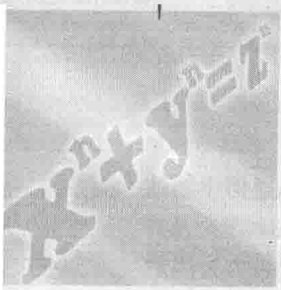
丛书主编：赵焕光

文化数学欣赏丛书 - 5

快乐相遇数论

黄忠裕 赵焕光 著

科学出版社



丛书主编：赵焕光

文化数学欣赏丛书 -5

快乐相遇数论

黄忠裕　赵焕光　著

科学出版社

北京

内 容 简 介

本书从初等数论学科的特色、人文欣赏的视野着手，运用通俗生动的语言、精彩有趣的故事、丰富典型的案例，介绍初等数论的基本理论及其在现实世界中的巧妙应用. 主要内容包括：整除概念与判定、最大公因数与最小公倍数、整数分解与素数分布、同余概念及应用、剩余类与剩余系、欧拉函数的计算与经典同余定理、一次同余方程、一次同余方程组与中国剩余定理、高次同余方程、二次剩余与二次同余方程、原根与离散对数、实用的一次不定方程、诱惑人的费马方程、魅力无限的同余与不定方程联姻.

本书可作为高等院校所有专业的本(专)科生、硕士研究生、中学数学智优生、中学数学教师、具有中学数学基础的高校教师及行政管理人员的数学与人文修养提高读本，也可作为高等院校本(专)科各个专业的选修课教材或教学参考书.

图书在版编目(CIP)数据

快乐相遇数论/黄忠裕，赵焕光著. —北京：科学出版社，2017.6
(文化数学欣赏丛书；5)
ISBN 978-7-03-053844-4

Ⅰ. ①快… Ⅱ. ①黄… ②赵… Ⅲ. ①数论-普及读物 Ⅳ. ①O156-49

中国版本图书馆 CIP 数据核字(2017) 第 139704 号

责任编辑：王丽平 / 责任校对：彭 涛
责任印制：张 伟 / 封面设计：陈 敬

科学出版社出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

北京虎彩文化传播有限公司 印刷

科学出版社发行 各地新华书店经销

*

2017 年 6 月第 一 版 开本：B5(720×1000)
2017 年 6 月第一次印刷 印张：14 3/4
字数：285 000

POD定价： 69.00元
(如有印装质量问题，我社负责调换)

前　言

初等数论是一门以整数为研究对象, 四则运算为研究工具的数学分支. 初等数论初看起来似乎很简单, 数论的主要概念以及一些真正能诱惑人的数学问题的提法, 简单到甚至连小学生都能看明白. 然而, 有些看似简单问题的解决却极其困难, 使得一代又一代的世界一流数学家为其付出一辈子的努力. 比如著名的费马大定理 (即当 n 是一个大于 2 的正整数时, 不定方程 $x^n + y^n = z^n$ 没有正整数解) 自从 17 世纪上半叶被提出, 困惑了全世界顶级数学家 350 余年, 直到 1995 年才最终被英国数学家怀尔斯证明. 而这类尚未解决的世界难题在数论中比比皆是, 例如, 哥德巴赫猜想、孪生素数猜想、奇完全数猜想、费马素数猜想、黎曼猜想等. 所有这些猜想的表述都很简单, 但它们的解决却需要极其复杂的数学工具.

历史上, 数论曾被喻为令人陶醉在象牙塔中的纯数学学科. 这就是说, 数论在实际应用中没有地位. 德国大数学家高斯曾把数论描绘成 "一座仓库, 贮藏着用之不尽的, 能引起人们兴趣的真理". 德国另一位大数学家希尔伯特则把数论看成 "一幢出奇的美丽而又和谐的大厦""它有简单的基本定律, 它有直截了当的概念, 它有纯正的真理". 高斯还认为数论作为数学的皇后, 不愿意用 "有用" 来弄脏她那洁白的双手. 而英国数论专家哈代则曾为自己所研究的数论问题无用而干杯. 或许正是美丽而无用的独特风格所造就的迷人魅力使得数论高居 "数学皇后" 的宝座之上, 并诱惑着无数门外汉与极富才智的顶级数学大师一起如痴如醉地去攀登数论殿堂的顶峰.

的确, 在哈代所处的那个时代, 居于数学中最美妙思想之列的数论, 从未被用于任何非常实际的应用目的. 然而, 随着电子计算机的出现, 却发生了连哈代做梦都想不到的改变. 如今, 涉及国家安全机密与商业利益的网络运行都需要大素数, 大素数分解问题已经与密码破译紧密地联系在一起. 谁能想到, 纯之又纯的数论, 最终会对百姓的日常生活产生如此之大的影响呢?

1948 年, 成功证明弱哥德巴赫猜想 (即每个大于 6 的偶数都可以表示为一个素数与一个整数的和, 该整数的素因子个数不超过某一很大的自然数) 的匈牙利数学家雷尼 (A.Renyi, 1921—1970) 曾经说过, "如果我感到忧伤, 我会做数学变得快乐; 如果我正快乐, 我会做数学保持快乐". 数学带给人们的快乐, 并非像其他娱乐活动所带给人们那种感官刺激上的快乐, 也并非像人们获得物质财富增加的那种外在快

乐, 而是智力自我挑战成功后所感悟到的一种精神快乐. 其实, 解决了一个困难数学问题的思想过程往往是曲折迂回的, 每当人们千辛万苦到胜利顶峰时, 都会记得“山阴道上, 应接不暇” 的沿途美景以及 “山重水复疑无路, 柳暗花明又一村” 那种神奇的快乐. 雷尼正是因为深切地感受到过那种快乐, 才会说出上述肺腑之言.

2015 年 3 月, 我从高校数学教师的岗位上正式退休. 退休之后凭着自己对传播文化数学的一股热情, 能够与自己的学生兼同事黄忠裕副教授合作, 将自己学习初等数论的点滴体会, 与他所具有的丰富教学积累相结合, 整理成书在科学出版社出版, 当然是一件非常快乐的事情. 本书如果作为文化数学普及传播能带给某些读者少许快乐的话, 那么我们就会乐上加乐. 借助多重快乐的构想, 本书取名《快乐相遇数论》.

全书分 4 章. 在正文之前加了一个引子, 简介了哥德巴赫猜想、孪生素数猜想、回文素数猜想以及梅森素数的故事. 第 1 章标题为 “整除理论”, 整除理论是初等数论的理论基础, 可以说初等数论中研究的问题大部分都与整除有关. 该章介绍整除的基本理论, 主要内容包括: 整除概念与判定、最大公因数与最小公倍数及整数分解与素数分布. 第 2 章标题为 “同余理论”, 同余理论是初等数论的核心, 同余思想、同余方法可以有效地简化涉及整除性的许多问题, 因此具有很重要的理论价值, 而且还有很广泛的实际应用. 该章介绍同余的基本知识及基本理论, 主要内容包括: 同余概念及应用、剩余类与剩余系及欧拉函数的计算与经典同余定理. 第 3 章标题为 “同余方程”, 求解同余方程是初等数论的核心问题, 同余方程是运用同余思想研究数论问题的途径与方法, 而且也是公钥密码学最重要的理论基础. 该章介绍同余方程的基本理论及其应用, 主要内容包括: 一次同余方程、一次同余方程组与中国剩余定理、高次同余方程、二次剩余与二次同余方程以及原根与离散对数. 第 4 章标题为 “不定方程”, 不论是理论还是实际应用, 不定方程都具有重要的地位. 该章介绍几类简单的不定方程的求解及其应用, 主要内容包括: 实用的一次不定方程、诱惑人的费马方程及魅力无限的同余与不定方程联姻.

本书的写作框架由我与黄忠裕副教授共同讨论形成, 初稿以及书中基础训练与拓展及解答提示由黄忠裕提供. 黄忠裕副教授长期从事高等学校初等数论课程的教学与研究工作, 积累了丰富的教学经验及教学资料. 就初等数论这门学科来说, 我与黄忠裕相比只能算是 “门外汉”, 不过我的数学人文修养方面可能比他稍许强一些. 因此, 我在他的写作基础上添加了数学人文修养方面的内容, 全书最终由我定稿.

吾妻钱亦青在书稿打印及文献查阅方面付出辛勤劳动, 在此表示特别的感谢! 温籍华人数学家季理真教授对本书初稿提出画龙点睛式的宝贵修改建议, 并热心提供关于素数方面的宝贵参考文献资料, 在此致以真诚的感谢! 本书写作过程中参阅了大量参考文献, 为此也向被本书引用的参考文献作者表示真诚的感谢! 本书在写

作过程中得到温州大学校领导、温州大学数学学院领导、浙江省重点学科 “应用数学”、温州大学重点学科 “数学”、温州大学重点专业 “数学与应用数学”、温州大学科研处、温州大学人文社科处等有关部门的大力支持, 在此一并表示感谢!

限于作者水平, 不妥之处在所难免, 敬请广大读者不吝批评指教.

赵焕光

2016 年 10 月 12 日

目　录

前言
引子　素数奇趣与猜想 …… 1
0.1　哥德巴赫猜想 …… 2
0.2　孪生素数猜想 …… 2
0.3　回文素数猜想 …… 4
0.4　梅森素数的故事 …… 5
第 1 章　整除理论 …… 9
1.1　整除概念与判定 …… 9
1.1.1　整除与带余除法 …… 9
1.1.2　奇数与偶数 …… 11
1.1.3　整除判定 …… 12
1.1.4　整除概念基础训练与拓展 …… 14
1.2　最大公因数与最小公倍数 …… 15
1.2.1　最大公因数 …… 15
1.2.2　最小公倍数 …… 23
1.2.3　最大公因数基础训练与拓展 …… 25
1.3　整数分解与素数分布 …… 27
1.3.1　素数与合数概念及特征 …… 27
1.3.2　算术基本定理 …… 30
1.3.3　两种初等整数分解方法 …… 33
1.3.4　$n!$ 素因数分解 …… 35
1.3.5　整数分解正因数定理与完全数 …… 39
1.3.6　素数分布及素数定理 …… 41
1.3.7　整数分解基础训练与拓展 …… 47
第 2 章　同余理论 …… 49
2.1　同余概念及应用 …… 49
2.1.1　同余概念 …… 49
2.1.2　同余四则运算 …… 51

2.1.3 同余在整除判别中的应用 ····· 53
2.1.4 同余在末位数判别中的应用 ····· 54
2.1.5 例说同余实际应用 ····· 56
2.1.6 同余概念基础训练与拓展 ····· 61
2.2 剩余类与剩余系 ····· 61
2.2.1 概念及其判别 ····· 62
2.2.2 剩余系构造 ····· 64
2.2.3 威尔逊定理与素数判别 ····· 68
2.2.4 例说完全系实际应用 ····· 69
2.2.5 剩余类基础训练与拓展 ····· 72
2.3 欧拉函数的计算与经典同余定理 ····· 72
2.3.1 欧拉函数的计算公式 ····· 73
2.3.2 欧拉定理与费马小定理 ····· 76
2.3.3 费马小定理之逆与伪素数 ····· 79
2.3.4 欧拉定理对循环小数的应用 ····· 83
2.3.5 欧拉定理对 RSA 体制的应用 ····· 85
2.3.6 欧拉函数基础训练与拓展 ····· 89
第 3 章 同余方程 ····· 91
3.1 一次同余方程 ····· 91
3.1.1 方程系数与模互素的一次同余方程 ····· 92
3.1.2 方程系数与模不互素的一次同余方程 ····· 94
3.1.3 一次同余方程对 RSA 体制的应用 ····· 96
3.1.4 一次同余方程基础训练与拓展 ····· 97
3.2 一次同余方程组与中国剩余定理 ····· 98
3.2.1 中国剩余定理 ····· 98
3.2.2 中国剩余定理的思想原则应用 ····· 102
3.2.3 模不互素的一次同余方程组 ····· 103
3.2.4 一次同余方程组基础训练与拓展 ····· 106
3.3 高次同余方程 ····· 107
3.3.1 高次同余方程的解与解数 ····· 107
3.3.2 模为素数的高次同余方程 ····· 110
3.3.3 模为素数幂的高次同余方程 ····· 113
3.3.4 高次同余方程基础训练与拓展 ····· 117
3.4 二次剩余与二次同余方程 ····· 117
3.4.1 二次剩余 ····· 118

3.4.2 勒让德符号 ····· 121
3.4.3 高斯二次互反律 ····· 128
3.4.4 雅可比符号 ····· 132
3.4.5 二次同余方程解的模式 ····· 135
3.4.6 二次剩余在零知识证明中的应用 ····· 139
3.4.7 二次剩余基础训练与拓展 ····· 141
3.5 原根与离散对数 ····· 142
3.5.1 阶与原根 ····· 142
3.5.2 原根存在定理 ····· 145
3.5.3 原根的个数与求法 ····· 148
3.5.4 离散对数 ····· 151
3.5.5 离散对数在密码学中的应用 ····· 155
3.5.6 n 次剩余 ····· 158
3.5.7 原根基础训练与拓展 ····· 161
第 4 章 不定方程 ····· 162
4.1 实用的一次不定方程 ····· 162
4.1.1 二元一次不定方程 ····· 163
4.1.2 二元一次不定方程实际应用 ····· 165
4.1.3 二元一次不定方程的非负解 ····· 167
4.1.4 多元一次不定方程 ····· 171
4.1.5 一次不定方程基础训练与拓展 ····· 174
4.2 诱惑人的费马方程 ····· 174
4.2.1 毕达哥拉斯方程 ····· 175
4.2.2 4 次幂费马方程 ····· 178
4.2.3 费马方程基础训练与拓展 ····· 182
4.3 魅力无限的同余与不定方程联姻 ····· 183
4.3.1 奇素数平方和表示 ····· 183
4.3.2 拉格朗日平方和定理 ····· 187
4.3.3 奇异的佩尔方程 ····· 191
4.3.4 同余观下的不定方程 ····· 196
4.3.5 同余观下的不定方程基础训练与拓展 ····· 199
基础训练与拓展解答提示 ····· 201
参考文献 ····· 225

引　子

素数奇趣与猜想

数学是什么？至今还没有令大家满意的答案，数学家仅仅从不同的侧面给予解释. 德国数学家克罗内克 (L. Kronecker, 1823—1891) 曾说过，“上帝创造了整数，其余一切都是人造的”. 那么，整数由什么构成？答案是素数. 事实上，初等数论中的算术基本定理告诉我们，每个整数都可以唯一地表示为若干素数的乘积. 这就是说，素数是构成一切整数的基本单元，其作用就相当于化学中的原子，或者说相当于物理中的基本粒子. 因此，有人把素数称作算术中的“原子”.

对数论研究做出杰出贡献的德国大数学家高斯 (C.F.Gauss, 1777—1855) 曾用“数学是科学的皇后，而数论是数学的皇后”这句话表达他对数论的钟爱. 在某种意义上说，数论是一门以素数作为其研究对象的学问，作为构筑数论大厦的基石，素数理所当然在数论中起着中心的作用. 远从古希腊开始，人们就对素数着迷，如今，信息保密、网络安全运行都离不开素数. 因此，有人把素数比作数学中美妙的音乐、美丽的女神.

所谓素数，就是指除自身与 1 之外没有其他真因数的正整数. 素数概念清晰易懂，只要学过小学数学就能轻松地描述它. 虽然素数表面上看起来简单朴素，但素数行踪不定，其秉性让人永远捉摸不透. 对数论研究做出很大贡献的瑞士大数学家欧拉 (L.Euler, 1707—1783) 曾说过：“一直以来，数学总是在孜孜不倦地寻找素数规律，但是很难成功. 我们可以把素数看作人类思维无法渗透的奥秘”. 越是难以征服的东西，越能激发人们的好奇心！从公元前到现在的 2400 多年间，世界各国的数学家义无反顾地追寻素数奥秘，如同飞蛾扑火，前赴后继. 沿途众多大学者创造出许多关于素数的美丽故事，同时提出许多至今悬而未决的猜想，诸如哥德巴赫猜想、孪生素数猜想、回文素数猜想、梅森素数猜想等. 接下来，我们将对这几个著名猜想作简单介绍.

0.1 哥德巴赫猜想

算术基本定理告诉我们, 素数的重要性就体现在所有整数都可表示成素因数的乘积. 因此, 在谈论素数的时候, 乘法便是理所当然的操作. 那么对加法来说, 是否也有相类似的结果呢? 这是到目前为止没有获得彻底解决的世界难题.

1742 年, 德国业余数学家哥德巴赫 (C. Goldbach, 1690—1764) 在和他的好朋友 —— 大数学家欧拉的几次通信中, 首先提出了关于素数之和的两个推测:

(A) 每一个不小于 6 的偶数都是两个奇素数之和;

(B) 每一个不小于 9 的奇数都是三个奇素数之和.

这就是著名的哥德巴赫猜想. 我们把猜想 (A) 称为 "关于偶数的哥德巴赫猜想", 把猜想 (B) 称为 "关于奇数的哥德巴赫猜想". 由于

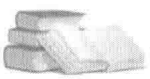
$$2n+1=2(n-1)+3,$$

所以, 从猜想 (A) 的正确性立即推出猜想 (B) 的正确性. 反之, 则推不出.

欧拉虽然没有能够证明这两个猜想, 但是对它们的正确性是深信不疑的. 1742 年 6 月 30 日, 在给哥德巴赫的一封信中他写道: 我认为这是一个肯定的定理, 尽管我还不能证明出来.

然而, 辗转几个世纪, 一直没有人证明它. 1920 年挪威数学家布朗建议将证明分成若干步骤, 就是先证明任何充分大的偶数都可以表示成两个正整数之和, 简称 "$a+b$", 其中一个正整数的素因子个数都不超过 a, 另一个素因子个数都不超过 b. 先对比较大的 a 和 b 证明, 然后逐步缩小, 如果最终缩小到 "$1+1$", 那么就证明了哥德巴赫猜想.

中国数学家在攻克这个世界著名猜想的征途上成就非凡. 1956 年, 中国数学家王元证明了命题 "$3+4$", 由此开启了中国数学家在哥德巴赫猜想 "$a+b$" 研究上的先河. 其后, 王元和另一位中国数学家潘承洞又得到了若干重要的结果, 使得我国在哥德巴赫猜想方面的研究达到了国际先进水平. 1966 年, 陈景润宣布证明了命题 "$1+2$"; 1973 年, 他发表了 "$1+2$" 的全部证明. 所谓 "$1+2$", 就是指所有充分大的整数都能表示成一个素数与一个至多两个素数乘积之数的和. 到目前为止, 陈景润的成果仍然是最好的.



0.2 孪生素数猜想

所谓孪生素数 (prime twins), 就是指差为 2 的素数对. 例如, 前几对孪生素数分别是 $(3,5)$, $(5,7)$, $(11,13)$, $(17,19)$, $(29,31)$, $(41,43)$, $(59,61)$ 等.

一般说来, 若 p 与 $p+2$ 都是素数, 则称 $(p,p+2)$ 为孪生素数. 到目前为止, 已知最大的孪生素数对为: $2003663613\cdot 2^{195000}\pm 1$. 这两个数都有 10 万多位, 这是在 2001 年由一批数学家通过国际合作, 在许多台计算机上运行他们的程序所得到的结果.

关于孪生素数有一个著名猜想: *存在无穷多对孪生素数*. 这个猜想至今没有被证明. 数学史家没有弄清楚何时何地何人首先提出孪生素数猜想, 然而可以肯定的事情是, 法国数学家德波利尼亚克 (Depolignac, 1817—1890) 于 1849 年提出了更一般的猜想:

对任意自然数 k, 存在无穷多个素数对 $(p,p+2k)$.

这就是说, 任意偶数都是无穷多对相邻素数的间隔. 特别地, 当 $k=1$ 时, 这个猜想就是著名的孪生素数猜想.

中国数学家陈景润在 1966 年所做的 "$1+2$" 的证明工作中可推出, 存在无穷多个素数 p, 使得 $p+2$ 的素因子不超过 2 个.

1982 年毕业于北京大学数学系的张益唐在美国沉默 20 多年后, 一鸣惊人于 2013 年 4 月, 向美国顶级数学杂志《数学年刊》(*Annals of Mathematics*) 提交了题为《素数间的有界距离》的文章. 文章中证明了:

存在无穷多个素数对 (p,q), 其中每一对中的两个素数之差, 即 p 和 q 的距离, 不超过 7000 万.

由此推出, 存在无穷多个素数对 (p,q), 以及一个不超过 7000 万的正偶数, 使得 $p-q=h$.

张益唐的工作在解决孪生素数猜想这一超越一百多年的数论难题的道路上前进了一大步, 这是值得所有华人骄傲的智力极限挑战.

有两项与孪生素数猜想有关的工作值得介绍. 一项工作是于 1919 年, 布伦 (V.Brun, 1885—1978) 证明了:

全体孪生素数的倒数之和收敛.

这个结果能说明孪生素数很稀疏, 但无法说明该级数只有有限项.

另一项工作是于 1949 年, 克利门特 (P.A.Clement) 给出了判定孪生素数的充要条件:

$$(n,n+2)\text{为孪生素数对当且仅当 } 4[(n-1)!+1]+n\equiv 0(\mathrm{mod}(n^2+2n)).$$

此外, 孪生素数还有多种推广, 其推广形式之一就是所谓素数等差数列, 即全部由素数组成的等差数列. 例如, $3,5,7$; $3,7,11$; $3,11,19$ 等都是 3 项素数等差数列. 又如 $61,67,73,79$ 是公差为 6 的 4 项素数等差数列, 而 $5,11,17,23,29$ 则是公差为

6 的 5 项素数等差数列. 通常把素数等差数列中的元素个数称为长度.

2007 年, 波兰数学家 Wroblewski 找到了长度为 24 的等差数列

$$468395662504823 + 45872132836530n \quad (0 \leqslant n \leqslant 23).$$

这是到目前为止所能找到的长度最长的素数等差数列.

2004 年, 华裔澳大利亚数学家陶哲轩 (Terence Tao, 1975—) 和英国数学家格林 (Green, 1977—) 利用分析中的遍历理论和组合中的拉姆齐理论证明了:

存在无穷多个任意长度的素数等差数列.

这是一项非常了不起的成就. 因为此前, 即使长度为 3 的素数等差数列, 人们也无法判定是否有无穷多项. 正是因为这项成就作为基础, 陶哲轩获得 2006 年度菲尔兹奖 (数学最高奖).

0.3 回文素数猜想

所谓回文素数就是指正读与反读都是同一个数的素数. 回文素数不算很多, 在 1000 以内只有下列 16 个:

$$11, 101, 131, 151, 181, 191, 313, 353, 373, 383, 727, 757, 787, 797, 919, 929.$$

1000 以上的回文素数非常稀少, "物以稀为贵", 人们用手工计算很难寻找, 数学家借助计算机找到数量不少的回文素数. 在寻找极大回文素数方面, 数学家杜勃讷 (H.Dubner) 一直保持着创纪录的成绩. 下面这些奇特的大回文素数就都是他发现的:

(1) *仅由 0 和 1 组成的一个大回文素数是这样的:* $1(0)_{2415}(1)_9(0)_{2415}1$, *式中* $(0)_{2415}$ *表示连续 2415 个 "0",* $(1)_9$ *表示连续 9 个 "1", 所以这个回文素数共有 4841 位, 是杜勃讷 1989 年发现的.*

(2) *同年, 杜勃讷还发现了仅由一个数字 2, 其余全是 9 所组成的回文素数:*

$$(9)_{2874}2(9)_{2874}.$$

这个回文素数有 5749 位.

(3) *一个超过 1 万位的回文素数:*

$$10^{11310} + 4661664 \times 10^{5652} + 1,$$

这个数实际上是 4661664 前后各持有 5652 个 0, 首尾为 1, 所以共有 11311 位. 这个回文素数的独特之处不但在于它极大, 还在于它的位数 11311 本身也是一个回文

素数. 如果把 11311 的位数 5 也看成是一个回文素数, 那么可以把这个回文素数叫成“三重回文素数”.

(4) 目前已知的最大回文素数如下:

$$10^{11810}+1465641\times 10^{5902}+1,$$

这个回文素数共有 11811 个数位.

是否存在无穷多个回文素数? 这是至今还没有被解决的著名猜想.

加拿大数学家格里奇曼 (N.Gridgeman) 在研究回文素数时发现了这一个奇异的现象, 即在奇数位的回文素数中常常出现仅数字差 1, 而两侧数字都相同的素数对, 他把这样的素数对叫做回文素数对. 例如, 在最前面的 47 个回文素数中, 就有近一半即 22 个组成回文素数对:

$$(181,191),(373,383),(787,797),(919,929),(10501,10601),(11311,11411),$$

$$(12721,12821),(13831,13931),(15451,15551),(16561,16661),(30103,30203).$$

目前已知的最大的回文素数对如下:

$$\left(\underbrace{11\cdots1}_{45个1}4\underbrace{11\cdots1}_{45个1},\underbrace{11\cdots1}_{45个1}5\underbrace{11\cdots1}_{45个1}\right).$$

是否存在无穷多对回文素数对? 也是至今没有获得解决的猜想.

0.4 梅森素数的故事

法国业余数学家梅森 (M.Mersenne, 1588—1648) 的职业是一位神父, 但他酷爱数学, 数学是他的第一业余爱好. 在数论中因发现以他的名字而命名的素数表达式而闻名. 梅森花了四年多的时间研究并检验形如 $2^n-1(n=1,2,\cdots)$ 的整数是否为素数, 直至 $2^{257}-1$ 的全部整数, 并于 1644 年在他的《物理数学随感》一书中写道:

“总结前人的工作和我个人的研究, 可以得到结论: 在 $n\leqslant 257$ 的数中, 除了当 $n=2,3,5,7,13,17,19$ 时, 2^n-1 是素数外, 猜想 $n=31,67,127$ 和 257 时, 2^n-1 也是素数. 而 $n<257$ 其他数值, 2^n-1 都是合数.”

梅森提出的这一大胆猜想, 大大缩短了人们寻觅最大素数的验证范围. 因此, 人们便将形如 $2^n-1(n$ 是素数) 的素数命名为 “梅森素数” 或 “梅森素数猜想”, 并且用他名字的头一个字母记梅森素数为 $M_n=2^n-1$, 这就是梅森素数的来历.

梅森素数的验证工作是十分艰辛的, 其中前 7 个 M_n(即 $n=2,3,5,7,13,17,19$) 是素数已为前人所知, 而其后 n 个数的验证异常困难, 无法断定真伪.

下面我们按时间的先后顺序, 讲述梅森素数的精彩故事.

1772 年大数学家欧拉在双目失明的情况下, 凭心算证明了 M_{31} 是素数, 即找到了第 8 个梅森素数.

1876 年法国数学家卢卡斯 (E.Lucas, 1842—1891) 证明了 M_{127} 是素数.

1883 年佩乌森 (J.pervusin) 证明了 M_{61} 是素数, 这是梅森漏掉的一个素数.

1903 年, 堪称梅森素数研究史上的奇迹发生了. 在美国纽约市一次数学学术报告会上, 美国数学家科尔 (Koler) 作了一次不讲话的学术报告. 他默默走上讲台, 一言不发, 在黑板上写出

$$M_{67}=2^{67}-1=147573952588676412927=193707721\times 761838257287.$$

他没有说一句话又回到自己的座位上, 会场顿时响起暴风雨般的祝贺掌声, 因为他已证明了 M_{67} 是一个合数, 而否定梅森说的 M_{67} 是素数的猜想. 据说获得这一结论, 花了科尔三年中全部星期天的时间.

从此以后, 人们不再盲从, 开始重新审查梅森的结果.

1911 年和 1914 年鲍尔斯 (R.E.Powers) 和福克贝尔古 (E.Fauquembergue) 分别独立找到了梅森漏掉的另外两个素数 M_{89} 和 M_{107}.

1922 年数学家克赖奇克 (M.Kraitchik) 验证了 M_{257} 不是素数, 但他当时没有给出这一合数的因子, 直到 20 世纪 80 年代人们才知道它有 3 个素因子. 按顺序来排, 当年梅森给出的 M_{127} 应该是第 12 个梅森素数. 在电子计算机发明前, 人们也只找到这 12 个梅森素数. 电子计算机的应用大大加快了寻找梅森素数的步伐.

1952 年数学家鲁宾逊 (R.M.Robinson) 等在洛杉矶使用 SWAC 型计算机在短短几小时之内就找到了 5 个梅森素数, 其中的 n 分别为 521, 607, 1279, 2203, 2281. 此后, 随着计算机性能和计算程序的改进, 新的梅森素数不断出现. 需要注意的是, 新的梅森素数也往往是新的最大素数.

1963 年美国伊利诺伊大学数学系的吉利斯 (D.Gillies) 使用 ILLIAC 型计算机找到第 21—23 个梅森素数, 其中第 23 个梅森素数的 $n=11213$. 该系为纪念这一突出成就, 在它寄出的每个信封上都印有 "$2^{11213}-1$ 是素数" 的字样.

1971 年 3 月 4 日晚, 美国哥伦比亚广播公司中断了正常节目播放, 发布了塔克曼 (B.Tuckerman) 使用 IBM360-91 型计算机找到新的梅森素数 M_{19937} 的消息, IBM 公司当仁不让, 将 "$2^{19937}-1$ 是素数" 的字样印到了它的办公信封上. 数学家利用各种最新计算机, 不停息不知疲倦地在巨大的天文数字运算中, 继续寻觅梅森素数.

1982 年到 1985 年的三年里, 英国数学家史诺云斯基 (D.Slowirski) 用运算速度最快的计算机分别求得三个梅森素数: M_{86243}, M_{132049} 和 M_{216091}.

1985 年美国休斯敦一家技术公司的研究人员发现 M_{216091} 是一个 65050 位的素数.

1988 年又有数学家发现史诺云斯基漏掉的梅森素数 M_{110503}.

1992 年 3 月到 1995 年, 史诺云斯基又发现第 32—34 三个梅森素数: M_{756839}(有 227832 位), M_{859433}(有 258716 位) 和 $M_{1257787}$(有 378632 位). 最后一个是当时宣布发现的最大一个素数. 若把这个数字印成书, 可有 200 多页, 真是一个布满数字的天书.

在因特网在全世界掀起热潮与广泛应用之际, 寻找梅森素数的工作又开始进入另一波高峰.

1996 年, 美国一位退休的计算机程序员, 创建了一个网民志愿者组织, 缩写名为 "GIMPS"(意为 "全球因特网梅森素数大搜索"), 利用因特网上极为丰富的资源, 来寻找梅森素数, 开展一场科学史上的人民战争. 这个组织动员了很多的数学爱好者, 将网上几万、几十万台计算机联合起来, 共同协作, 搞大兵团寻找梅森素数. 组织者公布寻找梅森素数的程序、方法等. 该年的 11 月 13 日, 作为当时的 700 多名志愿者之一, 年仅 29 岁的巴黎程序员, 经过 88 个小时的运算以后, 找到了第 35 个梅森素数, 即 $M_{1398269}$, 该数有 420921 位, 打印出来有 225 页之多.

时光像急流电飞逝, 参与向科学进军这一行动的网民成员迅速增加, 到 1997 年 8 月增至 2000 多人. 8 月 24 日, 从英国传来喜讯, 38 岁的信息技术主管, 用时 15 天找到了第 36 个梅森素数 $M_{2976221}$.

1998 年 1 月 27 日, 又传来了好消息. 美国加利福尼亚大学年仅 19 岁的大学生克拉克森 (L.Clarkson) 发现了第 37 个梅森素数 $M_{3021377}$, 该数有 909526 位. 克拉克森是 4000 多名志愿者中的幸运者, 他利用空闲时间, 经过 46 个日日夜夜的运算, 电脑屏幕上突然出现一行文字 "你找到了一个新的梅森素数! ", 让这位年轻人高兴地跳起来.

成就感像磁铁般地吸引着网民志愿者, 1999 年会员猛增到 12600 人, 参与计算机达 21500 台. 在美国工作的一位印度人, 在该年 6 月 1 日, 用 21 天的时间找到了第 38 个梅森素数 $M_{6972593}$, 位数达 2098960 位, 首次超过百万位大关. 由此, 他获得美国电子前沿基金会 5 万美元奖金, 成为历史上第一位因寻找到较大梅森素数而得奖的获奖人.

2001 年 11 月 14 日, 惊人的喜讯又传来, 一位 20 岁的加拿大青年, 白天上学, 晚上参加就业培训, 他利用闲暇时间与另一个人寻找, 用时 45 天, 终于找到了第 39 个梅森素数 $M_{13466917}$, 该数共有 4053846 位. 当时参与的计算机已超过 205000 台, 他是 13 万名志愿者中的幸运者.

美国人和德国人又相继在 2003—2006 年先后发现了 5 个更大的梅森素数, n 的值分别为 20996011, 24036583, 25964951, 30402457 和 32582657, 位数分别达到 6320430, 7235733, 7816230, 9152052 和 9808358 位. 至此, 共发现了 44 个梅森素数.

2008 年 8 月 23 日, 美国加利福尼亚大学洛杉矶分校以计算机专家史密斯 (E.Smith) 为首的专家组用 75 台计算机同时联网运行, 发现了第 47 个梅森素数 (第 45, 46 个的发现反在其后), 这距第 44 个梅森素数的发现已时隔两年之久. 这个梅森素数的 $n = 43112609$, 共有 12978189 位数! 如果用普通字号将它连续写下来, 长度可超过 50 公里! 这也是在加利福尼亚大学洛杉矶分校发现的第 8 个梅森素数.

2008 年 9 月 6 日德国一化学公司的电子工程师埃尔费尼希 (H.M.Elvenich) 发现了一个新的梅森素数 $M_{37156667}$, 该数字有 11185272 位数. 有趣的是, 它比早发现的那个要小一点 (这也是史无前例的).

2009 年斯特林莫 (O.M.Strindmo) 发现新的梅森素数 $M_{42643801}$, 仍比史密斯发现的要小. 这 3 个新发现的梅森素数也是首次突破 1000 万位的素数.

目前最大的梅森素数是 2016 年 1 月由美国密苏里州立大学柯蒂斯库珀 (Curtis Cooper) 通过大互联网梅森素数搜索 (GIMPS) 分布式计算项目发现的, 这是第 49 个梅森素数 $M_{74207281}$, 为 GIMPS 项目诞生 20 周年献礼. $M_{74207281}$ 这个超大素数有 22338618 位, 是目前已知的最大素数, 诞生自一台 Intel17-4790CPU 电脑. 这是库珀教授协同沃尔特曼 (Woltman)、库罗夫斯基 (Kurowski) 等第四次通过 GIMPS 项目发现的新的梅森素数, 刷新了他自己的记录. 他上次发现的第 48 个梅森素数 $M_{57885161}$ 是在 2013 年 1 月, 有 17425170 位.

不过人们仍不能保证寻找梅森素数是按由小到大的顺序, 而只能说已经找到了 49 个梅森素数.

人们为什么要投入那么多的精力研究梅森素数? 这是因为信息安全与密码学中需要大素数, 而到目前为止, 最大的素数都是从梅森素数中找到的, 科学家利用计算机寻找梅森素数并非仅仅是一种计算机游戏, 这项工作也不但是在信息科学与密码学等应用学科有广泛应用, 而且也是综合评判计算机软硬件水平的重要方式.

梅森素数研究任重而道远, 是否存在无穷多个梅森素数? 是否有无穷多个 M_n 是合数? 到目前为止仍是悬而未决的数论难题之一.