明心教育

刘 嘉/编著

明心数学资优教程

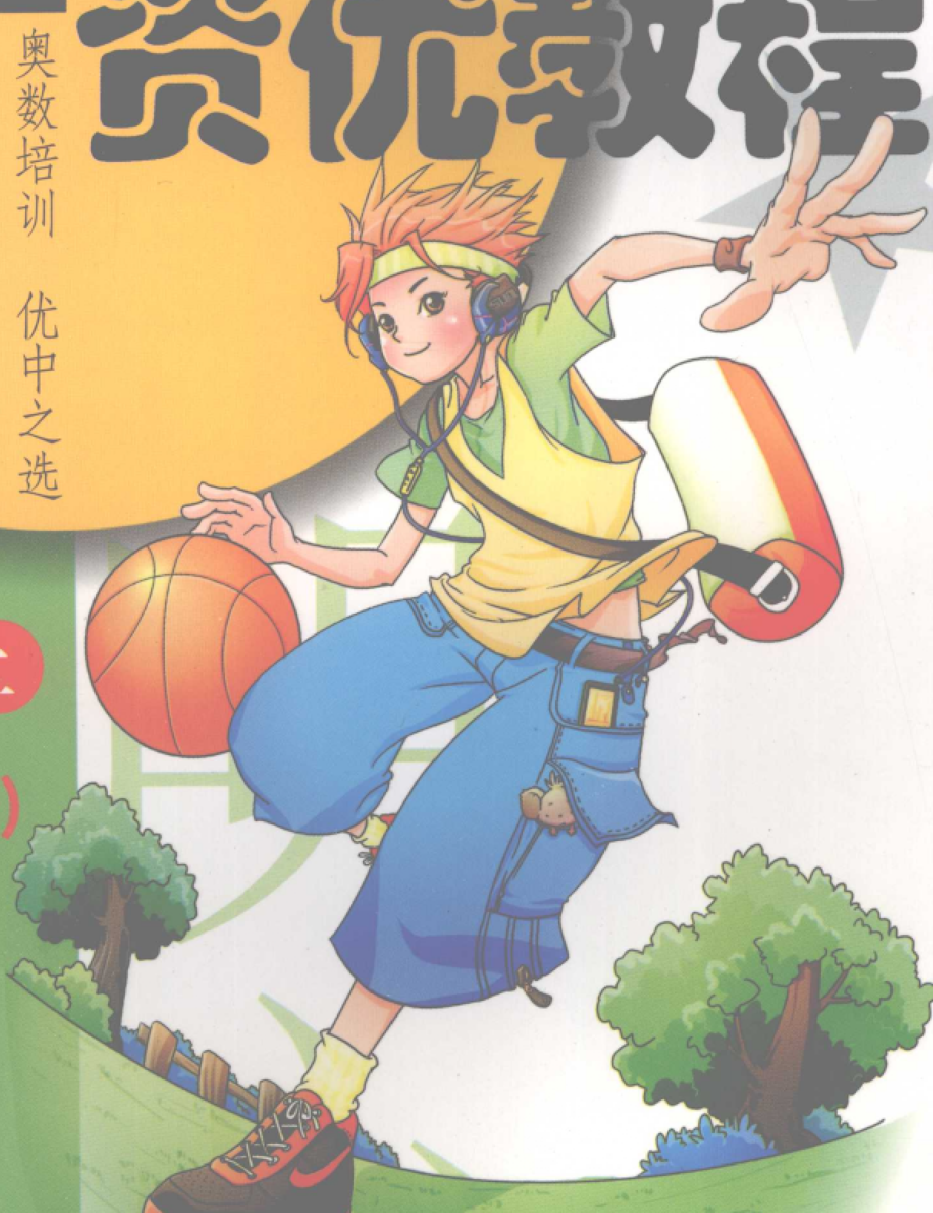
MINGXIN

奥数培训 优中之选

六年级以上学生专用

第四卷上

（第2分册）



湖北長江出版集團
湖北教育出版社

作者近照

刘嘉，1970年生于武汉。

由于小学酷爱文史而数学不及格屡遭训斥，所以中学发奋学习数学，导致偏科严重，无法成为“高考型人才”而辍学，索性一头扎进数学王国，在三尺讲台上找到了自己的人生坐标。

志趣：爱数学之智、钻数学之真、讲数学之美。

缺点：无学历、无文凭、无职称。

特长：用哲学讲思想、用禅宗讲方法、用文史讲精神。

信念：天道酬勤，格物致知，明心见性。

追求：传播数学思想，弘扬数学文化，培养资优人才。

明心教育

这是一套提高思维、丰富智慧、锤炼情操的好书，要认真读一读。读了它，会使我们能够更加精彩地求解人生这一道数学题。

——余其煌

〖中国科学院数学与系统科学研究院研究员，博士生导师，华罗庚金杯少年数学邀请赛主试委员会副主任〗

这套教材中丰富的学习材料、有趣的追根索源、深刻的理论方法、闪光的数学思维、平实的写作风格，都将给广大的数学爱好者、数学竞赛的指导者与参与者，带来耳目一新的感觉，也将会给“竞赛数学”的发展与提升带来可以预见的影响与推动。

——田化澜

〖湖北省数学特级教师，国务院津贴专家，湖北省首任十大名师，武汉市中学数学专业委员会理事长〗

“明星”关注的是荣誉，令星光耀眼，而“明心”关注的是智慧，让心灵升华；“明星”可以喧嚣一时，而“明心”才有益于一世；“明星”是世俗的追求，“明心”才是教育的旨趣；“明星”只偶尔把数学作为入场券，“明心”才会长久地把数学视为聪明泉。

——裴光亚

〖武汉市教育科学院数学教研室主任，鄂教版普通高中数学课程标准实验教科书副主编〗

这套书超越了竞赛解题的层次，找寻各种数学问题的历史源头，以朴素精要的数学思想为统摄，打通了知识的界限，将极其丰富的内容展现给我们。

——柳智宇

〖本书作者的学生之一，第47届国际数学奥林匹克（IMO）竞赛金牌得主，现就读于北京大学数学科学院〗

上架建议：小学(初中)奥数类

ISBN 978-7-5351-5165-0

责任编辑/彭永东
封面设计/牛　红
责任督印/张遇春

9 787535 151650 >

定价:28.00元

明心教育

刘 嘉/编著

明心数学资优教程

第四卷 上

第2分册

湖北长江出版集团
湖北教育出版社

(鄂)新登字 02 号

图书在版编目(CIP)数据

明心数学资优教程. 第 4 卷 · 上(第 2 分册)/刘嘉编著. —武汉:湖北教育出版社,2008. 8

ISBN 978 - 7 - 5351 - 5165 - 0

Ⅰ. 明… Ⅱ. 刘… Ⅲ. 数学课 - 小学 - 教材 Ⅳ. G624. 501

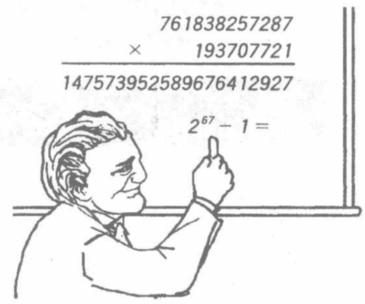
中国版本图书馆 CIP 数据核字(2008)第 102042 号

出版 发行:湖北教育出版社	武汉市青年路 277 号
网 址:http://www.hbedup.com	邮编:430015 电话:027 - 83619605

经 销:新 华 书 店	
印 刷:武汉中远印务有限公司	(430034 · 武汉市硚口区长丰大道特 6 号)
开 本:880mm × 1230mm 1/16	13. 5 印张
版 次:2008 年 8 月第 1 版	2008 年 8 月第 1 次印刷
字 数:400 千字	印数:1 - 8 000

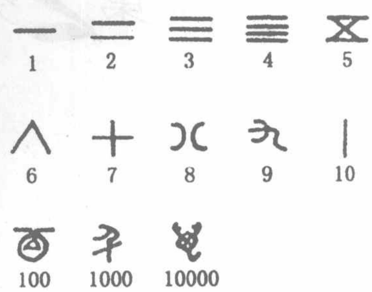
ISBN 978 - 7 - 5351 - 5165 - 0	定价:28. 00 元

目 录



761838257287
× 193707721
147573952589676412927
$2^{67}-1=$

AY7831976K1
10
ZEHN DEUTSCHE MARK



1 2 3 4 5
6 7 8 9 10
100 1000 10000

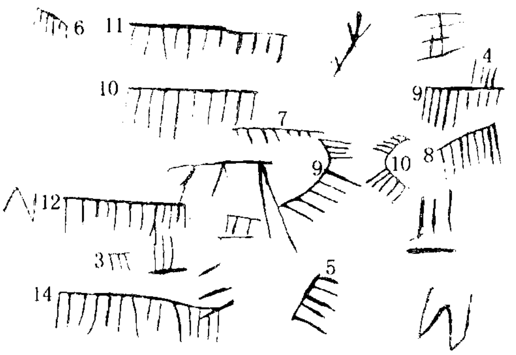
第11讲　素数与分解

数学经纬

一、数的起源

1. 数的产生：

我们每天都和数打交道，可你知道数的来历吗？数的发明，是人类祖先的一大创造！



在西班牙山洞中发现的距今25000年的石器时代数的式样

数（shù）源于数（shǔ），数的概念产生于原始人类的生活与生产的需要。

在远古时代，原始人在长期的狩猎、捕鱼、采集和分配过程中，常常需要把得到的捕获物进行分配，有时多一些，有时少一些，甚至有时狩猎是空手而归，这样就逐渐产生了“有”和“无”、“多”和“少”的概念。

以后随着狩猎技术的提高，捕获物数量也逐渐增加，原始人为了进行合理的分配，就需要对物品先数（shǔ）一数，这样就萌生了1、2、3、…数的概念。

人类学家发现，时至今日，世界上有些原始部落把大于3的数量看做“一群”或“一堆”。例如，澳大利亚境内的墨累河（澳大利亚境内的主要河流）地区的原始部落长期来只有1、2、3的概念，“4”叫做“2－2”，“5”叫做“2－3”，5以上统称为“多”。

历史注记

在数学中虽然不存在着最大的数，但在英语中有个表示大数的新词叫googol，因特网搜索引擎谷歌的名字就是源于googol——一个googol是1后面跟100个零！即10^{100}。

googol这个词是一位数学科普作家九岁的外甥造的。他的外甥还提出了另一个比googol更大的数，叫做googolplex。他把这个数描述为1后面跟许多零，零的个数则是尽你可能写到手累为止。googolplex的数学定义是1后面跟有googol个零，即$10^{googol}=10^{10^{100}}$，这个数字太长了，以至于它毫无现实的用途。即使每一位都写得比原子还小，整个宇宙也没有足够的空间写下这个数字。

10 000 000 000 000 000
000 000 000 000 000 000
000 000 000 000 000 000
000 000 000 000 000 000
000 000 000 000 000 000
000 000 000 000

从下面具体的例子你就可以感知到 googol 到底有多大了！

1. 如果整个宇宙充满了电子和质子而没有留下多余的空间，那么这些粒子的总数为 10^{110}。这是一个大于 googol 但远小于 googolplex 的数。

2. 据统计，位于美国纽约州科尼岛的沙粒总数大约为 10^{20}。

3. 从公元 1456 年印刷第一部《圣经》开始，到 1940 年为止，全世界所有印刷的词量约为 10^{16}。

2. 数的记录

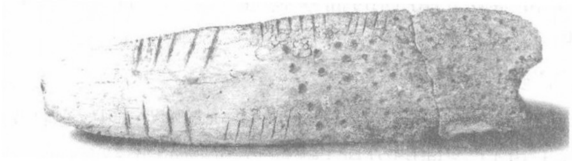
有了数的概念之后，生活在地球不同区域的先民们，采用了各种不同的方式来记录数。

人类文化中最早有数字记号，是起始于距今 2 万多年的旧古器时代，当时的人类学习把数字保留下来，就跟学习保留并使用火一般。

(1)刻痕记数

通常人们都喜欢就地取材，利用骨头。当然也有一些地方使用木头。

假设有一堆物体——动物、人类或其他东西。如果不晓得它们的数目，要如何记得总共有多少呢？方法就是为每件东西作记号，通常是个刻痕。于是一件东西，一个记号！这种“刻痕记数”的方式显然是世上最古老的记数方法之一。我们甚至发现有将近 30000 年前的“记数骨”。



刻痕记数的做法在人类历史初期就有了。左图是旧石器时代(约公元前 15000 年)刻有切痕的鹿角。刻纹是一种信用合约：相同的两块都被保存下来。一块交给卖方，另一块交由买方。当交易必须赊欠时，卖方将这两块并列，再切割代表交易数量的连续条纹。这无法作弊：买方不能少刻，卖方也不得增加刻痕。

甲骨文中的数字

(2)结绳记数

中国古书中曾有过“结绳记数”的记载，那是很早以前的事了。《周易·系辞上》(约公元前 11 世纪成书)上说：“结绳而治，后世圣人，易之以书契”就是说“上古时代人们用结绳记事或记数，后来的读书人才用记数符号去代替它”。

结绳记数在世界许多地方都使用过，在今天的某些原始地区，人们还在用这种方法。在绳子上打结用来记数还可以，但是要用来计算就不容易了。

公元前 3000 年的壁画记载了埃及人用打结的绳子丈量土地和估算收获(上排)。人们将收获的谷物送往粮仓，并有记录员做统计(下排)。

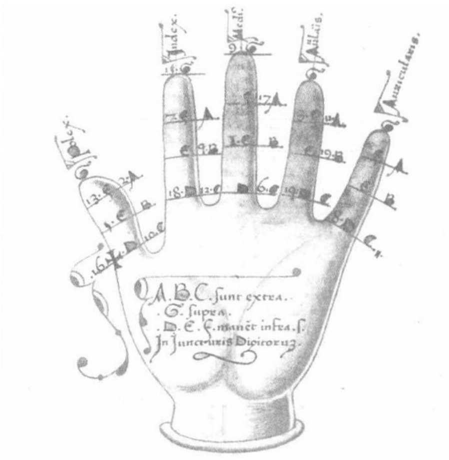
用天然的小石子记数，也是人类早期常用的一种计算办法，而且计算要方便许多。可以肯定地说，以石子作为计算工具，是每个民族都经历过的历史阶段。

在拉丁文中，“计算”一词写作“Calculus”，本意即为计算用的石子。

(3)肢体记数

除了以骨头、木头及石头当成记录的工具以外，人类还利用自己的身体当成记数的工具——身体的每个部位都对应着一个数字，如用两只手、两只眼睛等来表示 2，一只手表示 5 等。

原始人不单是手指用来记数，也用上了耳朵、手臂、双腿、躯干、头，还有每一个指掌间关节、手指关节。有很多文明也因此发展出复杂的数字人体图，并有一整套手势语法，主要是把手指头摆出不同的姿势——伸直、弯曲、卷起等等，直到现在，小孩常使用的“屈指记数”的方式就残留着这样记数方法的痕迹。



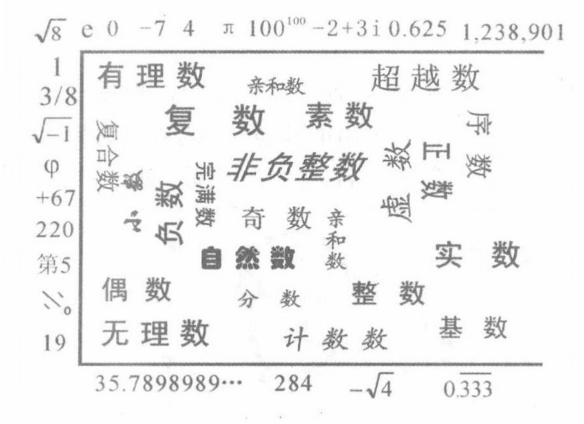
西方在 15 世纪出版的介绍以手指进行推算的书籍中的图片

8 世纪时，英国的一个修道士写了一本关于手指计算的著作，图中人类利用左手手指代表个位数及十位数。右手代表百位数及千位数，手的其他位置配合身体的某些部位代表万及十万。

二、自然数、整数与数论

19 世纪德国数学家克罗内克(1823—1891)在谈论数学时说到“上帝创造了自然数，其余的一切是人的工作”。

克罗内克



人类经过漫长的探索，建立了数的概念。在物体计数的过程中，人们把用来表示物体个数的数 0、1、2、3、4、…叫做自然数。之所以这样命名，大概是因为它们是自然而然地产生的吧。

依照一般惯例，我们用 **N** 来代表所有自然数所成的集合：

$$\mathbf{N}=\{0,1,2,3,\cdots,n,n+1,\cdots\}$$

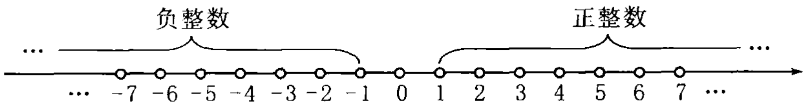
从直观上看，自然数无穷尽地延续着，自然数集合 N 有下列性质：

(1)0 是最小的自然数，以 0 开始，但却没有结束，没有最后一个自然数；

(2)每个自然数 n 后面都跟着下一个自然数 $n+1$。

后来由于实践的需要，数的概念进一步扩充，非零自然数被叫做正整数，而把它们的相反数叫做负整

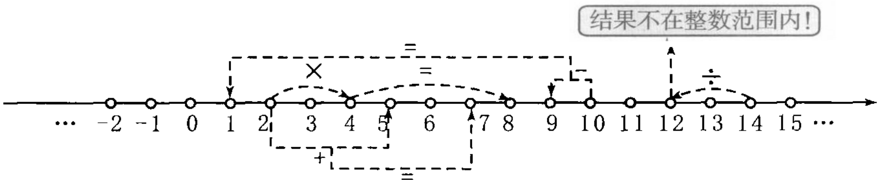
数，介于正整数和负整数中间的中性数叫做 0，它们和起来叫做整数，数学中用字母 **Z** 来表示整数。



对于整数进行加、减、乘、除四则运算可以产生新的数。但请注意：

加法、减法和乘法这三种运算，在整数范围内可以毫无阻碍地进行。也就是说，任意两个或两个以上的整数相加、相减、相乘的时候，它们的和、差、积仍是一个整数。

但整数之间的除法在整数范围内并不一定能够无阻碍地进行。换句话说，两个整数相除的结果不一定是整数。



那么，在什么情况下两个整数相除的结果仍然是整数呢？

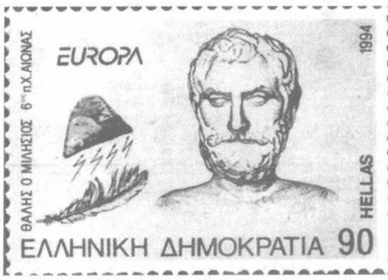
为了寻求其中的规律，古希腊时代的数学家对这个问题做出了系统的研究，从而发展成一门专门研究整数性质、脱离了算术而独立的一个数学分支——整数论，又叫初等数论。这门学科被德国“数学王子”高斯称为“数学的王后”。


哈代

20 世纪初最重要的英国著名数学家兼数论专家哈代（G·H·Hardy，1877～1947）对数论这门学科有过精辟的阐释：“初等数论应当是一种极好的早期数学教育素材。它需要的预备知识很少，材料很实在，可以触摸得到，又为人们所熟悉；它所用的推理过程非常简单，有普遍意义，而且为数不多；在数学科学中它非常独特，因为它能激发人们的天然好奇心。花上一个月时光，进行富有智慧的数论启蒙教育，它将会带来双倍效益，双倍作用，比起同等数量的给工程技术人员上的微积分来说，更将是十倍地有趣。”

三、整除性

古希腊数学家泰勒斯（公元前 625～前 547）根据土地测量创立了演绎几何学，毕达哥拉斯及其学派则把数的抽象观念提高到了突出的地位，并把数视为世界的基石，他们认为，世界构成于数量关系，数是整个自然的本原。这个学派的名言“万物皆数”对此作了很好的概括。



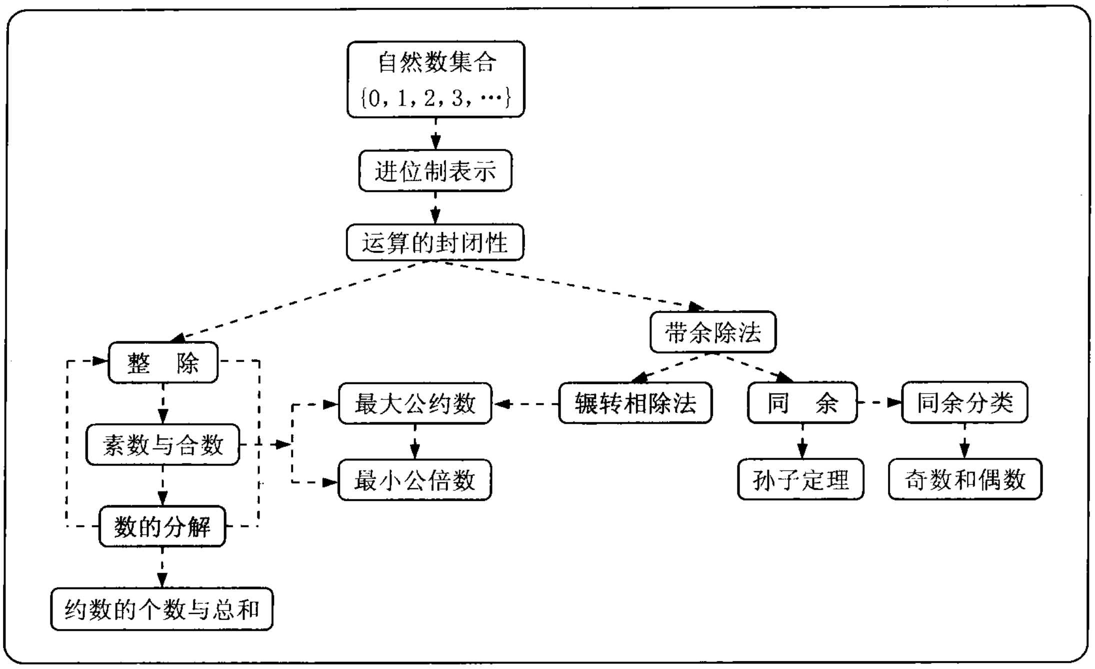
邮票上的泰勒斯

欧几里得及其学生

古希腊的数学家沿着毕达哥拉斯学派的思想对数展开了研究并做出了杰出的贡献。首先对数论中的一个最基本的问题——整除性问题进行了系统的研究，其后关于质数、和数、约数、倍数等一系列概念也被提出来了，这些结果都被欧几里得总结在《原本》的 7、8、9 卷中。

要确定数论的研究从何时开始是一件困难的事，然而大家都赞同数论的研究的起点应该从数的整除性开始。若“可整除”，则它是一个整除问题；若“不可整除”，则是一个余数问题。整除理论是数论中最古老的内容。

借助除法这个工具去测试自然数的可整除性，可以使我们更加清楚地认识自然数的结构。



整除的定义

【定义】 所谓“一个自然数 a 能被另一个自然数 b 整除”就是说“商 $\frac{a}{b}$ 是一个整数”；或者换句话说：存在着第三个自然数 c，使得 $a=b\times c$。这时我们就说“b 整除 a”或者“a 被 b 整除”，其中 b 叫 a 的约数，a 是 b 的倍数，记作：“$b|a$”。

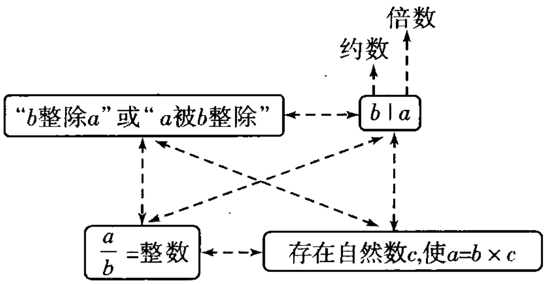
由整除的定义可得：

①1 是任何自然数的约数，即 $1|a$；

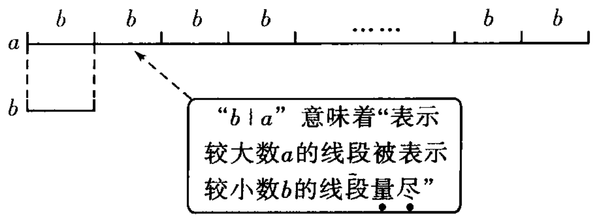
②任何自然数都是它本身的约数，即 $a|a$；

③非零自然数的约数个数是有限的；非零自然数的倍数个数是无限的。

如果不存在着这样的自然数 c，则称 a 不能被 b 整除（或 b 不能整除 a），记作 $b\nmid a$。



整除的几何意义



【例 1】 任意 n 个连续奇数的和都是 n 的倍数，例如：

$$3+5+7+9=4\times6;$$

$$21+23+25+27+29=5\times25;\cdots$$

你能说出这其中的道理吗？

【分析】不妨用 a 表示这 n 个连续奇数中的第一个数，那么 n 个连续奇数的和可表示为：

$$\begin{aligned}&a+(a+2)+(a+4)+\cdots+[(a+2(n-1))]\\=&na+2[1+2+3+\cdots+(n-1)]\\=&na+n(n-1)\\=&n(a-n-1)\end{aligned}$$

由此可得：$n|a+(a+2)+(a+4)+\cdots+[(a+2(n-1))]$

在整除的定义中，倍数和约数的关系犹如祖先和后代的关系！让我们看看为什么。

请看 36 这个数，哪两个数字相乘结果是 36 呢？

我们很容易便可得出：$1\times36,2\times18,3\times12,4\times9,6\times6$ 的结果是 36。

显然，自然数 1、2、3、4、6、9、12、18、36 是约数，36 是倍数。由 36 产生了 1 和 36，2 和 18、3 和 12……这些后代，这样，我们是不是可以称倍数是祖先，约数是后代呢！

从上面的例子中我们还可以发现约数的一个规律：自然数的约数是成对出现的！

36的约数的对应关系

1	2	3	4	6
↕	↕	↕	↕	↕
36	18	12	9	6

对自然数a，b，c，如果$a=b\times c$ → $b|a$，$c|a$

b与c是对应的！

这一点不难理解，如果“$b|a$”意味着“存在整数 c，使 $a=b\times c$ 成立”，这说明 c 也是 a 的约数。

历史注记

1. 完美无缺——完全数

早在 2000 多年前的古希腊，人们就发现自然数 6 与 28 具有如下奇妙的特征：除本身以外的所有约数之和恰等于该数。即

$$1+2+3=6,1+2+4+7+14=28$$

具备这种特征的自然数叫完全数。

纪念邮票上的毕达哥拉斯

完全数的发现是毕达哥拉斯学派的卓越贡献之一。中世纪的神秘主义者甚至将完全数披上了一层神秘的迷信色彩，他们把完全数 6 和 28 视为至高无上的建筑师——上帝的基本数字，认为它们是宇宙结构的一部分。其证据是世界万物是在 6 天之内创造完成的，而月亮的周期是 28 天。

欧几里得研究过完全数，他在《原本》中给出了完全数的定义，并证明了完全数的一个重要性质：

如果 2^p-1 是素数，则 $2^{p-1}(2^p-1)$ 是完全数。

两千年后，数学家欧拉证明每个偶完全数都具有这个形式。

完全数极其稀少，而且它们之间相隔的很开，前面几个完全数依次是：

n	完全数 $2^{n-1}(2^n-1)$	对应的素数(2^n-1)，又叫梅森数	发现时间
2	6	3	
3	28	7	公元前 1 世纪
5	496	31	尼克梅切斯(Nicomachus)
7	8,128	127	

n	完全数 $2^{n-1}(2^n-1)$	对应的素数(2^n-1)，又叫梅森数	发现时间
13	33,550,336	8,191	公元1460年(无名氏)
17	8,589,869,056	131,071	公元1603年意大利数学家
19	137,438,691,328	524,287	卡塔尔迪(P. A. Cataldi,1552～1626)
31	2,305,843,008,139,952,128	214,783,647	公元1772年欧拉

数学家们还在完全数中发现了更加令人惊叹的特征：

(1)$6=2^1+2^2$；$28=2^2+2^3+2^4$；$496=2^4+2^5+2^6+2^7+2^8$；…

(2)除6外，$28=1^3+3^3$；$496=1^3+3^3+5^3+7^3$；…

(3)完全数的全部因子的倒数和都等于2：

$$6:\frac{1}{1}+\frac{1}{2}+\frac{1}{3}+\frac{1}{6}=2;28:\frac{1}{1}+\frac{1}{2}+\frac{1}{4}+\frac{1}{7}+\frac{1}{14}+\frac{1}{28}=2;\cdots$$

多么美妙！难怪有人把完全数称为自然数中的瑰宝。

【完全数的未解之谜】总共有多少个完全数？有没有奇完全数？(至今没有发现一个奇完全数)

2.亲如手足——亲和数

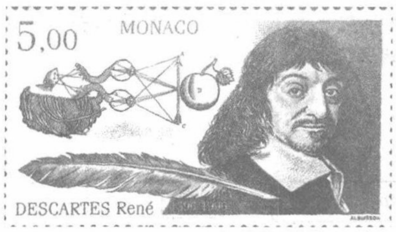
据说有人问毕达哥拉斯："朋友是什么？"他回答："朋友就是另一个自我，如同220与284一样。"

用数学语言来说，其意义是：220的真约数{1,2,4,5,10,11,20,22,44,55,110}之和是284；而284的真约数{1,2,4,71,142}之和正好是220。

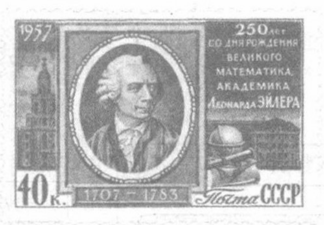
你看，220和284确实是你中有我，我中有你，难道不是朋友吗！

毕达哥拉斯称具有这种性质的数叫亲和数。

在中世纪，宗教学者往往利用亲和数的特征来为宗教披上神秘主义色彩。例如在《圣经·创世纪》的第32节14款中，耶各的礼物200只母山羊与20只公山羊，就被《圣经》的一位注释者说成是一种有意的秘密安排，因为220是亲和数对220、284中的一个。



笛卡儿



欧拉

费马

寻找亲和数的工作比想象的要难得多。

第一对亲和数(220,284)也是最小的一对，是毕达哥拉斯于2000多年前发现的；

第二对亲和数(17296,18416)是1636年由法国数学家费马找到的；

第三对亲和数(9363584,9437056)于1638年被法国数学家笛卡儿发现。

1750年，数学大师欧拉一口气竟找出了59对亲和数！

有人证明了最小的五对亲和数是(220,284)、(1184,1210)、(2620,2924)、(5020,5564)、(6232,6368)，其中后三对是欧拉发现的。有趣的是，比它们更小的第二对亲和数，却在大数学家们的鼻子底下溜过去了。100多年后，意大利少年尼科劳·帕格尼尼于1866年找到了在欧拉的亲和数表中没有的新亲和数：(1184,1210)。

10万以内的13对亲和数

(220,284)	(1184,1210)	(2620,2924)
(5020,5564)	(6232,6368)	(10744,10856)
(12285,14595)	(17296,18416)	(63020,76084)
(66928,66992)	(67095,71145)	(69615,87633)
(79750,88730)		

亲和数的一般性质我们知道的极少，更没有公式可使我们来求亲和数。现在求亲和数的方法是借助计算机。20世纪60年代，美国耶鲁大学的专家在计算机上，对全部100万以下的数进行了搜索，结果发现了42对亲和数，其中有些是过去已经知道的，也有新的。用这种方法对100万以上的数可进行同样的工作。

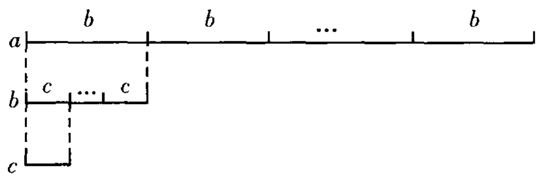
【亲和数的未解之谜】从上表可以看出，在这13对亲和数中，要么是偶数对要么是奇数对，没有一奇一偶的数对，在人们已发现的亲和数中也是如此！那么是否存在一奇一偶的一对亲和数呢？这个问题是欧拉提出来的，至今尚未解决，人们估计这是一个与“是否存在奇完全数?”一样困难的问题。另外，现在虽然发现了上千对亲和数，但是否有无穷多对亲和数也是一个未知的问题。

四、整除的性质

有了整除的概念，接下来就必须了解这个概念具备什么样的特征。

整除性质1——传递性 若$c|b$，$b|a$，则$c|a$。

几何意义：



“$c|b$”意味着“表示较小数c的线段可以量尽表示较大数b的线段”；

“$b|a$”意味着“表示较小数b的线段可以量尽表示较大数a的线段”；

所以“表示较小数c的线段可以量尽表示较大数a的线段”。

代数表达式：

$c|b$ → 存在着整数p，满足$b=cp$

$b|a$ → 存在着整数q，满足$a=bq$

→ $a=bq=(cp)q=c(pq)$ → $c|a$

【例2】 任意取三个数形成一个整数$\overline{abc}$。重复它的数字写出一个新数$\overline{abcabc}$。任一用这种方法形成的六位数肯定有约数7、11、13！这是怎么回事呢？

【分析】 把六位数$\overline{abcabc}$按十进制形式展开，我们得到：

$$\overline{abc}\times1000+\overline{abc}=\overline{abc}\times1001$$

所以：$1001|\overline{abcabc}$。

又因为$7|1001$，根据整除的传递性可以得到：$7|\overline{abcabc}$。

同理可对11、13进行分析。

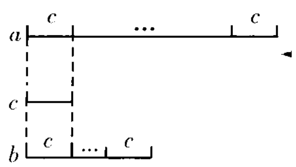
举一反三

1. 把任意一个两位数$\overline{ab}$重复写三遍形成一个六位数$\overline{ababab}$。这个六位数肯定有约数 3、7、13、37。为什么？

2. 把一个一位数重复写五遍形成一个五位数$\overline{aaaaa}$。这个五位数肯定有约数 41 与 271。为什么？

整除性质 2——可加性 若 $c|a$，$c|b$，则 $c|(a\pm b)$。

几何意义：



"$c|a$"意味着"表示较小数 c 的线段可以量尽表示较大数 a 的线段"；

"$c|b$"意味着"表示较小数 c 的线段可以量尽表示较大数 b 的线段"；

所以"表示较小数 c 的线段显然可以量尽表示较大数 a 与 b 的两根线段的和或者差"。

代数表达式：

$\boxed{c|a}$ ⇢ $\boxed{\text{存在着整数}p\text{，满足}a=cp}$

$\boxed{c|b}$ ⇢ $\boxed{\text{存在着整数}q\text{，满足}b=cq}$

⇢ $\boxed{a+b=cp+cq=c(p+q)}$ ⇢ $\boxed{c|(a+b)}$

【例 3】 设 a、b 为整数，取合适的值使算式 $2+a$ 与 $35-b$ 都是 11 的倍数，那么把 a、b 的值代入到算式 $a+b$ 时，算出的结果将是 11 的倍数！为什么？

【分析】 我们把算式 $a+b$ 代换成下列形式：

$$a+b=(2+a)-(35-b)+33$$

根据条件：$11|(2+a)$，$11|(35-b)$，$11|33$。

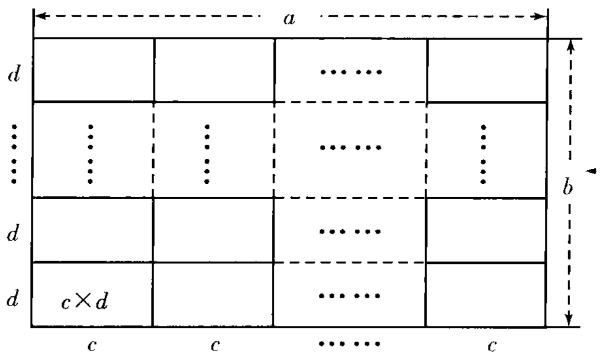
结合整除的可加性可知：$11|[(2+a)-(35-b)+33]=a+b$。

举一反三

a 为自然数，取合适的 a 的值使 $a+1$ 是 3 的倍数。那么当把 a 的值代入到算式 $4+7a$ 中时，所得的结果也是 3 的倍数！为什么呢？

整除性质 3——可乘性 若 $c|a$，$d|b$，则 $cd|ab$。

几何意义：



"$c|a$"意味着"表示较小数 c 的线段可以量尽表示较大数 a 的线段"；

"$d|b$"意味着"表示较小数 d 的线段可以量尽表示较大数 b 的线段"；

显然，表示 $b\times c$ 的小长方形就可以量尽表示 $a\times b$ 的大长方形，这说明"$cd|ab$"。

请读者自己写出代数表达式。

【例 4】 m、n 均为整数，如果选取合适的 m 与 n 的值使算式“$m+9n$”是 5 的倍数，那么当把 m、n 的值代入算式“$8m+7n$”时，结果也会是 5 的倍数！为什么呢？

【分析】 解决问题的关键是要把算式“$8m+7n$”代换成含有“$m+9n$”的算式：

$$8m+7n=(10m+25n)-(2m+18n)$$

根据整除的可加性，下一步分析的重点是考虑等式右边两个代数式的整除特征。

因为：$5|5$ 且 $1|(2m+25n)$，根据整除的可乘性：

$$5|(10m+25n)$$

因为：$5|(m+9n)$ 且 $1|2$，根据整除的可乘性：

$$5|(2m+18n)$$

结合整除的可加性可得：$5|(8m+7n)$。

举一反三

如果 $\overline{abc}+\overline{def}$ 能被 37 整除，证明：$37|\overline{abcdef}$。

整除的传递性、可加性、可乘性描述了约数与倍数之间最基本的规律，它们是研究整除性的基本出发点。

五、素数与分解

为了从根本上揭示自然数中整除的规律，必须去认识自然数自身的结构，而对素数的研究是打开这扇门的钥匙。

1. 算式基本定理

在自然数中，有一类称为素数的数扮演着非常重要的角色。事实上，素数(又叫质数)在整数理论中的地位就像元素在化学中或基本粒子在物理学中的地位一样。

素 数 的 定 义

【定义】 素数是指那些大于 1 的，且除了 1 和它自身外再没有其他约数的自然数。合数是指一个正整数具有除了 1 和自身以外的其他约数的自然数。

【含义】 素数从几何上看，就是表示素数长度的线段只能被单位线段和自身量尽；而合数则是除了单位线段与自身外，还可以被其他整数长度的线段量尽。

【实例】 自然数{2,3,5,7,11,13,…}都是素数；素数中只有 2 是偶数！

自然数{4,6,8,9,10,12,…}都是合数。

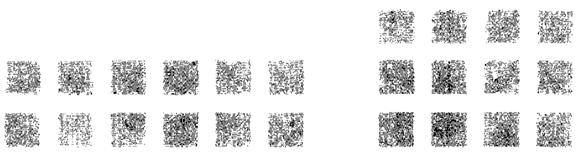
素 数 的 几 何 意 义

从几何上去理解数学概念，常常赋予数学概念一种直觉上的意义。

现在我们取 12 块单位正方形(如下图)：

可以摆成一个 1×12 的长方形。

通过对这 12 块单位正方形的重新排列，可以进一步的使之形成不同形状的长方形：



2×6　　　　3×4

素数的几何意义

正如从图中所看到的，除了上面的三种摆法外再不存在着其他形成长方形的摆法了。每个长方形的图都显示了自然数 12 可表示成：

$$12=1\times 12=2\times 6=3\times 4$$

它的约数有 1、2、3、4、6、12。

如果是一个素数，例如素数 7 会出现什么状况呢？

显然，当你取 7 块单位正方形时，无论你怎样去摆放，它只能摆成一种形式的长方形：

1×7

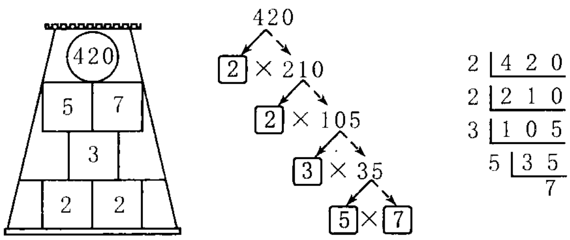
这表示自然数 7 是一个素数。

有了素数的定义，我们就可以把所有的正整数以约数的个数为标准分成三类：

{1，2，3，4，5，…} → $\boxed{1}$：只有1个约数；
→ $\boxed{素数}$：只有2个约数；
→ $\boxed{合数}$：至少有3个约数。

例如 420 就是一个合数，因为 $420=42\times 10$。但 42 和 10 又都是合数，因为 $42=6\times 7$，$10=2\times 5$，由于 $6=2\times 3$，因此最终得知 $420=42\times 10=6\times 7\times 2\times 5=2\times 3\times 7\times 2\times 5=2\times 2\times 3\times 5\times 7$，这样便把 420 分解为素数的连乘积。

一些数学家将素数称为构成数学大厦的砖头。



素数扮演着数字产生器的功能；它们可以创造所有的自然数。素数是整个自然数系的建构支撑点，对它们的了解成为数学家的中心课题。

素数的概念——可以追溯到古希腊的数学家，甚至现代数学的许多传统都要归功于他们。欧几里得在他那伟大的 13 卷著作《原本》中就用了许多篇幅（第 7、8、9 卷）来讨论素数。他证明了我们上面看到的把合数可以分解成若干个素数之积的这个事实——这个事实现在被称为“算术基本定理”，这个定理是数学中的核心定理之一。

算术基本定理

【表述 1】 每个大于 1 的自然数均可以分解为有限个素数的乘积，并且具有唯一（不计次序变化）的素数分解式。

【表述 2】 大于 1 的自然数 N 可以分解为具有下列形式的有限个素数的乘积：

$$N=p_1^{a_1}\times p_2^{a_2}\times\cdots\times p_{n-1}^{a_{n-1}}\times p_n^{a_n}$$

其中 $p_1,p_2,\cdots,p_n$ 均为素数，且 $p_1<p_2<\cdots<p_n$，$a_1,a_2,\cdots,a_n$ 均为非零自然数，这种形式叫做 N 的**标准分解式**。

自然数标准分解式的表示

直接分解式

$420=2^2\times3\times5\times7$

$\boxed{2}\times210$

$\boxed{2}\times105$

$\boxed{3}\times35$

$\boxed{5}\times\boxed{7}$

短除法

$$\begin{array}{r|l} 2 & 420=2^2\times3\times5\times7 \\ \hline 2 & 210 \\ \hline 3 & 105 \\ \hline 5 & 35 \\ \hline & \ \ 7 \end{array}$$

算术基本定理的内容由两部分组成：

1. 分解的存在性：

指的是每个大于 1 的正整数均可分解成一些素数的乘积。

例如，105 可以分解成素数 3，5，7 的乘积，即 $105=3\times5\times7$。

2. 分解的唯一性：

即不考虑诸素数的排列顺序的话，则把正整数分解成素数乘积的方式还是唯一的。

例如，35 的素数分解只有 $35=5\times7$ 和 $35=7\times5$，但本质上属于同一种分解。

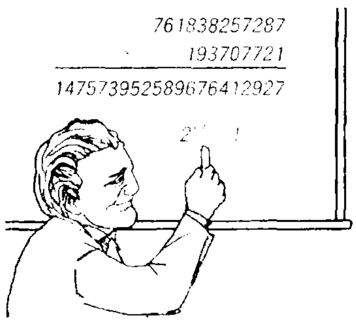
算术基本定理告诉我们素数好比物理中的基本粒子——所有整数得以构成的基本砖块，也好比化学中的原子——物质独特的原子结构知识就能告诉我们该物质的很多特性一样，掌握了某个整数的唯一素数分解就能告诉我们这个整数的许多数学性质。

正如高斯在《算术研究》(1801)一书中写到：

“把素数和合成数区分开来和把合成数分解出素因子是算术中最重要和有益的问题之一……科学本身的自尊要求人们采用一切可能的手段来探索去解决这个如此精美和著名的问题。”

历史注记

1. 一场无声的报告——大数的分解



在颇具声望的美国数学会于 1903 年 10 月举行的会议上，数学家 F. N. 科尔提交了一篇文章，它的题目相当平凡：“关于大数的因子分解”。当轮到他讲演时，科尔走到黑板前，一言未发便做起 2 的次幂的演算，直到 2 的 67 次幂，然后从所得结果中减去 1；他沉默无言地走到黑板的空白处，又将下述两数相乘：

193707721 和 761838257287

两次演算的答案是一样的。然后他还是未吐一字回到座位上，这时全场听众站了起来为他热烈鼓掌，这在美国数学会开会的历史上是绝无仅有的一次。

当有的数学家询问科尔花多长时间去解决这个问题时，科尔回答：三年来的所有周末！

2. 素数与密码

将几个素数相乘非常简单，反过来——将一个数分解成素数相乘的形式是不是很难呢？对于非常大的数字这几乎是不可能的。这使得素数在设定密码方面相当适合。当你在互联网上消费的时候，交易的细节都是通过这种方式隐藏起来的。代码的“锁”是非常大的数字，而“钥匙”则是由它的素数组成，现在人们已将大素数用于现代密码设计领域。