Beyond the probability of coprimality

20 juillet 2017

A rather famous claim

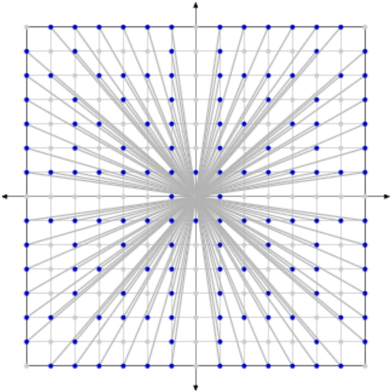
« The probability for two random integers to be relatively prime is $\frac{6}{\pi^2}$ »
First mention of this result by Dirichlet

Short « proof » :
They are not relatively prime if they are never both divisible by some prime p. Assuming these events are independant,

$$\begin{aligned}
\mathbb{P}(\text{coprime}) &= \prod_{p \text{ prime}} \mathbb{P}(\text{not both divisible by } p) \\
&= \prod_{p \text{ prime}} \left(1 - \frac{1}{p^2}\right) \\
&= \left(\sum_{n \geq 1} \frac{1}{n^2}\right)^{-1} = \frac{6}{\pi^2}
\end{aligned}$$

An other point of view

If we think of our two numbers as the coordinates of a point, then coprimality $\Leftrightarrow$ there is no other point in front of it.



from the blog « The Lumber Room »

$\Rightarrow$ About the proportion of points we can see from the origin.

A little more rigor

What does « random integers » mean ? What does a « proportion » of all the integers mean ?

It only makes sense with a finite number of points *a priori*, for instance the proportion of points in $[-N, N] \times [-N, N]$ visible from the origin, and then make $N \to \infty$.
We can then rigorously prove that it tends to $\frac{6}{\pi^2} \approx 60.8$.

Let's generalize !

- What happens in dimensions greater than 2 ?
  It actually tends to $\zeta(d)^{-1}$.
- What if we sample vectors according to a probability distribution ?

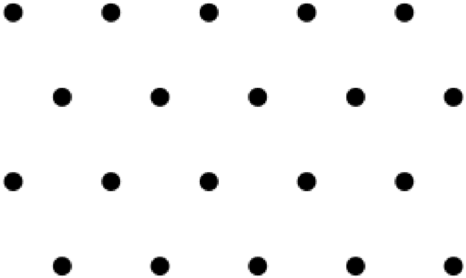
Theorem

Let $f : \mathbb{R}^d \to \mathbb{R}_+$ be a measurable function such that $\int_{\mathbb{R}^d} f < \infty$ and $f^{-1}([a, b[)$ is Jordan measurable for all a, b.
Then the probability for an integer vector drawn from Nf to be visible from the origin tends to $\zeta(d)^{-1}$ when $N \to \infty$.

- Do we have to restrict ourselves to integer vectors ?

Lattices

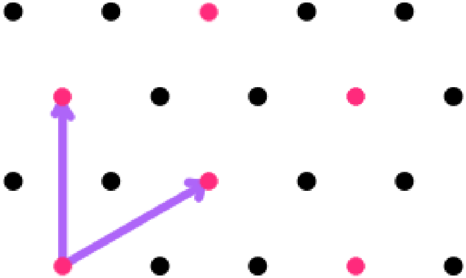
A lattice is a discrete subgroupe of $(\mathbb{R}^n, +)$.
One can show that every lattice can be seen as integer combinations of a set of independant vectors.



All lattices can be interpreted as a skewed version of integers vectors (which are called square lattices).

Primitive families

A family of k vectors in a lattice L is called *primitive* if the lattice they generate is equal to the intersection of L and the subspace they generate.



Not a primitive family

Drawing primitive families

What is the asymptotic probability of drawing a primitive family ?

- If $k < n$, it is $\zeta(n)^{-1}\zeta(n-1)^{-1}\ldots\zeta(n-k+1)^{-1}$
- If $k = n$, it is 0
- If $k > n$, it is $\zeta(k)^{-1}\zeta(k-1)^{-1}\ldots\zeta(k-n+1)^{-1}$

Some links with quantum computing

Some key exchange protocols, analogous to Diffie-Hellman, are based on number fields (suggested by Buchmann and Williams, 1988). There is no known feasible way to break them, however there is a quantum algorithm proposed by Hallgren in 2006 which does break them.
An important component of it happens to rely on generating a lattice with ramdomly sampled vectors.