数学有用

田刚

提到数学这个学科，很多人会觉得很抽象，难以理解。我常会遭遇这样的情形，当别人问起我是做什么的，我说是做数学的，他们就会一笑说，好，好。边说边离开了。也就是说，没有话题再继续聊下去了。确实在很多人看来，数学似乎只是一些聪明人研究的学问或者只是数学高手之间的过招，数学所探讨的很多问题太过于抽象，与现实没有太多关联。其实不然。数学在我们生活中到处都是，与我们密切相关，只不过我们有时候不会注意到它而已。

数学源远流长

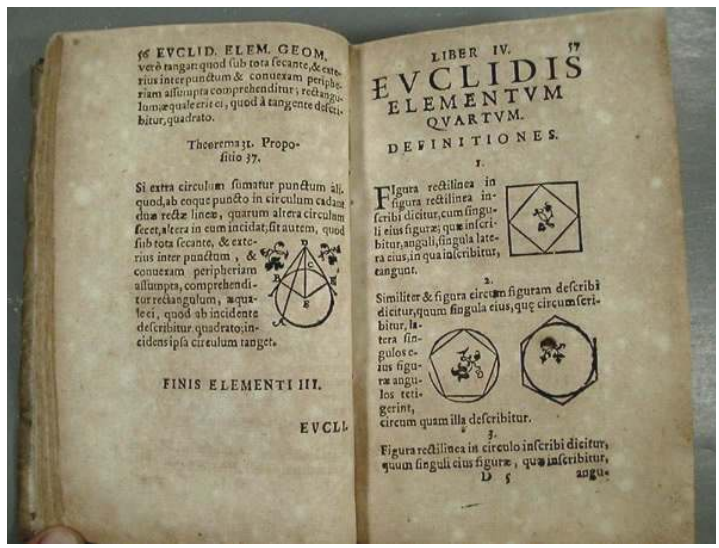
数学作为自然科学之母，有着非常悠久的历史。在早期，数学主要是用于商贸、土地测量、绣制及日历等。由于实际的需要，到公元前 3000 年左右，在古巴比伦、古埃及以及中国相继出现了算术、代数和几何等学科，这些学科较为复杂，主要用于税收、商业计算、建筑和天文等领域。

作为独立学科，数学的系统研究起自于古希腊，大约在公元前 600 年左右。虽然数学所涉及的对象跟实际问题密切相关，但数学却又是一个抽象的东西。它同生活中的实物有关，但又不是来自于某一具体事物。数学，尤其是几何学，在古希腊具有很

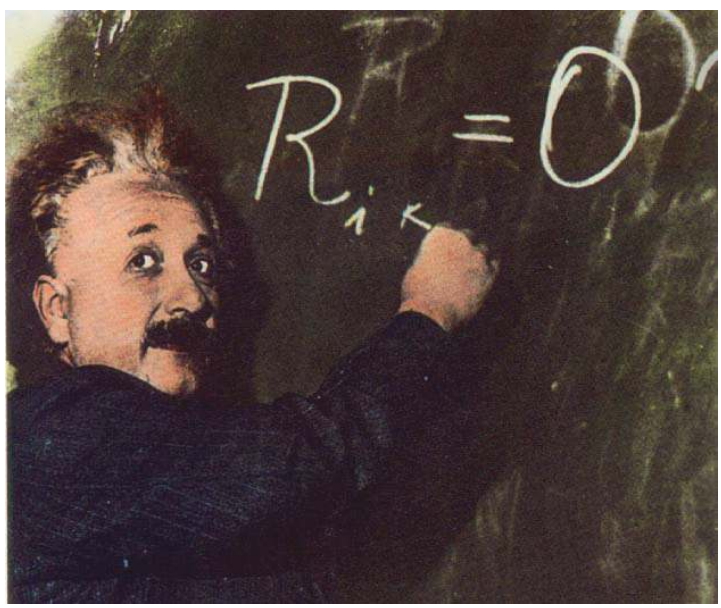
高的地位，学习数学被认为是寻求真理的一个最佳途径。据称，古希腊的著名哲学家柏拉图曾说过：上帝就是几何学家。西方语言中的数学一词，如英文 Mathematics，源自古希腊语，有学习、学问、科学的意思。这些都说明在古希腊文化中数学的地位是非常高的。

数学追求的是抽象美和终极真理。它逻辑性强并以兴趣和好奇心为首要驱动，令很多人常常疑惑它到底有没有用。1883 年 8 月，美国著名物理学家亨利·奥古斯特·罗兰（Henry Augustus Rowland）做了题为“为纯科学呼吁”的演讲。罗兰说“假如我们停止科学的追求而只关注科学的应用，我们很快就会变成中国人那样，他们在很多朝代以来都没有在科学上取得什么大的进步，因为他们只满足于科学的应用，却从来没有追问过他们所做事情中的原理”。罗兰的话非常尖锐，刺到了我们的痛处，却也指出了诸如数学这样的纯基础科学的重要性。如果只满足于现实的技术引进和复制，怠于原创性研发，忽视基础科学研究，那么我们将永远不会在科技方面取得真正的进步。以数学为代表的基础科学，就像是一个强大的引擎，它的有效运转将带动与之相关的科学研究和具体技术的巨大发展。这样的例子在科学发展的历史中比比皆是。

欧几里得是生活在公元前 300 年左右的希腊几何学家，他的巨著《几何原本》，是



欧几里得的《几何原本》



爱因斯坦的黎曼几何

第一本系统研究几何的书。全书分 13 卷，有 5 条“公理”或“公设”、23 个定义和 467 个命题。欧几里得用公理化方法建立起来几何学，是数学演绎体系的最早典范。在之后的 2000 多年间，这一严格的思维形式，不仅用于数学，也用于其他科学，甚至用于神学、哲学和伦理学中。自面世之后，《几何原本》历经多次翻译和修订，至今已有 1000 多种不同的版本，据说它的发行量曾仅次于《圣经》而位居第二。我想欧几里得当初研究的动机肯定不是任何实际应用，而是美的追求，真理的追求。后来事实证明，他的成果应用广泛，影响深远。

著名数学家黎曼是大名鼎鼎的德国数学家高斯的学生，他在 1851 年创立黎曼几何。黎曼引进了流形和度量的概念，证明曲率是度量的唯一内涵不变量，具有划时代的意义。

图灵和密码破译

黎曼几何是现代几何研究的基础，是研究生学习阶段的关键课程之一，在物理学和天文学等很多学科的研究当中有着许许多多的应用。1915 年，爱因斯坦创立了新的引力理论——广义相对论，也使用到了黎曼创立的几何。黎曼几何及其运算方法为广义相对论研究提供了有效的数学工具。在广义相对论中，宇宙一切物质的运动都可以用曲率来描述，引力场实际上就是一个弯曲的时空，而时空就是数学中的度量化的流形。

数学应用广泛

虽然许多数学问题来源于生活，有实际的现实需要，但基础数学研究的最初目的往往不是为了功利，而是纯学术性的，如欧几里得几何、黎曼几何的研究和发展，最后却意外获得特别的效果和重要的应用。这样的例子在近代也有很多。

数论是一个古老的纯数学分支，但在我们生活中有许多应用，特别是密码学。第二次世界大战期间，交战双方——德国、日本、英国，尤其是美国——都请了一批出色的数学家来从事加密和破译工作。其中，英国人图灵等优秀数学家利用数学工具破译了德军所用的密码体制“恩尼格玛”（enigma）。美国密码分析学家利用数论、群论等数学工具在1940年破译了日本战时所用的“紫密”（purple）。1942年日本突袭中途岛海战的失败，一个重要原因是美国破译了日本攻击中途岛的情报。1943 年 4 月，利用所破译的情报，美国还打下日本海军司令山本五十六的座机，成就了密码史上精彩的一页。

在今天的电子商务中，密码学中经典的 RSA 算法被广泛使用。这是由麻省理工学院研究人员在 1978 年公开推广的，其基本原理正是依赖于数论中的素数理论。RSA 算法的安全性是因为素数分解的困难。近十几年来，利用椭圆曲线的密码系统（ECC，Elliptic curve cryptography）已经越来越受到重视，因为椭圆曲线密码的安全性远高于 RSA 算法。椭圆曲线属代数曲线，与三次多项式紧密相关，这个领域的应用也是始自于纯粹数学研究。