# 一段关于好奇心与现实意义的人文故事

**Claire Burrin（苏黎世大学）**

数学正在发生变化。计算机能够验证证明、检查计算，并探索复杂结构，这些任务曾经会让人类不堪重负。尽管如此，人类的创造力仍不可替代：我们提出问题，并想象各种可能性。这种合作关系正在改变研究，也对教学产生了影响。

计算机能够进行计算并检查证明，但理解、质疑和验证的责任仍在我们肩上。数学思维有助于区分可靠知识与单纯的输出。要确保我们日益依赖黑箱（计算机、算法、人工智能）能够增强而非削弱我们的智识判断力，这种严谨的学科素养不可或缺。因此，我们将越来越多地承担起引导学生解读输出、提出有意义的问题，并欣赏数学的概念性与创造性一面的责任。

数学家为何研究某些问题，而不研究另一些问题？最初是什么问题激发了他们的研究？抽象的理念有时在数百年后会如何塑造我们所生活的世界？数字安全、数据传输、压缩和数学建模，都会让人想到这些问题。

当然，其他科学也有类似的发展轨迹。物理学家可能会提到量子力学：它曾纯粹是理论研究，如今却已成为半导体和激光器领域的核心。化学家则可能会提到元素周期表，如今它已成为药物设计和材料领域的基础。由好奇心驱动的研究，正是悄然孕育明日突破之处。让学生——下一代——清楚地认识到这一点，也是优质数学教育的使命之一。

我想用几个轶事来阐释这些想法，讲讲一种对我自己的研究至关重要的数学对象：格。

## 从巴比伦到数字安全

每当我们发送电子邮件或在线使用信用卡时，都会依靠密码协议来保障数据安全。互联网安全的支柱之一是 RSA算法，其原理在每一门代数课程中都会讲授：每个整数都能唯一地分解为素数的乘积——这就是所谓的算术基本定理。

人们对因数分解的着迷由来已久。距今近四千年的古巴比伦尼亚泥板上，记载着精密的倒数表和乘积表，暗示当时的人们已初步理解数字如何分解为因数并组合起来。亚里士多德曾思考那些无法再被分解的数，即素数。实际上，素数就像数字的原子，是构成所有整数的简单积木。

将两个大质数相乘很容易，计算机几毫秒就能完成。然而，逆向这一过程、将乘积重新分解为质数，则完全是另一回事：一旦质数达到几百位，已知的最佳算法就需要以指数时间解决这一问题。

现代安全建立在这样一个假设之上：对于计算机而言，这类问题将始终很难解决。然而，自20世纪90年代以来，我们就知道，量子计算机原则上能够更高效地分解整数，从而使 RSA 及类似协议失效。尽管制造量子计算机仍是一项巨大的技术挑战，但围绕它的不确定性已加速了后量子密码学的竞赛。在最有前景的候选方案中，我们发现了基于格的协议。

简单来说，格就是延伸于空间中的规则点阵。这个定义可以向线性代数专业的学生解释。选取一组

线性无关向量 $v_1, v_2, \ldots, v_n$ in $\mathrm{R}^n$，并取所有可能的整数线性组合

$$\mathbb{Z}v_1 + \mathbb{Z}v_2 + \ldots + \mathbb{Z}v_n$$

这些向量构成了一个格：一种有序结构，可以存在于任意维度。

与基于格的密码学相关的最简单、也最著名的困难问题是最短向量问题（SVP）：给定一个格，找出其中长度最短的非零向量。在二维或三维空间中，这很容易：只要看一眼就行。但在数千甚至数百万维的空间里，基向量可能指向许多奇特的方向，因此极难预测哪种整数线性组合能得到最短的向量。找到它，就像是在多维草堆中寻找那根 proverbial 针。

早期的基础加密协议只需依赖素数这一基本概念，而如今，要保障最强大的协议，运用的则是高阶现代数论。例如，今年夏天，我在莱迪亚布勒雷的 SwissMAP 研究站共同组织的一场研讨会上，公布了一项关于 SVP 的新稳健性结果，该结果与数论中的深层问题有关，例如广义黎曼猜想。

**维数灾难**

科学家之间流传着这样一个笑话：工程师问数学家："你怎么想象十一维空间？"数学家耸耸肩："我想象一个 n 维空间，然后令 n 等于十一。"数学常常被指责过于艰深晦涩！但在信息时代的应用中，处理极高维度的数据其实是常态。机器学习算法将数据作为向量，在拥有数百万个坐标的空间中进行处理。搜索引擎对网页进行排名时，会操作庞大的矩阵。事实上，搜索引擎谷歌的名字就源自古戈尔[2] $10^{100}$，这个词用来表示一个大得难以想象的数字，远远超过可观测宇宙中估计的原子总数。

由此可见，为十一维乃至十亿维空间构建图景是有意义的。事实上，高维几何的表现方式往往有悖于我们对日常二维、三维空间的直觉。例如，在高维立方体中，大部分体积并不集中在中心，而是聚集在角落附近，这与我们在低维空间中观察到的情况恰恰相反。随着维度增加，许多问题的复杂度也会呈指数级增长。要理解这一点，不妨想象用间距为 0.1 的均匀点来覆盖单位正方形——这些点就是格点。为此我们需要一百个点；但要在九维空间中做到同样的事，则需要十亿个点。

另一个引人注目的例子是球体堆积问题：如何在空间中以最高效的方式排列大小相同的球体？[3] 在三维空间中，最理想的排列方式正如你所料：炮弹堆积，也就是将炮弹以金字塔式堆叠起来。但在（大多数）高维空间中，我们甚至无法想象最密堆积会是什么样子。这里我们再次看到，一个抽象问题也会带来非常具体的影响；在这个例子中，影响涉及编码理论。设想在噪声信道中传输一条消息。每条消息都可以表示为高维空间中的一个点，而噪声会使这个点发生轻微偏移。以一个球体包围每个点，表示可容忍的噪声范围，就仍然能够正确解码接收信号。于是，目标就是尽可能密集地堆积这些球体，从而可靠地传输更多信息。

尽管过去几年取得了令人振奋的快速进展，但人们对高维空间中的球体堆积问题仍知之甚少。今年早些时候，魏茨曼科学研究所的 Boaz Klartag——目前正在苏黎世联邦理工学院进行秋季学期访问——宣布了一项基于

1参见https://swissmaprs.ch/。2 "古戈尔"一词本质上是一个杜撰的名称，其词源颇有争议，相关说明可见 Wikipedia.org/wiki/Googol，这与通俗数学这一主题形成了有趣的联系。3参见爱因斯坦讲座：Maryna Viazovska——球体堆积问题。

几何学与概率论相结合的非凡成果：存在一种高维格球体堆积，其密度远高于此前已知的任何结果。我们能否给出具有这一性质的具体格？这些构造能否改进编码协议或其他技术？

**证明与确定性**

抽象思维并非数学独有；物理学家、工程师或计算机科学家都各自发展出概念推理的方式。数学有一个本质上的不同之处：它的凭据不是实验，而是证明。

证明是一条严谨的推理链，表明某个命题必然为真。与其他科学不同，已经证明的定理不会被推翻；其真理性是永恒的。这一传统可以追溯到古希腊，在《几何原本》（公元前300年）中初具形态，并延续至今，持续界定着数学实践。其重要性如此之高，以至于数学家的职业成就要看他们证明了什么样的定理、证明了多少定理，以及推理有多优雅。

开普勒猜想的解决历程很好地展示了数学研究实践正在发生的变化。该猜想认为，三维空间中的炮弹堆积是球体最有效的排列方式。如果球体必须沿着格排列，那么开普勒猜想很容易证明。但对这种刚性排列稍作扰动，能否形成空间利用效率更高的堆积？几个世纪以来，凭直觉始终无法解决这个问题。

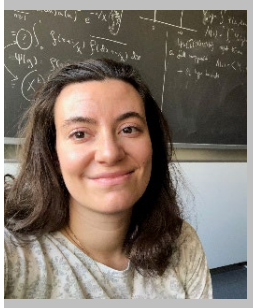
直到20$^{th}$ 世纪计算机的出现，这一构想才终于得以实现。拉斯洛·费耶什·托特在20世纪50年代指出，原则上可以将开普勒猜想归结为有限次、但数量极其庞大的计算。20世纪90年代初，托马斯·黑尔斯和他的学生塞缪尔·弗格森实施了这一方案：通过穷举所有情形，以计算机辅助证明开普勒猜想[4]。最终成果是一份不到300页的手稿，另附40000行代码，求解了约100000个线性规划问题。

当时，评估正确性意味着 painstakingly 手工检查每一个细节。一个由十二位专家组成的评审团花了五年时间审查这项工作，最终宣布其正确性的把握为“99%”……这一裁决对任何数学家来说都难免令人沮丧。二十年后，原论文又增补了一份形式化的、也就是可由计算机验证的证明。

证明的性质或许正在演变，但数学依然如初：是一门源于好奇的学科。每个定理都始于一个问题，有时是天真的，有时是纯理论性的，由某个想要理解某种形式的对称性或某种模式的形状的人提出。好奇心激发理解，而理解又促成应用——其中一些应用是我们目前还无法想象的。

苏黎世大学，数学研究所，Winterthurerstrasse 190，

电子邮箱：claire.burrin@math.uzh.ch网站：



**Claire Burrin**，ETH理学博士，她此前曾任新泽西州罗格斯大学的希尔助理教授、苏黎世

照片来源：私人

[4]关于海尔斯证明开普勒猜想的参考资料包括发表于数学年刊（https://annals.math.princeton.edu/wp-content/uploads/annals-v162-n3-p01.pdf），以及他在美国数学学会会刊上的一篇更易读的综述（https://www.ams.org/notices/200004/fea-hales.pdf）。