互質的機率

許介彥 大葉大學電信工程學系

chsu@mail.dyu.edu.tw

假設我們將 100 顆球 (編號 1 到 100) 放入一個大袋子裡,經過充分攪拌後從袋中隨機 摸出一顆球,檢視其編號後將球放回袋中,然後從袋中再隨機摸出一顆球。請您猜猜看,我 們剛才摸出來的兩顆球的編號互質的機率大不大?是大於1/2 還是小於1/2 ?

如果球總共有n 顆,n 爲任意正整數(上述過程中的n 爲 100),數學上可以証明,當n 趨於無窮大,我們所摸出來的兩顆球的編號互質的機率將趨於某個常數;本文接下來將設法求出此數。

我們相當於要求由全部無窮多個正整數中隨機選出的兩數互質的機率是多少。假設這兩數爲 a 與 b。如果 a 和 b 互質(即 a 和 b 的最大公因數 $\gcd(a,b)$ 等於 1),那麼對任意質數 p, a 和 b 一定不會同時是 p 的倍數,也就是說,a 和 b 不會同時是 2 的倍數,也不會同時是 3 的倍數,也不會同時是 5 的倍數。反過來說也成立:如果對任意質數 p,a 和 b 都不同時是 p 的倍數,那麼 a 和 b 一定互質。

a 和 b 不同時是 2 的倍數的機率是多少呢?由於數線上每連續兩個正整數就有一個是偶數,因此隨機選出的整數 a 是偶數的機率爲1/2,整數 b 是偶數的機率同樣也是1/2,所以 a 和 b 同時是 2 的倍數的機率爲 $(1/2)^2$,不同時是 2 的倍數的機率爲 $1-(1/2)^2$ (這包括了 a 與 b 兩數中只有一數是偶數或兩數皆不是偶數的情形)。依此類推,a 和 b 不同時是 3 的倍數的機率爲 $1-(1/3)^2$,不同時是 5 的倍數的機率爲 $1-(1/5)^2$ 等;因此 a 與 b 万質的機率等於

$$\left(1-\frac{1}{2^2}\right)\left(1-\frac{1}{3^2}\right)\left(1-\frac{1}{5^2}\right)\left(1-\frac{1}{7^2}\right)\left(1-\frac{1}{11^2}\right)\cdots$$

我們剩下的問題是:上式的值是多少?

要求出此數,我們可以借助大數學家<u>尤拉</u>(Leonhard Euler,1707–1783)曾經証明的一個很有名的式子:

$$1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \frac{1}{5^2} + \dots = \frac{\pi^2}{6}$$

以下我們說明:上式與我們所要求的機率的乘積正好等於1,也就是

$$\left(1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \frac{1}{5^2} + \cdots\right) \left(1 - \frac{1}{2^2}\right) \left(1 - \frac{1}{3^2}\right) \left(1 - \frac{1}{5^2}\right) \left(1 - \frac{1}{7^2}\right) \left(1 - \frac{1}{11^2}\right) \cdots = 1$$

這不難由將括號由左而右依序乘開的過程看出來,例如將最左邊的兩個括號乘開得

$$1 + \frac{1}{2^{2}} + \frac{1}{3^{2}} + \frac{1}{4^{2}} + \frac{1}{5^{2}} + \frac{1}{6^{2}} + \cdots$$

$$1 - \frac{1}{2^{2}}$$

$$1 + \frac{1}{2^{2}} + \frac{1}{3^{2}} + \frac{1}{4^{2}} + \frac{1}{5^{2}} + \frac{1}{6^{2}} + \cdots$$

$$- \frac{1}{2^{2}} - \frac{1}{4^{2}} - \frac{1}{6^{2}} - \cdots$$

$$1 + \frac{1}{3^{2}} + \frac{1}{5^{2}} + \cdots$$

因此所有形如 $1/(2k)^2$ 的項都不見了;將上面的結果與下一個括號相乘得

$$1 + \frac{1}{3^{2}} + \frac{1}{5^{2}} + \frac{1}{7^{2}} + \frac{1}{9^{2}} + \frac{1}{11^{2}} + \cdots$$

$$1 - \frac{1}{3^{2}}$$

$$1 + \frac{1}{3^{2}} + \frac{1}{5^{2}} + \frac{1}{7^{2}} + \frac{1}{9^{2}} + \frac{1}{11^{2}} + \cdots$$

$$- \frac{1}{3^{2}} - \frac{1}{9^{2}} - \cdots$$

$$1 + \frac{1}{5^{2}} + \frac{1}{7^{2}} + \frac{1}{11^{2}} + \cdots$$

所有形如 $1/(3k)^2$ 的項也都不見了。讀者不難看出如果將上面的結果繼續乘以 $1-(1/5)^2$,所有形如 $1/(5k)^2$ 的項也都將消失;將結果繼續乘以 $1-(1/7)^2$,所有形如 $1/(7k)^2$ 的項也都將消失……。對任意一個大於 1 的整數 n,由於 n 必有質因數,因此 $1/n^2$ 必定會在某個階段被消掉;隨著括號一個一個展開,每個階段所得的結果爲 1 加上一個越來越小的正數,結果顯然將趨近於 1。

既然我們希望求得的機率與 $\pi^2/6$ 的乘積為1,我們所求的機率為

$$\frac{6}{\pi^2} = 0.6079...$$

因此,從所有正整數中隨機選出的兩數互質的機率不僅超過六成,而且此機率竟然還和圓周 率 π 有關,這樣的結論想必會讓許多讀者感到訝異。

如果從所有正整數中隨機選出三數,這三數互質 (最大公因數爲 1)的機率又是多少呢? 由類似前面的推論不難得知:對任意正整數 $k \ge 2$,從所有正整數中隨機選出的 k 個數互質的 機率都等於

$$\left(1-\frac{1}{2^k}\right)\left(1-\frac{1}{3^k}\right)\left(1-\frac{1}{5^k}\right)\left(1-\frac{1}{7^k}\right)\left(1-\frac{1}{11^k}\right)\cdots$$

數學上可求出當k = 3時,上式的值約爲 0.8319,而當k = 4,其值爲 $90/\pi^4 \approx 0.9239$ 等。

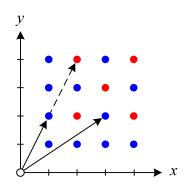
另一個相關的問題是:如果從所有正整數中隨機選出一個數 a, a 不能被任何質數的平方整除的機率是多少?也就是說,a 不是 2^2 , 3^2 , 5^2 , 7^2 , 11^2 , ... 等數的任一數的倍數的機率是多少?

對任意一個質數 p ,a 是 p^2 的倍數的機率為 $1/p^2$,因此 a 不是 p^2 的倍數的機率為 $1-(1/p^2)$,而 a 不是 $2^2,3^2,5^2,7^2,11^2,...$ 的任一數的倍數的機率為

$$\left(1-\frac{1}{2^2}\right)\left(1-\frac{1}{3^2}\right)\left(1-\frac{1}{5^2}\right)\left(1-\frac{1}{7^2}\right)\left(1-\frac{1}{11^2}\right)\cdots$$

相同的式子再度出現了;我們已知其值爲 $6/\pi^2$ 。

在幾何裡, $6/\pi^2$ 還和平面上從原點所能「看到」的格子點的比例有關;這裡的格子點指的是坐標平面上x坐標與y坐標皆爲整數的點。想像我們站在原點朝第一象限裡面看,有些格子點與原點之間由於受到其他格子點阻隔以至於無法從原點看到;例如下圖中藍色的點爲可從原點看到的點,而紅點則是從原點看不到的點:



在第一象限的無窮多個格子點中,能從原點看到的點佔了多大比例呢?上圖中,連到紅點的虛線顯示由於原點、點(1,2)與點(2,4)等三個點位在同一條直線上,所以從原點看時,點(2,4)會被點(1,2)遮住。一般而言,如果整數 a 與整數 b 不互質,它們的最大公因數 $d=\gcd(a,b)>1$ 且 a=ds,b=dt,那麼原點與點(s,t)及點(a,b)一定位於同一條直線上,而且由於點(s,t)較靠近原點,從原點往這兩個點的方向看時,點(a,b)一定會被點(s,t)遮住。另一方面,如果 a 與 b 互質的話則從原點一定能看到點(a,b),因爲此時連接原點與點(a,b)的線段上不可能有其他格子點存在。

由上面的論述可知第一象限中由原點所能看到的格子點就是x 坐標與y 坐標互質的點,這樣的點在第一象限中所佔的比例正相當於隨機選出的兩數互質的機率,其值爲 $6/\pi^2$ 。

雖然 $6/\pi^2$ 是當 n 趨於無窮大時,由不大於 n 的正整數中隨機選出的兩數互質的機率的極限値,不過隨著 n 的增大,此機率的値其實收斂得相當快,例如當 n=4 時其値爲 0.6875 (即 11/16,由上圖可看出);當 n=10 時其値爲 0.6300,而當 n=100 時其値爲 0.6087 (在全部 10000 組可能的數對中總共有 6087 對互質),與極限値的誤差已在 0.2% 以內。如果讀者學過程式設計的話,這些數據不難於彈指間取得;透過程式還可方便地觀察此機率值隨著 n 的增大而趨穩定的情形。