数学奥林匹克小丛书·高中卷

数学竞赛中的数论问题

余红兵摇著

华东师范大学出版社

摇图书在版编目（悦陨孕）数据

摇数学奥林匹克小丛书援高中卷援数学竞赛中的数论问题 辕余红兵著援—上海：华东师范大学出版社，圆园园源
摇陨杂月晕 苑鄄缘远员苑鄄源员远员鄄愿

摇Ⅰ援数援摇Ⅱ援余援摇Ⅲ援数学课—高中—教学参考资料摇Ⅳ援郧远猿源援远园猿

摇中国版本图书馆 悦陨孕 数据核字（圆园园源）第 园猿缘愿源远号

数学奥林匹克小丛书 · 高中卷
数学竞赛中的数论问题

著摇摇者摇余红兵
策划组稿摇倪摇明
责任编辑摇审校部编辑工作组
特约编辑摇余海峰
封面设计摇高摇山
版式设计摇蒋摇克

出版发行摇华东师范大学出版社
市场部 电话 021-62865537
门市（邮购）电话 021-62869887
门市地址 华东师大校内先锋路口
业务电话 上海地区 021-62232873
华东 中南地区 021-62458734
华北 东北地区 021-62571961
西南 西北地区 021-62232893
业务传真 021-62860410 62602316
http：// www援cnupress援com援cn
社　　址 上海市中山北路 3663 号
邮编 200062

照　　排 南京理工出版信息技术有限公司
印 刷 者 印刷厂
开　　本 787×960 16 开
印　　张 5.5
字　　数 千字
版　　次 2004 年 4 月第一版
印　　次 2004 年 4 月第一次
印　　数
书　　号 ISBN 7-5617-4161-8/G · 2386
定　　价 8.00 元

出 版 人 朱杰人

总摇摇序

摇摇数学竞赛像其他竞赛活动一样，是青少年学生的一种智力竞赛援在类似的以基础科学为竞赛内容的智力竞赛活动中，数学竞赛的历史最悠久、国际性强，影响也最大援我国于 [illegible] 年开始举行数学竞赛，当时最有威望的著名数学家华罗庚、苏步青、江泽涵等都积极参加领导和组织竞赛活动，并组织出版了一系列青少年数学读物，激励了一大批青年学生立志从事科学事业援我国于 [illegible] 年起参加国际数学奥林匹克，多次获得团体总分第一，并于 [illegible] 年在北京成功地举办了第 [illegible] 届国际数学奥林匹克，这标志着我国数学竞赛水平在国际上居领先地位，为各国科学家与教育家所瞩目援

我国数学竞赛活动表明，凡是开展好的地区和单位，都能大大激发学生的学习数学的兴趣，有利于培养创造性思维，提高学生的学习效率援这项竞赛活动，将健康的竞争机制引进数学教学过程中，有利于选拔人才援由数学竞赛选拔的优胜者，既有踏实广泛的数学基础，又有刻苦钻研、科学的学习方法，其中的不少青年学生将来会成为出色的科学工作者援在美国，数学竞赛的优胜者中后来成名如米尔诺（[illegible]）、芒福德（[illegible]）、奎伦（[illegible]）等都是菲尔兹数学奖的获得者；在波兰，著名数论专家辛哲尔（[illegible]）学生时代是一位数学竞赛优胜者；在匈牙利，著名数学家费叶尔（[illegible]）、里斯（[illegible]）、舍贵（[illegible]）、哈尔（[illegible]）、拉多（[illegible]）等都曾是数学竞赛获奖者援匈牙利是开展数学竞赛活动最早的国家，产生了同它的人口不成比例的许多大数学家！

在开展数学竞赛的活动同时，各学校能加强联系，彼此交流数学教学经验，从这种意义上来说，数学竞赛可能成为数学课程改革的“催化剂”，成为培养优秀人才的有力措施援

不过，应当注意在数学竞赛活动中，注意普及与提高相结合，而且要以普

及为主,使竞赛具有广泛的群众基础,否则难以持久援

当然,现在有些人过于关注数学竞赛的成绩,组织和参与都具有很强的功利目的,过分扩大数学竞赛的作用,这些都是不正确的,违背了开展数学竞赛活动的本意援这些缺点有其深层次的社会原因,需要逐步加以克服,不必因为有某些缺点,就否定这项活动援

我十分高兴看到这套《数学奥林匹克小丛书》的正式出版援这套书,规模大、专题细援据我所知,这样的丛书还不多见援这套书不仅对数学竞赛中出现的常用方法作了阐述,而且对竞赛题作了精到的分析解答,不少出自作者自己的研究所得,是一套很好的数学竞赛专题教程,也是中小学生和教师的参考书援

这套小丛书的作者都是数学竞赛教学和研究人员,不少是国家集训队的教练和国家队的领队援他们为我国开展数学竞赛的活动和我国学生在 IMO 上取得成绩、为国争光作出了贡献,为这套书尽早面世付出了艰辛的劳动援华东师大出版社在出版《奥数教程》和《走向 IMO》等竞赛图书基础上,策划组织了这套丛书,花了不少心血援我非常感谢作者们和编辑们在这方面所做的工作,并衷心祝愿我国的数学竞赛活动开展得越来越好援

王元

王元,著名数学家,中国科学院院士,曾任中国数学会理事长、中国数学奥林匹克委员会主席援

目摇摇录

1 整摇摇除

本书中所涉及的数都是整数,所用的字母除特别申明外也都表示整数援

设 葬 遭是给定的数,遭≠园援若存在整数 糟使得 葬越遭糟 则称 遭整除 葬,记作 遭凿葬 并称 遭是 葬的一个约数(或因子),而称 葬为 遭的一个倍数援如果不存在上述的整数 糟则称 遭不能整除 葬,记作 遭 葬援

由整除的定义,容易推出整除的几个简单性质(证明请读者自己完成):

(员) 若 遭凿糟 且 糟凿葬 则 遭凿葬 即整除性质具有传递性援

(圆) 若 遭凿葬 且 遭凿糟 则 遭凿(葬依糟),即为某一整数倍数的整数之集关于加、减运算封闭援

反复应用这一性质,易知:若 遭凿葬员,及 遭凿糟 则对任意整数 怎,增有 遭凿(葬员怎垣糟)援更一般地,若 葬员, 葬圆, …, 葬 都是 遭的倍数,则 遭凿(葬员 垣葬圆 垣… 垣葬)援

(猿) 若 遭凿葬 则或者 葬越园 或者 渍葬渍逸渍遭渍援因此,若 遭凿葬且 葬≠遭 则渍葬渍越渍遭渍援

对任意两个整数 葬 遭(遭跃园),葬当然未必被 遭整除,但我们有下面的结论——带余除法,这是初等数论中最为基本的一个结果援

(源) (带余除法) 设 葬 遭为整数,遭跃园 则存在整数 择和 则使得

$$葬越遭择垣则 \quad 其中 \quad 园\leqslant 则<遭$$

并且 择和 则由上述条件惟一确定援

整数 择称为 葬被 遭除得的(不完全)商,数 则称为 葬被 遭除得的余数援注意,则共有 遭种可能的取值:园, 员, …, 遭原员援若 则越园,即为前面说的 葬被 遭整除的情形援

易知,带余除法中的商 择实际上为$\left[\dfrac{葬}{遭}\right]$$\left(\text{不超过}\dfrac{葬}{遭}\text{的最大整数}\right)$,而带余除法的核心是关于余数 则的不等式:园≤ 则<遭 我们在后面将看到这一点援

证明 遭凿葬的基本手法是将 葬分解为 遭与一个整数之积援在较初级的问题

中，这种数的分解常通过在一些代数式的分解中取特殊值而产生援下面两个分解式在这类论证中应用很多援

（缘 若 灶是正整数，则

曾 原赠 越（曾原赠（曾 垣曾 赠垣… 垣曾赠 垣赠）援

（远 若 灶是正奇数，则（在上式中用 原赠代换 赠

曾 垣赠 越（曾垣赠（曾 原曾 赠垣… 原曾赠 垣赠）援

例 员摇证明 员园…园员被 员园园员整除援

证明摇由分解式（远，我们有

员园…园员越员园 垣员越（员园）垣员摇摇摇摇摇摇摇摇

越（员园 垣员）[（员园）原（员园）垣… 原员园 垣员]，

所以，员园 垣员（越员园园员）整除 员园…园员援

例 圆摇设 皂 跃灶≥ 园 证明：（圆 垣员）渣（圆 原员）援

证明摇在分解式（缘 中取 曾越圆，赠越员 并以 圆 代替那里的 灶，得出

圆 原员越（圆 原员）[（圆）垣… 垣圆 垣员]，

故摇 （圆 原员）渣（圆 原员）援

又 圆 原员越（圆 原员）（圆 垣员），

从而摇 （圆 垣员）渣（圆 原员）援

于是由整除性质（员 知 （圆 垣员）渣（圆 原员）援

注摇整除问题中，有时直接证明 遭渣葬不易入手，我们可以尝试着选择适当的“中间量”糟来证明 遭渣糟及 糟渣葬，由此及整除性质（员，便导出了结论援

例 猿摇对正整数 灶，记 杂（灶）为 灶的十进制表示中数码之和援证明：怨渣灶的充分必要条件是 怨渣杂（灶）援

证明摇设 灶越葬 伊员园 垣… 垣葬 伊员园垣葬（这里 园≤ 葬≤ 怨且 葬≠ 园），则 杂（灶） 越葬 垣葬 垣… 垣葬援我们有

灶原杂（灶） 越葬（员园 原员） 垣… 垣葬（员园原员）援 ①

对 员≤ 蚤≤ 噪 由分解式 (缘 知 怨渣(灾蚤原灾员，故①式右端 噪个加项中的每一个都是 怨的倍数，从而由整除性质 (圆 知，它们的和也被 怨整除，即 怨渣(灶原杂(灶) 援由此易推出结论的两个方面援

注 员摇整除性质 (圆 提供了证明 遭渣(葬员 垣葬圆 垣… 垣葬灶) 的一种基本的想法，我们可尝试着证明更强的 (也往往是更易于证明的) 命题：

遭整除每个 葬蚤(蚤越员，圆，…，灶 援

这一更强的命题当然并非一定成立，即使在它不成立时，上述想法仍有一种常常奏效的变通 :将和 葬员 垣葬圆 垣… 垣葬灶适当地分组成为 糟员垣糟圆 垣… 垣糟噪，而 遭渣糟蚤(蚤越员，圆，…，噪 援读者将看到，为了证明 遭渣葬，我们有时针对具体问题将 葬表示为适当数之和，以应用上述想法论证援

注 圆摇例 猿的证明，实际上给出了更强的结论 :对任意正整数 灶，数 灶与杂(灶 之差总是 怨的倍数援由此易知，灶与 杂(灶 被 怨除得的余数相同 (这可表述为 灶与 杂(灶 模 怨同余，请看第 远单元) 援

注 猿摇有些情形，我们能够由正整数十进制表示中的数码 (字) 的性质，推断这整数能否被另一个整数整除，这样的结论，常称为“整除的数字特征”援被圆 缘 员园整除的数的数字特征是显而易见的援例 猿则给出了被 怨整除的数的数字特征援这一结果，应用相当广泛而且灵活多样援另外，习题 员第 猿题给出了被 员员整除的数的数字特征，这也是一个应用较多的结论援

例 源摇设 噪≥ 员是一个奇数，证明 :对任意正整数 灶，数 员噪 垣圆噪 垣… 垣灶噪不能被 灶垣圆整除援

证明摇 灶越员时结论显然成立援设 灶≥ 圆 记所说的和为 粤，则

圆粤 越圆垣 (圆噪 垣灶噪) 垣 (猿噪 垣 (灶原员) 噪) 垣… 垣 (灶噪 垣圆噪) 援

因 噪是正奇数，故由分解式 (远 可知，对每个 蚤≥ 圆 数 蚤噪垣 (灶垣圆原蚤) 噪被蚤垣 (灶垣圆原蚤 越灶垣圆整除，故 圆粤被 灶垣圆除得的余数是 圆，从而 粤不可能被灶垣圆整除 (注意 灶垣圆 跃圆 援

注摇论证中我们应用了“配对法”，这是数论中变形和式的一种常用手法援

例 缘摇设 皂、灶为正整数，皂 跃圆 证明：(圆皂 原员 ∤ (圆灶 垣员 援

证明摇首先，当 灶≤ 皂时，易知结论成立援事实上，皂 越灶时，结论平凡；灶约皂时，结果可由 圆灶 垣员≤ 圆皂原员 垣员约圆皂 原员推出来 (注意 皂 跃圆 并参看整除性质 (猿) 援

最后，灶跃皂的情形可化为上述特殊情形 :由带余除法，灶越皂择垣则 园≤

则约皂, 而 择跃园援由于

圆灶 垣员越 (圆择 原员)(圆灶 垣圆灶 垣员),

由分解式 (缘)知 (圆灶 原员) 渣(圆择 原员);而 园≤ 则约皂, 故由上面证明了的结论知 (圆灶 原员) ∤ (圆灶 垣员) 援(注意 则越园时,结论平凡援) 从而当 灶跃皂时也有 (圆灶 原员) ∤ (圆灶 垣员) 援这就证明了本题结论援

摇摇摇习摇题摇员

员 设 灶和 噪都是正整数,则 员, 圆, …, 灶中恰有 [灶/噪] 个数被 噪整除援

圆 灾个女孩与 灶个男孩去采蘑菇援所有这些孩子共采到 灶圆 垣怨灶原圆个蘑菇,并且每个孩子采到的个数都相同援试确定,采蘑菇的孩子中是女孩多还是男孩多援

猿 设正整数 灶的十进制表示为 灶越葬噪…葬员葬园 (园≤ 葬蚤≤ 怨, 葬噪≠ 园),记 栽(灶) 越葬园 原葬员 垣… 垣(原员)噪葬噪 (由 灶的个位起始的数码的正、负交错和) 援证明 灶原栽(灶) 被 员员整除援由此得出被 员员整除的数的数字特征:员员整除 灶的充分必要条件是 员员整除 栽(灶) 援

源 设 灶个整数具有下述性质:其中任意 灶原员个数之积与剩下那个数的差都能被 灶整除援证明:这 灶个数的平方和也能被 灶整除援

缘 设整数 葬, 遭, 糟, 凿满足 葬凿原遭糟跃员, 证明:葬, 遭, 糟, 凿中至少有一个数不被 葬凿原遭糟整除援

004

2 最大公约数与最小公倍数

最大公约数是数论中的一个重要概念援

设 葬 遭不全为零,同时整除 葬 遭的整数 (如 依员 称为它们的公约数援因葬 遭不全为零,故由第 员单元中性质 (猿 推知,葬 遭的公约数只有有限多个,我们将其中最大的一个称为 葬 遭的最大公约数,用符号 (葬 遭表示援显然,最大公约数是一个正整数援

当 (葬 遭 越员时 (即 葬 遭的公约数只有 依员 ,我们称 葬与 遭互素 (互质) 援读者在后面将看到,这种情形特别重要援

对于多于两个的 (不全为零的) 整数 葬 遭 …, 糟可类似地定义它们的最大公约数 (葬 遭 …, 糟援若 (葬 遭 …, 糟 越员,则称 葬 遭 …, 糟互素援请注意,此时并不能推出 葬 遭 …, 糟两两互素 (即其中任意两个都互素) ;但反过来,若 葬 遭 …, 糟两两互素,则显然有 (葬 遭 …, 糟 越员援

由定义不难得出最大公约数的一些简单性质:

任意改变 葬 遭的符号不改变 (葬 遭的值,即有 (依葬 依遭 越 (葬 遭;

(葬 遭关于 葬 遭对称,即有 (葬 遭 越 (遭 葬;

(葬 遭作为 遭的函数,以 葬为周期,即对任意整数 曾有 (葬 遭垣葬曾 越 (葬 遭援

下面 (员 中的结论,是建立最大公约数的性质的基础援

(员 设 葬 遭是不全为 园的整数,则存在整数 曾 赠使得

$$葬曾垣遭赠越(葬\ 遭)$$

顺便提及,若 曾越曾$_0$, 赠越赠$_0$是满足上式的一对整数,则等式

$$葬(曾_0垣遭\cdot\frac{遭}{(葬\ 遭)})垣遭(赠_0原葬\cdot\frac{葬}{(葬\ 遭)})越(葬\ 遭)\quad(怎为任意整数)$$

表明,满足上式的 曾 赠有无穷多组;并且,在 葬遭跃园时,可选择 曾为正 (负) 数,此时 赠则相应地为负 (正) 数援

由 (员 易于推出下面的

(圆 两个整数 葬 遭互素的充分必要条件是存在整数 曾 赠使得

$$葬曾+遭赠=越员$$

这通常称为 葬 遭适合的裴蜀等式援

事实上,条件的必要性是 (员 的特例援反过来,若有 曾 赠使等式成立,设 (葬 遭 越凿 则 凿|葬曾+遭赠且 凿|遭 故 凿|葬曾+遭赠及 凿|遭赠,于是 凿|(葬曾+遭赠),即 凿|员,从而 凿越员援

由 (员 及 (圆 不难导出下面的几个基本结论:

(猿 若 皂≠园,葬 皂|遭 则 皂|(葬,遭),即 葬 遭的任一个公约数都是它们的最大公约数的约数援

(源 若 皂 跃园 则 (皂葬,皂遭)越皂(葬,遭)援

(缘 若 (葬,遭)越凿 则 $\left(\frac{葬}{凿},\frac{遭}{凿}\right)$越员援因此,由两个不互素的整数,可自然地产生一对互素的整数援

(远 若 (葬,皂)越员,(遭,皂)越员 则 (葬遭,皂)越员援这表明,与一个固定整数互素的整数之集关于乘法封闭援由此可推出:若 (葬,遭)越员 则对任意 噪跃园有 (葬噪,遭)越员 进而对任意 造跃园有 (葬噪,遭造)越员援

(苑 设 遭≠园,葬|遭糟 若 (遭,糟)越员 则 遭|葬援

(愿 设正整数 葬,遭之积是一个整数的 噪次幂 (噪≥圆)援若 (葬,遭)越员 则 葬,遭都是整数的 噪次幂援一般地,设正整数 葬,遭,…,糟之积是一个整数的 噪次幂援若 葬,遭,…,糟两两互素,则 葬,遭,…,糟都是整数的 噪次幂援

(远)、(苑)、(愿 表现了互素的重要性,它们的应用也最为广泛援

现在,我们简单地谈谈最小公倍数援

设 葬,遭是两个非零整数,一个同时为 葬,遭倍数的数称为它们的一个公倍数援葬,遭的公倍数显然有无穷多个,这其中最小的正数称为 葬,遭的最小公倍数,记作 [葬,遭]援对于多个非零整数 葬,遭,…,糟可类似地定义它们的最小公倍数 [葬,遭,…,糟]援

下面是最小公倍数的主要性质援

(怨 葬与 遭的任一公倍数都是 [葬,遭]的倍数援对于多于两个整数的情形,类似的结论也成立援

(员园 两个整数 葬,遭的最大公约数与最小公倍数满足

$$(葬,遭)[葬,遭]=越葬遭越援$$

但请注意,对于多于两个整数的情形,类似的结论不成立 (请读者举出例

子）摇然而我们有下面的

（缘）摇若 葬，遭 …，糟两两互素，则有

[葬，遭 …，糟] 越葬遭·糟援

由此及（缘）可知，若 葬渣凿，遭渣凿，…，糟渣凿，且 葬，遭 …，糟两两互素，则有 葬遭·糟渣凿援

互素，在数论中相当重要，往往是许多问题的关键或基础援数学竞赛中，有一些问题要求证明两个整数互素（或求它们的最大公约数），下面几个例子体现了处理这些问题的一个基本方法援

例 员摇对任意整数 灶，证明分数 $\frac{圆员灶垣源}{员源灶垣猿}$ 是既约分数援

证明摇问题即要证明 圆员灶垣源与 员源灶垣猿互素援易知这两数适合裴蜀等式

猿（员源灶垣猿）原圆（圆员灶垣源）越员，

因此所说的结论成立援

一般来说，互素整数 葬，遭适合的裴蜀等式不易导出，因此我们常采用下述的变通手法：制造一个与裴蜀等式类似的辅助等式

葬曾垣遭增越则，

其中 则是一个适当的整数援若设（葬，遭）越凿，则由上式知 凿渣则援所谓适当的 则是指：由 凿渣则能够通过进一步的论证导出 凿越员，或者 则的约数较少，可以由排除法证得结论援

此外，上述辅助等式等价于 葬渣（遭增原则）或 遭渣（葬曾原则），有时，这些由整除更容易导出来援

例 圆摇设 灶是正整数，证明（灶！垣员，（灶垣员）！垣员）越员援

证明摇我们有等式

（灶！垣员）（灶垣员）原（（灶垣员）！垣员）越灶援 ①

设 凿越（灶！垣员，（灶垣员）！垣员），则由①知 凿渣灶援

进一步，因 凿渣灶！故 凿渣员，结合 凿渣（灶！垣员）可知 凿渣员，故 凿越员援

例 猿摇记 云$_{噪}$越圆$^{圆^{噪}}$垣员，噪≥园援证明：若 皂≠灶，则（云$_{皂}$，云$_{灶}$）越员援

证明摇不妨设 皂跃灶援论证的关键是利用 云$_{灶}$渣（云$_{皂}$原圆）（见第 员单元例圆），即有一个整数 曾使得

云$_{皂}$垣曾云$_{灶}$越圆援

007

设 凿越(云皂, 云灶)，则由上式推出 凿渣园. 所以 凿越员或 园援但 云灶显然是奇数，故必须 凿越员援

注摇 云噪(噪≥ 园) 称为费马(云藻则皂葬贼)数援例 猿表明，费马数两两互素，这是费马数的一个有趣的基本性质援

下面例 源的结论用处颇多，值得记住援

例 源摇设 葬跃员, 皂, 灶跃园. 证明：

(葬皂 原员, 葬灶 原员) 越葬(皂, 灶) 原员援

证明摇设 阅越(葬皂 原员, 葬灶 原员)援我们通过证明 (葬(皂, 灶) 原员) 渣阅及 阅渣(葬(皂, 灶) 原员) 来导出 阅越葬(皂, 灶) 原员. 这是数论中证明两数相等的常用手法援

因为 (皂, 灶) 渣皂, (皂, 灶) 渣灶. 由第 员单元中分解公式 (缘) 即知 (葬(皂, 灶) 原员) 渣(葬皂 原员)，以及 (葬(皂, 灶) 原员) 渣(葬灶 原员) 援故由本单元的性质 (猿) 可知，葬(皂, 灶) 原员整除 (葬皂 原员, 葬灶 原员)，即 (葬(皂, 灶) 原员) 渣阅援

为了证明 阅渣(葬(皂, 灶) 原员)，我们设 凿越(皂, 灶)援因 皂, 灶跃园. 故可选择 怎, 增跃园, 使得 (参见本单元性质 (员) 中的注释)

皂怎原灶增越凿援 ①

因为 阅渣(葬皂 原员)，故更有 阅渣(葬皂怎 原员) 援同样，阅渣(葬灶增 原员) 援故 阅渣(葬皂怎 原葬灶增)，从而由①，得

阅渣葬灶增(葬凿 原员) 援 ②

此外，因 葬跃员 及 阅渣(葬皂 原员)，故 (阅, 葬) 越员. 进而 (阅, 葬灶增) 越员援于是，从②及性质 (苑) 导出 阅渣(葬凿 原员)，即 阅渣(葬(皂, 灶) 原员) 援

综合已证得的两方面的结果，可知 阅越葬(皂, 灶) 原员援

例 缘摇设 皂, 灶跃园, 皂灶渣(皂圆 垣灶圆)，则 皂越灶援

证明摇设 (皂, 灶) 越凿. 则 皂越皂员凿, 灶越灶员凿. 其中 (皂员, 灶员) 越员援

于是，已知条件化为 皂员灶员渣(皂员圆 垣灶员圆)，故更有 皂员渣(皂员圆 垣灶员圆)，从而 皂员渣灶员圆援但 (皂员, 灶员) 越员, 故 (皂员, 灶员圆) 越员援结合 皂员渣灶员圆，可知必须 皂员越员援同理 灶员越员. 因此 皂越灶援

注 员摇对两个给定的不全为零的整数，我们常借助它们的最大公约数，并应用性质 (缘)，产生两个互素的整数，以利用互素的性质作进一步论证 (参见性质 (远)、(苑)) 援就本题而言，由于 皂灶为二次式，皂圆 垣灶圆为二次齐次式，上述手续的功效，实质上是将问题化归成 皂, 灶互素这种特殊情形援

注 圆摇在某些问题中，已知的条件 (或已证得的结论) 糟葬灶并不适用，我们

可试着选取 糟的一个适当的约数 遭并从 糟越葬遭过渡到 (较弱的结论) 遭渣葬以期望后者提供适宜于进一步论证的信息援例 缘中,我们便是由 皂员灶员 渣(皂圆员 垣灶圆员)产生了 皂员渣灶圆员,进而导出 皂员 越员援

例 远援设正整数 葬 遭 糟的最大公约数为 员并且

$$\frac{葬遭}{葬原遭}越糟援$$

证明:葬原遭是一个完全平方数援

证明援设 (葬 遭 越凿 则 葬越凿葬员,遭越凿遭员,其中 (葬员,遭员) 越员援由于 (葬 遭 糟 越员 故有 (凿 糟 越员援

现在,问题中的等式可化为

凿葬员遭员 越糟(葬员 原遭员), ①

由此可见 葬员 整除 糟遭员援因 (葬员,遭员) 越员 故 葬员 渣糟援同样得 遭员 渣糟援再由 (葬员,遭员) 越员便推出 葬员遭员 渣糟(参考性质 (怨与 (员园)) 援

设 糟越葬员遭员噪 其中 噪是一个正整数援一方面,显然 噪整除 糟另一方面,结合①式得 凿越噪(葬员 原遭员) ,故 噪渣凿援从而 噪渣(糟 凿 (见性质 (猿)) 援但 (糟 凿 越员 故 噪越员援

因此 凿越葬员 原遭员援故 葬原遭越凿(葬员 原遭员) 越凿圆援这就证明了 葬原遭是一个完全平方数援

注援借助素数,则可以给予本题一个更为直接的证明 (习题 猿第 缘题) 援

例 苑援设 噪为正奇数,证明:员垣圆垣… 垣灶整除 员噪 垣圆噪 垣… 垣灶噪援

证明援因为 员垣圆垣… 垣灶越$\frac{灶(灶垣员)}{圆}$,故问题等价于证明:灶(灶垣员) 整除 圆(员噪 垣圆噪 垣… 垣灶噪) 援因 灶与 灶垣员互素,所以这又等价于证明

灶渣圆(员噪 垣圆噪 垣… 垣灶噪)

及

(灶垣员) 渣圆(员噪 垣圆噪 垣… 垣灶噪) 援

事实上,由于 噪为奇数,故由第 员单元中分解公式 (远) ,可知

援圆(员噪 垣圆噪 垣… 垣灶噪) 援援援援援援援援援援援援援援援援援援

越 [员噪 垣 (灶原员) 噪] 垣 [圆噪 垣 (灶原圆) 噪] 垣… 垣 [(灶原员) 噪 垣员噪] 垣圆灶噪

是 灶的倍数援同理,

圆(贸 垣圆 垣… 垣灶) 越 [贸 垣灶] 垣 [圆 垣(灶原员)] 垣… 垣 [灶 垣贸]

是 灶垣员的倍数援

注摇整除问题中,有时直接证明 遭渣葬不易入手援若 遭可分解为 遭越遭员遭圆,其中 (遭员, 遭圆) 越员, 则我们可将原命题 遭渣葬分解为等价的两个命题 遭员渣葬及遭圆渣葬, 后者可能更容易导出来援例 苑应用了这一基本手法,例 远中证明 葬遭员渣遭圆槽也是这样做的援

更一般地,为了证明 遭渣葬, 可将 遭分解为若干个两两互素的整数 遭员, 遭圆, …, 遭k之积,而证明等价的 遭i渣葬(i越员, 圆, …, 灶) (参见性质 (员),并可比较第 员单元例 猿的注 员中说的想法) 援关于这种手法的一种标准应用,请参考第 猿单元例 缘援

摇摇摇习摇题摇圆

员 设 灶为整数,证明:(员圆灶垣缘) 怨灶垣原 越员援

圆 设 皂, 灶都是正整数,皂是奇数,证明:(圆 原员, 圆 垣员) 越员援

猿 设 (葬, 遭) 越员, 证明:(葬 垣遭, 葬遭) 越员援

源 若一个有理数的 噪次幂是整数 (噪≥ 员),则这有理数必是整数援更一般地,证明:一个首项系数为 依员的整系数多项式的有理数根,必定是一个整数援

缘 设 皂, 灶, 噪都是正整数,满足 [皂 垣噪, 皂] 越 [灶垣噪, 灶],证明:皂 越灶援

3 素数及惟一分解定理

大于 员的整数 灶总有两个不同的正约数:员和 灶援若 灶仅有这两个正约数(称 灶没有真因子),则称 灶为素数(或质数)援若 灶有真因子,即 灶可表示为 葬·遭的形式(这里 葬,遭为大于 员的整数),则称 灶为合数援于是,正整数被分成三类:数 员单独作一类,素数类及合数类援

素数在正整数中特别重要,我们常用字母 责表示素数援由定义易得出下面的基本结论:

(员) 大于 员的整数必有素约数援

这是因为,大于 员的整数当然有大于 员的正约数,这些约数中的最小数必然没有真因子,从而是素数援

(圆) 设 责是素数,灶是任意一个整数,则或者 责整除 灶,或者 责与 灶互素援

事实上,责与 灶的最大公约数(责,灶)必整除 责,故由素数的定义推知,或者(责,灶)越员,或者(责,灶)越责,即或者 责与 灶互素,或者 责渣灶援

素数的最为锐利的性质是下面的

(猿) 设 责是素数,葬,遭为整数援若 责渣葬遭,则 葬,遭中至少有一个数被 责整除援

实际上,若 责不整除 葬和 遭,则由上述的(圆),责与 葬,遭均互素,从而 责与 葬遭互素(见第 圆单元(远)),这与已知的 责渣葬遭相违!

由(猿)特别地推出,若素数 责整除 葬^{灶}(灶≥员),则 责渣葬援

关于素数的最为经典的一个结果是公元前欧几里得证明的:

(源) 素数有无穷多个援

我们用反证法来证明这一事实援假设素数只有有限多个,设全体素数为 责$_{员}$,责$_{圆}$,…,责$_{噪}$援考虑数 晕越责$_{员}$责$_{圆}$…责$_{噪}$垣员,显然 晕跃员,故 晕有素因子 责援因 责$_{员}$,责$_{圆}$,…,责$_{噪}$是全部素数,故 责必等于某个 责$_{蚤}$(员≤蚤≤噪),从而 责整除 晕原责$_{员}$责$_{圆}$…责$_{噪}$,即 责整除 员,这不可能援因此素数有无穷多个援(请注意,责$_{员}$…责$_{噪}$垣员并不一定是素数援)

011

(源 中的断言,也可由第 圆单元例 猿推出来. 设 $云_{噪}$ 越$圆^{噪}$ 垣员 (噪≥ 园) ,则 $云_{噪}$ 跃员, 故 $云_{噪}$ 有素约数援因已证明无穷数列 $\{云_{噪}\}$ (噪≥ 园) 中的项两两互素,故每个 $云_{噪}$ 的素约数与这个数列中其他项的素约数不同,因此素数必有无穷多个援

现在我们转向初等数论中最为基本的一个结果,即正整数的惟一分解定理,或算术基本定理,它表现了素数在正整数集合中的真正分量援

(缘 (惟一分解定理) 每个大于 员的正整数均可分解为有限个素数的积;并且,若不计素因数在乘积中的次序,这样的分解是惟一的援

换句话说,设 灶跃员, 则 灶必可表示为 灶越$责_{员}责_{圆}$…$责_{噪}$, 其中 $责_{蚤}$(员≤ 蚤≤ 噪) 都是素数;并且,若 灶有两种素因数分解

$$灶越责_{员}责_{圆}\cdots责_{噪} 越择_{员}择_{圆}\cdots择_{造}$$

则必有 噪越造并且 $责_{员}$, $责_{圆}$, …, $责_{噪}$是 $择_{员}$, $择_{圆}$, …, $择_{造}$的一个排列援

将 灶的素因数分解中的相同的素因子收集在一起,可知每个大于 员的正整数 灶可惟一地表示为

$$灶越责_{员}^{\alpha_{员}}责_{圆}^{\alpha_{圆}}\cdots责_{噪}^{\alpha_{噪}},$$

其中 $责_{员}$, $责_{圆}$, …, $责_{噪}$是互不相同的素数,$\alpha_{员}$, $\alpha_{圆}$, …, $\alpha_{噪}$是正整数,这称为 灶的标准分解援

若已知正整数 灶的 (如上所述的) 标准分解,则由惟一分解定理,可确定其全部的正约数:

(远 灶的全部正约数为 $责_{员}^{\beta_{员}}责_{圆}^{\beta_{圆}}\cdots责_{噪}^{\beta_{噪}}$,其中 $\beta_{蚤}$是满足 园≤ $\beta_{蚤}$≤ $\alpha_{蚤}$(蚤越员, …, 噪) 的任意整数援

由此易知,若证 τ (灶) 为 灶的正约数的个数,σ (灶) 为 灶的正约数之和,则有

$$\tau(灶) 越(\alpha_{员} 垣员)(\alpha_{圆} 垣员)\cdots(\alpha_{噪} 垣员),$$

$$\sigma(灶) 越\frac{责_{员}^{\alpha_{员}垣员}原员}{责_{员}原员}\cdot\frac{责_{圆}^{\alpha_{圆}垣员}原员}{责_{圆}原员}\cdot\cdots\cdot\frac{责_{噪}^{\alpha_{噪}垣员}原员}{责_{噪}原员}援$$

虽然素数有无穷多,但它们在自然数中的分布却极不规则 (参见习题 猿第 员题) 援给定一个大整数,判定它是否为素数,通常是极其困难的,要作出其标准分解,则更为困难援下面 (苑) 中的结果相当有趣,它对任意 灶跃员, 给出了 灶! 的标准分解援

(苑) 对任意正整数 皂及素数 责记号 $责^{\alpha}\|$ 皂表示 责渣皂, 但 $责^{\alpha垣员}\nmid$ 皂, 即 责