

2025 年【科學探究競賽-這樣教我就懂】

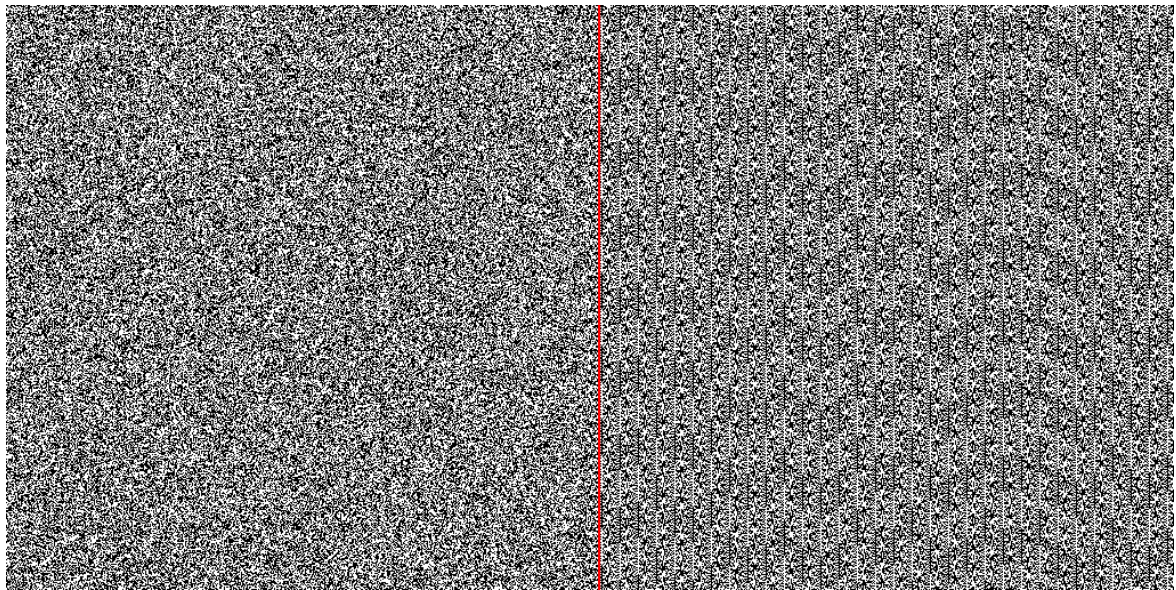
大專/社會組 科學文章格式

文章題目： 隨機、偽隨機，計算機下隨機

摘要： 介紹隨機與偽隨機、計算機下如何用算發來生成隨機數。以及現在的科技能否令計算機生成真隨機。

文章內容： (限 500 字~1,500 字)

在我們的日常生活中，「隨機」這個詞彷彿代表著不可預測與無秩序。丟骰子、抽籤、彩票號碼的產生，這些行為我們往往會視為「純粹的隨機」。但當我們走入計算機科學的世界，這個看似自然的觀念卻變得更加複雜：計算機如何產生「隨機數」？它們真的隨機嗎？這就是我們今天要探討的主題：隨機、偽隨機，與計算機下的隨機。



圖一、真隨機 vs 偽隨機

真隨機與偽隨機的區別

所謂「真隨機數 (True Random Number)」，指的是完全無法預測、無模式、源於自然物理現象的隨機數字。例如，利用放射性衰變、熱噪聲或電路中的量子波動所測得的訊號，可以視為真隨機。這些數據無法被演算法重現，因為它們來自不可控、無法複製的自然過程。

與之相對的，是「偽隨機數 (Pseudorandom Number)」。這些是由演算法產生的數字序列，雖然表面上看起來像是真隨機，但實際上是可重複、可預測的，只要你知道初始的「種子值 (Seed)」。

偽隨機的數學基礎：線性同餘法 (LCG)

最簡單的偽隨機生成器公式如下：

$$X_{n+1} = (aX_n + c) \bmod m$$

其中：

X0 是種子

a、c、m 是常數參數

結果是介於 0 到 m-1 之間的整數

這種演算法簡單快速，但若選參數不當，很容易出現明顯規律。

計算機如何「假裝」隨機？

從本質上看，計算機是一種決定性系統，它執行的是預先編好的指令，因此無法產生真正的隨機。當我們在程式中呼叫隨機數時，實際上是根據一個初始值運行演算法，生成一連串表面上看起來無規則的數列。

```
In [6]: import random

random.seed(42)
print([random.randint(1, 100) for _ in range(5)])
# 每次結果相同:[82, 15, 4, 95, 36]

[82, 15, 4, 95, 36]
```

圖二、Python 中的偽隨機

只要種子固定，每次結果都一樣。這在遊戲開發、科學模擬中非常實用，因為它讓隨機「可重現」。

未來的希望：量子隨機

當今最接近「完美隨機」的技術，源自量子力學的基本原理。量子事件，如光子的偏振或電子的穿隧行為，具有本質上的不可預測性。

真隨機的實例：

- **2025 年 3 月 31 日的突破**：一個由美國麻省理工學院（MIT）與 Google 合作的研究團隊宣布，他們成功利用量子計算機生成並驗證了「真隨機數字」。該實驗基於量子超疊加態與測量坍縮的不可預測性，並透過大量數據交叉驗證，證實其隨機性符合理論預期。
- **Quantinuum 的貢獻**：同樣在 2025 年 3 月，Quantinuum 公司與 JPMorganChase、阿貢國家實驗室、橡樹嶺國家實驗室及德克薩斯大學奧斯汀分校的研究人員合作，使用 56 位元量子計算機實驗性地展示了「認證隨機性（certified randomness）」，這是首次利用量子計算機生成並驗證真隨機數字的實驗。
- **Google 的量子處理器 Willow**：2024 年 12 月，Google 開發了名為 Willow 的量子晶片，顯著降低了錯誤率，這對於實現大規模、實用的量子計算機至關重要。

雖然這些量子硬體目前成本高昂且產量有限，速度也不及傳統演算法，但這些成果意味著「絕對不可預測」的隨機性已從理論走向現實。

結語：在秩序中創造不確定

計算機雖然是秩序的象徵，但我們卻能利用它的秩序來模擬混亂。這種人造隨機已廣泛應用於科學模擬、密碼學、人工智慧、藝術創作等領域。如今，隨著量子隨機技術的突破——例如 2025 年美國團隊的量子真隨機實驗成功——我們正從模擬走向實現真正的「隨機本質」。

隨機，究竟是自然的謎題，還是我們對未知的想像？或許正如一位物理學家所言：「真正的隨機，是當你再

也找不到規律時，仍願意相信它存在。」

參考資料

1. Knuth, Donald E. *The Art of Computer Programming*, Vol. 2: Seminumerical Algorithms
2. Eastlake et al., [RFC 4086: Randomness Requirements for Security](#)
3. Matsumoto & Nishimura, *Mersenne Twister: A 623-dimensionally equidistributed uniform pseudorandom number generator*
4. IDQ: [Quantum Random Number Generators](#)
5. <https://cns.utexas.edu/news/research/researchers-achieve-quantum-computing-milestone-realizing-certified-randomness>
6. <https://learn.xiaowai.co/random-numbers-in-computer-science-real-vs-pseudorandom-number/>

註：

1. 未使用本競賽官網提供「科學文章表單」格式投稿，**將不予審查**。
2. 字數沒按照本競賽官網規定之限 500 字~1,500 字，**將不予審查**。

PS.摘要、參考資料與圖表說明文字不計入。

3. 建議格式如下：

- 中文字型：微軟正黑體；英文、阿拉伯數字字型：Times New Roman
- 字體：12pt 為原則，若有需要，圖、表及附錄內的文字、數字得略小於 12pt，不得低於 10pt
- 字體行距，以固定行高 20 點為原則
- 表標題的排列方式為向表上方置中、對齊該表。圖標題的排列方式為向圖下方置中、對齊該圖