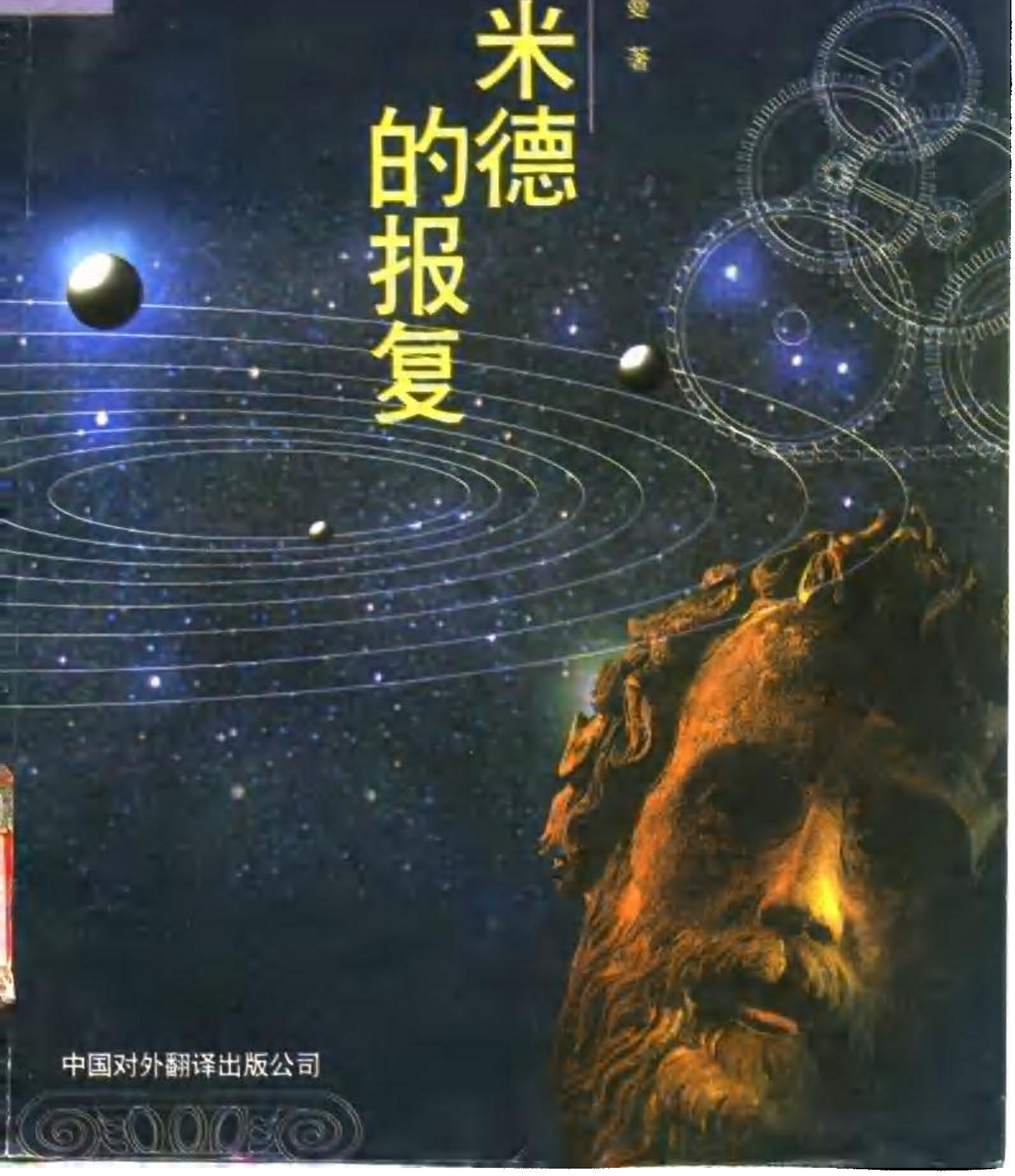
第一辑

科学与人译丛

阿基米德的报复

[美] 保罗·霍夫曼 著



中国对外翻译出版公司

阿基米德的报复

[美] 保罗·霍夫曼 著
尘土 文小凡
刘青 李京建 译

中国对外翻译出版公司

图书在版编目(CIP)数据

阿基米德的报复/(美)霍夫曼(Hoffmam,P.);尘土等译.
—北京:中国对外翻译出版公司,1993.5
(科学与人译丛)
书名原文:Archimedes' Revenge
ISBN 7-5001-0228-3
Ⅰ.阿… Ⅱ.①霍… ②陈… Ⅲ.数学-普及读物
Ⅳ.01-49
中国版本图书馆 CIP 数据核字(94)第 00938 号

出版发行/中国对外翻译出版公司
地　址/北京市西城区太平桥大街 4 号
电　话/66168195
邮　编/100810
责任编辑/马新林
责任校对/燕桂珍
印　刷/北京市振华印刷厂
经　销/新华书店北京发行所
规　格/850×1168 毫米　1/32
印　张/7.375
字　数/150(千)
版　次/1994 年 12 月第 1 版
印　次/1997 年 2 月第 2 次印刷

ISBN 7-5001-0228-3/G·42　定价:8.80 元

1311 58118

“科学与人译丛”出版说明

英国著名科学专栏作家布赖恩·阿普尔亚德在其《理解现在——科学与现代人的灵魂》一书中有这样一段话：

“1609年，加利莱奥·伽利略使用一架望远镜观看月亮。这一时刻，对世界的意义如此重大，以至人们将它与耶稣的诞生相提并论。因为，就像在伯利恒，自这一时刻，人类生活中的不可能成为可能。”

阿普尔亚德据此将科学划分为伽利略之前的科学，或称“智慧”，以及从1609年开始的现代科学。前一科学建立在推理基础上，后一科学建立在观察与实验基础上。经过如此划分，我们习以为常的科学，竟然只有400年的历史。

但人类就在这400年内经历了飞速发展。

我们有了蒸汽机，有了轮船，有了电话、电报，有了飞机、火箭，有了电视、电脑、互联网络，我们还有重力场理论、元素周期表、量子力学、相对论乃至被称为“自然中最基本物体”的超弦。工业革命、农业革命、信息革命使人类的社会生活发生了前人难以想象的变化。

人类改造了自然，也改造了人类自己。回顾这一切，人类完全有理由感到自豪。因为，人类就像上帝，也有自己的“创世纪”。人说，要有科学，就有了科学。科学是好的，它行之有效。

然而，“创世纪”中写道“到第七日，上帝造物的工已经完毕，就在第七日歇了他一切的工，安息了”。而人类的工却没有完毕，400年后的今天仍然不能安息。

就像有光必有影，人在发现、发明、创造、拥有上述一切的同时，还得到了原子弹、氢弹、核泄漏、酸雨、温室效应、臭氧层空洞乃至伴随科学技术而来的种种风险。

人类曾以为已找到了通往自由王国的必由之路，他将乘着科学的飞船，摆脱一切束缚，重新确立自己在宇宙中的位置。但在科学爆炸的二十世纪，人类终于开始反思：

科学行之有效，但它是否就是真理？

为此，我们编辑了这套《科学与人译丛》，陆续分辑推出。其中，有对信息崇拜的批判，有对生命起源的求索，有对技术所导致风险的分析，有对世界最新科学动态和研究方向的展望。数学家用对策论证明，完全的民主实际上并无可能；物理学家提出全新的超弦理论，试图统一描述所有的力、物质的所有基本粒子和时空，继量子力学和相对论之后，成为“第三次物理学革命的重要标志”……《译丛》汇集了物理学家、数学家、生物学家、天文学家、哲学家、人类学家、伦理学家……自本世纪后半期、尤其是在本世纪末打通自然科学与社会科学之间的隔膜，对科学这一决定人类命运的工具的深刻思索。通过这套丛书，我们期望读者可以对科学的现状、科学的未来、科学的正面与负面效应，有一个较为全面的了解，更好地认识科学、掌握科学、利用科学。

中国对外翻译出版公司

1997 年 2 月

目　录

前　言

阿基米德的头脑较之荷马有更丰富的想象力。

——伏尔泰

伊萨克·牛顿有句著名而又谦逊的格言："我所以比别人看得更远，是因为我站在巨人的肩膀上。"当时，他心中确实铭记着古代最伟大的一位数学家，希腊叙拉古城的阿基米德。然而，阿基米德还是一位力学天才，在他众多的机械发明中，有水车，又称作阿基米德螺旋泵，是一种用于抽水进行灌溉的螺旋状泵。虽然人们对于阿基米德的生平以及他对自己的功绩的评价知之甚少，但多数评论家猜测，他对于自己在理论数学上的发现比实用发明更重视。例如，一个叫普卢塔克的写道："而阿基米德具有这样一种崇高的精神，这样一种深奥的魂灵和这样一种科学理论的财富，虽然他的许许多多的发明为他赢得了声誉，并使他以'超人的精明'而闻名，但他并不愿为这些课题著书立说，流传后世，而把一个工程师的工作和有助于生活需求的每一件艺术品都视为卑贱和庸俗。他只潜心于研究那些不受生活品需求影响的精妙而有魅力的学科。"其他评论家则进一步认为，甚至当他从事杠杆、滑轮或其他机械研究时，他也是为了探索力学的普遍原理，而不是为了实际应用。

实际上，阿基米德对于理论的偏重胜于实际到什么程度可能永远不得而知。但有一点是清楚的：在他的作品中，理论和应用之间的关系是紧张的，而这种紧张的关系一直持续渗透到以后22个

世纪的数学之中。

本书主要概述了数学所涉及的领域和范畴。我并不认为这本书包罗万象，然而它选择的主题很离奇，但它也只能如此。数学是世间每所大学都从事研究的一门学科，它至少像生物学一样有广泛的领域，在生物界中，某个研究人员正努力研究艾滋病毒，而另一个研究人员则在研究袋熊的社会化问题。

我对数学的探讨犹如我在研究中国菜谱，到处品尝，识别常见的配料和特殊的风味。在仅仅用过一次中餐之后，你很难成为一名中餐美食家，但比起从未吃过中餐的人却又知之较多。数学亦如此。研究几个数学课题，是不可能掌握数学中一切重要的内容的，但比起那些一窍不通的人来，你对这些课题的感受却又深得多。

目前已出版了许多论及数学方面的哲学基础的书籍，从某种程度上讲这是必然性的科学，因为它的结论在逻辑上是无懈可击的。还有许多作品却狂热地详述数学无穷大的性质和高维度的美。这种带有哲学式的、富有诗意的离题的论述却有它的市场，但却远没有涉及大多数数学家们所关切的问题。我在本书中主要描述的是那些数学工作者在实际中所遇到的地地道道的实用的问题。

我还想批驳一个错误观点：仅仅肯花力气进行足够的运算，就可得到数学的任何结果，换句话说，如果你想解一道数学题，只需做足够量的运算就行了。即使你我缺乏解数学难题的能力，但我们也怀疑内行人士——这些理解数学符号的人——是否都能够对他们选择的任何一个问题经过潜心研究后找到答案。毕竟，我们的知识使我们相信数学是属于演绎推理，推断一个数学结果要像推论“所有人都必定要死的”和“苏格拉底是人”，因此“苏格拉底必定要死的”一样简单就好了！

我写作本书的目的之一是要说明一种数学知识的局限性。在我们所考查的每个数学领域中，我要指出什么是已知的和什么是未知的。有时我们的知识是有局限的，因为某些领域刚刚开发，还

没有多少数学家投身于对它的研究。知之甚少是这一问题的主要困难。此外，数学家的知识的局限性也是比较重要的因素。它表明，这些问题要从数学方面获得快速解决简直是不可能的。

数字中充满了新奇。数字和形状是人文科学中最早关心的课题，但有关的许多问题仍然令人费解。比一个素数的概念更简单的能是什么——一个大于 1 的整数，像 3,5,17 或 31 等不能被 1 和本身之外的其它整数整除的数？早在古希腊人的时代就知道素数是无穷尽的，但是没有一个人知道孪生素数——成对的素数，如 3 和 5，相差 2，它们是否也是无穷尽的。没有人知道是否存在无限多的完全数，像 6 一样等于它所有因子(当然除去它本身外，即 3,2 和 1)之和的整数。而且没有人知道一个完全数是否是奇数。匈牙利伟大的数论家保罗·厄尔多斯是一个证明素数基本定理的大师——他在 18 岁的时候，就提出了著名的论证：在每个大于 1 的整数和它的倍数之间一定有一个素数——他认为，数学家们还远远没有理解整数，更何况其他类型的数。他说："至少还得再过 100 万年，我们才可能理解素数。"

在数学上，对形状的理解也远远不够。在二维方面，关于什么形状可以在一定条件下用砖瓦贴盖表面的问题还有许多疑难未解之处。在三维的砖瓦贴面模拟中，形状的填充要尽可能使给定的空间密集，这对于许多基本形状来说仍悬而未决。但是，缺乏理论知识未必总是实用主义者的拦路虎，设计师罗纳德·雷施制造出三层半的复活节彩蛋就是明证。

由于有关数字和形状的基本问题仍未解决，因此对计算机——一种复杂的数字工具——能做什么和不能做什么常常众说纷纭，并出现一些混乱状态，这不足为怪。我尽量避开那些关于人和机器的本质的含糊不清的形而上学问题，便于向人们展示人们所不了解的关于计算的理论局限性方面的问题。我要讲述图灵通用计算机的惊人之处——分成若干单元的一条纸。我要考查一种可

能出现的局限性:计算机科学家认为,他们将能够证明某些仅仅在探索阶段的计算问题——包括旅行推销员在一连串的城市之间要选择的最短路线的问题——从来没有被计算机(或数学家)有效地解决。从理论转移到实践,我特意检验了汉斯·伯林纳和丹尼·希尔设计的对奕机和通用计算机,使“三个臭皮匠,顶过诸葛亮”的构想走向极端。要知道这些努力的整个结局如何还为时过早,但这两种机器的性能在某些领域,已经超过了传统计算机。

从根本上说,旅行推销员问题无疑是数学问题,可是实际上已证明,用传统的数学方法解答它是无效的。在这本书里,我将介绍一种出现在设计选举系统或分配代表的问题中的类似的解决办法。从绝对意义上说,数学对这些问题是毫无帮助的。的确,数学证明了,它虽然对开创一个完善的民主选举制在理论上无益,尽管缺乏完善的民主体制,但数学为公正的选举制和国会的公正分配方法指出了道路。

传说阿基米德是在一时的愤怒之中设计出一个关于牧牛的极其困难的数字问题。他的报复一直持续了22个世纪,直到1981年,使用刚诞生的一台巨型计算机才彻底解决了这一问题。牧牛的问题多少有些编造的味道。但是,面对阿基米德的报复,一代代数学家所感受到的挫折常常类似于那些比较自然地出现的较简单的数学问题所造成的报复。这种数学本身造成的报复看来还没有迹象会消退。

一个令人惊奇的宗教学生,
解出了无穷大的平方根,
这使他对计数烦躁不宁,
他终于放弃了数学又继续学神。

——无名氏

第一篇

数字

在古希腊，没有社会保险号码，没有电话号码，没有人口调查统计数字。没有选举后的投票数字，没有统计数据，也没有1099个表格要填。当时，世界还没有数字化，但数字在希腊知识分子的头脑中至关重要。确实，在公元前6世纪，萨摩斯的毕达哥拉斯通过研究数字创立了一种宗教，因为，他不仅把数字看成记数的工具，而且看成神圣、完善、友好、幸运及邪恶的符号。数学的一个分支称作数论，研究的是整数的性质，就是由古希腊人开创而且至今不衰的。

以下3章专谈数论。在这几章里，我强调指出，某些最古老并且听起来是最为基础的问题仍然悬而未决。虽说其原因尚不清楚，但至今悬而未决这一事实本身却赫然耸立，从而排除了认为数字不过是某种刻板活动的看法。数论曾被视为数学最纯的分支；似乎对现实世界毫无实用价值。然而近年来，数论已变成密码学的一个强有力的工具。不过，正如我在第四章“比尔密码之谜”中所探讨的，至今还存在着数学分析无法破译的传奇密码。

第　一　章

邪恶的数和友好的数

现为麻省理工学院大学生的米歇尔·弗里德曼，1985年在布鲁克林高中毕业班就读时春风得意，获得了当年的威斯汀豪斯科学天才奖的第三名。为了他这一获奖项目，他不想用海虾、果蝇或扁虫来弄脏自己的手，也不想处理随便任何一个多年遗留下的理论上的问题。不，他只是挑选了堪称数学上最古老而未决的问题来对付。那是困扰着古希腊人和自那以后的每个人的一个问题：即存在奇数完全数吗？

毕达哥拉斯及其好友认为，整数的完满性，即完全数是任何其所有除数之和（该除数本身外）等于该数本身的整数。第一个完全数是6。它可被1、2和3整除并且是1、2和3之和。第二个完全数是28。它的除数是1、2、4、7和14，这些数加起来为28。希腊人所知道的就是这些，尽管他们做过尝试，但没有发现奇数完全数。

圣经评论家注意到，完全数6和28反映在宇宙的结构中：上帝在6天内创造了世界，月亮每28天绕地球一周。然而，使这些数字成为完全数的是其本身，而不是凭经验所了解的世界的任何联系。圣·奥古斯丁是这样表述的："6本身是一个完全数，并不是因为上帝在6天内创造了万物才如此；倒不如反过来说才对：因为6是完全数，所以上帝在6天内创造了万物。即使不存在6天工作一说，6依然会是个完全数。"

“数学的整个领域都极其散漫”，坦普尔大学数学教授小彼得·哈及斯说，“我研究完全数是出于闲散的好奇心，因为它可能是最古老的未决问题。研究它也许意义不大，然而这一问题如此古老，没有人认为对之进行研究完全是浪费时间。如果这一问题是5年前第一次提出来的，那它是决不会令人感兴趣的。”

无论在哪 一领域，达到完善总是很难的，偶数完全数也不例外。但是，人们至少知道它们是存在的。我们已发现了30个偶数完全数，最大的是一个由13万位阿拉伯数字组成的庞然大物：$2^{216,090}(2^{216,090}-1)$。也许第三十一个完全数不会出现了，因为早在2300多年前数学家就已知道有无穷多的素数（即只能被1和它本身整除的数），但在同一时期，他们却不能决定完全数是不是无限的。

要是在俄国茶室或“四季”咖啡馆里喝着可乐会见米歇尔·弗里德曼我会很高兴的，但他宁可让我们在斯替韦桑特中学他的校长办公室中见面，而该校是曼哈顿数学家和科学家的中心。传说，爱因斯坦不能做加减运算，但可在睡梦中研究高深的数学。米歇尔的情况也可以这么说。在选择我们会见时间这种简单的事情中就体现了出来，因为这位杰出的小伙子不适于将中学时间——“第三节”和“第五节”——转换成我们常人所遵照的小时和分钟。然而一旦我们真聚到了一起，这位腼腆的天才就口若悬河地谈论起来，一下成了使人兴趣盎然的人了。

米歇尔告诉我，“去年我为一位数学老师写一篇论文，我知道关于奇数完全数的问题。这问题使我感兴趣，因为它很简单，可还没人找到答案。”接着，米歇尔首先回顾了完全数的历史。

古人只知道4个完全数，它们是：6，28，496和8，128。欧几里得认识到——大概只有古希腊的神祇才晓得他是如何知道——的

完全数	位数
1. $2^{1}(2^{2}-1)=6$	1
2. $2^{2}(2^{3}-1)=28$	2
3. $2^{4}(2^{5}-1)=496$	3
4. $2^{6}(2^{7}-1)=8,128$	4
5. $2^{12}(2^{13}-1)=33,550,336$	8
6. $2^{16}(2^{17}-1)=8,589,869,056$	10
7. $2^{18}(2^{19}-1)=137,438,691,328$	12
8. $2^{30}(2^{31}-1)=$	19
9. $2^{60}(2^{61}-1)=$	37
10. $2^{88}(2^{89}-1)=$	54
11. $2^{106}(2^{107}-1)=$	65
12. $2^{126}(2^{127}-1)=$	77
13. $2^{520}(2^{521}-1)=$	314
14. $2^{606}(2^{607}-1)=$	366
15. $2^{1,278}(2^{1,279}-1)=$	770
16. $2^{2,202}(2^{2,203}-1)=$	1,327
17. $2^{2,280}(2^{2.281}-1)=$	1,373
18. $2^{3,216}(2^{2.317}-1)=$	1,937
19. $2^{4,252}(2^{4,253}-1)=$	2,561
20. $2^{4,422}(2^{4,423}-1)=$	2,663
21. $2^{9,688}(2^{9,689}-1)=$	5,834
22. $2^{9,940}(2^{9,941}-1)=$	5,985
23. $2^{11,212}(2^{11,213}-1)=$	6,751
24. $2^{19,936}(2^{19,937}-1)=$	12,003
25. $2^{21,700}(2^{21,701}-1)=$	13,066
26. $2^{23,208}(2^{23,209}-1)=$	13,973
27. $2^{44,496}(2^{44,497}-1)=$	26,790
28. $2^{86,242}(2^{86,243}-1)=$	51,924
29. $2^{132,048}(2^{132,049}-1)=$	79,502
30. $2^{216,090}(2^{216,091}-1)=$	130,100

30 个完全数

这 4 个数是由公式 $2^{n-1}(2^n-1)$当 n=2,3,5 和 7 时推出来的。算式如下：

$$n=2,2^1(2^2-1)=2(3)=6$$

$$n=3,2^2(2^3-1)=4(7)=28$$

$$n=5,2^4(2^5-1)=16(31)=496$$

$$n=7,2^6(2^7-1)=64(127)=8,128$$

欧几里得看出，在全部的 4 个算式中，2^n-1 是素数(3,7,31 和 127)。这种发现促使他证明一个重要的定理：当 2^n-1 为素数时，那么公式 $2^{n-1}(2^n-1)$则得出偶数完全数。

欧几里得的证明使得完全数理论有了一个兴旺的开端。但由于其他数学家的短视，这一理论进展缓慢。许多思想精微的人自以为他们看出了数字模式，其实这些数字并不存在。如果他们看得更远一点，他们就会发现这种模式是虚幻的。

古人观察到，前 4 个完全数都是以 6 或 8 结尾的。进一步说，最后一个阿拉伯数字似乎是 6,8,6,8 地交替出现。所以有人推测，完全数最后一个阿拉伯数总会是 6 或 8，并且它们会继续交替出现。第五个完全数——古代人并不知道——的确是以 6 结尾的。但第六个完全数也是以 6 结尾的，这就打破了交替出现的模式。然而，关于最后一个阿拉伯数字总是 6 或 8 这一点，古人还是正确的。今天，数学家可以研究 30 个完全数——比古人多出 7 倍以上——但他们还必须找出尾数为 6 和 8 的模式。

古人还观察到，第一个完全数有一位数字，第二位完全数有 2 位数字，第三个有 3 位数，第四个有 4 位数。所以他们推测，第五个完全数会有 5 位数。在欧几里得故去 17 个世纪后发现了第五个完全数，它赫然具有 8 位数：33,550,336。并且位数继续迅速增多，以下 3 个完全数分别为 8,589,869,056；137,438,691,328；和 2,305,843,008,139,952,128。

欧几里得证明了一旦 2^n-1 是素数，那么 $2^{n-1}(2^n-1)$就会得

出一个完全数，但他并没有说 n 的哪一个整数值会使 2^n-1 成为素数。由于使 2^n-1 为素数的前 4 个 n 值为前 4 个素数(2,3,5,7)，可能有人推测：如 n 为素数，2^n-1 也会是素数。那么，让我们来试试看第五个素数：11。如 n＝11，2^n-1 则为 2,047，而 2,047 并非素数(它是 23 和 89 的积)。真实情况是：要使 2^n-1 为素数，n 必须是素数，而 n 为素数并不就意味着 2^n-1 是素数。事实上，对于 n 的大多数素数值来说，2^n-1 并不是素数。

由 2^n-1 一式得出的数列现在称作默塞纳数列，马林·默塞纳是 17 世纪的巴黎僧侣，他在尽僧职之余抽空进行数论的研究。根据欧几里德的公式，每发现一个新的默塞纳素数，就会自动出现一个完全数。1644 年，默塞纳自己说，$2^{13}-1$，$2^{17}-1$ 和 $2^{19}-1$ 这 3 个默塞纳数是素数(8,191；131,071 和 524,287)。这位僧侣还声称 $2^{67}-1$ 这个巨大的默塞纳数会是位素数。在 250 多年的时间里，没有人对这一大胆的声言提出疑问。

1903 年，在美国数学协会的一次会议上，哥伦比亚大学教授弗兰克·纳尔逊·科尔提交了一篇慎重的论文，题为：论大数的分解因子。数学史家埃里克·坦普·贝尔记下这一时刻所发生的事：“一向沉默寡言的科尔走上台去，不言不语地开始在黑板上计算 2^{67}。然后小心地减去 1，得出 21 位的庞大数字：147,573,952,589,676,412,927。他仍一语不发地移到黑板上的空白处，一步步做起了乘法运算：

193,707,721×761,838,257,287。

“两次计算结果相同。默塞纳的猜想——假如确曾如此的话——就此消失在数学神话的废物堆里了。据记载，这是第一次也是惟一的一次，美国数学协会的一位听众在宣读论文之前向其作者热烈欢呼。科尔一声不吱在他座位上坐下。没人向他提任何问题。”

在欧几里得证明他的公式总是得出偶数完全数的大约 2,000

年之后，18 世纪的瑞士数学家伦纳德·尤勒证明，该公式将得出全部的偶数完全数。这样，我们就可以用另一种方式提出奇数完全数问题：是否存在不是由欧几里得公式得出的完全数呢？

为弄清最近取得的进展，年轻的米歇尔·弗里德曼埋头翻阅过期杂志：《计算数学》、《数论杂志》、《数学学报》及一堆决不会在咖啡桌上看到的其它期刊。他甚至参阅理查德·盖伊的艰深的经典著作《数论中的未决问题》，该书不仅讨论完全数，而且还探讨十几个其它神秘专题："近超完全数"，"友谊图表"，"优雅图"，"贪婪规则系统"，"纽环游戏"，达文波特-施尼茨尔系列"，"半友善数"，"友善数"和"不可接触数"。

米歇尔知道，困于这一棘手问题的数论学家们验明：如果真有奇数完全数存在的话，所必须具备的各类特征有：它必须被至少 8 个不同的素数整除，其中最大的一定要大于 300,000，次大的也要大于 1,000。如果奇数完全数不能被 3 除，它至少应被 11 个不同的素数整除。此外，当一个奇数完全数除以 12 时，它应有余数 1；当它除以 36 时，它的余数应该是 9。

我们从这些验证中能得出什么结论呢？对奇数完全数的限制越多，奇数完全数存在的可能性就越小。1973 年，彼得·哈吉斯运用这样的限制条件并借助于计算机肯定地证明了 10^{50}以下没有奇数完全数。米歇尔从盖伊的书中看到，自 1973 年以来，其他数论家"渐渐地把奇数完全数不可能存在的上限推到 10^{200}，尽管有人对后面这一证明表示怀疑。"

既然与盖伊一样有权威的人对这些证明提出质疑，米歇尔决定重新研究更低限问题。他运用 IBM PC 机及一组限制因素，包括一些文献中极少提到的来自印度的限制因素，证明在 10^{79}之下不存在奇数完全数，10^{79}有 8 个素数因数——这是一个奇数完全数所能有的最少的素数因数的数目。

米歇尔说："我在论文中只是引用了盖伊的话：以前(关于奇数