

Queste de savoir

On a retrouvé au beau milieu du hasard !

16 juin 2020

Table des matières

1.	tiré au sort ?	1
1.1.	Une histoire de nombres premiers entre eux	2
1.2.	Expérimentons : tirons plein de nombres !	2
2.	Pourquoi ça marche ?	4
2.1.	Alors, dans quels cas est-ce que $\text{pgcd}(a, b) = k$?	5
2.2.	Revenons donc à ce qu'on cherchait...	6
3.	Une méthode efficace pour obtenir ?	8
	Contenu masqué	9
3.1.	Sources et références pour aller plus loin	11
3.2.	Crédits	11

, ce nombre si emblématique des mathématiques, a cette fâcheuse tendance à apparaître partout, et surtout là où on ne l'attend pas. Facétieux, il se cache dans tous les recoins des mathématiques... même les plus inattendus !

À l'origine, est le rapport entre la circonférence d'un cercle et son diamètre : c'est comme ça qu'on l'a découvert dans l'antiquité et que sa folle histoire a commencé. Déjà en 2000 avant notre ère, on en retrouvait la trace, certes très approximative.

$$\pi \approx 3, 14 15 92 65 35 89 79 32$$

On retrouve dans beaucoup de formules de géométrie bien sûr, étant issu de cette branche des mathématiques, mais aussi dans des séries, autour des nombres complexes, en statistiques, dans bien des branches de la physique ou de la chimie au détour d'équations...

Aujourd'hui, histoire de parler d'inattendu dans tous les sens du terme, retrouvons-le dans *le hasard*. Car il s'y cache aussi !

1. π tiré au sort ?

Alors bien sûr on ne va pas tirer des nombres au hasard jusqu'à tomber par (énorme) chance sur ! On va être un peu plus intelligent que ça... en tirant *deux* nombres. Attendez, vous allez comprendre...

1. tiré au sort ?

1.1. Une histoire de nombres premiers entre eux

Tout nombre entier peut s'écrire comme le produit d'autres nombres : jusque-là, rien de bien compliqué. Si on prend quelques nombres et qu'on les écrit de la sorte, on obtient quelque chose comme ça :

$$12 = 3 \times 4$$

$$11 = 11 \text{ (il n'y a rien de mieux)}$$

$$100 = 4 \times 5 \times 5$$

$$40 = 2 \times 2 \times 2 \times 5$$

Si on regarde les nombres deux par deux, on aura dans certains cas des facteurs en commun (par exemple, 100 et 40 partagent 2 et 5). Dans d'autres cas, il n'y en a pas (11 et 12 ne partagent rien) : on dit alors que ces nombres sont **premiers entre eux**.

Quand on tire deux nombres au hasard, il y a donc deux possibilités : ils peuvent être *premiers entre eux*, ou ne pas l'être.

Par exemple, j'ai tiré avec deux dés à cent faces les nombres **77** et **87** : 87 s'écrit 3×29 et $77 = 7 \times 11$ — ils sont premiers entre eux, ne partageant aucun facteur commun. J'ai relancé mes dés pour trouver **2** et **14** : 2 est premier et 14 s'écrit 2×7 — ils ne sont donc, eux, pas premiers entre eux.

1.2. Expérimentons : tirons plein de nombres !

Mais *so what*, me diriez-vous, où trouve-t-on là-dedans ? Dans les probabilités ! Car en tirant deux nombres au hasard, on n'a pas autant de chance d'avoir deux nombres premiers entre eux que de nombres qui ne le sont pas. Lancez plein de dés, vous verrez : **vous obtiendrez plus souvent des nombres premiers entre eux que le contraire**. Cette probabilité se calcule, et devinez quoi ? Elle est liée à !

En effet (et je le justifierai plus loin),

Théorème de Cèsaro en théorie des nombres

La probabilité que deux nombres tirés au hasard soient premiers entre eux vaut

$$\frac{6}{\pi^2}$$

Comment vérifier ça ? Un moyen simple est de... tirer plein de nombres. En réalisant l'expérience tout plein de fois et en comptant quel pourcentage de couples premiers entre eux on a obtenu, on approche la probabilité expérimentalement 🍊 .

Oh, on pourrait tirer des milliers de couples de dés et vérifier que les nombres obtenus sont premiers entre eux... mais ce serait un peu longuet.¹ Comme j'ai un peu la flemme, j'ai décidé

1. tiré au sort ?

d'écrire un petit programme qui fait tout le boulot pour moi, ce qui me permet de faire des millions (ou milliards si l'envie m'en prend) de tirages sans effort. Ha !

1.2.1. Commencer doucement...

Comme il faut savoir commencer petit, j'ai démarré avec un millier de tirages. J'ai obtenu **643** couples de nombres premiers entre eux, ce qui fait une probabilité expérimentale, basée sur ce tirage, de :

$$P = \frac{643}{1000} = 0,643$$

On aurait donc $6/\pi^2 = 0,643$? Si oui, ça donnerait :

$$\pi^2 = 6 \times \frac{1}{0,643} \approx 9,331$$

et donc :

$$\pi \approx \sqrt{6 \times \frac{1}{0,643}} \approx 3,054$$

Je vous l'accorde, la précision n'est pas extraordinaire... mais tout de même, pour à peine un millier de paires de nombres tirés au hasard, retrouver avec une précision de 2 %, c'est pas si mal ! Cela dit, *on peut faire mieux*.

Comme ce n'est pas moi qui lance les dés, autant se faire plaisir : partons sur **un million de tirages**. En moins d'une seconde, c'est bon, et on a trouvé **607 780 couples de nombres premiers entre eux**. En appliquant le même calcul que plus haut, avec une probabilité expérimentale de $\frac{607\,780}{1\,000\,000} = 0,607\,780$, on trouve :

$$\pi \approx 3,141\,972$$

Voilà qui n'est pas si mal ! Certes, dès la quatrième décimale on perd la précision (elle devrait être un 5, la vraie valeur commençant par 3,14159) — mais encore une fois, on tire cette valeur du hasard complet, donc une précision de 0,01 % c'est relativement acceptable. Surtout qu'en pratique, prendre 3,14 comme approximation de π , ça suffit à la majorité des usages...

2. Pourquoi ça marche ?

1.2.2. ...mais finir gourmand

Dans un brin de folie (et surtout car ça travaille tout seul pendant que je fais autre chose), j'ai demandé dix milliards de tirages (oui, 10 000 000 000 de tirages). Après seulement trois heures et quart de calcul (ahrem)², 6 079 281 509 couples de nombres premiers entre eux avaient été tirés, ce qui nous permet d'estimer que π a pour valeur...

$$\pi \approx 3,141\,589\,943$$

C'est déjà mieux : on a quatre décimales justes (la vraie valeur étant $\pi = 3,141592\dots$)!

☞ Le code source, pour les curieuses et les curieux

2. Pourquoi ça marche ?

Bon allez, il est temps de rentrer un peu dans les mathématiques afin de comprendre d'où vient cette probabilité!



Une formule peut en cacher une autre

Cette section rentre dans des détails mathématiques. J'ai tenté d'être le plus clair possible même si vous n'avez pas de grosses connaissances (les maths du collège français, étudiées vers 14/15 ans, devraient suffire), mais si vous n'êtes pas à l'aise ou que l'explication ne vous intéresse pas, vous pouvez me faire confiance et sauter à la partie suivante.

Partons de ce qu'on cherche. Avec a et b deux entiers naturels quelconques (ceux qu'on tire au dé), on cherche la probabilité qu'ils soient premiers entre eux, autrement dit que leur plus grand diviseur commun (PGCD) soit égal à 1.



En effet, si le PGCD vaut 1, les deux nombres ne peuvent partager aucun autre facteur commun (car alors il serait plus grand que 1, et donc le PGCD ne vaudrait pas 1); ils sont donc premiers entre eux.

Pour la suite, on va noter p_1 cette probabilité (vous comprendrez assez vite pourquoi ce 1 en indice), et on la note ainsi :

$$p_1 = P(\text{pgcd}(a, b) = 1)$$

1. Cela dit, si vraiment vous y tenez, [Matt Parker l'a fait](#)  (en anglais, avec 500 couples de nombres tirés).
2. Comme vous pouvez le voir dans le bloc secret un peu après, le code qui a fait ce calcul n'est pas parallélisé, ce qui explique la durée énorme de calcul alors qu'on aurait pu faire beaucoup mieux en tirant plein de nombres en même temps. Cela dit et comme nous le verrons plus loin, même avec un système massivement parallélisé pour faire le plus de tirages possibles, cette méthode n'est franchement pas la meilleure, et certainement pas celle qu'est utilisée pour calculer des dizaines de milliards de décimales de !

2. Pourquoi ça marche ?

Une première observation que l'on peut faire, c'est qu'on peut avoir des nombres arbitrairement grands ici (et même potentiellement *très* grands, la seule limite étant l'infini). Le plus grand diviseur commun de deux nombres peut donc être, lui aussi, *aussi grand que l'on veut*. $\text{pgcd}(a, b)$ peut valoir 1, ou 2, ou 3, ou... ou k , ou $k + 1$, ou... jusqu'à l'infini.

Mais alors, il est *certain* que le PGCD a l'une de ces valeurs. Donc si on somme la probabilité que le PGCD soit 1, et soit 2, et 3, et..., et k , et..., jusqu'à l'infini, on doit trouver 1 (la probabilité certaine).

Autrement dit, si on note p_k la probabilité que le PGCD de a et b soit k :

$$p_k = P(\text{pgcd}(a, b) = k)$$

...alors on sait que :

$$p_1 + p_2 + \dots + p_k + \dots = 1$$

Ce qu'on peut écrire d'une façon un peu plus compacte :

$$\sum_{k=1}^{\infty} p_k = 1$$

On va donc tenter de déterminer la probabilité que le PGCD de a et b soit k , c'est peut-être plus simple...

2.1. Alors, dans quels cas est-ce que $\text{pgcd}(a, b) = k$?

Réfléchissons. Pour que le PGCD de a et b soit k , il faut respecter deux critères en même temps :

- k doit diviser a et b (c'est mieux... sinon il aura du mal à être le plus grand *diviseur*); et
- il ne doit pas y avoir de diviseur *plus grand que* k .

Pour trouver la probabilité p_k , il nous faut donc trouver la probabilité de ces deux événements et les multiplier (car on veut les deux *en même temps*, et que ces événements sont indépendants les uns des autres).

2.1.1. Probabilité que k divise a et b

Quand on y pense,

- 2 divise la moitié des nombres (tous les nombres pairs);
- 3 en divise un tiers (3, 6, 9, 12, ...);
- 4 en divise un quart...

2. Pourquoi ça marche ?

En généralisant, un nombre quelconque k divise un k -ième des nombres... la probabilité qu'il en divise un en particulier est donc $1/k$ — par exemple, 2 divise la moitié des nombres, donc en prenant un nombre au hasard, il y a une chance sur deux qu'il soit divisible par deux (autrement dit, pair).

i

Une autre façon de s'en convaincre est que dans la division d'un nombre quelconque par k , il peut y avoir k restes différents : 0, 1, 2, ..., et $k - 1$. Le seul bon cas est celui où le reste est nul ; comme on a autant de chance de tomber sur l'un ou l'autre des restes, la probabilité de tomber sur zéro est bien $1/k$.

Ici on veut que k divise a et b . La probabilité qu'on cherche est donc celle que k divise a multipliée par celle que k divise b . Les deux nombres n'ayant pas particulièrement de différence de traitement, cette probabilité est bien sûr la même, et **la probabilité que k divise a et b vaut donc $1/k^2$** .

2.1.2. Probabilité qu'il n'y ait pas de diviseur plus grand que k

On veut qu'il n'y ait pas de diviseur commun plus grand que k : c'est équivalent au fait qu'il n'y ait pas de diviseur plus grand que 1 si on divise par k (autrement dit que le pgcd $(\frac{a}{k}, \frac{b}{k})$ soit 1)³.

i

Pour s'en convaincre, il suffit de regarder un cas particulier : disons 42 et 70. $42 = 2 \times 3 \times 7$, et $70 = 2 \times 5 \times 7$, donc leur plus grand commun diviseur est $2 \times 7 = 14$. Si on divise par quatorze, il ne nous reste que 3 d'un côté, et 5 de l'autre.

Si 14 n'avait pas été le plus grand diviseur commun, en divisant par lui, il serait resté de tels diviseurs, et alors le PGCD des versions divisées n'aurait pas été 1. Par exemple, si on s'était trompé et qu'on avait considéré 7 comme le PGCD, il serait resté 2×3 d'un côté et 2×5 de l'autre : le PGCD de ces deux nombres vaut 2 (ça se voit), et non 1.

Mais attendez, la probabilité que deux nombres aient un PGCD de 1... on l'a déjà nommée plus haut, c'est p_1 !

2.2. Revenons donc à ce qu'on cherchait...

Si on rassemble ces deux points, on peut donc affirmer que p_k , la probabilité que le PGCD de a et b vaille k , vaut le produit de ces deux valeurs trouvées, donc :

$$p_k = \frac{1}{k^2} \times p_1 = \frac{p_1}{k^2}$$

Or, on avait plus haut une relation avec p_k ! Et si on essayait d'injecter cette nouvelle valeur ? On obtient :

3. a/k est bien un entier, car on se place dans le cas où k divise a (sinon ça n'a pas d'intérêt, vu qu'on veut que les deux soient vrais en même temps).

2. Pourquoi ça marche ?

$$\sum_{k=1}^{\infty} p_k = p_1 + \frac{p_1}{2^2} + \frac{p_1}{3^2} + \frac{p_1}{4^2} + \dots = 1$$

Or p_1 est une constante, on peut donc factoriser pour la sortir de la somme :

$$p_1 \times \left(1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \dots \right) = 1$$

Et donc en réorganisant :

$$p_1 = \frac{1}{1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \dots} = \frac{1}{\sum_{k=1}^{\infty} \frac{1}{k^2}}$$

On avance ! Il ne nous reste plus qu'à déterminer ce mystérieux terme : la somme des inverses des carrés de tous les nombres entiers positifs non nuls... mais il se trouve que c'est un problème connu, le **problème de Bâle** [☞](#), résolu par Euler en 1741. Et il se trouve que justement... on y retrouve... !

$$\sum_{k=1}^{\infty} \frac{1}{k^2} = \frac{\pi^2}{6}$$

De là, il est trivial de conclure que :

$$p_1 = \frac{1}{\pi^2/6} = \frac{6}{\pi^2}$$

Et voilà.

i

Point rigueur : les limites de cette démonstration

Il y a une faiblesse dans cette démonstration : il n'existe pas de probabilité uniforme sur l'ensemble des entiers strictement positifs \mathbb{N}^* . La démonstration ci-dessus est juste (avec quelques menus ajustements) si on considère qu'on calcule la probabilité P_N d'avoir deux nombres premiers entre eux dans un ensemble fini $[1; N]$ ($N \in \mathbb{N}^*$), et qu'on prend pour probabilité finale la limite de cette valeur quand N tend vers l'infini :

$$\lim_{N \rightarrow \infty} P_N = \frac{6}{\pi^2}$$

On peut justifier que prendre ainsi la limite a un sens en terme de probabilités, mais je ne l'ai absolument pas fait ici — faites-moi confiance, ou consultez d'autres preuves certes plus rigoureuses, mais bien moins accessibles.

3. Une méthode efficace pour obtenir ?

3. Une méthode efficace pour obtenir π ?

Alors oui, on *peut* calculer avec cette méthode, en tirant plein de nombres au dé... mais est-elle efficace? En pratique, pas vraiment. Ou plutôt, **vraiment pas**.

Le problème, c'est que pour que ça fonctionne correctement, il faudrait pouvoir tirer des nombres sur *l'ensemble des nombres entiers positifs qui existent*, donc jusqu'à l'infini. Et l'infini, c'est grand.

Si on ne tire pas des nombres sur tout ça, la précision s'en ressent beaucoup (vraiment beaucoup). Avec un gros dé on tire entre quoi, un et deux-cent ? C'est ridiculement petit... et on obtient au mieux zéro ou une décimale. Et même avec le logiciel que j'ai écrit pour faire les tirages à ma place, en prenant le plus grand nombre possible facilement, un nombre à trente-huit chiffres tout de même⁴, tellement grand qu'il est difficile de se l'imaginer — on est très, très loin de l'infini, et on peine à dépasser quatre ou cinq décimales.

Lorsqu'on calcule avec une très grande précision, espérant des milliards de chiffres après la virgule, on utilise des méthodes très différentes et bien plus efficaces, donc on pourrait éventuellement parler s'il y a de l'intérêt parmi mes lecteurs. Mais ces méthodes n'ont pas la poésie de tirer du hasard le plus total...

i

Un peu plus de détails mathématiques pour les intéressées

La valeur de la probabilité est juste, certes, c'est bien $6/\pi^2$. Mais le fait est que cette probabilité vaut $6/\pi^2$ *uniquement si on tire un nombre dans l'ensemble des entiers positifs non nuls* (cf. la formulation sous forme de limite plus haut, si vous connaissez cette notion). Problème : **la convergence est extrêmement lente**. Il faut énormément augmenter la taille de l'échantillon pour avoir une précision de $6/\pi^2$ qui augmente *un peu*. Et quand ce n'est pas le cas, on peut toujours faire des centaines de milliards de tirages : la probabilité ne permet pas d'atteindre, mais une valeur qui s'en approche.

J'aime beaucoup cette tendance de à pointer le bout de son nez un peu partout en mathématiques sans vraiment qu'on s'y attende. Tel un discret ange gardien qui n'est jamais très loin, caché derrière un mur prêt à bondir dans tous les domaines des sciences...



4. Pour ceux à qui ça parle, j'ai pris la valeur maximale d'un entier non-signé de 128 bits. Ce nombre vaut environ 3×10^{38} , ou exactement 340 282 366 920 938 463 463 374 607 431 768 211 455.

FIGURE 3.1. – , allégorie.

Le tirer du hasard est d'autant plus surprenant, c'est pourquoi j'avais envie d'en parler à l'occasion du *-day* de cette année. Cela dit, la démonstration ci-dessus pourrait vous laisser un peu... frustrée. *semble* arriver tel un cheveu sur la soupe qu'il faut accepter sans broncher, ce qui n'est, je l'admets, pas très satisfaisant.

Il existe une démonstration que je trouve très élégante et compréhensible du problème de Bâle, qui permet de très bien comprendre *d'où sort* ce . On peut relier ce problème à un problème géométrique impliquant des cercles, et qui dit cercle... dit 🍊 . La preuve est assez longue et ne sera pas traitée dans cet article — cela dit, une suite est prévue pour justement la présenter, et ainsi comprendre complètement comment on obtient à partir du hasard 🍊 .

i

Les curieux anglophones et à l'aise avec les mathématiques pourront également consulter la sixième source dans le bloc masqué ci-dessous.

Cette méthode n'est pas la seule qui existe pour extraire du hasard, sois dit en passant. Il existe notamment la [méthode de Monte-Carlo](#) qui permet d'estimer une valeur de $\pi/4$ (et donc par extension de) assez simplement. J'ai préféré traiter le théorème de Cesàro car je le trouve plus amusant, mais c'est complètement subjectif.

Je tiens à remercier Pifra pour ses conseils sur le traitement d'une partie de l'article, ainsi que @Aabu pour la relecture et validation de cet article dans des délais assez courts !

👁 Sources, références, et crédits

Contenu masqué

Contenu masqué n°1 :

Le code source, pour les curieuses et les curieux

Il n'y a en soit rien de très complexe dans le programme de tirage, pour qui connaît un peu la programmation : il s'agit juste de calculer le PGCD de plein de nombres tirés au hasard, et de compter ceux pour lesquels le PGCD vaut 1 (correspondant au cas où les nombres sont premiers entre eux). Ensuite, en divisant ce nombre par le nombre total de tirages, on obtient la probabilité d'avoir deux nombres premiers entre eux, soit une approximation de $6/\pi^2$. Un peu de maths en plus et on extrait une approximation de 🍊 .

J'ai juste ajouté par dessus un petit calcul de la précision en se basant sur la valeur de "réelle" (à 15 décimales).

Le programme a été fait en Rust, parce que c'est rapide (j'avais pour volonté de tirer *beaucoup* de couples de nombres pour avoir une précision correcte) et que j'aime bien le langage (totalement subjectif, oui).

```

1  extern crate gcd;
2  extern crate rand;
3
4  use std::env;
5
6  use gcd::Gcd;
7  use rand::Rng;
8
9  use std::f64::consts::PI;
10
11 const DEFAULT_DRAWS: u64 = 1_000_000;
12 const MAX_NUMBER: u128 = std::u128::MAX;
13
14 #[inline(always)]
15 fn are_randoms_coprime<R: Rng>(rng: &mut R) -> bool {
16     rng.gen_range(1, MAX_NUMBER).gcd(rng.gen_range(1, MAX_NUMBER))
17     == 1
18 }
19 fn main() {
20     let args: Vec<String> = env::args().collect();
21     let draws: u64 =
22         args.get(1).unwrap_or(&String::new()).parse().unwrap_or(DEFAULT_DRAWS);
23
24     let mut rng = rand::thread_rng();
25
26     let coprimes = (1..draws)
27         .filter(|_| are_randoms_coprime(&mut rng))
28         .count() as f64;
29
30     let pi = (6_f64 / (coprimes / draws as f64)).sqrt();
31     let precision = (pi - PI).abs() / PI * 100_f64;
32
33     println!("{}", coprimes in {} draws", coprimes, draws);
34     println!("π ≈ {} (precision {} %)", pi, precision);
35 }

```

En le lançant pour un million de tirages, on peut trouver la valeur obtenue plus haut — bien sûr, comme c'est aléatoire, la valeur exacte change un peu à chaque fois mais la précision reste sensiblement la même, entre 0,1 et 0,01 %.

```

1  $ cargo run --release --quiet
2  607780 coprimes in 1000000 draws
3  π ≈ 3.141972812647824 (precision 0.01210083864935896 %)

```

Avec dix milliards de tirages, c'est... un peu plus long, mais le résultat est bien meilleur !

```
1 $ cargo run --release --quiet -- 10000000000
2 6079281509 coprimes in 10000000000 draws
3  $\pi \approx 3.14158994300916$  (precision 0.0000862804128715215 %)
```

[Retourner au texte.](#)

Contenu masqué n°2 : Sources, références, et crédits

3.1. Sources et références pour aller plus loin

1. Hardy, G. H., & Wright, E. M. (2007). *Introduction à la théorie des nombres*. Vuibert; Springer.
2. *Pi et les nombres premiers : $6/\pi^2$* [↗](#). (s. d.). Consulté 11 mars 2020.
3. *Probability of Two Integers Being Coprime* [↗](#). (s. d.). Consulté 11 mars 2020.
4. *Probability that two random numbers are coprime is $\frac{6}{\pi^2}$* [↗](#). (s. d.). Mathematics Stack Exchange. Consulté 11 mars 2020.
5. *Problème de Bâle* [↗](#). (2020). In *Wikipédia*.
6. Wastlund, J. (s. d.). *Summing inverse squares by euclidean geometry* [↗](#). 10.

3.2. Crédits

- L'allégorie de , *blob peek*, est diffusée sous licence Apache 2 par Google / [blobs.gg](#) [↗](#).
- Le logo est un travail dérivé de *Dice* par [Flaticon / Those Icons](#) [↗](#).

[Retourner au texte.](#)