



数学是所有科学的基础，具有极富实用意义的内容。数学是科学桂冠上的明珠，闪烁着人类智慧的光芒，千百年来吸引无数的俊杰去奉献着自己的智慧和才华……

图文版

$$x+y=z$$



# 数学的奥秘

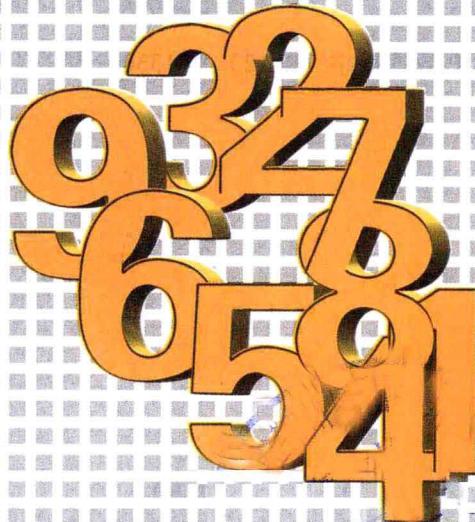
本书编委会◎编著



中国长安出版社

探索魅力科学

TANSUOMEILIKEXUE



# 数学的奥秘

SHUXUEDEAOMI



中国长安出版社

**图书在版编目 (CIP) 数据**

数学的奥秘 / 《探索魅力科学》编委会编. —北京：  
中国长安出版社，2012.6

(探索魅力科学)

ISBN 978 - 7 - 5107 - 0537 - 3

I . ①数… II . ①探… III . ①数学 - 普及读物 IV.  
①O1 - 49

中国版本图书馆 CIP 数据核字 (2012) 第 133092 号

## **数学的奥秘**

《探索魅力科学》编委会 编

---

出 版：中国长安出版社

社 址：北京市东城区北池子大街 14 号 (100006)

网 址：<http://www.ccapress.com>

邮 箱：[ccapress@yahoo.com.cn](mailto:ccapress@yahoo.com.cn)

发 行：中国长安出版社

电 话：(010) 85099947 85099948

印 刷：北京市艺辉印刷有限公司

开 本：710 毫米×1000 毫米 16 开

印 张：9

字 数：120 千字

版 本：2012 年 10 月第 1 版 2012 年 10 月第 1 次印刷

---

书 号：ISBN 978-7-5107-0537-7

定 价：21.40 元

# 1 生活中的数学

几何与日常生活	2
条形码中的数学原理	3
不查日历算星期几	4
电脑算命	5
怎样买门票最省钱	7
最美的黄金分割	8
民间数学诗	9
家庭主妇怎么当	10
揭开密码的神秘面纱	11
怎样分牛	13
神秘的大自然	14
田忌赛马	16
足球数学	18
做聪明的消费者	20
人生格言	21
分类销售与混合销售	
哪个更合算	22
巧用数学解难题	24
巧测超速行驶	25
巧用数学惩恶主	26



# 2 数学桂冠上的明珠

哥德巴赫猜想	28
费马最后定理	30
从蜂窝猜想到蜂窝定理	32
令人着迷的四色问题	34
哥尼斯堡七桥问题	36
庞加莱猜想	38
黎曼假设	40
引人入胜的三大尺规作图问题	42
六度空间理论	44
梅森素数	46
孪生素数猜想	48
霍奇猜想	50

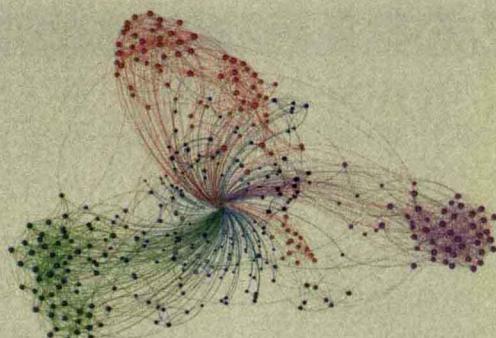
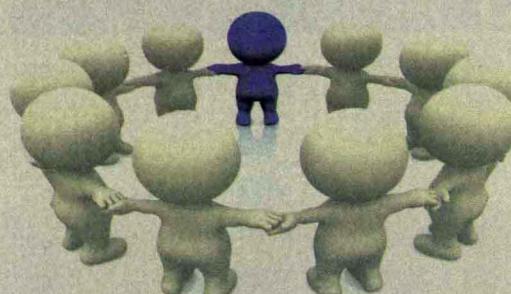
# 3 趣味数学

圆周率记趣	52
有趣的速算	54
数学符号的由来	56
三角形面积公式的推广	58
欺骗眼睛的几何问题	60
国王无法完成的赏赐	62

阿拉丙的藏宝箱	64
米兰芬算灯	66
阿基里斯追不上乌龟	68
扑克牌中的数学游戏	70
富兰克林的遗嘱与	
拿破仑的诺言	72
爱因斯坦的谜题	74
数学笑话六则	76
雪花曲线	78
从植物解方程谈起	79
趣谈地球上的数学	80
3根指挥棒和12个直角	82
奇怪的遗嘱	84
数学侦探	85
数学黑洞	86
没有秤砣称西瓜	87
有限与无限的纠结	88
难倒你的古代算术题	90

## 4 著名数学家小传

数学史上第一人——泰勒斯	92
神秘的科学始祖	
——毕达哥拉斯	94
几何学之父——欧几里德	96
伟大的智者——阿基米德	98
现代科学之父——牛顿	100
二进制发明者——莱布尼茨	102



数学界的莎士比亚——欧拉	104
弃儿数学家——达朗贝尔	106
数学王子——高斯	108
大分析学家——柯西	110
早逝的数学家——伽罗瓦	112
出色的教师数学家	
——魏尔斯特拉斯	114
羞怯又大胆的数学家——黎曼	116
世界上第一个女数学博士	
——索菲娅	118
世界数学巨人——希尔伯特	120
神奇的数学预言家	
——拉玛努贾	122
举世闻名的“神童”——维纳	124
计算机之父——冯·诺伊曼	126
《九章算术》注释者——刘徽	128
圆周率计算的巨大贡献者	
——祖冲之	130
中国函数论的开拓者	
——陈建功	132
把拓扑学引入中国的第一人	
——江泽涵	134
中国现代数学之父——华罗庚	136
了不起的中国数学家	
——陈景润	138
微分几何之父——陈省身	140

第一部分  
PART ONE

## 生活中的数学

SHENGHUOZHONGDESHUXUE

在我们的生活中存在着许许多多的数学问题，它们有时会以实际问题的形式出现；有时又会以游戏的形式出现。它们就像一个个顽皮的孩子，或隐或现地与我们捉迷藏、玩游戏，激起我们探索它们的兴趣。



# 几何与日常生活

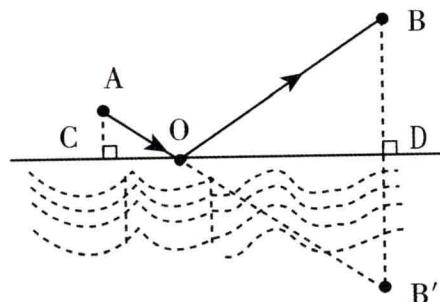
JIHEYURICHANGSHENGHUO

初学几何时，你往往会感到这门学科枯燥乏味，有的知识似曾相识，似懂非懂；有的知识则似乎很“玄”，离我们很远！其实，在我们的日常生活中，几何问题无时无刻的陪伴着我们。

比如，唐代诗人李颀在《古从军行》开篇写道：“白日登山望烽火，黄昏饮马傍交河”。引出著名的“将军饮马问题”，将军们白天登上山巅眺望报警的烽火，傍晚到交河岸边饮马。如下图所示，假如将军们从山脚的A点出发到交河边饮马，然后回到驻地B点。则怎样选择饮马地点，才能使得路程最短？

## ● 现象

如图从A点到河边C点最近，但回驻地的路程较远，如果选择饮马地点为河边D点，回驻地的路程最近，但是从出发点A到饮马地点D的距离又太远了。这怎么办呢？



古代纸莎草纸上的几何图案

## ● 分析

我们可以运用轴对称的方法把它转化成两点之间线段最短的问题来解决。如图，以河边为对称轴（假定河边是一条直线），作出点B关于河边为对称轴的B'点，这样就把问题解决掉了，即，连接AB'交河边于O点，这里就是使得从A点出发到河马饮马回驻地B点路程最短的最佳地点。

## ● 论证

由于B'点是关于以河边为对称轴的点B的对称点，所以 $OB=OB'$ ，饮马路程 $AO+BO$ 就等于 $AO+OB'$ ， $AOB'$ 是连接AB'的线段，其余的地点饮马路程一定大于这条路径。



条形码是将宽度不等的多个黑条和空白，按照一定的编码规则排列，用以表达一组信息的图行标识符。常见的条形码是由反射率相差很大的黑条（简称条）和白条（简称空）排成的平行线图案。



# 条形码中的数学原理

TIAOXINGMAZHONGDESHUXUEYUANLI



3白2黑1白1黑

表示：0



2白2黑2白1黑

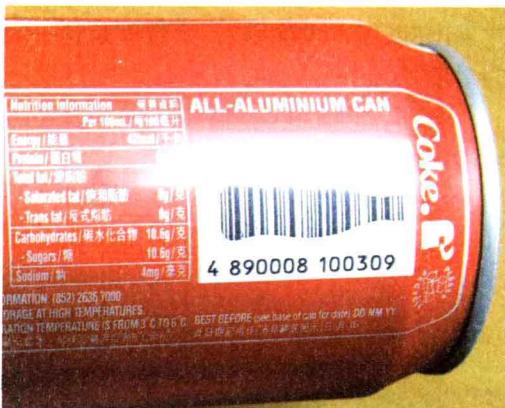
表示：1

## ● 条形码与商品条形码

国际流行的条形码有很多种，本文所讲的是在超级市场上使用的商品条形码。

## ● 起始符，终止符和中心符

超级市场使用的商品条形码左侧，右侧和中间均有2条较长的细线，分别表示起始符、终止符和中心符。这六条线只起分隔作用，并无数字与它们对应，在起始



以可口可乐瓶子的曲线为条形码的造型

符与中心符之间有12条黑条纹，在中心符与终止符之间也有12条黑条纹，这些黑白条纹下面是对应的数字，中心符左，右侧分别为左，右侧数据符。

## ● 黑白条纹如何表示不同的数字

在大多数的条形码中，由黑白相间的四条线组成一个数字（左侧数据符中，左起第一条是白的。右侧数据符中，左起第一条是黑的）。这四条线中每一条的宽度可以取1至4个单位，但四条线的总宽度为7个单位。

例如：表示0和1，见左上图。

这样四条线能够表示多少不同的信号呢？这就与中学数学中的排列组合有关了。

提示：因为这四条线的宽度至少为1个单位，因此首先取每条线宽度为1个单位，然后增加分配3个单位到这四个位置，使总宽度为7个单位。

## 知识链接

条形码技术是随着计算机与信息技术的发展和应用而诞生的，它是集编码、印刷、识别、数据采集和处理于一身的新型技术。

最早被打上条形码的产品是箭牌口香糖。条形码技术最早产生在20世纪20年代，诞生于威斯汀豪斯的实验室里。一位名叫约翰·科芒德性格古怪的发明家。“异想天开”地想对邮政单据实现自动分检，那时候对电子技术应用方面的每一个设想都使人感到非常新奇。

# 不查日历算星期几

BUCHARILISUANXINGQIJI

在日常生活中，如果我们想要知道历史上的某一个重要的日子或者未来的某一天是星期几，通常我们解决这个问题的有效办法是看日历，但是我们总不能随时随地带着日历，更不可能随时随地带着厚厚的万年历。我们有什么好方法，不用借助工具，就可以很快的计算出某一天是星期几呢？下边我们一起学习一个公式。

## ● 基本公式

$$S = (Y-1) + \frac{Y-1}{4} - \frac{Y-1}{100} + \frac{Y-1}{400} + D$$

其中Y是年份数，D是从元旦起到这一天为止（包含这一天）的天数，也就是这一天在这一年中是第几天。公式中只取计算结果的整数部分。算出来的S除以7，其余数便表示这一天是星期几：如果余数是0，则为星期日；余数是1，则为星期

一；依次类推。

例如：1949年10月1日是我们伟大祖国成立的日子，这天是星期几？好了，让我们按照上边的公式计算一下：

$$\begin{aligned} S &= (1949-1) + \frac{1949-1}{4} - \frac{1949-1}{100} + \\ &\quad \frac{1949-1}{400} + 244 \\ &= 1948 + 487 - 19 + 4 + 244 \\ &= 2664 \end{aligned}$$

用2664除以7所得的余数是6，所以说1949年10月1日是星期六。

但是这个方法相对来说比较复杂，不是直接把月和日代入公式，而是要计算这一天是全年的第几天。

## ● 蔡勒公式

$$S = \frac{C}{4} - 2C + Y + \frac{Y+26 \times (M+1)}{10} + D - 1$$

C是年份的前两位数，Y是年份后两位数，M是月份，D是日数。1月和2月要按上一年的13月和14月来算。按照蔡勒公式求出S以后，再除以7，余数就是这一天的星期几。

好了，再让我们用蔡勒公式计算一下新中国成立那一天是不是和第一个公式算出来的是一样的。

$$\begin{aligned} S &= \frac{19}{4} - 2 \times 19 + 49 + \frac{49+26 \times (10+1)}{10} + \\ &\quad 1 - 1 \\ &= 4 - 38 + 49 + 12 + 28 + 1 - 1 \\ &= 55 \end{aligned}$$

用55除以7得余数是6，这个结果和上边的答案是一样的。

日历是我们生活中必不可少的查看日期的工具

我认为数学这个词是专为科学的应用而设的，正像我们论及逻辑学、修辞学或音乐那样，数学也有它自身的专门含义与特性。

——塞尔维斯脱



# 电脑算命

DIANNAOSUANMING

现在生活中，相当一部分人还是相信算命这一说。而且不论是信与不信，可能很多人都玩过“电脑算命”，即按要求填写自己出生的年、月、日和性别，然后点击开始，电脑屏幕上就会出现相关的例如性格、命运等的论述。那这种算命到底是真是假呢？今天就让我们一起来探讨一下吧。

## ● 电脑算命与抽屉原理

电脑算命看起来确实很玄乎，但实际上，这仅仅是一个普通的电脑游戏而已，我们用数学中的抽屉原理便可以很容易地说明它的荒谬。

那抽屉原理又是什么呢？其实它是德国数学家狄利克雷，为了阐明一个数学问题而首先提出的一个原则，后来为了纪念他，抽屉原理也被称为“狄利克雷原则”。

简单地说，现在桌上正好有十个苹果，而我们想要把这十个苹果放到九个抽屉里，那么无论怎样放，都会发现至少有一个抽屉里面得放两个苹果，这一直观的现象也就是我们所说的“抽屉原理”。我们用更为普遍的叙述来表述抽屉原理的含义为：“如果每个抽屉代表一个集合，每个苹果就可以代表一个元素，假如有 $n+1$ 或多于 $n+1$ 个元素放到 $n$ 个集合中去，其中必定且至少有一个集合里包含两个或两个以上的元素。”它是组合数学中一个极其重要的原理。

后来，数学家对这个基本定则做了

推广，得到另一个复杂一些的原理：当我们试图把多于 $m \times n$ 个物体放入到 $n$ 个抽屉里，则至少有一个抽屉中放有 $m+1$ 个或多于 $m+1$ 个物体。同学们能证明上述定理的正确性吗？让我们假设现在恰好有 $m \times n$ 个物体需要放入 $n$ 个抽屉中，只能在每个抽屉中放 $m$ 个可以将物体全部放入，并且保证每个抽屉中的物体数不大于 $m$ 。而当这时又多了一个或多个物体时（即总物体大于 $m \times n$ 个），那么就必定会再向其中的抽屉中放入物体，至少会有一个抽屉中的物体数大于 $m$ 个了。

明白了抽屉原理以后，让我们再来用科学的眼光看看电脑算命是真是假吧。

首先，需要计算出电脑算命要求输入的出生的年、月、日、时辰和性别五个约束条件中可以出现多少种不同的情况，假设人的平均寿命为70年，每年有365天，每天有12个时辰（古人将一天分为12个时辰），人的性别数为2，那么约束条件中一共包含有 $70 \times 365 \times 12 \times 2 = 613200$ 种不同的情况，而现在我国人口数量约为14亿。

然后，我们应用刚刚学习的抽屉原理发现，那么每种情况（即相当于每个抽屉中）必须至少包含22830个人，也就是说全国将会有22830个人得到相同的结果具有相同的命运。

我们都知道世界上没有两片完全相同的树叶，那电脑算命的结果岂不是很荒谬吗？



## ● 抽屉原理古时的应用

其实，早在春秋战国时代，齐国上大夫晏子便已经熟练的运用了抽屉原理，也正因为如此，齐国成为了春秋五霸之一。

齐景公时期在齐国有三位勇士，分别是田开疆、公孙接、古冶子，号称“齐国三杰”。田氏势力很大，直接威胁着国君的统治。而田开疆正属于田氏宗族，相国晏子担心“三杰”为田氏效力，屡次建议景公除掉“三杰”以绝后患，但景公爱惜勇士，没有表态。

一日鲁昭公访问齐国，齐景公设宴款待，“齐国三杰”佩剑立于堂下，态度十分傲慢。此时晏子突然心生一计，决定借机除掉这三个心腹之患。

当两位君主酒至半酣时，晏子向齐景公提出自己想去园子中摘桃给二位国君品尝，齐景公很高兴的同意了。不一会儿，晏子便端着玉盘献上六个桃子。他将鲜桃献给鲁昭公和齐景公一人一个，鲁昭公边吃边夸桃味甘美。景公说：“这桃子实在难得，鲁国叔孙大夫天下闻名，应该吃一个。”叔孙忙谦让道：“我哪里赶得上贵国晏大夫呢？相国劳苦功高，这个桃子应该他吃。”齐景公见状，便说道：“既然二位谦让，那就每人吃一个桃子吧！”两位大臣谢过齐景公，各吃桃一枚。

这时，盘中还剩下两个桃子。晏子于是说道：“这还有两个桃子，不如请君王将其赐给功劳大的臣子，如何？”齐景公觉得这个想法不错，于是传令下去。谁知话音刚落，公孙接率先走上前来，拍着胸膛说：“有一次我随国君打猎，突然从林

中蹿出一头猛虎，是我冲上去，用尽平生之力将虎打死，保护了国君。如此大功，还不应该吃个桃吗？”晏子听后说：“冒死救主，功比泰山，当赐桃一个。”公孙接拿着一个桃子十分得意的吃起来。

古冶子见状，忙喝道：“打死一只老虎有何稀奇！当年我送国君过黄河时，跳进河中，舍命保住了国君的性命。这样的功劳，该不该吃个桃子？”景公说：“当时黄河波涛汹涌，要不是古将军，我的命早就没了。这是盖世奇功，理应吃桃。”晏子把最后一个桃子送给了古冶子。

这时，一旁的田开疆眼看桃子分完了，急叫道：“当年我奉命讨伐徐国，舍生入死，斩其名将，俘虏无数，吓得徐国国君俯首称臣，就连邻近的邾国和莒国也望风归附。如此大功，难道就不能吃个桃子吗？”晏子说：“这样看来，田将军的功劳当然高出公孙捷和古冶子二位，然而桃子已经没有了。”

田开疆手按剑把，难抑愤怒道：“打虎、过河有什么了不起。我南征北战，出生入死，反而吃不到桃子，在两位国君面前受到这样的羞辱，我还有什么面目站在朝廷之上呢？”说罢，挥剑自刎。公孙接见状大惊，拔出剑来，说道：“我因小功而吃桃，田将军功大却吃不到。我还有什么脸面活在世上？”说罢也自杀了。古冶子沉不住气了，大喊道：“我们三人结为兄弟，誓同生死，亲如骨肉，如今他俩已死，我如果苟活，于心何安？”也拔剑自刎。

而在一旁的晏子也不费吹灰之力消除了心中之患，“二桃杀三士”正是抽屉原理的成功应用！

时间是个常数，但对勤奋者来说，是个‘变数’。用‘分’来计算时间的人比用‘小时’来计算时间的人时间多59倍。

——雷巴柯夫



# 怎样买门票最省钱

ZEN YANG MAI MENPIAO ZUISHENG QIAN

关于生活中的省钱问题，一直都是理财族最热衷的话题，怎样花钱最合算，说到底还是离不开计算和比较啊！王明在一家旅行社任导游。因为他总是尽心为游客服务，想方设法帮游客省钱，所以他经常受到游客们的来信表扬。

## ● 巧买门票

某地一处古典园林人为地制定了两种购票方法。

甲方案是成人民票每张120元，小孩门票每张40元；乙方案是不问大人小孩，只要是5人以上的团体（包括5人），每人收80元。

今有7个成人，3个小孩，请问：怎样购票才最合算？

王明心想，如果采用甲方案入园，7个大人要花840元，3个小孩要120元，总费用是960元，将近1000元了。价钱这么贵，有没有办法节约一部分呢？

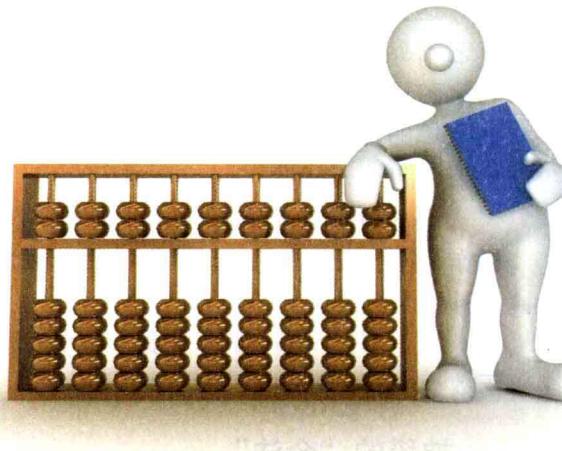
如果采用乙方案，不论大人、小孩，全部买团体票，可以算出进门费是

### 知识链接

问题：妈妈烙一张饼用两分钟，烙正、反面各用一分钟，锅里最多同时放两张饼，那么烙三张饼最少用几分钟？

解答：至少需要3分钟。

方法：先取两张饼烙1分钟，取出其中一张，另一张的反面和新放入的第三张饼烙1分钟，把烙好的第一张饼取出，剩下两张饼烙反面1分钟。



旅游也是一门学问，买门票也要精确计算才能花最少的钱参观最多的景点。

$10 \times 80 = 800$ 元。这样，一下子就可省掉160元？

两种方案合起来使用是不是更好一些呢？王明又开动脑筋想，让7个大人按照乙方案购票，由于 $7 > 5$ ，已符合园方自说自话的规定，所以只要付 $7 \times 80 = 560$ 元；至于3个小孩呢，就照甲方案规定，要付 $3 \times 40 = 120$ 元。这样一来，只需付出 $560 + 120 = 680$ 元就够了，比乙方案还要便宜！

另外，许多地方还规定，离休干部、军人是可以免票入园的，70岁以上老人与残疾人可以享受八折优待，这些因素也不能不考虑。

“门票太贵”一直是社会上的普遍现象，但一直没有得到很好的解决。有趣的是，它倒成了数学游戏的素材。



# 最美的黄金分割

ZUIMEIDEHUANGJINFENG

达芬奇的名作《蒙娜丽莎》可谓西方艺术界的巅峰之作，特别是画中人物的笑容达到恰如其分的神韵之境，从而使蒙娜丽莎的微笑具有一种神秘莫测的千古奇韵。

那如梦似的妩媚微笑，不是所有的画作都能够表现出来的。因而被后人称为“神秘的微笑”。

而很多人不知道的是造就这一切的源于数学中的黄金分割。

## ● 神秘的“金法”

黄金分割在文艺复兴前后，经阿拉伯人传入欧洲，他们将之称为“金法”。德国天文学家开普勒称黄金分割为神圣的分割。

17世纪欧洲的一位数学家，甚至尊称黄金分割为“各种算法中最可宝贵的算法”。

后来，这种算法在印度被称为“三率法”或“三数法则”。在那时人们对这个奇特而美丽的比例推崇至极，并在数学界、西方艺术界产生了深远的影响。

## ● 黄金分割——0.618

科学家们发现，黄金分割具有严格的比例性、艺术性、和谐性，蕴藏着丰富的美学价值，在我们日常的长宽设计中，采用这一比值也更能够引起人们的美感。

比如，在画正方形的时候，我们将长方形的长、宽、对角线按照 $4:3:5$ 的比例设计的时候，肯定会得到一个完美的正

方形。

许多名画、雕塑、摄影作品的主题，大都在画面的0.618处，而这个0.618就是我们所说的黄金分割数。

黄金分割数0.618的出现不仅解决了许多数学难题（如五等分圆周、求 $18^\circ$ 角的正余弦值等），而且还使生产中广泛应用的优选法成为可能。但是，黄金分割比对人类的影响还远远不只这些，经过研究证实，我们的身体比例同样遵循着黄金分割这一规律。

## ● 人体的黄金分割点

在达芬奇的一幅名作《维特鲁威人》中，画面中一个裸体的健壮中年男子，两臂微斜上举，两腿叉开，以他的头、足和手指各为端点，正好外接一个圆形。同时在画中还清晰可见地叠着另一幅图像，这幅图像中，这名男子两臂平伸站立，以他的头、足和手指各为端点，正好外接一个正方形。

如果仔细研究，我们会发现，这幅完美的人体标准画像中同样蕴含了很多黄金分割比：身高除以肚脐到地面的距离，臀部到地面距离除以膝盖到地面距离都是黄金分割比，肩膀到指尖距离除以肘关节到指尖距离也是黄金分割比。

更有科学家在研究黄金分割与人体关系时，发现了人体结构中有14个“黄金点”因此，我们不得不说黄金分割比真是一个最美也最神奇的数字。

天才=1%的灵感+99%的血汗。

——托马斯·阿尔瓦·爱迪生

要利用时间，思考一下一天之中做了些什么，是‘正号’还是‘负号’，倘若是‘+’，则进步；倘若是‘-’，就得吸取教训，采取措施。

——季米特洛夫



# 民间数学诗

MINJIANSHUXUESHI

所谓数学诗，就是借用形象的诗歌形式表达抽象的数学命题。如好记易懂的“九九歌”、“归除歌”等。借助“诗歌”这一文学形式表示数学的量间关系，将抽象的数学知识寓于诗歌的形象之中，使其数论知识更有趣味性，形象逼真、易学易记。

## ● 数学诗

留传至今的几首数学诗分别为：

其一：

三百七十八里关，初行健步不为难。  
脚痛每日减一半，六天才能到其关。  
要问每天行里数，请君仔细算周详。  
(答案：192、96、48、24、12、6)

其二：

三百六十一口缸，任君分作几船装。  
不许一船多一只，不容一船少一缸。  
(答案：19只船，每船装19口缸。)

其三：

程大位的《算法统宗》中有这样一道题：  
甲赶羊群逐草原，乙拽一羊随其后，  
戏问甲及一百否？甲云所说无差谬，  
若得这般一群凑，于添半群小半群，  
得您一只来方凑，玄机奥妙谁猜透。  
(小半即四分之一) (答案：36只)

还有一种是诗中嵌入数字的，如：一别之后，二地相思。只说是三四月，又谁知五六年。七弦琴无心弹，八行书不可传，九连环从中折断，十里长亭望眼穿。百思想，千系念，万般无奈把郎怨。



徐渭 (1521~1593)

## ● 数学诗的意义

数学诗风格别致，熔数学与文学为一炉，浑然一体，文理交融，使读者在学习数学中受到了文学的熏陶，可谓是一举两得。

而我国著名的明代书法家徐渭(字文长)更是利用数学作诗、填词的高手。

徐文长一天邀请几位朋友游西湖。结果一位朋友迟到，徐文长作一上联，罚他对出下联。徐文长的上联是：一叶孤舟，坐了二、三个游客，启用四桨五帆，经过六滩七湾，历尽八颠九簸，可叹十分来迟。

迟到友人的下联是：十年寒窗，进了九、八家书院，抛却七情六欲，苦读五经四书，考了三番两次，今日一定要中。



# 家庭主妇怎么当

JIATINGZHUFUZENMEDANG

平时你会干一些家务活吗？也许你觉得那还有什么？不就是洗洗涮涮吗？当个家庭主妇比当个科学家容易多了。如果你存在着这种想法，那就大错特错了。要知道一个好的家庭主妇可以抵得上一个数学家呢！做个好的家庭主妇可不是一件容易的事。

比如，你早上起床时，妈妈就已经给你准备好了热腾腾的面包、牛奶，平时的家务活中还有扫地、拖地、洗衣、买菜、浇花等等。

如果一个糟糕的家庭主妇去做这些工作，可能会搞得自己头晕脑胀，家里也是凌乱不堪，但是一个好的家庭主妇则可以充分利用所有的时间，统筹分配，让自己不仅可以做好所有的家务，还能在空余的时间里得到充分的休息。那么，这就涉及到了数学当中最实用的一个分支——统筹学。

## ● 统筹学概述

统筹学主要研究如何在实现整体目标的全过程中施行统筹管理的有关理论、模型、方法和手段，是数学与社会科学交叉的一个学科分支。它通过对整体目标的分析，选择适当的模型来描述整体的各部分、各部分之间、各部分与整体之间以及它们与外部之间的关系和相应的评审指标体系，进而综合成一个整体模型，用以进行分析并求出全局的最优决策以及与之协调的各部分的目标和决策。

### 知识链接

统筹学在企业管理的运用中体现的是兼顾方方面面，从而激发管理者的智力，真正实现权力、智力的统一，发挥知识的杠杆作用。

### ● 巧做家庭主妇

著名数学家华罗庚曾经用喝茶来讲述了生活统筹安排的重要性。生活中我们经常喝茶，但是，喝茶需要开水，而且开水壶、茶壶、茶杯都要洗，还需要准备茶叶，应该怎么安排？

最节省时间的方法就是先洗净开水壶后，灌水，烧水。利用等待水开的时间，洗茶具，拿茶叶。如果你把这个顺序打乱了，就会浪费时间。

我们再来看一个好的家庭妇女是如何利用统筹学做饭的？首先洗米，放入电饭煲中；然后用电热壶来烧水；接下来用淘米水洗第一道要做的蔬菜；洗完之后，就可以热锅、热油，在热油的同时切菜；油热时，菜也正好切完，这样就可以炒菜了；趁着盖上锅盖等菜熟的时间，就可以洗第二道菜了；而当第一道菜熟的时候，第二道菜也准备好了，就正好不用关火接着炒第二道菜；当第二道菜熟的时候，热水也刚刚烧好，接着将热水倒入锅中准备做汤。这就是利用统筹方法。

小到一个家庭，大到一个国家，统筹学无处不在。如果我们无法很好地运用统筹法就会因为缺乏整体、系统观念而顾此失彼。



# 揭开密码的神秘面纱

JIEKAIMIMADESHENMIMIANSHA

我们在观看好莱坞电影的时候常常可以看见这样的场景：一位神秘的入侵者装备着高级的电子设备，来到紧锁的防盗门前面，并在几秒钟内破译系统的密码，然后潇洒地走了进去。

这个场景是不是很酷？而他是如何做到破译密码的？真的能做到吗？那今天就让我们来研究神秘的密码，一同揭开它那神秘的面纱。

## ● 早期的密码雏形

密码技术其实由来已久，早在公元前405年，雅典和斯巴达之间发生了一场著名的伯罗奔尼撒战争。随着战事的进展，斯巴达军队在交战中逐渐占据了优势地位，准备对雅典都城发动最后一击。

这时，原来站在斯巴达一边的波斯帝国突然改变态度，停止了对斯巴达的援助，它希望雅典和斯巴达双方在持续的战争中两败俱伤，以便自己从中渔利。而这个突然出现的情况也打乱了斯巴达的进攻计划，他们急需摸清波斯帝国的下一步具体行动计划，以便采取新的战略方针。

正在这时，斯巴达军队捕获了一名从波斯帝国回雅典送信的雅典信使。斯巴达士兵仔细搜查了这名信使，可是除了从他身上搜出一条布满杂乱无章的雅典字母的普通腰带外，别无他获。

情报究竟藏在什么地方呢？斯巴达军队统帅莱桑德只能把注意力集中到了那唯一的线索——腰带，他相信情报一定就

隐藏在那些看似普通的字母之中。每天他都会反复琢磨研究这些天书似的文字，把腰带上的字母用各种方法重新排列组合，却怎么也解不出来。最后，莱桑德也对此失去了信心，他一边无奈地摆弄着那条腰带，一边思考着采用其他途径获取情报。而当他无意中把腰带呈螺旋形缠绕在手中的剑鞘上时，奇迹出现了。原来腰带上那些杂乱无章的字母，竟组成了一段情报文字。就在这份波斯信使送给雅典的情报中，它告诉雅典，波斯军队准备在斯巴达军队向雅典发起最后攻击时，突然对斯巴达军队进行袭击。斯巴达统帅莱桑德根据这份情报马上制定了新的作战计划，先以迅雷不及掩耳之势攻击了毫无防备的波斯军队，并一举将它击溃，解除了后顾之忧。随后，斯巴达军队回师征伐雅典，终于取得了战争的最后胜利。

这种腰带密码的通信方式成为了最早的密码雏形，后来许多先进的密码算法也是根据这种思路设计的。

## ● 神奇的密码技术

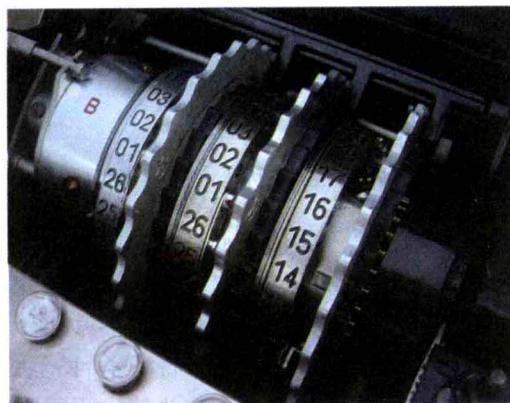
密码就是一种用来混淆信息的技术，它希望将正常的（可识别的）信息转变为普通人无法识别的信息。然而对部分特定的人（密码使用者）来说，这种无法识别的信息是可以通过一定的技术手段再加工并恢复出原信息的。其中所采用的加密解密技术往往都包含着复杂的数学原理和公式。

密码这个神秘的学科从最早的军事用途，到如今已广泛应用于社会的各个方面，特别是电脑的发明和普及，促使更加先进的数字加密系统层出不穷，密码学也开始占据越来越重要的地位。而密码学与数学密不可分的关系反过来也为数学各种新理论、新算法的出现创造了条件。

## ● 密码的分类

我们从密匙的类型可以将加密方式分为私钥加密和公钥加密两种。顾名思义，私钥加密就是指使用者采用自己私有的密匙对信息进行加密和解密，整个过程就像我们用自己的钥匙开自家的们一样，只要我们获得了这把私有的钥匙，那么就可以随心所欲的开关这扇门了。

而随着技术的发展，人们发现私钥加密也有一些缺点，其中最大的问题就在于人们不能保证密匙传输的安全性，当传输信号被别人窃听以后，那他也可以用这个密匙来解密信息。为了更好的适应新的应



格玛密码机转子组。三个转子位于右边的固定接口和左边（标着B）的反射器两个装置之间。

### 知识链接

在密码学中，消息被称为明文，用某种方法伪装消息以隐藏它的内容的过程称为加密，加了密的消息称为密文，而把密文转变为明文的过程称为解密。而解密的过程往往需要一段特殊的消息，这就叫做密匙，就像我们开锁用的钥匙一样，当你授权获得密匙以后，就可以通过已知的数学算法完成解密获取信息了。

用场合，人们又发明了一种新的加密方式叫做公钥加密。在公钥加密系统中其实包含有公用密匙和私有密匙两把密匙，它们是相互对应的，用其中一个密匙加密的信息只能用对应的那个密匙才能解密。信息的接受者首先生成两把对应的密匙，然后将一把留给自己保存作为私有密匙，另一把传送给发信者作为公用密匙，当它收到公用密匙以后就可以对信息进行加密并发送出去了，而私有密匙只有接受者才有，也就是只有接受者才能对密文进行解密，这样就避免了私有密匙流出而被人窃取。

同样在电子商务中流行的数字认证领域公钥加密方式也有它不可取代的优势。与信息加密相反，数字认证并不是要让别人无法知道发送者的信息，而是要确认发送者的身份，保证密文信息一定是这个发送者发出的，而且它也无法抵赖。于是人们设计了一种流程，让发送者产生两把密匙，它采用自己保留的私有密匙对信息进行加密，然后将密文和另一把公用密匙一同传送给接收方，这时接收方就可以完成解密并且确认这个密文一定是特定的发送者发出的，因为没有第二个人知道它的私有密匙，也不可能生成这份密文。