一、现代数学

神秘的哥德巴赫猜想

多年以前一篇题为《哥德巴赫猜想》的报告文学发表后，让中国的老百姓认识了中国数学家陈景润，同时也知道了哥德巴赫猜想。这个猜想让世界许多国家的数学家呕心沥血。

哥德巴赫猜想是德国数学家哥德巴赫于1742年在给瑞士大数学家欧拉的一封信中提出的一个关于整数表示为素数之和的猜想。这个猜想经过250多年许多世界顶尖的数学家的努力，至今还没有最终解决。现在保持世界领先成果的是中国数学家陈景润的（1+2）。

哥德巴赫猜想说的是什么呢？它说明的是每一个不小于6的偶数可表示为两个奇素数之和。如果我们把一个大偶数可表示为一个素数和一个素因子的个数不超过P的整数之和的命题简记为（1+P）的话，哥德巴赫猜想则可简记为（1+1），即一个大的偶数可表为两个素数之和。

有数学家验证了对于不大于5×10^8的偶数哥德巴赫猜想是对的，所以只要证明对充分大的偶数哥德巴赫猜想是对的。对这个猜想的研究到20世纪20年代才出现重要的进展。1947年匈牙利数学家瑞尼证明了（1+P），但他无法给出P的上界，按他的方法计算将是个天文数字；1962年山东大学的潘

承洞院士独立地推出了关于算术数列中素数分布的一条中值定理，从而证明了（1+5），这个突破是至关重要的，因为中值定理的改进对猜想的证明是关键；随后王元院士、潘承洞院士和苏联数学家巴尔巴恩证明了（1+4）；1965年苏联数学家维诺格拉朵夫又推出（1+3）；1966年陈景润院士在《科学通报》上声明他已证明（1+2），并于1973年将证明的全文发表在《中国科学》上。从上可见，试图解决哥德巴赫猜想的过程真是个世界级数学竞赛，而且这个竞赛还没有结束。

数学的证明是建立在严密的逻辑推演之上的，而不是可通过描述性的说明来完成。哥德巴赫猜想的叙述是简单明了的，但从解决这个猜想的历史来看，它无疑是个世界级难题，要最终解决这个猜想需要现代数学的手段。谁来走（1+2）到（1+1）这最后的一步呢？新世纪的我们在等待着。

◆ 极限中的微积分

微积分是数学史上最伟大的创造之一，是由英国的牛顿和德国的莱布尼兹于17世纪创造的。牛顿的出发点是变化率，而莱布尼兹的则是微分。创立微积分的动力来自于17世纪的主要的科学问题：

如：甲求运动物体的瞬时速度；乙求曲线的切线；丙求一个物体对另一个物体的引力；丁求曲线所围的面积等。

甲和乙、丙和丁看似毫不相干的问题，在数学上却发现是相同的，前者就是求导数，后者则可归为积分——反微分。数学就是从一些特殊的问题中提炼出来，研究其普遍规律的，而这种普遍性使得数学具有广泛的应用性，并渗透到各个领域。

我们来计算半径为1的圆的周长，请画个图想一想。这儿

有个简便的方法：在圆内画个内接正六边形，然后在正六边形每个边对应的弧的中点连接边的两端，画正十二边形，如此画下去，可以发现正边形的周边，越来越逼近圆周。可设想圆周长就是正边形的周边长的极限——这是微积分中的一个重要概念。在这个计算过程中，我们用了易测量的直线段来代替弧，这就是微分的思想：以直代曲。这样做显然会有误差，解决误差的办法，就是精细地、无限地做下去的极限。积分就是无限精细下去的“累加”，所以圆周长就是个积分值，它正是内接正边形的边长总和的极限。

微积分中的一个重要概念就是：函数在一点处的极限是函数值随自变量趋于一个确定的点时所趋于的那个惟一确定的数；导数是函数对自变量的变化率，即函数平均变化率的极限。微分是微积分中与导数密切相关的另一个重要的概念，在确定的一点 x_0 处任给一个增量 h，如果函数具有如下表示式：

$$f(x_0+h)-f(x_0)=Ah+\alpha(h)$$

其中 A 是个确定的数，$\alpha(h)$ 是一个较 h 趋于零速度更快地趋于零的量，那么 Ah 就是函数 $f(x)$ 在 x_0 处的微分 $y=f(x_0+h)$ 是个曲线，$y=Ah$ 是个线段，而 $\alpha(h)$ 就是误差。从导数的定义容易看出 A 就是 $f(x)$ 在 x_0 处的导数。如果我们把式中的 $\alpha(h)$ 扔掉，就得到微分在近似计算上的应用；积分是微分的逆运算，有关求和的问题可用它来计算；级数可以说明为无限个数按照一定的顺序逐个加起来的形式，这个形式可能有一个确定的和数，也可能没有，这是有限向无限在思想上的一个飞跃。

◆ 有精确边界的模糊数学

康德的经典集合论基于同一律、矛盾律和排中律这三大定律。也就是说，对于任何给定的集合，我们研究的对象要么属于这个集合，要么不属于这个集合，二者必居其一，且仅居其一。然而，在现实生活中，很多情况并不具有这种清晰性。例如“老人”、“高个子”、“高温”、“秃头”、“阴天”、“黄昏”等。

于是查德于 1965 年给出了“模糊集合”的概念。这一概念是相对于经典集合而提出的。我们可以回想一下什么是经典集合。通常地，一个集合被描述成某个论域 X 上的元素的总和，其中元素个数可以是有限的，可数的或连续的。对于给定的论域 X，则 X 上的集合 A 是有精确边界的，即任何的 $x \in X$，x 要么属于 A 要么不属于 A。这样的经典集合可由特征函数来描述，即特征函数值为 1 表示 $x \in A$，特征函数值为 0 表示 $x \notin A$。而模糊集合的定义为：设 X 为一个论域，则 X 上的模糊集合是指如下的有序对的集合：

$$A = \{ (x, \mu_A(x)) \mid x \in X \}$$

其中 $\mu_A(x)$ 称为 A 的隶属函数 U_{AO}；通常地，隶属函数是 X 到区间 [0, 1] 的一个映射。隶属函数 μ_A（x 越接近 1，说明 x 属于 A 的程度越高。如果区间 [0, 1] 退化成 {0, 1} 两点，则 μ_A（x）即是 A 的特征函数，而 A 就是我们熟知的经典集合。

模糊集合是模糊数学的基础。模糊数学是研究处理模糊现象的数学，其中模糊性是指事物的差异的中间过渡性所引起的划分上的“亦此亦彼”性。模糊数学的研究受到了越来越广泛

的重视，其应用范围已遍及理、工、农、医和社会科学等诸多领域，并已显示出巨大的力量。

引发金融革命的金融数学

金融数学是 20 世纪 90 年代起蓬勃发展的新兴边缘学科，在国际金融界和应用数学界受到高度重视。 1997 年 Nobel 经济学奖授予 Scholes 和 Merton，就是为了奖励他们在期权定价（如著名的 Black－Scholes 公式）等金融数学方面的贡献。

长期以来，由于金融市场的不确定性与高风险性，人们一直在探索利用各种因素正确评估资产风险和期权（或衍生证券）价格的有效方法。金融数学模型的建立，对金融市场风险分析、预测与监控有着非常重要的作用。 20 世纪 50 年代末 60 年代初，Markowitz 的投资组合的均值一方差理论与 Sharpe 的资本资产定价理论，开创了金融数学理论的先河，他们的理论引发了所谓的第一次“华尔街革命”。第二次“华尔街革命”是由 Black 和 Scholes 于 1973 年提出的衍生证券定价理论促成的。正是这两次“革命”构成了蓬勃发展的新学科——金融数学的主要内容；同时也是研究新型衍生证券设计的新学科——金融工程的理论基础。

在衍生证券定价理论中，最典型的是所谓欧式看涨期权的定价，通俗地说，此期权就是一份合约，合约双方在 $t=0$ 时刻商定一个执行合约，规定买方在给定的时刻 t （到期日）以执行价格买入卖方的一份股票，但只有买方有优先权，即在 T 时刻买方认为不合适，就可以放弃合约。显然，若该期权到期，则该期权的价值（亦即买方在 t 时刻获益）为股票市价与执行价格的差价的正部，这是一种只有到了 t 时刻才能确定其

真正获益大小的随机变量，称为或有债权，一般情形的或有债权的一个重要用途就是帮助各类投资者在风险迭起的生产和贸易活动中进行套期保值，以回避风险，它也构成了目前很流行的金融工程的主要数学基础。

利用金融数学技巧获得的期权定价理论，已被推广到其他金融问题的研究之中，如期货、债券、可转换债券、利率掉期、外汇汇率等，并广泛应用于包括公司债券、可变利率抵押、抵押贷款、保险和税法在内的金融证券和合同的广阔领域。该理论和方法不仅适用于证券市场的资产定价，也适应于证券市场的风险分析。它的应用已受到各国政府的重视，而且取得了很好的实效。

数学技术化的运筹学

运筹学是半个世纪以来发展兴起的新兴学科。学术界比较统一的观点认为运筹学起源于第二次世界大战期间英美等国军事部门成立的研究小组，就战争中的一些战略和战术研究而形成的理论和方法。在词汇的使用上欧洲习惯于 operational research，美国习惯于 poerations research。基于这样的背景，我们选用古人“运筹帷幄，决胜千里”这一寓意相似的“运筹”两字。

人们试图给运筹学下一些简单的定义，如：“运筹学是一种科学决策的方法”；“运筹学是依据给定目标和条件从候选方案中选择最佳或较佳的方法”等。无论如何，运筹学是一种数学技术，它通过给实际问题以优化目标、约束条件等的数学模型描述，以计算求解给决策者提供解决问题的方法和方案。运筹学主要内容包括：线性规划、非线性规划、整数规划、多目

标规划、动态规划、随机规划、组合最优化、对策论、网络优化和决策分析等。

作为一种数学技术，运筹学在军事上有着巨大的应用价值。在第二次世界大战英美两国海空军的雷达布置、轰炸机编队等有成功的应用。正因为如此，第二次世界大战后，运筹学无论从理论还是方法应用上都得到非常迅速的发展和完善。目前，军事领域仍然是应用的一个重点，诸如军队的后勤供给、作战方案等的管理。美国在海湾战争中成功的后勤管理充分说明这种技术的效率性。无论是在企业的发展计划、营销策略，还是物料管理、生产过程、质量控制中，都涉及运筹学问题。因此，管理科学中将运筹学方法视为基础技术，这无不说明运筹学的重要性。信息科学中的密码编译、计算的并行处理、通讯网络的控制、电力系统的稳定高效等等，无一不涉及到运筹学这门数学技术。因此，运筹学这门数学技术必将有较大的发展并通过成功的应用而带来更大的经济效益。

◈ 博大精深的数论

被称为“世界第八奇迹”的中国西安秦始皇兵马俑气势恢弘，面对这威武雄壮的众多方阵，任何人都可以想像当年“扫六合吞八荒”的秦兵的气势。真要点出秦兵确切总数，岂是易事？我国自古有“秦王暗点兵”奇法，例如：“秦兵列队，每列百人则余一人，九九人则余二人，百零一人则不足二人。问秦兵几何？”一报完情况秦王就心中有“数”了！数学王子高斯说过：“数学是科学的女皇，而数论是数学的女皇”，此话不虚。这可能是因为，数论的研究对象特别基本，问题特别神奇，意境特别深远；也是因为，数论在历史上常是推动数学发

展的原动力，随着数字计算机和数字通信为标志的信息时代的到来，数论，更显示出空前的重要性。大量数字化信息的传播、处理、储存和应用是知识经济时代的特征，数论及其关联的数学正是这一切的灵魂、基础和智囊。事实上，早在半个多世纪前的第二次世界大战中，盟国集合了一批优秀数论学家，破译德国密码，为二战胜利作出难以估量的贡献。这其中就包括计算机的鼻祖图灵，从而直接导致计算机的发明！数论不仅应用十分广泛、深层（例如从弦的振动，音乐理论，到现代物理，微观粒子等各领域，常发生出人意料的应用），尤其是它的理论优美深刻，直通向最现代前沿的数学。数论起源很早，自古至 19 世纪初的阶段，常称“初等数论”。这包括上述“秦王暗点兵”、同余式、二次剩余等。这部分历史久远，影响广泛，留下了丰富有趣的问题，例如费尔马大定理、哥德巴赫猜想等等。微积分和复变函数论发展以后，应用于数论，产生了“解析数论”,例如 L 函数等，可解决算术数列中存在无穷个素数等问题。数论中有些问题必须由解析方法才能提出或解决。我国华罗庚、王元、陈景润等在哥德巴赫、华林等解析数论问题上取得世界领先成就。随着两个世纪以来，尤其是 20 世纪以来数学的巨大发展，特别是代数、代数几何等的巨大发展，现代的数论已经高度发展融合，远不只是研究整数了，它还研究代数数论、研究代数函数、算术代数几何、椭圆曲线、模形式、局部域、表示论、超越数等等。现代数论的方法也已是代数、解析几何等的高度综合，融合着数学最现代的思想和成就。

源于博弈的概率论

假如甲、乙两人赌技相同，各出赌注 100 元。约定：谁先胜三局，则谁就拿走全部 200 元。现已赌了三局，甲二胜一负而因故要中止赌博，问这 200元要如何分，才算分平？这是一个典型的博弈问题，每局赌博的胜负都要凭机会，也就是我们所说的概率。这类机会游戏的解决需要用到概率论的知识。

概率论的起源正是来自于赌博与靠运气取胜的游戏，大约在 17 世纪，欧洲的数学家们就开始探索用古典概率来解决赌博中提出的一些问题。目前，概率论已成为研究自然界、人类社会及技术过程中大量随机现象中的规律性的一门重要的数学分支。在一定的条件下，人们能准确地预言将发生什么。例如，一初速度为零的物体从某一高度做自由落体运动，则该物体下落的距离 $s=\frac{1}{2}gt^2$（其中，g 为重力加速度，t 为时间）。但在实际情形中，人们会发现实验的结果经常会与上述结论有所出入，原因在于此结论仅适用于在真空状态下进行的试验，从而导致了随机误差的产生。因此，在一高精度的试验中，就需要把不确定的因素考虑进去，此时的模型便变成了一个随机模型 $s=\frac{1}{2}gt^2+\varepsilon$，其中 ε 表示该模型的随机因素，而概率论正是研究此类现象的统计规律性的。

正如上面所讲的那样，目前，概率论的理论与方法已经卓有成效地广泛应用于各个科学技术领域中。在实际应用中，有着广泛的重要意义。概率论的目的就是为了帮助人们透过表面的偶然性找出内在的必然规律，并以概率的形式来描述这些规律。

目前，概率论的主要研究内容大致可分为极限理论、独立增量过程、马尔可夫过程、点过程、随机微分方程、随机分析等，它还是数理统计学的基础。概率论的应用几乎涉及生活中的所有领域，如气象预报、天文观测、通讯工程、计算机科学、管理科学、生物医学、运筹决策、经济分析、金融理论、人口理论、可靠性与质量控制等许许多多领域都已离不开用概率论的理论和方法来建立各种数学模型。

神奇的代数

世界是连续的，还是离散的？一根铜棒，一束光线，看起来都是连续不断的。但古希腊的德谟克利特就认为，万物都是离散的，由极小的原子组成，甚至包括灵魂。现在我们确实已知道，“月魂日魄”的光是由一个个的“光子”组成的，就连时间和空间似乎也是量子化的。代数（学）就是专门研究离散对象的数学，它是现代数学的三大支柱之一（另两个为分析与几何）。代数从19世纪以来有惊人的发展，带动了整个数学的现代化。随着信息时代的到来，计算机，信息都是数字化（离散化）的，甚至电视机，摄像机、照相机都在数字化。知识经济有人也称为数字经济。这一切的背后的科学基础，就是数学，尤其是专门研究离散对象的代数。现在的代数已经是外延极广的综合科学，不是指中学的代数，那只是代数的萌芽。代数发端于“用符号代替数”，后来发展到以符号代替各种事物，乃至于概念、作用、映射。代数的基础研究各种代数系统，即定义了运算的抽象集合。主要的代数系统有：群、环、域、模、格、各种空间等。“群”是最基本的系统，就是有一个运算的集合。

而“环”就是有一又半个运算的集合（所谓半个运算是指它可能无逆运算）。

代数以如下成果光照历史：解决了困扰人类 2000 多年的古希腊三大历史名题（三等分角，化圆为方，立方倍积），解决了五次方程不可解问题，画正 17 边形，破译密码等问题。此外，代数还研究更抽象的“范畴”函子等。与代数相关的数学有：线性代数、抽象代数、代数数论、代数几何、代数拓扑、同调代数、拓扑代数、表示论、泛函分析、代数函数论等等。在我们人类的生活中，神奇的代数发挥着神奇的作用。

◆ 图形漂亮的分形

分形数学是用来研究不规则集的数学，这里的不规则是相对于经典的几何图形的微积分而言的，其研究的对象——不规则集就是分形。

下面我们画一个图形，其步骤是简单的。给定一直线段，将中间的 1/3 部分用其上的等边三角形的另外两条边来替代，而得到一条由四条线段组成的折线，对此折线上的每条线段作上述同样的替换，如此无穷下去，就生成一个称为冯·科赫曲线的图形。

冯·科赫曲线处处不具有切线，因为曲线的尖点处没有切线；取出曲线的任一部分将其按倍数放大，将得到整个曲线。即具有自相似性；按作图过程来计算曲线的长度，会发现曲线具有无穷长度，这不符合常规。

分形这个新词是曼德尔布罗特引入的，意思是细片、破碎及分数等。到目前分形还没有一个确切的数学定义，曼德尔布罗特曾给出过几个定义，但都不够精确、全面。现在人们更接

受英国数学家法尔科内的观点，像生物学家用生命的特征，如新陈代谢、繁殖能力等来定义生命那样，用分形的特性定义分形如下：它具有精细结构；整体和局部不规则，而又不能用传统的几何语言来描述；具有某种可能是近似的或统计的自相似形式；在某种方式下定义的“分形维数”通常大于其拓扑维数，可以用非常简单的方法来确定，迭代或递归就可能产生。

分形的维数是分形数学的主要研究内容之一，它能在某种程度上定量刻画分形的复杂性、充满空间程度以及包含了分形的几何性质的许多信息。

分形理论已经应用于自然科学的许多领域，如自然图形的模拟、力学中的断裂与破坏、计算机编码压缩等不胜枚举。分形这个过去被认为“病态”甚至认为在研究上可以忽略的不光滑、不规则的图形，事实上在自然界中随处可见，如海岸线、地表面形状、人体毛血管的分布等等。但自然界中的分形与数学中的分形是有区别的，就象在自然界中没有真正的直线那样。

分形的计算机图形很漂亮，即使不懂数学知识也不影响对它的欣赏。

◆ 普适的费根鲍姆常数

费根鲍姆在数学研究过程中发现，与分岔相对应的参数值之间具有一种几何收敛的规律，参数值间距存在一种比率，随着分岔的增加此比率趋向于一常数 δ：

$$\delta=\lim_{n\to\infty}\frac{\mu n+1\ \mu n}{\mu n+2\ \mu n+1}=4.6692016090\cdots\cdots$$

δ 即为费根鲍姆第一常数。它反映的是各分岔点之间距离按特

定的比例缩小着，这个缩小比例趋向的极限是 δ。

费根鲍姆还发现了倍周期分岔过程中的另一个常数 α：

$$\alpha=\lim_{n\to\Delta n+1}\frac{\Delta n}{}=2.502907875$$

α 为费根鲍姆第二常数，它意味着在倍周期分岔的过程中，其几何图像具有无穷自嵌的几何结构，同一种行为在越来越小的尺度上重复出现。与分岔有关的几何特征，在每次分岔后按比例缩小，这个缩小比例趋向的极限就是 α。

费根鲍姆常数 δ 和 α 与人们早已熟悉的 e 和 π 一样，都是自然界的普适常数。它们与具体的迭代形式无关，一切可以经过倍周期分岔而走向混沌的函数，不论是正弦函数还是抛物线函数，均可导出。这表示着一种更为深刻的东西——一种统一的规律在起作用。

◆ 解释飞跃的突变理论

在自然现象和社会现象中，有许多突变和飞跃的过程，飞跃造成的不连续性把系统的行为空间变成不可微的。例如，水突然沸腾，冰突然溶化，火山爆发，某地突然地震，病人突然死亡等。这种由渐变、量变发展为突变、质变的过程，用微积分就不能描述。为了描述各种飞跃和不连续过程，数学上建立了一种关于突变现象的一般性数学理论。1972 年法国数学家雷内·托姆在《结构的稳定性和形态发生学》一书中，明确地阐明了突变理论，宣告了突变理论的诞生。

突变理论以拓扑学为工具，结构稳定性理论为基础，提出了一条新的判别突变、飞跃的原则。这就是说：在严格控制条件下，如果质变中经历的中间过渡态是不稳定的，那么它就是

一个突变、飞跃过程；如果中间过渡态是稳定的，那么它就是一个渐变过程。例如拆一堵墙，如果从上面开始一块块地把砖头拆下来，整个过程就是结构稳定的渐变过程。如果从底脚开始拆墙，拆到一定程度，就会破坏墙的结构稳定性，墙就会哗啦一声倒塌下来，这种结构不稳定性就是突变、飞跃过程。突变理论用势函数的洼的存在表示稳定，势函数的洼取消表示不稳定。

托姆的突变理论，用数学工具描述系统状态的飞跃，给出系统处于稳定态的参数区域，以及系统处于不稳定态时的参数区域。参数变化时，系统状态也随着变化，当参数通过某些特定位置时，状态就会出现突变。

突变理论把社会现象归结为某种量的突变问题，说明了人们施加控制因素影响社会状态是有一定条件的，只有在控制因素达到临界点之前，状态才是可以控制的。一旦带根本性的质变发生，它就表现为控制因素所无法控制的突变过程。用突变理论可以研究事物状态与控制因素之间的相互关系，以及稳定区域、非稳定区域、临界曲线的分布特点，研究突变的方向与幅度，设法对社会进行高层次的有效控制。

◈ 天才的不可判定性定理

1931年，哥德尔出版了他的书《数学原理及有关系统中的形式不可判定命题》，其中包含了他的所谓不可判定性定理。

哥德尔证明了要想创立一个完全的、相容的数学体系是一件不可能做到的事情。他的思想可以浓缩为两个命题：

第一不可判定性定理：如果公理集合论是相容的，那么存在既不能证明又不能否定的定理。

第二不可判定性定理：不存在能证明公理系统是相容的构造性过程。

本质上，哥德尔的第一个定理说，不管使用哪一套公理，总有数学家不能回答的问题存在——完全性是不可能达到的。更糟的是，第二个定理说，数学家永远不可能确定他们选择的公理不会导致矛盾出现——相容性永远不可能证明。

虽然哥德尔的第二个定理说，不可能证明公理系统是相容的，但这并不一定意味着它们是不相容的。在许多数学家的心目中，他们仍然相信他们的数学依旧是相容的，只是用他们的思想无法证明这一点而已。许多数学家相信哥德尔的不可判定命题只有在数学的最不引人注目和最极端之处才可能发现，因而可能永远也不会碰到。可是到了 1963 年，哥德尔的理论上的恶梦竟然变成了有血有肉的事实。

斯坦福大学的一位 29 岁的数学家保罗·科恩发展了一种可以检验给定的命题是不是不可判定的方法。这个方法只适用于少数非常特殊的情形。完成他的发现之后，科恩立即飞到普林斯顿，带着他的证明，希望由哥德尔本人来证实他的证明。

科恩证明了大卫·希尔伯特提出的数学中最重要的 23 个问题之一——连续统假设是不可判定的，这有点令人啼笑皆非。

哥德尔的工作，再加上科恩给出的不可判定的命题，给所有正在坚持尝试证明建立确定性数学大厦的工作带来毁灭性的打击。

◆ 历史悠久的费尔马大定理

费尔马大定理，起源于两千多年前，挑战人类 3 个多世纪，多次震惊全世界，耗尽人类众多最杰出大脑的精力，也让

千千万万业余者痴迷。终于在 1994 年被安德鲁·怀尔斯攻克。

古希腊的丢番图写过一本著名的“算术”，经历中世纪的愚昧黑暗到文艺复兴的时候，“算术”的残本重新被发现研究。1637年，法国业余大数学家费尔马在“算术”的关于勾股数问题的页边上，写下猜想： $a^n+b^n=c^n$ 是不可能的。此猜想后来就称为费尔马大定理。费尔马还写道“我对此有绝妙的证明，但此页边太窄写不下”。一般公认，他当时不可能有正确的证明。猜想提出后，经欧拉等数代天才努力， 200 年间只解决了 $n=3$、4、5、7 四种情形。历史的新转机发生在 1986 年夏，贝克莱·瑞波特证明了：费尔马大定理包含在“谷山丰－志村五郎猜想”之中。童年就痴迷于此的怀尔斯，闻此立刻潜心于顶楼书房 7 年，曲折卓绝，汇集了 20 世纪数论所有的突破性成果。最后终于在 1993 年 6 月 23 日英国剑桥大学牛顿研究所的“世纪演讲”，宣布证明了费尔马大定理。立刻震动世界，普天同庆。不幸的是，数月后逐渐发现此证明有漏洞，一时更成世界焦点。这个证明体系是千万个深奥数学推理连接着成千个最现代的定理、事实和计算所组成的千回百转的逻辑网络，任何一环节的问题都会导致前功尽弃。怀尔斯绝境搏斗，毫无出路。1994年 9月 19 日，星期一的早晨，怀尔斯在思维的闪电中突然找到了迷失的钥匙：答案原来就在废墟中！他热泪夺眶而出。10 月 6 日他把证明完稿送给爱妻娜妲作生日礼物。怀尔斯的历史性长文“模椭圆曲线和费尔马大定理” 1995 年 5 月发表在美国《数学年刊》第 142 卷，实际占满了全卷，共五章，130 页。他先后获得沃尔夫奖，美国国家科学院奖，费尔兹特别奖。他的证明用的是代数数论与算术代数几何理论，主要用到椭圆曲线等。“这个证明堪与发现原子分裂或DNA链相比美。是人类智慧的凯歌” ——怀尔斯的老师寇茨

如此评论。

◆ 概率化的蒙特卡罗方法

蒙特卡罗方法，或称计算机随机模拟方法，是一种基于“随机数”的计算方法。这一方法源于美国在第二次世界大战时研制原子弹的“曼哈顿计划”。该计划的主持人之一、数学家冯·诺伊曼用驰名世界的赌城——摩纳哥的蒙特卡罗——来命名这种方法，为它蒙上了一层神秘色彩。

蒙特卡罗方法的基本思想很早以前就被人们所发现和利用。早在 17 世纪，人们就知道用事件发生的“频率”来决定事件的“概率”。19 世纪人们用投针试验的方法来决定圆周率 π。20 世纪 40 年代电子计算机的出现，特别是近年来高速电子计算机的出现，使得用数学方法在计算机上大量、快速地模拟这样的试验成为可能。

考虑平面上的一个边长为 1 的正方形及其内部的一个形状不规则的“图形”，如何求出这个“图形”的面积呢？蒙特卡罗方法是这样一种“随机化”的方法：向该正方形“随机地”投掷 N 个点，假设有 M 个点落于“图形”内，则该“图形”的面积近似为 M/N。

科技计算中的问题比这要复杂得多。比如金融衍生产品（期权、期货、掉期等）的定价及交易风险估算，问题的维数（即交量的个数）可能高达数百甚至数千。对这类问题，难度随维数的增加呈指数增长，这就是所谓的“维数的灾难”，传统的数值方法难以对付（即使使用速度最快的计算机）。蒙特卡罗方法能很好地用来对付维数的灾难，因为该方法的计算复杂性不再依赖于维数。以前那些本来是无法计算的问题现在也