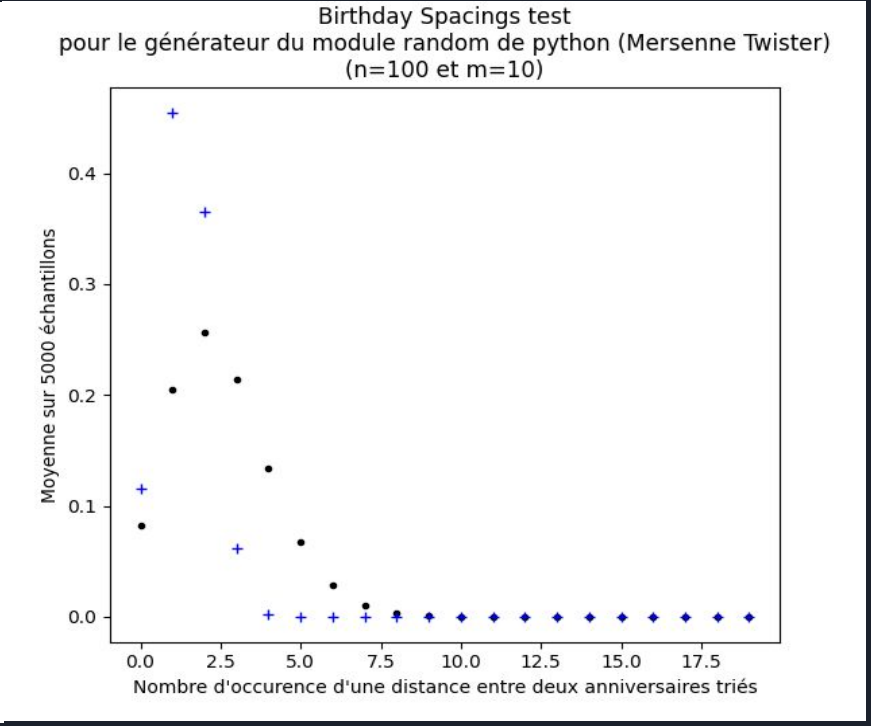
n : nombre de jours

m : nombres de dates d'anniversaire

Etude Statistique : Birthday test

Nos données soumisent au test





Conclusion

- Imaginer un dispositif plus grand avec un budget d'entreprise
- Le birthday test qui mets en lumière une des limites de ce générateur, c'est à dire la vitesse de génération des nombres
- Conclusion: Il peut être intéressant de voir ce générateur de comme un générateur de graines et non de nombres aléatoires.
- Les graines peuvent être du coup utilisées dans des générateurs numériques pseudo-aléatoires qui eux passent les testes et ont une vitesse de génération largement supérieur à notre dispositif