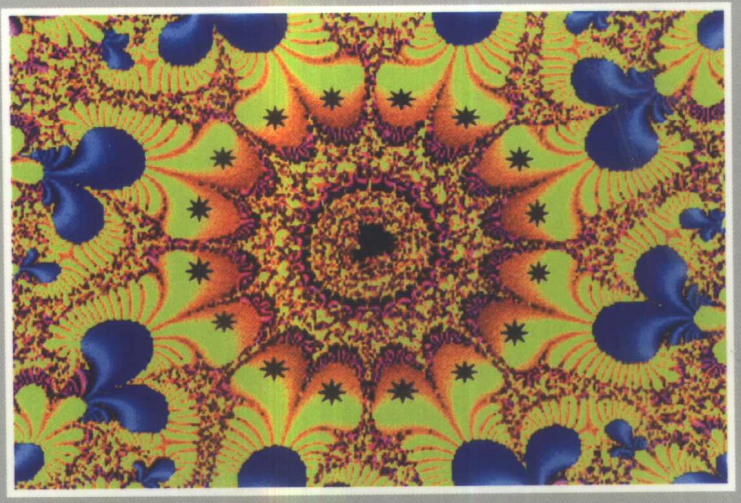
数学欣赏

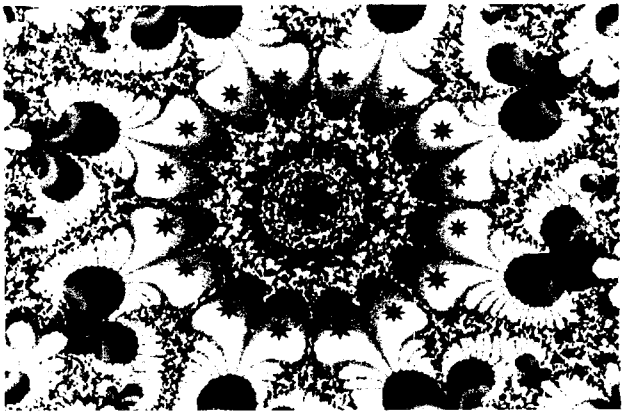
黄文璋 著



中国统计出版社
China Statistics Press

数学欣赏

黄文璋 著



中国统计出版社
China Statistics Press

(京)新登字 041 号

图书在版编目(CIP)数据

数学欣赏/黄文璋著.
-北京:中国统计出版社,2001.12

ISBN 7-5037-3411-6

Ⅰ.数…
Ⅱ.黄…
Ⅲ.数学-普及读物
Ⅳ.01-49

中国版本图书馆 CIP 数据核字(2000)第 77399 号

数学欣赏

作　　者/黄文璋
责任编辑/吕　军
出版发行/中国统计出版社
通信地址/北京市西城区月坛南街 75 号　邮政编码/100826
办公地址/北京市丰台区西三环南路甲 6 号
电　　话/(010)63459084　63266600-22500(发行部)
印　　刷/科伦克三莱印务(北京)有限公司
经　　销/新华书店
开　　本/787×1092mm　1/18
字　　数/290 千字
印　　张/15.75
印　　数/1-3000 册
版　　别/2001 年 12 月第 1 版
版　　次/2001 年 12 月北京第 1 次印刷
书　　号/ISBN 7-5037-3411-6/O·39
定　　价/30.00 元

序

本书主要是为喜好数学的高中生及一般的大学生写的，试图让他们了解数学中有趣及有用的一面，及获得一些数学常识，因而更乐意去亲近数学及使用数学。对中学教师或准备日后去中学任教者，本书应也适合当做他们的参考书。教师要让学生了解数学的有趣及有用，才易激发他们学习数学的动机。为方便读者能从任何一章开始阅读，各章尽量做到独立，非必要时不引用他章。但因需求有异，同一事物，在不同的章，其说明有时较详细有时却较简略。

因个人所学及能力皆很有限，本书之选材一方面很主观，一方面涵盖面也很局限，各章内容自然也不见得皆有趣或完备。书名欣赏，实乃野人献曝，只表作者对数学通识之一些心意。

为了使读者获得正确之知识及易于进一步探索，本书资料力求详实，该有之参考文献也尽量附上。唯仍因受制于个人才学之不足，疏漏谬误之无法避免乃可预期。只好阿Q式的敬告读者，尽信书不如无书。

同事化学系李良修教授，常提供一些有关数学的资讯给我。他虽专长为化学，但对各种知识的勤于吸收，仅在数学方面就已令我汗颜了。他常能激发着我该努力为数学通识教育尽力。另外，在本书的初稿打字期间，因身体微恙，经由黄采菽女士之助，得以结识高雄荣民总医院的王任贤医师，获得他许多协助。他对发掘出病人病因的兴趣，使我对医师的印象大为改观，原来也有医师技艺高超，又如此重视病人的。

不少同事先后提供资料及意见，改善及丰富了本书的内容。又近年来，常与本校不同学院的几位同事共进午餐，在那快乐的午餐时间，本书的一些材料也得到试讲的机会，灵感常因而产生。谢谢他们几位桌友。我的女儿彦宁，目前就读高中，是我的第一号读者，每次看她津津有味的读着稿子，还能给出建议，使我相信将本书出版是值得的。内人梦娜对本书的帮助，也一如以往，接近笔墨难以形容的程度。

本书之打字编排，获吴昭宛小姐、陈彦宏先生、王秀英小姐、吴兰屏小姐及卓世明先生之大力协助。很谢谢他们几位。邱千惠小姐，她在公务家务两忙之下，还挤出时间将全书完成最后的总整理工作。我再度感谢她多年来对我的帮忙。

最后感谢中国统计出版社对学术及教育的支持，使本书得以顺利出版。

黄文璋

2001 年 6 月

目　　录

第一章

完全数与梅仙尼质数

1　完全数

由自然数(又称正整数)、整数、有理数、实数至复数,数学中所讨论的问题往往与数有关。而其中数字的诸多优美及特异的性质,一直吸引着许多职业及业余数学家去探讨。这探讨可归于数学中的整数论,或者说数论的问题。数论起源甚早,与几何学的发展相当,但数论的题材似乎是取之不尽的,影响也较深远。数论中的优美及丰富的内容,不知倾倒多少数学家,许多中学生着迷数学,也往往是喜欢数论。数学家高斯(Gauss,1777-1855,有史以来三大数学家之一。另两位为阿基米德(Archimedes,公元前 287-212 年)及牛顿(Newton,1642-1727)曾说"数学是科学的皇后,而数论是数学的皇后(Mathematics is the queen of the sciences and the theory of numbers is the queen of mathematics)"。至于高斯则被称为数学王子。数论中的有些结果,后来发现有其实际的用途。如同余数及质数的分解,可用在编码及解码上。不过大部分的时候,去探讨数论中的问题,只是数学家纯粹觉得有趣,追求心智上的满足。本质上十个阿拉伯数字 0,1,…,9 所衍生出的问题,与音乐中七个音阶所组合出的各种曲调,都能带给人们在不同方面的喜乐。古希腊时代,毕达哥拉斯(Pythagoras,约公元前 580-500 年)门生极多,称为毕氏学派(the Pythagorean school),他们研究的范畴主要为几何、算术、天文及音乐,而这些研究均以数字为其基础。毕达哥拉斯就曾说万有皆数(All is number)。古希腊的大哲学家亚里斯多德(Aristotle,公元前 384-322 年)也曾说"毕达哥拉斯认为宇宙是由音阶和数相辅相成"。

爱看武侠小说的人,对金庸在其武侠小说中,将数字运用的极为熟练应留下深刻印象。例如,在射雕英雄传(金庸(1996)第二十九回"黑沼隐女"中,隐居中的瑛姑何以排除孤寂?乃是在解各种数学问题,如求 55,225 的平方根,

求 34,012,224 的立方根,求 3×3 的魔方阵(Magic square,关于魔方阵的文章很多,可参考林克瀛(1980a)、林克瀛(1980b)、林克瀛(1981)、梁培基、张航辅(1993)、梁彩丽、梁培基(1996))。

英国大数学家 Hardy(1877-1947),曾藉下述故事(见 Hill(1987/88)),来说明印度的传奇数学家 Ramanujan(1887-1920,其部分事迹可见曹亮吉(1984)"不按牌理出牌"一文),能以各种难以想像的方式来记住各个数字。当 Ramanujan 因病在 Putney 休养时,在 1919 年 1 月,有一次 Hardy 乘坐计程车去看他,车牌号码为 1729。Hardy 觉得这是一个没什么特性的数字。Ramanujan 马上说"恰恰相反,这是一个很有趣的数字,它是能以两种不同的方式,表示成二整数的立方和的最小正数"。读者能试将此两种表示法写出吗?Hardy 接着又问 Ramanujan 是否知道四次方和的对应解?Ramanujan 想了一下回答说"我给不出答案,但此最小正整数若存在一定是很大的"。日后 Hardy 在传述此故事时,指出瑞士数学家欧拉(Euler,1707-1783)曾给出此数为 $158^4 + 59^4 = 134^4 + 133^4$。此数当然是很大的,所以不能怪 Ramanujan 一时想不出。Hardy 的长期合作者,也是英国大数学家 Littlewood(1885-1977)曾说过"每一正整数皆为 Ramanujan 的密友"。

古希腊时,有些数字令人觉得具有特别的象征及神秘的意义。例如,毕氏学派在一些数字中,看到一完美的性质:这些数等于小于它的所有因数(即真因数)之和。他们称这种数为完全数(perfect number,事实上称呼完美数也许较恰当,不过约定俗成,我们仍采用完全数)。6 是第一个完全数,6 = 1 + 2 + 3。6 也确实与宗教里的一些完美性相关连。在西方圣经里记载,上帝在六天内创造了世界,因此古代人认为 6 是一个很完美的数字。中国人说六六大顺,显然对 6 也很偏好。28 是第二个完全数,28 = 1 + 2 + 4 + 7 + 14。妇女担负着传宗接代的神圣使命,月经为其间的极纽,而月经之每周期约 28 天,这是巧合或有意的?

欧几里得(Euclid,约公元前 375-330 年)写过原本(Elements),也被称为几何原本,后来成为中学几何学的基础(蓝纪正、朱恩宽译(1992))。在原本的第九卷,亦为讨论算术的第三卷也是最后一卷,此卷除包含质数有无限多个的证明,其最后一命题(命题 36),即为完全数的讨论。古希腊哲学家柏拉图(Plato,约公元前 428-347 年)在其所著共和国(Republic)一书中,也提到完全数。

古希腊时代只知道四个完全数,在原本第九卷的最后一句话写着"6,28,496,8,128 等皆是完全数"。欧几里得发现(只有希腊神才知道他怎么发现

的),这四个完全数皆可表示为 $2^{n-1}(2^n-1)$的型式,n 分别为 2,3,5,7:

$n=2$,　$2^1(2^2-1)=2\cdot3=6$,

$n=3$,　$2^2(2^3-1)=4\cdot7=28$,

$n=5$,　$2^4(2^5-1)=16\cdot31=496$,

$n=7$,　$2^6(2^7-1)=64\cdot127=8,128$。

欧几里得也看出当 $n=2,3,5,7$ 时,2^n-1 皆为质数(一大于 1 之整数,若除了 1 与本身外无其他因数,便称为质数(prime number 或 prime),否则称为合成数(composite number))。这项观察使他在原本里,证明了下述定理。

定理 1. 若 2^n-1 为一质数,则 $2^{n-1}(2^n-1)$为一完全数。

证明. 设 $p=2^n-1$ 为一质数,则 $2^{n-1}(2^n-1)=2^{n-1}p$ 之因数有 $1,2,2^2,\cdots,2^{n-1},p,2p,2^2p,\cdots,2^{n-1}p$。因此 $2^{n-1}(2^n-1)$之所有真因数之和为

$$\begin{aligned}&1+2+2^2+\cdots+2^{n-1}+p+2p+2^2p+\cdots+2^{n-2}p\\&=2^n-1+p(2^{n-1}-1)\\&=p+p(2^{n-1}-1)=2^{n-1}p=2^{n-1}(2^n-1)\ 。\end{aligned}$$

证毕。

我们又有下述定理。

定理 2. 对每一正整数 n,若 2^n-1 为一质数,则 n 为质数。

证明. 设 n 不为质数,令 $n=pq$,$p>1$,$q>1$。则

$$\begin{aligned}2^n-1&=(2^q)^p-1\\&=(2^q-1)((2^q)^{p-1}+(2^q)^{p-2}+\cdots+2^q+1)\\&=A\cdot B。\end{aligned}$$

因 $p>2$ 且 $q>1$,故 A,B 皆大于 1,因此 2^n-1 不为质数,与假设不合。故得证 n 为质数。

由上定理立即可看出为何首四个完全数对应的 $n=2,3,5,7$ 皆为质数。试看 $n=4$,则 $2^{4-1}(2^4-1)=120$。而 120 的真因数和为 $1+2+3+4+5+6+8+10+12+15+20+30+40+60=216\neq120$,故 120 不为一完全数。

首四个完全数分别为一位数、二位数、三位数及四位数。读者是否猜测第五个完全数为五位数?结果是不对的。又定理 2 之逆不真,因第五个质数为 11,但在 1536 年 Regius 证明 $2^{11}-1=2,047=23\cdot89$ 并不为质数。事实上 $2^{10}(2^{11}-1)=2,096,128$ 的确不是一个完全数。但定理 1 并未指出当 2^n-1 不为质数时,$2^{n-1}(2^n-1)$是否为一完全数,此问题我们稍后再回答。古希腊人亦看出,首四个完全数,其个位数为 6,8 交替(约在公元前一世纪,Nicomachus 在其著作中虽也只列出首四个完全数,但他指出偶完全数的个位数不是 6 就

是8。且当个位数为6时，十位数必为奇数，当个位数为8时，十位数必为2)。后来证实第五个完全数的个位数的确是6，只是第六个完全数的字尾仍为6，这便打破了6,8交替的型式。不过目前已知的完全数，其个位数皆为6或8。

定理1给出了找偶完全数的充分条件，但是否尚有其他偶完全数呢？欧几里得之后约两千年，欧拉在一篇他去世后才发表的论文中，给出了下述找偶完全数的必要条件，至此偶完全数的型式便完全决定了。

定理3. 偶完全数必呈$2^{n-1}(2^n-1)$的型式，其中n为一正整数，且2^n-1为一质数。

证明. 设A为一偶完全数，则A可表示为$A=2^{n-1}p$，其中$n\geq 2$为一整数，p为一奇数。则A的所有因数和为(证明留在习题第5题)

(1) $$2s(A)=(2^{n-1}\text{的所有因数和})\cdot(p\text{的所有因数和})$$
$$=(2^n-1)(s(p)+p),$$

其中$s(A)$及$s(p)$分别表A及p之所有真因数之和。因A为一完全数，故$s(A)=A$，即

$$(2^n-1)(s(p)+p)=2A=2^np。$$

由此即得

(2) $$p=(2^n-1)s(p)。$$

由上式知$s(p)$为一p的因数(以$s(p)\mid p$表之)。又$2^n-1>1$，故$s(p)$为一p的真因数。但$s(p)$为p之所有真因数之和，由此便得$s(p)=1$。而$s(p)=1$又导出p为一质数。故由(2)知，$p=2^n-1$为一质数。证毕。

第五个完全数，是在1461年左右，于一份前人留下的文稿中发现的，其位数达到八位，即33,550,336。第六个质数为13，由定理3知，欲检验$2^{12}(2^{13}-1)=33,550,336$是否为一完全数，只须检验$2^{13}-1=8,191$是否为一质数。在初等数论中，有下二关于质数的检验定理。

定理4. 每一大于1之整数必有一质因数。

定理5. 若整数A为一合成数，则A必有小于或等于$\sqrt{A}$之质因数。

但即使有上二定理，在那计算不发达的时代，检验质数仍是一件艰辛的工作。由于$\sqrt{8,191}=90.5\cdots\cdots$，必须验证24个小于91的质数是否能除尽8,191。早期数学家可能没有去尝试。在1588年，针对13的下两个质数17及19，意大利数学家Cataldi(1548-1626)证明$2^{17}-1=131,071$及$2^{19}-1=524,287$皆为质数。因$724<\sqrt{2^{19}-1}<725$，欲检验$2^{19}-1$为一质数，他先建立一小于725之质数表。然后证明其中总共的128个质数皆无法除尽$2^{19}-1$。这是一不小的工程。他也因此得到第六个完全数$2^{16}(2^{17}-1)=8,589,869,$

056,及第七个 $2^{18}(2^{19}-1)=137,438,691,328$。他亦宣称当 $n=23,29,31$ 及 37(19 的下四个质数)时,2^n-1 皆为质数。在 1640 年,法国大数学家费马(Fermat,1601-1655,他是一位职业律师,但在现代数论中,扮演着极重要的角色)证明 $n=23$ 及 37 时,2^n-1 皆非质数。欧拉在 1738 年证明 Cataldi 对 n=29 亦犯了错。不过后来在 1772 年(一说 1750 年),欧拉证明 $2^{31}-1$ 确为质数,因而得到第八个完全数。距上一个完全数之发现已近两百年。

有了定理 3,决定偶完全数,本来成为了决定 2^n-1 是否为质数的问题。但由于计算工作愈来愈大,即使愿做如 Cataldi 的苦工,也不可行了。除非有更好的检验质数的方法,否则虽知道该如何去找完全数,但却不易产生新的完全数。十七世纪法国数学家笛卡儿(Descartes,1596-1650)曾预言:能找出的完全数是不会太多的,好比要在人类中找到完人(perfect man),亦非易事。

2　梅仙尼质数

在 Cataldi 之后,下一阶段寻找完全数工作的重心,便转移到法国。找偶完全数与检验 2^n-1 是否为一质数,是等价的。

型如 2^n-1 的质数(n 当然须为一质数),最早以笛卡儿的好朋友,法国神父梅仙尼(Mersenne,1588-1647)最有兴趣,故后来对一质数 p,便称 $M_p=2^p-1$ 为一梅仙尼数(Mersenne number),且当 M_p 为质数时,称此为一梅仙尼质数(Mersenne prime)。

梅仙尼经常与那时的法国著名的数学家通信,讨论的问题包含完全数及型如 M_p 的质数。但为何这种质数以他的名字命名,则不是很清楚。因他并未得到任何显著的结果,而只做了一个有名的断言。不过那时的数学家倒是常受到梅仙尼的鼓舞,而去研究他所提出的问题。

梅仙尼在 1644 年说:若 p 为一不超过 257 的质数,则当 $p=2,3,5,7,13,17,19,31,67,127,257$ 时,2^p-1 为质数,否则为合成数。

对 $p\leqslant 257$ 之梅仙尼数 M_p,梅仙尼已去掉许多不为质数的 M_p,如 M_{23},M_{29}等。但他仍犯了一些错:多列了两个,即 $p=67,257$,少列了 3 个,即 $p=61,89,107$。此因如前所述,当 p 很大时,欲检验 M_p 是否为质数,便很难困难。所以梅仙尼留给后世此一以他名字命名的他在质数方面唯一的断言也是错的。正确地说,在 2 到 257 间共有 12 个梅仙尼质数,其对应的 p 值为

$$2,3,5,7,13,17,19,31,61,89,107,127。$$

这就是人们只用纸笔所得的全部十二个梅仙尼质数。虽然梅仙尼在其宣称中

犯了错,但在没有电子计算机的帮助下,而当 p 很大时,M_p 又是极巨大,能有此成果,已是很惊人的成绩了(换一个观点来看,在 2 到 257 间共有 55 个质数,若对每一个其间的质数 p,皆问 M_p 是否为质数,梅仙尼说对了 50 个)。一直要到 1947 年,对 $p\leqslant 257$ 时,M_p 为质数的名单才完全确定。

虽对首四个质数 $p=2,3,5,7$,M_p 皆为质数,但由在 257 之前共有 55 个质数,却只产生 12 个梅仙尼质数,你大约可以猜出许多梅仙尼数并非质数。事实上底下我们会看到梅仙尼质数之稀少,远超出我们的想像,且当 p 愈大,M_p 愈不易为质数。

由定理 5 知,欲检验 A 是否为一质数,只要用不超过$\sqrt{A}$的质数去除 A 即可。但即使如此,当 p 很大时,便需要做许多次除法,并不易检验出 M_p 是否为一质数。于是又有下述定理。

定理 6. 设 p 为一质数,则 M_p 的质因数必为 $ap+1$ 的型式,其中 a 为一正整数。

证明. 设 $M_p=2^p-1$ 有一质因数 $\ell=ap+b$,其中 $1\leqslant b\leqslant p-1$,$a$ 为一正整数。在此由费马小定理(Fermat's Little Theorem,即对任一质数 q 及正整数 m,$q\mid(m^q-m)$)知,$p\nmid(2^p-1)$,故 $b\neq 0$。因 $\ell\mid(2^p-1)$,故

$$2^{\ell-1}-2^{b-1}=2^{ap+b-1}-2^{b-1}=2^{b-1}((2^p)^a-1) \tag{3}$$

为 ℓ 之整数倍。又因 $\ell\neq 2$,费马小定理再度导出 $\ell\mid(2^{\ell-1}-1)$。故由(3)式得 $\ell\mid(2^{b-1}-1)$。

现设 $b>1$。因 p 为质数,且 $p>b>b-1>0$,故 p 与 $b-1$ 互质。故存在二正整数 α,β,使得

$$ap=\beta(b-1)+1 \text{ 或 } \alpha(b-1)=\beta p+1。$$

当 $ap=\beta(b-1)+1$ 时,因 $2^{b-1}-1$ 为 ℓ 之倍数,且

$$2^{ap}=2^{\beta(b-1)+1}=((2^{b-1}-1)+1)^{\beta}\cdot 2,$$

故 2^{ap}除以 ℓ 余 2。但由 $2^{ap}=((2^p-1)+1)^{\alpha}$ 又得 2^{ap}除以 ℓ 除 1。同理当 $\alpha(b-1)=\beta p+1$ 亦导至矛盾。故得 $b=1$。本定理证毕。

有了定理 6,检验 M_p 是否为质数的工作当然减轻不少。尤有进者,费马在 1640 年时向梅仙尼提出法(一):当 $p>2$ 时,M_p 的质因数必为 $2kp+1$ 的型式(欧拉在 1747 年利用二项式定理证明此结果)。例如,当 $p=11$ 时,$2kp+1=22k+1$,$k=1$ 可得质数 23,且 $23\mid M_{11}=23\cdot 89$,又 $89=22\cdot 4+1$ 亦为一质数;当 $p=23$ 时,$2kp+1=46k+1$,$k=1$ 得质数 47,且 $47\mid M_{23}$;当 $p=29$ 时,$2kp+1=58k+1$,$k=1,4$ 皆使此数为质数,但 $59\nmid M_{29}$,而 $233\mid M_{29}=536,870,911$。所以只需做一次除法,即检验出 M_{23}为一合成数;只需做两次除法

即验出 M_{29}为一合成数。同理，对 $p=37,41,43,47,53,59$，甚至对一些很大的质数 p，如 $p=16,035,002,279$（对此 p，$q=2p+1$ 为质数，且 $q\mid M_p$），皆可利用此法检验出 M_p 为合成数。

若 Cataldi 知道法（一），则只需检验 6 个小于 725，且为 $38k+1$ 型式的质数（即 191，229，419，457，571 及 647），是否能除尽 M_{19}即可，工作量显然大幅度地减轻。不过对于 M_{31}，就要将 157 个 $62k+1$ 型的质数去除 M_{31}。因此欧拉又提出下述法（二）：M_p 的质因数可写成 $8n+1$ 或 $8n-1$ 的型式。例如，

$$M_{11}=23\cdot 89=(8\cdot 3-1)(8\cdot 11+1)。$$

结合法（一）及法（二）将使 M_p所可能具有的质因数又减少很多。例如，对 M_{19}现只需检验 191，457 及 647 等三数，能否除尽 M_{19}。而 M_{31}的质因数必为 $248k+1$ 或 $248k+63$ 的型式，可使检验 M_{31}的除法减少至 84 次。欧拉也因此于 1772 年证明 $M_{31}=2,147,483,647$ 为 M_{19}的下一个梅仙尼质数。虽距 M_{19}的发现已隔了近二百年，但若无前述这些好方法，显然要隔得更久。早期寻找梅仙尼质数的工作，至此告一段落。

附带一提，那时的数学家持续地在研究判断一梅仙尼数是否为质数的方法。欧拉尚有下述检定法，我们称之为法（三）：若 $p=4m+3$，$m\geqslant 1$，为一质数，且 $q=2p+1$ 亦为一质数，即 $q\mid M_p$，因此 M_p 为一合成数。诸如 $p=11$，23，83，131，179，191，239，251 等，皆为这类质数。再度地，亦有一些很大的这类质数，如 $p=16,035,002,279$ 及 $16,188,302,111$（对此二 p，M_p 的位数约有 $5\cdot 10^9$ 位）。

1876 年，法国数学家 Lucas（1842-1891）发现一个可很快地测出一梅仙尼数是否为质数的方法。利用该法他发现 M_{67}不为质数（不过他无法给出其因数），且 M_{127}为质数。M_{127}位居最大质数的时期长达近四分之三世纪。至于 M_{61}，则是在 1883 年由 Pervushin 证明为质数。M_{89}及 M_{107}则分别在 1911 年及 1913 年，由 Powers 及 Fauquembergue 证明为质数。不过有些书将 M_{107}也归于 Powers 所发现。

Lucas 证明当 p 为型如 $8k-1$ 的质数时，则 $p\mid M_{(p-1)/2}$。此一结果可用来检验出许多 M_p 为合成数。例如，$47\mid M_{23}$，$167\mid M_{83}$，$263\mid M_{131}$，$359\mid M_{179}$，$383\mid M_{191}$，$479\mid M_{239}$。虽然有这些方法来减少检验时的负担，但对 p 很大时，检验的工作并非易事。如虽知 $M_{101}=2^{101}-1$ 的质因数为 $202k+1$ 型式，但 M_{101}的质因数并不易找出（显然 k 很大）。1930 年，Lehmer 改良 Lucas 的方

法，提出了底下定理7所谓Lucas-Lehmer质数测试法，并于1932年证明M_{257}为质数(梅仙尼质数名单的最后一个错误)。不利用Lucas-Lehmer法，后来那些梅仙尼质数是无法发现的。

定理7. 令$u_1=4$，且对$n\geqslant 1$，令$u_{n+1}=u_n^2-2$。则对每一大于2之质数p，M_p为质数的充要条件为$M_p \mid u_{p-1}$。

定理7之证明可参考Bruce(1993)。在定理7中数列u_n之前四项为4，14，194，37，634，增加快速，检验似乎也不易。不过由定理7不难导出$M_p \mid u_{p-1}$之充要条件为$r_{p-1}=0$，其中$r_1=4$，而对$n\geqslant 1$，令r_{n+1}为r_n^2-2除以M_p之余数。显见每一$r_n\leqslant M_p-1$，所以我们把一成长很快的数列，降成每一项皆不超过M_p的数列，对计算上方便许多。例如，若$p=5$，$M_5=31$，则$r_1=4$，$r_2=14$，$r_3=8$，$r_4=0$，故M_5为一质数。又M_{101}有31位，而因$r_{100}\neq 0$，故得M_{101}为一合成数。诸位是否留意到自定理6以来，我们数次提到余数？事实上同余(即只考虑余数)为数论中一重要的概念，在"同余数及质数在密码学上的应用"一文我们再讨论。

有人进一步猜测，若M_n为一质数，则M_{M_n}也是一质数(真是一群狂热的数学家)。对首四个梅仙尼质数(3，7，31，127)，此猜测是对的，但对第五个梅仙尼质数，即$M_{13}=8,191$，1953年，Wheeler证出$M_{M_{13}}=2^{8,191}-1$(有2，466位)为一合成数，所以此猜测是错的。此事之验证(仍藉助Lucas-Lehmer法)，花了那时计算机一百小时之久(但并未找出其因数)。后来又发现$M_{M_{17}}$为合成数，且有质因数$1,768(2^{17}-1)+1$，而$M_{M_{19}}$亦为合成数，并有质因数$120(2^{19}-1)+1$。除此之外，尚有一些其他的猜测，我们就此打住。

1952年，美国的Robinson以SWAC计算机(这是人类首度以计算机来寻找梅仙尼质数)，找出第十三至第十七等五个梅仙尼质数：M_{521}，M_{607}，$M_{1,279}$，$M_{2,203}$，$M_{2,281}$。1957年Riesel利用瑞典计算机BESK花了五个半小时找出第十八个梅仙尼质数$M_{3,217}$。1961年，美国数学家Hurwitz利用IBM7090计算机找出$M_{4,253}$及$M_{4,423}$两个。接着在1963年，美国伊利诺大学(University of Illinois)的教授Gillies找出下三个$M_{9,689}$，$M_{9,941}$及$M_{11,213}$。其中$M_{11,213}$共有3，376位。伊利诺大学对此发现很高兴，就在该校加盖邮资戳记的机器上加进"$2^{11213}-1$ IS PRIME"一句。于是这句话就出现在该校寄出的每一封邮件上。

第二十四个梅仙尼质数$M_{19,937}$，是由纽约的Tuckerman于1971年找到的。七年后，1978年10月，两位美国加州十八岁的高中学生Nickel及Noll合