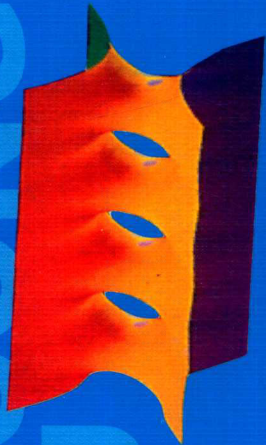
数学奥林匹克小丛书 高中卷 12

Shuxue Aolinpike XIAOCONG SHU



数学竞赛中的 数论问题

余红兵 著

华东师范大学出版社

Shuxue A

Xiao

Congshu

Shuxue

olinpike

数学奥林匹克小丛书

高中卷 12

数学竞赛中的数论问题

olinpike Xiao Congshu

余红兵 著

华东师范大学出版社

图书在版编目（CIP）数据

数学奥林匹克小丛书．高中卷．数学竞赛中的数论问题/余红兵著．—上海：华东师范大学出版社，2005.3
ISBN 7-5617-4161-8

I.数...　II.余...　III.数学课-高中-教学参考资料　IV.G634.603

中国版本图书馆CIP数据核字(2005)第019481号

数学奥林匹克小丛书·高中卷

数学竞赛中的数论问题

著　　者　余红兵
策划组稿　倪　明
责任编辑　审校部编辑工作组
特约编辑　余海峰
封面设计　高　山
版式设计　蒋　克

出版发行　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.ecnupress.com.cn
社　　址　上海市中山北路3663号
　　　　　邮编 200062

印·刷 者　江苏句容市排印厂
开　　本　787x960 16开
印　　张　5.5
字　　数　88千字
版　　次　2005年4月第一版
印　　次　2005年4月第一次
印　　数　11 000
书　　号　ISBN 7-5617-4161-8/G·2386
定　　价　8.00元

出 版 人　朱杰人

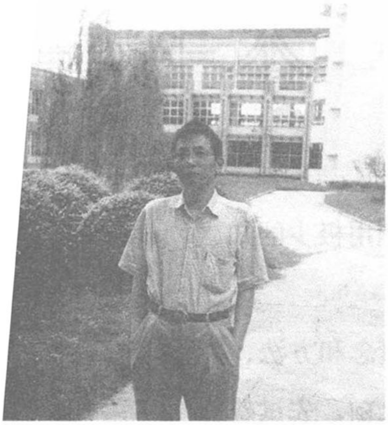
《数学竞赛中的数论问题》

本书导读

数论，是一个重要的数学分支，肇源极古.

数学竞赛中常常出现初等数论问题. 这类问题，利用极少的知识，生出无穷的变化，千姿百态，灵活多样.

本书通过数学竞赛问题介绍初等数论的一些基本概念和方法. 希望读者阅读此书时，带着纸和笔，在看例题的解答之前，先试着自己动手，这样才能真正体味出解题的窍门.



余红兵　中国数学奥林匹克委员会委员，数学奥林匹克国家集训队教练．苏州大学数学科学学院教授、博士生导师，理学博士．主要研究方向是数论，并长期有兴趣于数学普及工作，著作主要有《不定方程》、《组合几何》、《构造法解题》、《奥数教程（高三年级）》等．

数学奥林匹克小丛书

冯志刚	第44届IMO中国队副领队 上海中学特级教师
葛　军	中国数学奥林匹克高级教练、江苏省数学会普委会副主任 南京师范大学副教授
冷岗松	中国数学奥林匹克委员会委员、国家集训队教练 上海大学教授、博士生导师
李胜宏	第44届IMO中国队领队、中国数学奥林匹克委员会委员 浙江大学教授、博士生导师
李伟固	中国数学奥林匹克委员会委员、国家集训队教练 北京大学教授、博士生导师
刘诗雄	中国数学奥林匹克委员会委员 武钢三中校长、特级教师
倪　明	数学奥林匹克小丛书总策划 华东师范大学出版社副总编辑
单　墫	第30、31届IMO中国队领队 南京师范大学教授、博士生导师
吴建平	中国数学会普委会副主任、中国数学奥委会副主席 第40届IMO中国队副领队、《中学生数学》主编
熊　斌	第46届IMO中国队领队、中国数学奥林匹克委员会委员 华东师范大学副教授
余红兵	中国数学奥林匹克委员会委员、国家集训队教练 苏州大学教授、博士生导师
朱华伟	中国数学奥林匹克委员会委员、国家集训队教练 广州大学软件所常务副所长、研究员

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．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．我国于1956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．我国于1986年起参加国际数学奥林匹克，多次获得团体总分第一，并于1990年在北京成功地举办了第31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．

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．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．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．在美国，数学竞赛的优胜者中后来成名如米尔诺(J. W. Milnor)、芒福德(D. B. Mumford)、奎伦(D. Quillen)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(A. Schinzel)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(L. Fejér)、里斯(M. Riesz)、舍贵(G. Szegö)、哈尔(A. Haar)、拉多(T. Radó)等都曾是数学竞赛获奖者．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．

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.

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. 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.

我十分高兴看到这套《数学奥林匹克小丛书》的正式出版. 这套书，规模大、专题细. 据我所知，这样的丛书还不多见. 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.

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. 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. 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. 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.

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.

目　录

1 整除

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.

设 a、b 是给定的数，$b \neq 0$. 若存在整数 c，使得 $a = bc$，则称 b 整除 a，记作 $b \mid a$，并称 b 是 a 的一个约数(或因子)，而称 a 为 b 的一个倍数. 如果不存在上述的整数 c，则称 b 不能整除 a，记作 $b \nmid a$.

由整除的定义，容易推出整除的几个简单性质(证明请读者自已完成)：

(1) 若 $b \mid c$，且 $c \mid a$，则 $b \mid a$，即整除性质具有传递性.

(2) 若 $b \mid a$，且 $b \mid c$，则 $b \mid (a \pm c)$，即为某一整数倍数的整数之集关于加、减运算封闭.

反复应用这一性质，易知：若 $b \mid a$ 及 $b \mid c$，则对任意整数 u、v 有 $b \mid (au + cv)$. 更一般地，若 a_1，a_2，…，a_n 都是 b 的倍数，则 $b \mid (a_1 + a_2 + \cdots + a_n)$.

(3) 若 $b \mid a$，则或者 $a = 0$，或者 $|a| \geqslant |b|$. 因此，若 $b \mid a$ 且 $a \mid b$，则 $|a| = |b|$.

对任意两个整数 a、b $(b > 0)$，a 当然未必被 b 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.

(4) (带余除法) 设 a、b 为整数，$b > 0$，则存在整数 q 和 r，使得

$$a = bq + r，其中\ 0 \leqslant r < b,$$

并且 q 和 r 由上述条件惟一确定.

整数 q 称为 a 被 b 除得的(不完全)商，数 r 称为 a 被 b 除得的余数. 注意，r 共有 b 种可能的取值：0，1，…，$b-1$. 若 $r = 0$，即为前面说的 a 被 b 整除的情形.

易知，带余除法中的商 q 实际上为 $\left[\frac{a}{b}\right]$ $\left(不超过\frac{a}{b}的最大整数\right)$，而带余除法的核心是关于余数 r 的不等式：$0 \leqslant r < b$，我们在后面将看到这一点.

证明 $b \mid a$ 的基本手法是将 a 分解为 b 与一个整数之积. 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.下面两个分解式在这类论证中应用很多.

(5) 若 n 是正整数,则

$$x^n - y^n = (x-y)(x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1}).$$

(6) 若 n 是正奇数,则(在上式中用 $-y$ 代换 y)

$$x^n + y^n = (x+y)(x^{n-1} - x^{n-2}y + \cdots - xy^{n-2} + y^{n-1}).$$

例 1 证明:$1\underbrace{0\cdots0}_{200个0}1$ 被 1 001 整除.

证明 由分解式(6),我们有

$$\begin{aligned} 1\underbrace{0\cdots0}_{200个0}1 &= 10^{201} + 1 = (10^3)^{67} + 1 \\ &= (10^3 + 1)[(10^3)^{66} - (10^3)^{65} + \cdots - 10^3 + 1], \end{aligned}$$

所以,$10^3 + 1(= 1\,001)$ 整除 $1\underbrace{0\cdots0}_{200个0}1$.

例 2 设 $m > n \geqslant 0$,证明:$(2^{2^n} + 1) \mid (2^{2^m} - 1)$.

证明 在分解式(5)中取 $x = 2^{2^{n+1}}$,$y = 1$,并以 2^{m-n-1} 代替那里的 n,得出

$$2^{2^m} - 1 = (2^{2^{n+1}} - 1)[(2^{2^{n+1}})^{2^{m-n-1}-1} + \cdots + 2^{2^{n+1}} + 1],$$

故 $$(2^{2^{n+1}} - 1) \mid (2^{2^m} - 1).$$

又 $$2^{2^{n+1}} - 1 = (2^{2^n} - 1)(2^{2^n} + 1),$$

从而 $$(2^{2^n} + 1) \mid (2^{2^{n+1}} - 1).$$

于是由整除性质(1)知 $(2^{2^n} + 1) \mid (2^{2^m} - 1)$.

注 整除问题中,有时直接证明 $b \mid a$ 不易入手,我们可以尝试着选择适当的"中间量"c,来证明 $b \mid c$ 及 $c \mid a$,由此及整除性质(1),便导出了结论.

例 3 对正整数 n,记 $S(n)$ 为 n 的十进制表示中数码之和.证明:$9 \mid n$ 的充分必要条件是 $9 \mid S(n)$.

证明 设 $n = a_k \times 10^k + \cdots + a_1 \times 10 + a_0$(这里 $0 \leqslant a_i \leqslant 9$,且 $a_k \neq 0$),则 $S(n) = a_0 + a_1 + \cdots + a_k$.我们有

$$n-S(n)=a_k(10^k-1)+\cdots+a_1(10-1). \quad ①$$

对 $1\leqslant i\leqslant k$，由分解式(5)知 $9\mid(10^i-1)$，故①式右端 k 个加项中的每一个都是 9 的倍数，从而由整除性质(2)知，它们的和也被 9 整除，即 $9\mid(n-S(n))$. 由此易推出结论的两个方面.

注 1 整除性质(2)提供了证明 $b\mid(a_1+a_2+\cdots+a_n)$ 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：

$$b\text{ 整除每个 }a_i(i=1,\ 2,\ \cdots,\ n).$$

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 $a_1+a_2+\cdots+a_n$ 适当地分组成为 $c_1+c_2+\cdots+c_k$，而 $b\mid c_i(i=1,\ 2,\ \cdots,\ k)$. 读者将看到，为了证明 $b\mid a$，我们有时针对具体问题将 a 表示为适当数之和，以应用上述想法论证.

注 2 例 3 的证明，实际上给出了更强的结论：对任意正整数 n，数 n 与 $S(n)$之差总是 9 的倍数. 由此易知，n 与 $S(n)$被 9 除得的余数相同(这可表述为 n 与 $S(n)$模 9 同余，请看第 6 单元).

注 3 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”. 被 2、5、10 整除的数的数字特征是显而易见的. 例 3 则给出了被 9 整除的数的数字特征. 这一结果，应用相当广泛而且灵活多样. 另外，习题 1 第 3 题给出了被 11 整除的数的数字特征，这也是一个应用较多的结论.

例 4 设 $k\geqslant1$ 是一个奇数，证明：对任意正整数 n，数 $1^k+2^k+\cdots+n^k$ 不能被 $n+2$ 整除.

证明 $n=1$ 时结论显然成立. 设 $n\geqslant2$，记所说的和为 A，则

$$2A=2+(2^k+n^k)+(3^k+(n-1)^k)+\cdots+(n^k+2^k).$$

因 k 是正奇数，故由分解式(6)可知，对每个 $i\geqslant2$，数 $i^k+(n+2-i)^k$ 被 $i+(n+2-i)=n+2$ 整除，故 $2A$ 被 $n+2$ 除得的余数是 2，从而 A 不可能被 $n+2$ 整除(注意 $n+2>2$).

注 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.

例 5 设 m、n 为正整数，$m>2$，证明：$(2^m-1)\nmid(2^n+1)$.

证明 首先，当 $n\leqslant m$ 时，易知结论成立. 事实上，$m=n$ 时，结论平凡；$n<m$ 时，结果可由 $2^n+1\leqslant2^{m-1}+1<2^m-1$ 推出来(注意 $m>2$，并参看整除性质(3)).

最后，$n > m$ 的情形可化为上述特殊情形：由带余除法，$n = mq + r$，$0 \leqslant r < m$，而 $q > 0$. 由于

$$2^n + 1 = (2^{mq} - 1)2^r + 2^r + 1,$$

由分解式(5)知 $(2^m - 1) \mid (2^{mq} - 1)$；而 $0 \leqslant r < m$，故由上面证明了的结论知 $(2^m - 1) \nmid (2^r + 1)$.（注意 $r = 0$ 时，结论平凡.）从而当 $n > m$ 时也有 $(2^m - 1) \nmid (2^n + 1)$. 这就证明了本题结论.

习 题 1

1 设 n 和 k 都是正整数，则 $1, 2, \cdots, n$ 中恰有 $\left[\dfrac{n}{k}\right]$ 个数被 k 整除.

2 11 个女孩与 n 个男孩去采蘑菇. 所有这些孩子共采到 $n^2 + 9n - 2$ 个蘑菇，并且每个孩子采到的个数都相同. 试确定，采蘑菇的孩子中是女孩多还是男孩多.

3 设正整数 n 的十进制表示为 $n = \overline{a_k \cdots a_1 a_0}$ $(0 \leqslant a_i \leqslant 9,\ a_k \neq 0)$，记 $T(n) = a_0 - a_1 + \cdots + (-1)^k a_k$（由 n 的个位起始的数码的正、负交错和）. 证明 $n - T(n)$ 被 11 整除. 由此得出被 11 整除的数的数字特征：11 整除 n 的充分必要条件是 11 整除 $T(n)$.

4 设 n 个整数具有下述性质：其中任意 $n-1$ 个数之积与剩下那个数的差都能被 n 整除. 证明：这 n 个数的平方和也能被 n 整除.

5 设整数 a、b、c、d 满足 $ad - bc > 1$，证明：a、b、c、d 中至少有一个数不被 $ad - bc$ 整除.

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.

设 a、b 不全为零,同时整除 a、b 的整数(如± 1)称为它们的公约数.因 a、b 不全为零,故由第1单元中性质(3)推知,a、b 的公约数只有有限多个,我们将其中最大的一个称为 a、b 的最大公约数,用符号(a, b)表示.显然,最大公约数是一个正整数.

当 $(a, b) = 1$ 时(即 a, b 的公约数只有± 1),我们称 a 与 b 互素(互质).读者在后面将看到,这种情形特别重要.

对于多于两个的(不全为零的)整数 $a, b, \cdots, c$,可类似地定义它们的最大公约数$(a, b, \cdots, c)$.若 $(a, b, \cdots, c) = 1$,则称 $a, b, \cdots, c$ 互素.请注意,此时并不能推出 $a, b, \cdots, c$ 两两互素(即其中任意两个都互素);但反过来,若 $a, b, \cdots, c$ 两两互素,则显然有 $(a, b, \cdots, c) = 1$.

由定义不难得出最大公约数的一些简单性质:

任意改变 a、b 的符号不改变(a, b)的值,即有 $(\pm a, \pm b) = (a, b)$;

(a, b)关于 a、b 对称,即有 $(a, b) = (b, a)$;

(a, b)作为 b 的函数,以 a 为周期,即对任意整数 x,有 $(a, b+ax) = (a, b)$.

下面(1)中的结论,是建立最大公约数的性质的基础.

(1) 设 a、b 是不全为0的整数,则存在整数 x、y,使得

$$ax + by = (a, b).$$

顺便提及,若 $x = x_0$, $y = y_0$ 是满足上式的一对整数,则等式

$$a(x_0 + bu) + b(y_0 - au) = (a, b)\ (u \text{ 为任意整数})$$

表明,满足上式的 x、y 有无穷多组;并且,在 $ab > 0$ 时,可选择 x 为正(负)数,此时 y 则相应地为负(正)数.

由(1)易于推出下面的

(2) 两个整数 a、b 互素的充分必要条件是存在整数 x、y,使得

$$ax+by=1,$$

这通常称为 a、b 适合的裴蜀等式.

事实上,条件的必要性是(1)的特例. 反过来,若有 x、y 使等式成立,设 $(a,\ b)=d$, 则 $d\mid a$ 且 $d\mid b$, 故 $d\mid ax$ 及 $d\mid by$,于是 $d\mid (ax+by)$, 即 $d\mid 1$, 从而 $d=1$.

由(1)及(2)不难导出下面的几个基本结论:

(3) 若 $m\mid a,\ m\mid b$, 则 $m\mid (a,\ b)$, 即 a、b 的任一个公约数都是它们的最大公约数的约数.

(4) 若 $m>0$, 则 $(ma,\ mb)=m(a,\ b)$.

(5) 若 $(a,\ b)=d$, 则 $\left(\dfrac{a}{d},\ \dfrac{b}{d}\right)=1$. 因此,由两个不互素的整数,可自然地产生一对互素的整数.

(6) 若 $(a,\ m)=1,\ (b,\ m)=1$, 则 $(ab,\ m)=1$. 这表明,与一个固定整数互素的整数之集关于乘法封闭. 由此可推出:若 $(a,\ b)=1$, 则对任意 $k>0$ 有 $(a^k,\ b)=1$, 进而对任意 $l>0$ 有 $(a^k,\ b^l)=1$.

(7) 设 $b\mid ac$. 若 $(b,\ c)=1$, 则 $b\mid a$.

(8) 设正整数 a、b 之积是一个整数的 k 次幂 $(k\geqslant 2)$. 若 $(a,\ b)=1$, 则 a、b 都是整数的 k 次幂. 一般地,设正整数 $a,\ b,\ \cdots,\ c$ 之积是一个整数的 k 次幂. 若 $a,\ b,\ \cdots,\ c$ 两两互素,则 $a,\ b,\ \cdots,\ c$ 都是整数的 k 次幂.

(6)、(7)、(8)表现了互素的重要性,它们的应用也最为广泛.

现在,我们简单地谈谈最小公倍数.

设 a、b 是两个非零整数,一个同时为 a、b 倍数的数称为它们的一个公倍数. a、b 的公倍数显然有无穷多个,这其中最小的正数称为 a、b 的最小公倍数,记作$[a,\ b]$. 对于多个非零整数 $a,\ b,\ \cdots,\ c$,可类似地定义它们的最小公倍数$[a,\ b,\ \cdots,\ c]$.

下面是最小公倍数的主要性质.

(9) a 与 b 的任一公倍数都是$[a,\ b]$的倍数. 对于多于两个整数的情形,类似的结论也成立.

(10) 两个整数 a、b 的最大公约数与最小公倍数满足

$$(a,\ b)[a,\ b]=|ab|.$$

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).然而我们有下面的

(11) 若 $a, b, \cdots, c$ 两两互素,则有

$$[a, b, \cdots, c]=|ab\cdots c|.$$

由此及(9)可知,若 $a \mid d, b \mid d, \cdots, c \mid d$, 且 $a, b, \cdots, c$ 两两互素,则有 $ab\cdots c \mid d$.

互素,在数论中相当重要,往往是许多问题的关键或基础.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.

例 1 对任意整数 n,证明分数 $\dfrac{21n+4}{14n+3}$ 是既约分数.

证明 问题即要证明 $21n+4$ 与 $14n+3$ 互素.易知这两数适合裴蜀等式

$$3(14n+3)-2(21n+4)=1,$$

因此所说的结论成立.

一般来说,互素整数 a、b 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

$$ax+by=r,$$

其中 r 是一个适当的整数.若设 $(a, b)=d$, 则由上式知 $d \mid r$. 所谓适当的 r 是指:由 $d \mid r$ 能够通过进一步的论证导出 $d=1$, 或者 r 的约数较少,可以由排除法证得结论.

此外,上述辅助等式等价于 $a \mid (by-r)$ 或 $b \mid (ax-r)$, 有时,这些由整除更容易导出来.

例 2 设 n 是正整数,证明 $(n!+1, (n+1)!+1)=1$.

证明 我们有等式

$$(n!+1)(n+1)-((n+1)!+1)=n. \quad ①$$

设 $d=(n!+1, (n+1)!+1)$, 则由①知 $d \mid n$.

进一步,因 $d \mid n$ 故 $d \mid n!$, 结合 $d \mid (n!+1)$ 可知 $d \mid 1$, 故 $d=1$.

例 3 记 $F_k=2^{2^k}+1$, $k \geqslant 0$. 证明:若 $m \neq n$, 则 $(F_m, F_n)=1$.

证明 不妨设 $m>n$. 论证的关键是利用 $F_n \mid (F_m-2)$ (见第 1 单元例 2),即有一个整数 x,使得

$$F_m+xF_n=2.$$