# 一種預測動盪時期股市波動的新方法

## 2024 年沃爾夫數學獎


「沃爾夫獎」（Wolf Prize）是以色列頒發的國際獎項；沃爾夫基金會表示，沃爾夫獎每年頒發一次，「表彰世界各地的科學家和藝術家為人類利益而在推動科學和藝術方面取得的傑出成就」。此外，「三分之一以上的沃爾夫獎得主隨後都獲得了相應學科的諾貝爾獎」。

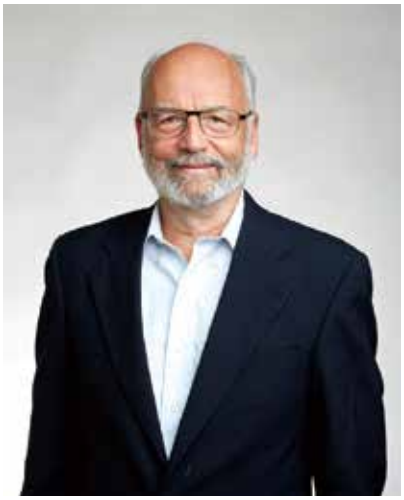
在 2024 年 7 月 4 日公佈了 2024 年度的九位得獎人，他們分別來自美國、英國、法國、瑞士、以色列和匈牙利六個不同的國家，領域包括醫學、數學、物理學、農業和音樂。

2024 年沃爾夫數學獎頒發給以色列魏茲曼科學研究院（Weizmann Institute of Science）的夏米爾（Adi Shamir）和美國普林斯頓大學的阿隆（Noga Alon），「以表彰他們對數學密碼學、組合學和計算機科學理論的開創性貢獻」。

## 夏米爾

夏米爾獲得沃爾夫獎，是因為他是一位真正卓越的科學家，並且是將密碼學轉變為一門以數學為重要基礎的科學學科的領導力量。他的奠基性發現結合了數學獨創性與一系列分析工具。這些發現對許多數學領域產生了巨大的影響，以無與倫比的方式推動了數學和社會的發展。

夏米爾 1952 年出生於以色列臺拉維夫，他是魏茲曼科學研究院資訊科學與應用數學系教授，也是全球最資深的資訊科學家之一。他是資訊加密和解密領域的頂尖專家。夏米爾是 RSA 方法的開發者之一，改變了世界電腦通訊的面貌，並且是電子商務和資訊安全的基本支柱。


夏米爾。（維基，英國皇家學會提供）

夏米爾自幼就對科學有濃厚的興趣，並參加了魏茲曼科學研究院的青少年學術計劃和科學夏令營。1973 年在臺拉維夫大學（Tel Aviv University）以優異成績取得數學學士學位後，夏米爾在魏茲曼研究所繼續深造，專攻資訊科學，並分別於 1975 年和 1977 年取得理學碩士學位和博士學位。在他的博士論文中，他研究了某些與程式語言語義相關的數學函數的特性。完成博士學業後，他在英國科芬特里（Coventry）的華威大學（University of Warwick）進行短期博士後研究，之後前往美國 MIT 繼續他的學術旅程，並開始研究加密和解碼的理論。

在傳統的加密技術中，金鑰對於訊息的加密與解密都至關重要，因此在金鑰分發的安全性上是一項挑戰。為了尋求解決方案，1977 年，MIT 的研究人員李維斯特（Ronald Rivest）、夏米爾和艾得曼（Leonard Adelman）設計出一種突破性的公開金鑰加密演算法，稱為 RSA（這三個研發人員姓氏的縮寫）。這種方法利用基於質數相乘的單向數學函數，確保原始的解決方案無法被擷取。RSA 使用兩個不同但在數學上有關聯的金鑰，一個是用於加密的公開金鑰，另一個是用於解密的私人金鑰，因此不需要分發金鑰。RSA 加密技術已獲得全球認可，是保護線上通訊、電子商務和交易中機密資料的基石。其意義已超越實際用途，獲得數學家、公司、政府和情報機關的重視。RSA 方法已成為保護電腦資訊和電子

商務的基本且近乎專屬的元素。他們三位也因為這項工作於 2002 年獲頒有資訊界諾貝爾獎的「涂林獎」（Turing Award）。

夏米爾對資訊安全做出了許多貢獻，其中包括開創性的秘密共享方法（secret-sharing method）。該技術將秘密轉換為亂數集，需要特定的組合來重建原始秘密，形成安全計算的基礎。他與同行合作，透過零知識證明（zero-knowledge proof）改進了身份識別和簽名方法，並設計了基於群組的加密的環簽名（ring signature）。夏米爾的獨創性擴展到電視廣播加密，允許專門為付費接收者進行加密傳輸。近年來，他深入研究了 T 函數，這是用於資訊加密的複雜數學工具。夏米爾的影響也延伸到揭露加密系統中的漏洞、開發攻擊的通用數學方法以及針對硬體和軟體實現的首創旁通道攻擊（side channel attack）。除了資訊安全之外，他的貢獻還在核心資訊科學領域引起了共鳴，特別是塑造了計算複雜性理論（theory of computational complexity）。

## 阿隆

阿隆因其對離散數學及相關領域的深遠影響而獲得沃爾夫獎。他的開創性貢獻包括組合數學、圖論和理論資訊科學領域的巧妙技術發展，以及這些領域以及解析數論、組合幾何學和資訊論（information theory）中長期存在問題的解決。

阿隆 1956 年出生於以色列海法，是普林斯頓大學數學教授、臺拉維夫大學數學和資訊科學鮑姆里特（Baumritter）名譽教授，也是全球最有影響力的數學家之一。他的研究和發展改變了該領域的面貌，創造了新概念和原創方法，並對離散數學、資訊論、圖論及其在資訊科學理論中的應用的理論研究及其應用的發展做出了巨大貢獻。

阿隆從小就對數學感興趣，被數學的客觀性和對絕對真理的追求所吸引。在父母和數學老師的鼓勵下，阿隆追尋自己的熱情，鑽研數學並參加數學競賽。1983 年，他在以色列理工學院（Technion）數學系畢業後，繼續在耶路撒冷希伯來大學（Hebrew University of Jerusalem）分別於 1979 年和 1980 年取得碩士和博士學位，並在 MIT、哈佛大學、普林斯頓高等研究所、IBM 阿爾馬登（Almaden）研究中心、貝爾實驗室和微軟研究院等多家研究機構擔任客座研究員。他於 1985 年加入臺拉維夫大學，1999 ～ 2000 年擔任數學科學學院院長，從臺拉維夫退休後，於 2018 年搬到普林斯頓工作至今，並指導許多博士生。他是十多本國際專業期刊的編輯委員會成員，並在許多會議上發表過受邀演講。他曾擔任 2006 年在馬德里舉辦的世界數學家大會（ICM）科學委員會主席，也是全球多個著名獎項委員會的成員。他發表了六百多篇研究論文和一本著作。他是世界上最多產的數學家之一，發表了數百篇文章，並培養了許多數學和資訊科學的研究生。

阿隆。（維基，Nurit Alon 攝）

阿隆對數學的貢獻廣泛，影響了理論與應用科學的許多相關領域。他與他的合作者建立了圖的擴展特性與其譜特性之間的緊密聯繫，並發現了擴展器


（expander）在組合學和理論資訊科學中的許多應用。他的成果激勵了大量的進一步工作，並在該領域後續的廣泛工作中被引用。在相關的工作中，他率先將譜方法應用於演算法問題的研究。阿隆證明了組合零點定理（Combinatorial Nullstellensatz，1995），這是一種強大的代數技術，在圖論、組合學和堆疊數論（additive number theory）中都有非常重要的應用，包括四色定理（Four-Color Theorem）的擴展。他與納坦森（Melvyn Nathanson）和魯札（Imre Ruzsa）在 1996 年一起推廣了柯西／戴文波特定理（Cauchy-Davenport Theorem）。1992 年與克萊特曼（Daniel Kleitman）的共同研究中，解決了哈德維格（Hugo Hadwiger）和德布倫納（Hans Debrunner）在 1957 年所提出的組合幾何問題，證明了海利定理（Helly's Theorem）的深遠推廣。這個方法已被證明是非常有影響力的，在最近的書籍和關於這個主題的綜述文章中都有所描述。1998 年推翻了夏農（Claude Shannon）在 1956 年提出的猜想，證明了一個令人驚訝的事實，即兩個通道的不相交連集的夏農容量（Shannon capacity）可以比它們的容量之和大很多，甚至比這個容量之和的任何固定冪次大很多。

阿隆在組合學機率方法的發展中扮演了重要的角色，他與史賓塞（Joel Spencer）合著的書《機率方法》（*The Probabilistic Method*，Wiley，2016 年第四版）是該領域無可爭議的領先著作。他與尤斯特（Raphael Yuster）和茨威克（Uri Zwick）在 1995 年共同開發的色碼方法（color-coding method）在其他幾個領域得到了應用，包括固定參數易處理性理論（theory of fixed parameter tractability）和生物資訊學（bioinformatics）。他與馬蒂亞斯（Yossi Matias）和塞格狄（Mario Szegedy）1999 年的合作啟動了串流演算法（streaming algorithm）的研究，研究資料流的哪些統計屬性可以動態取樣和估計。這確實創建了串流和速寫演算法（streaming and sketching algorithm）的新興活躍領域，並有許多的理論和應用。

阿隆與他的合作者在 1994 年開發了塞邁雷迪（Endre Szemerédi，匈牙利數學家，他主要的研究領域為組合數學與理論計算機科學，他是 2012 年阿貝爾獎得主）正則性引理的演算法版本，發現了它與格羅騰迪克的經典不等式之間的關係，並利用它解決了密集圖（dense graph）的屬性測試理論（theory of property testing）中所有主要的未解問題。這引起了廣泛的研究，並在洛瓦茲（László Lovász，匈牙利數學家，他主要的研究領域為組合數學，他是 1999 年沃爾夫獎、2010 年京都獎和 2021 年阿貝爾獎的得主）及其合作者的收斂圖序列理論的後續發展中扮演了重要角色。

阿隆一些最有影響力的研究工作涉及「擴展圖」。這些是具有強連通性（strong connectivity）的稀疏網路。它們最初被認為是建立經濟且有韌性的網路（如電話或電腦）的一種方式，並在資訊科學、設計演算法、糾錯碼、偽隨機生成器（pseudorandom generator）等領域得到了廣泛的應用。阿隆與米爾曼（Vitali Milman）一起，在圖的擴展性質與其「譜」性質之間建立了緊密的聯繫，讓人想起經典力學和量子力學之間的關係，並發現了擴展器在組合學和理論資訊科學中的大量應用。阿隆的結果激勵了大量的進一步工作，並且基本上在這個領域所有後續的廣泛工作中都被引用。

阿隆因「對離散數學和模型理論的傑出貢獻，特別是與代數幾何、拓樸和計算機科學的相互影響」而獲頒 2022 年度的邵逸夫數學獎。（編輯部）

# 2024 年自然界質數的黃金時刻


至少從古希臘時代起，對質數的研究已有二千多年的歷史，在歐幾里得的《幾何原本》的第九卷的命題 14 證明了算數基本定理，以及命題 20 證明了質數有無窮多個。一般群眾或許會好奇質數這觀念到底是被創造的還是被發現的？

2024 年 4 月下旬到 2024 年 6 月間，一個歷史性的罕見自然現象在美國的東岸和中西部地區「響」亮發生，從馬里蘭往西到愛荷華，往南到阿肯色、阿拉巴馬、喬治亞北部、南、北卡羅萊納和維吉尼亞等，影響的範圍涵蓋了 17 州。這裡的事件指的是週期蟬屬（學名：Magicicada）中分布區域最大的「19 號群」（Brood XIX）的 13 年蟬與「13 號群」（Brood XIII）的 17 年蟬同時破土而出。在這短暫的數周內達數千億到上兆大批兩類不同的週期蟬成蟲群竭盡全力發出如汽機車駛過的 80 至 100 分貝蟬鳴求偶，繼而交配並產卵，啟動下一代的周期蟬繁衍與生長周期。上一次發生這自然現象奇景是 13 與 17 的最小公倍數 221 年前的 1803 年，當時還是第三任總統傑佛遜（Thomas Jefferson）當政，歐洲拿破崙稱帝的前一年，中國則是清朝嘉慶八年。

全世界大約有 4,000 多種蟬，只有 9 種會同步週期性出現。但生命週期性演化的假設一般分為兩類：第一類周期性是因冰河的週期所形成的；第二類是周期性是由捕食壓力所形成。然而，這兩種解釋似乎都不夠充分 —— 生活在溫帶地區的大多數昆蟲物種都生活在受冰河作用影響的地方，但卻很少有週期性的，而且所有昆蟲物種都面臨捕食者的壓力，但卻很少有週期性的。冰河作用及／或捕食顯然不足以解釋生命周期性的演化史，否則周期性會更常見。顯然，在這些不尋常昆蟲的演化過程中，還有其他一些尚未為人所知的因素。

美國東部的 13 年和 17 年週期蟬似乎是獨一無二的，是最不尋常的昆蟲之一，具有長生命週期、罕見、週期性的大規模出現、引人注目的外觀和吵鬧的行為。

大約一萬到兩萬年前，當冰川從現在的美國地區退縮時，週期性的蟬充滿了東部森林。目前仍存在 12 個 17 年周期的群體和 3 個 13 年周期的群體。田野調查與基因檢測定位證據表明北美中部大片地區的 13 年周期蟬是 17 年周期蟬的後代，它們的生命週期長度變為 13 年，而生命週期的演化，與氣候相關，17 年周期蟬群組分布比 13 年周期蟬群組更北，幼年延長4年可能有利於在較冷的北方環境中生存。

但是，為什麼是 13 或 17 呢？而不是 7 或 11 其它質數數，甚至其他非質數周期呢？任何以蟬為食的掠食者，不論是狐狸、松鼠、蝙蝠或鳥類，都會在吃光該區域所有昆蟲之前先吃飽，留下許多倖存者，這是所謂的「捕食者飽和效應」（predator-satiation），而捕食者的數量無法因應而增加，因為蟬週期每 13 或 17 年才有一次在地面上作為食物的機會。如果蟬能夠在其捕食者處於休眠狀態時從地裡鑽出來，那麼它就有最大的生存機會。因此，最有機會生存的蟬將是那些設法避免與掠食者同時出現的蟬。事實證明，避免週期性掠奪者的最佳方法是進入持續質數年的生命週期。還有，13 與 17 的質數可避免與其他週期蟬同一年出現，造成相互爭鬥或雜交而減損自己的族群。話又說回來，如果大多數蟬的生命週期都在 1 到 20 年之間，又這區間包含非典型的高密度質數。因此，13 或 17 本身可能不那麼令人意外了。

儘管週期性蟬更喜歡森林邊緣並在郊區繁衍生息，但它們無法在森林砍伐中生存或在沒有樹木的地區成功繁殖。目前仍不清楚蟬是否能夠像人類改變環境一樣繼續進化。研究人員需要詳細的高品質數據來追蹤蟬隨時間的分佈。（編輯部）