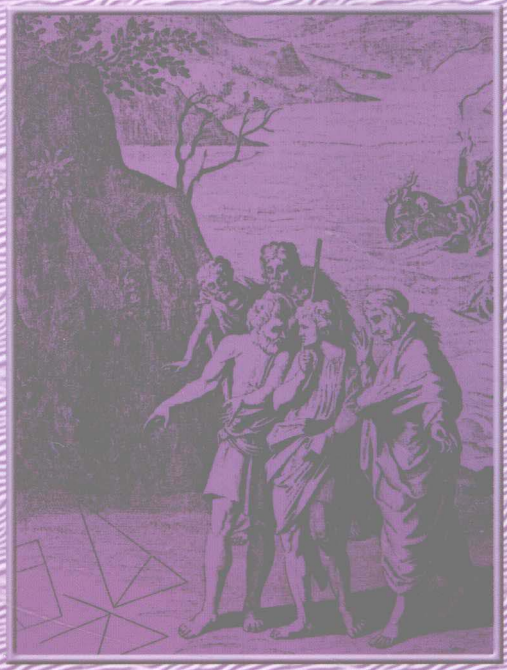
《数学中的小问题大定理》丛书（第二辑）

初等数论经典例题



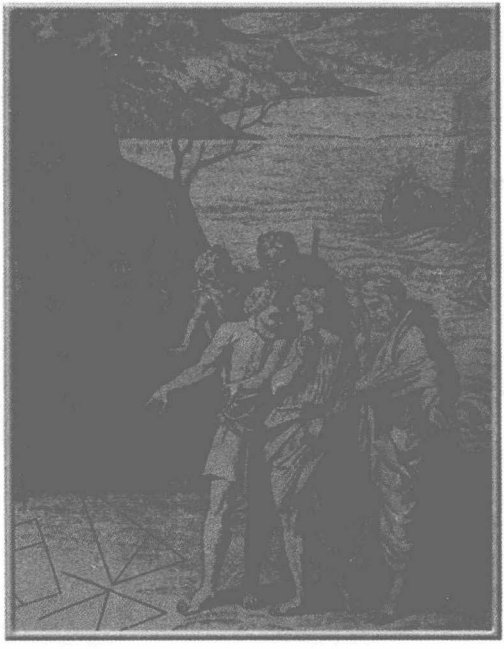
孙琦　曹珍富　编著

◎整　除
◎有限域上的本原多项式
◎费马小定理
◎切比雪夫不等式
◎p^2三方程

HITP

《数学中的小问题大定理》丛书（第二辑）

初等数论经典例题



孙琦　曹珍富　编著

◎整除
◎有限域上的本原多项式
◎费马小定理
◎切比雪夫不等式
◎Pell方程

哈尔滨工业大学出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS

内容简介

本书主要涉及初等数论的相关知识,共选编了62道较经典的初等数论题目和它们的解答,并在后面列出了所需要的定义和定理.通过这些题目和解答,能增强读者解决数学问题的能力.

本书可供从事这一数学分支或相关学科的数学工作者、大学生以及数学爱好者研读.

图书在版编目(CIP)数据

初等数论经典例题/孙琦,曹珍富编著.—哈尔滨:哈尔滨工业大学出版社,2012.7

ISBN 978-7-5603-3647-3

Ⅰ.①初… Ⅱ.①孙… ②曹… Ⅲ.①初等数论-题解 Ⅳ.①O156.1-44

中国版本图书馆CIP数据核字(2012)第160483号

策划编辑 刘培杰 张永芹
责任编辑 王 慧 张 佳
封面设计 孙茵艾
出版发行 哈尔滨工业大学出版社
社 址 哈尔滨市南岗区复华四道街10号 邮编150006
传 真 0451-86414749
网 址 http://hitpress.hit.edu.cn
印 刷 哈尔滨市石桥印务有限公司
开 本 787mm×960mm 1/16 印张8.75 字数81千字
版 次 2012年7月第1版 2012年7月第1次印刷
书 号 ISBN 978-7-5603-3647-3
定 价 18.00元

前　言

这里编著了62个初等数论经典例题，除每题都有详细解答外，大多数例题都给出了评注和参考文献，以指明其出处，或介绍它们的背景，供读者进一步阅读．这些例题包含以下三方面内容：

1. 与初等数论基础知识有关的习题，涉及整除性理论、同余式、数论函数（$\varphi(n)$，$d(n)$，$\pi(n)$等）、二次剩余中的Jacobi符号、元根、Pell方程等．

2. 某些经典结果和问题的有关研究工作，如早期Fermat大定理研究中的Germain定理，偶指数情形的Catalan猜想和柯召方法，Chevally定理

及其应用，一个同余式的解数在 Weil 猜想中的应用，运用 Pell 方程的性质研究组合数学中的 Hall 方程，不定方程的幂数比较法，加法数论的一些结果，计算 Smith 矩阵的行列式值，多元置换多项式的几个基本性质，等.

3. 初等数论在密码学、计算数论、有限域上的算术等领域的若干应用，如 RSA 的小指数攻击和共模攻击，基于二次剩余的公钥加密方案及其改进，有限域 F_p 上 n 阶可逆阵与经典 Hill 对称密码，正整数的标准二进制表示及其含零元最少的良好性质(可用于有限域上椭圆曲线公钥密码体制)，有限域上元根的 Golomb 猜想，在一定条件下分解 N 和计算 $\varphi(N)$ 或计算 $\mathrm{ord}_N(2)$ 的等价性，等.

众所周知，初等数论是数论的一个分支，主要用算术方法研究整数的性质，是一门重要的数学基础课. 它的许多定理和方法，不仅在数学的其他分支，而且在一些应用学科中，都有广泛的应用. 初等数论课程中的习题，是学习初等数论的重要环节. 通过阅读例题和做习题，可以更好地理解和掌握课程中的概念、定理和方法. 因此，我们希望《初等数论经典例题》这本小册子，能够为学习初等数论的读者，提供一点帮助. 此外，这本小册子的大部分题目是我们在长期教学和科研实践中提出的，尤其是在现代密码学中提炼的题目，希望对从事数论和密码学研究的有关读者也能有一点帮助.

1979 年，上海教育出版社出版了柯召先生和孙琦合编的一本小册子，叫做《初等数论 100 例》，是他们

在教学中积累的一部分题目．最近，哈尔滨工业大学出版社重版了该书．可以说，这里编著的62道例题传承了《初等数论100例》的风格，用到的知识虽然不多，但比较灵活，有一定难度，其中有的例题构思精巧，证明简洁，体现了数学之美，这也为数学的素质教育提供了一些例题．

2012年11月8日，是柯召先生逝世10周年的日子，我们谨以此书作为对柯召先生的纪念．

作者也感谢为本书的整理、打字付出劳动的几位研究生．

限于我们的水平，书中难免有缺点和疏漏，尚祈读者指正．

作者

2012年3月

⊙目录

初等数论62例

第1章

1. 证明不定方程

$$4xyz-x-y-t^2=0 \qquad (1)$$

无正整数解 x,y,z,t.

证 由方程(1)可得

$$(4xz-1)(4yz-1)=4zt^2+1 \qquad (2)$$

如果方程(1)有正整数解,则由式(2)推出

$$(2zt)^2\equiv -z(\mathrm{mod}(4yz-1)) \qquad (3)$$

设 $z=2^{\alpha}z'$,$\alpha\geqslant 0$ 是整数,z'是奇数.于是,Jacobi 符号

$$\left(\frac{-z}{4yz-1}\right)=\left(\frac{-1}{4yz-1}\right)\left(\frac{2^{\alpha}}{4yz-1}\right)\cdot\left(\frac{z'}{4yz-1}\right)$$

$$=(-1)\left(\frac{2}{4yz-1}\right)^{\alpha}\cdot$$

$$(-1)^{(\frac{4yz-2}{2})(\frac{z'-1}{2})}\left(\frac{4yz-1}{z'}\right)$$

$$=(-1)(-1)^{(\frac{z'-1}{2})}\left(\frac{-1}{z'}\right)$$

$$=-1$$

与式(3)矛盾,故方程(1)无正整数解.

2. 设正整数 ξ 和 η 是 Pell 方程

$$x^2-Dy^2=1 \tag{1}$$

的一组解,且满足

$$\xi>\frac{1}{2}\eta^2-1 \tag{2}$$

则(ξ,η)是方程(1)的基本解.

证 设(x_0,y_0)是方程(1)的基本解,$\varepsilon=x_0+y_0\sqrt{D}$,则有

$$\xi+\eta\sqrt{D}=\varepsilon^n,n>0 \tag{3}$$

故

$$\xi=\frac{\varepsilon^n+\bar{\varepsilon}^n}{2},\eta=\frac{\varepsilon^n-\bar{\varepsilon}^n}{2\sqrt{D}},\bar{\varepsilon}=x_0-y_0\sqrt{D} \tag{4}$$

由式(2)和式(4)得

$$\xi=\frac{\varepsilon^n+\bar{\varepsilon}^n}{2}>\frac{1}{2}\eta^2-1=\frac{\varepsilon^{2n}+\bar{\varepsilon}^{2n}-2}{8D}-1$$

即得

$$4D(\varepsilon^n+\bar{\varepsilon}^n)>\varepsilon^{2n}+\bar{\varepsilon}^{2n}-2-8D$$

$$(\varepsilon^n+\bar{\varepsilon}^n)^2-4D(\varepsilon^n+\bar{\varepsilon}^n)-8D-4<0$$

$$(\varepsilon^n+\bar{\varepsilon}^n+2)(\varepsilon^n+\bar{\varepsilon}^n-(4D+2))<0$$

故

$$\varepsilon^n + \bar{\varepsilon}^n < 4D + 2 \tag{5}$$

然而，当 $n \geqslant 2$ 时，有

$$\begin{aligned}\varepsilon^n + \bar{\varepsilon}^n &\geqslant \varepsilon^2 + \bar{\varepsilon}^2 \\ &= 2(x_0^2 + Dy_0^2) \\ &= 2(2Dy_0^2 + 1) \geqslant 4D + 2\end{aligned}$$

与式(5)矛盾．故得

$$n = 1$$

由式(3)推出

$$\varepsilon = \xi + \eta\sqrt{D}$$

注　此题的另一证明，可参阅[1]，[2].

Pell 方程的基本解与二次域的基本单位数，有着密切联系；在本书中我们还将看到用 Pell 方程来解高次不定方程的例子．20 世纪 20 年代末，Perron 曾得到有关 Pell 方程的一个经典结果：设 $D > 2$ 是一个无平方因子的整数，则在下面三个不定方程中，至多有一个方程有整数解

$$x^2 - Dy^2 = -1, x^2 - Dy^2 = 2, x^2 - Dy^2 = -2 \tag{6}$$

Yokoi 在研究类数为 1 的实二次域 $Q(\sqrt{D})$ 时，引进了一些新的 D - 不变量，及其与式(6)中三个方程可解性之间的关系，同时提出了一个猜想(参阅文献[3])．1996 年，袁平之把 Perron 的结果推广到广义 Pell 方程 $kx^2 - ly^2 = 1, 2, k > 1, l > 0, (k, l) = 1$，并证明了 Yokoi 提出的猜想(参阅文献[4]).

关于广义 Pell 方程的基本性质及其应用，可参阅文献[5]，[6].

[1] 柯召，孙琦．谈谈不定方程[M]．上海：上海教育出版社，1980；哈尔滨：哈尔滨工业大学出版社，

2011.

[2] 曹珍富. 丢番图方程引论[M]. 哈尔滨:哈尔滨工业大学出版社,2012.

[3] YOKOI H. New invariants and class number problem in quadratic fields[J]. Nagoya Math. J. ,1993,132:175 - 197.

[4] YUAN Pingzhi. D-invariants and the solvability of $kx^2 - ly^2 = 1,2$[J]. Japanese:J. of Math. ,1996(2):355 - 361.

[5] 孙琦,袁平之. 关于丢番图方程$\frac{ax^n - 1}{ax - 1} = y^2$和$\frac{ax^n + 1}{ax + 1}$[J]. 四川大学学报:自然科学版,1989(26):20 - 24.

[6] 曹珍富. 不定方程及其应用[M]. 上海:上海交通大学出版社,2000.

3. 证明:设p是一个素数,$p \equiv 1 \pmod 4$,则 Pell 方程

$$x^2 - py^2 = -1 \tag{1}$$

有整数解x,y.

证 设(x_0,y_0)是$x^2 - py^2 = 1$的基本解. 显然,x_0,y_0是一奇一偶. 如果x_0是偶,y_0是奇,则有

$$x_0^2 - py_0^2 = 1$$

取模 4 得矛盾结果$-1 \equiv 1 \pmod 4$. 因此,只能是x_0是奇,y_0是偶. 由$\frac{x_0 + 1}{2}$与$\frac{x_0 - 1}{2}$相差 1 知

$$\left(\frac{x_0 + 1}{2}, \frac{x_0 - 1}{2}\right) = 1$$

再由

$$\frac{x_0-1}{2}\cdot\frac{x_0+1}{2}=\frac{x_0^2-1}{4}=\frac{py_0^2}{4}=p(\frac{y_0}{2})^2$$

得

$$\frac{x_0-1}{2}=pu^2,\frac{x_0+1}{2}=v^2,y_0=2uv,v>0,u>0 \quad (2)$$

或

$$\frac{x_0-1}{2}=u^2,\frac{x_0+1}{2}=pv^2,y_0=2uv,v>0,u>0 \quad (3)$$

式(2)给出

$$v^2-pu^2=1$$

而 $u=\frac{y_0}{2v}<y_0$，与 y_0 最小矛盾．式(3)给出

$$u^2-pv^2=-1$$

故 Pell 方程(1)有整数解 $x=u,y=v$.

注　Pell 方程(1)的全部整数解 x,y，由

$$x+y\sqrt{p}=\pm(u+v\sqrt{p})^{2n+1}$$

给出，其中 n 取任意整数，u,v 由式(3)给出．2题和3题是 Pell 方程的两个基本性质，最早出现在 Nagell 的一本名著中，参见[1]．2题所引的文献[1]和[2]也曾编入．

[1] NAGELL T. Introduction to Number Theory. Almqvist and Wiksen, Stockholm; John Wiley and Sons Inc., New York, 1959.

4. 证明不定方程

$$x^2+x=y^4+y^3+y^2+y \quad (1)$$

仅有6组整数解 $(x,y)=(0,-1),(-1,-1),$

$(0,0),(-1,0),(5,2),(-6,2)$.

证 在方程(1)的两边乘以4,再加1,可得

$$\begin{aligned}(2x+1)^2 &= (2y^2+y)^2+3y^2+4y+1\\ &= (2y^2+y+1)^2-(y^2-2y) \qquad (2)\end{aligned}$$

易知,如果 y 是整数且不等于 $-1,0,1$ 和2,则

$$3y^2+4y+1=(3y+1)(y+1)>0$$

和

$$y^2-2y>0$$

同时成立,由式(2)即得

$$(2y^2+y)^2<(2x+1)^2<(2y^2+y+1)^2 \qquad (3)$$

这表明,$(2x+1)^2$ 在两个连续的平方数之间. 当 x 是整数时,式(3)不成立. 这就证明了在 $y\neq -1,0,1,2$ 时,方程(1)无整数解 x,y. 于是,在方程(1)中令 $y=-1,0,1,2$,除 $y=1$ 无解外,$y=-1,0$ 和2得到题中仅有的6组解.

注 这个题目源于一个著名的数论问题:设 p,q 是两个不同的素数,求不定方程

$$\frac{x^p-1}{x-1}=\frac{y^q-1}{y-1}$$

的整数解. 当 $p=3,q=5$ 时,此问题就退化为本题. 更多研究可参看文献[1].

[1] 曹珍富. 不定方程及其应用[M]. 上海:上海交通大学出版社,2000.

5. 设 p 是一个素数,而且把它的各位数字交换后仍是素数,则称 p 是一个绝对素数. 证明:绝对素数不能有多于3个不同的数字.

证　显然,能组成绝对素数的数字只可能有1,3,7,9. 由计算知

1 379,3 179,9 137,7 913,1 397,3 197,7 139

是模7的一组完全剩余系. 故对任给的整数 M,数组

$$M+1\ 379, M+3\ 179, M+9\ 137, M+7\ 913,$$
$$M+1\ 397, M+3\ 197, M+7\ 139 \qquad (1)$$

也是模7的一组完全剩余系,即知数组(1)中恰有一个被7整除. 这就证明了绝对素数不能有多于3个不同的数字.

6. 求出所有的正整数,使得其中每一个都等于这个数本身因数个数的平方.

证　显然,1满足要求. 现设

$$n>1, n=p_1^{\alpha_1}\cdots p_l^{\alpha_l}$$

是 n 的标准分解式. 令 $m=d(n)$,$d(n)$表示 n 的因子的个数,熟知,$m=(\alpha_1+1)\cdots(\alpha_l+1)$. 设 $n=m^2$,可得 $\alpha_i, i=1,\cdots,l$ 均为偶数,故 $m>1$ 是一个奇数,设 $m=2k+1(k>0)$. n 的因子除去 m 外,n 的任一对因子 a_i,$\frac{n}{a_i}$,其中恰有一个,不妨设为 $a_i, a_i<m, i=1,\cdots,k$,它们正好是小于 m 的全体奇数 $1,3,\cdots,2k-1$,故 $2k-1$ 整除 n. 而

$$n=m^2=(2k+1)^2=(2k-1)^2+8k$$

由此推出 $2k-1$ 整除 k. 此时仅当 $k=1$,即 $n=9$ 才成立. 而 $n=9$ 时,满足题目的要求. 这就证明了仅当 $n=1$ 和9时,$n=d^2(n)$ 成立.

注　著名数学问题的特例经常会成为数学竞赛试题.

第4,5,6三题分别选自“全苏数学奥林匹克试题”第89,386,426三题[1]. 其中89题较难,解题方法是一种常用的平方数处理手段,我们采用了该书的解答. 对于第386,426题,该书只给出简单的提示,我们给出了详细解答,并改正了386题提示中一处错误:“而对任意的 M,数 $M+1\ 379, M+3\ 179, M+9\ 137, M+7\ 913, M+1\ 397, M+3\ 197, M+7\ 139$ 都能被7整除”,应改为“恰有一个数被7整除”.

[1] ВАСИЛЬЕВ Н Б, ЕГОРОВ А А, 著. 李墨卿, 等译. 济南:山东教育出版社,1990.

7. 设 n 是一个正整数,$a_1,\cdots,a_n$ 是 n 个正整数,满足 $a_i \mid n, i=1,2,\cdots,n$,则存在一个非空子集 $S\subseteq\{1,2,\cdots,n\}$,使得

$$\sum_{j\in S} a_j = n \tag{1}$$

证 不妨设 $n>1$,对 $1\leqslant i\leqslant n$,令

$$L_i = \{a_{j_1}+\cdots+a_{j_t} \mid 1\leqslant j_1<\cdots<j_t\leqslant i, 1\leqslant t\leqslant i\} \cap \{1,2,\cdots,n\}$$

例如

$$L_1=\{a_1\}, L_2=\{a_1,a_2,a_1+a_2\}\cap\{1,2,\cdots,n\},\cdots$$

显然有

$$L_1\subseteq L_2\subseteq\cdots\subseteq L_n \tag{2}$$

由于 L_n 表示 $\{1,2,\cdots,n\}$ 与 $\{a_1,\cdots,a_n\}$ 的每一个非空子集中诸元之和所组成的集的交集,所以式(1)成立等价于 $n\in L_n$.

如果 $n\notin L_n$,由式(2)知 $n\notin L_j, j=1,\cdots,n-1$,且 $|L_n|<n$,而 $L_1=\{a_1\}$ 推出 $|L_1|\geqslant 1$,从而有 k 使得

$$|L_{k-1}| \geqslant k-1, |L_k| < k$$

这里 $2 \leqslant k \leqslant n$，故

$$|L_k| \leqslant k-1$$

另一方面，由式(2)可得

$$|L_{k-1}| \leqslant |L_k| \leqslant k-1 \leqslant |L_{k-1}|$$

故

$$|L_{k-1}| = |L_k|, L_k = L_{k-1}, a_k \in L_k, a_k \in L_{k-1}$$

于是

$$a_k = a_{j_1} + \cdots + a_{j_t}, 1 \leqslant j_1 < \cdots < j_t \leqslant k-1$$

可得

$$2a_k = a_k + a_{j_1} + \cdots + a_{j_t} \in L_k = L_{k-1}$$

同理

$$3a_k = a_k + 2a_k \in L_k = L_{k-1}, \cdots$$

$$n = \frac{n}{a_k} a_k$$

$$= \alpha_k + (\frac{n}{a_k} - 1) a_k \in L_k = L_{k-1}$$

即

$$n \in L_k$$

由式(2)，与 $n \notin L_k$ 矛盾.

注　此问题是由 Erdös 和 Lemke 提出的一个猜想中最值得探讨的部分. 猜想的完整证明见[1]，这里是部分猜想的简化证明，编选时略加改动.

[1] LEMKE P, KLEITMAN D. An addition theorem on the integer modulo n [J]. J. Number Theory, 1989(31):335-345.

8. 证明：一正整数为其诸因数(除本身外)之积的充分必要条件是此数为一素数的立方，或为两个不

同素数的积.

证 设 $n=p^3$ 或 $n=pq$,这里 p,q 为素数,$p\neq q$,则

$$\prod_{d\mid p^3,d\neq p^3} d=p\cdot p^2=p^3$$

或

$$\prod_{d\mid pq,d\neq pq} d=pq$$

反之,设 $n>1$ 是一个整数,满足

$$\prod_{d\mid n} d=n^2,\prod_{d\mid n}\frac{n}{d}=n^2$$

可得

$$\prod_{d\mid n} n=n^4 \tag{1}$$

设 $n=p_1^{\alpha_1}\cdots p_l^{\alpha_l}$ 为 n 的标准分解式,故

$$d(n)=(\alpha_1+1)\cdots(\alpha_l+1)$$

为 n 的因子个数. 由式(1)可得

$$n^{d(n)}=n^4 \tag{2}$$

再由式(2)得

$$(\alpha_1+1)\cdots(\alpha_l+1)=4$$

推出

$$l=1,\alpha_1=3 \text{ 或 } l=2,\alpha_1=\alpha_2=1$$

即 n 为一素数的立方或 n 为两个不同素数之积.

注 本题选自文献[1]中的一个习题.

[1] 华罗庚. 数论导引[M]. 北京:科学出版社,1957.

9. 设 $2k>0$,集 $A=\{a_1,\cdots,a_{\varphi(2k)}\}$ 表示小于 $2k$ 且与 $2k$ 互素的全体正整数所组成的集,定义

$$A+A=\{<a_i+a_j>_{2k}\mid a_i\in A,a_j\in A,i,j=1,2,\cdots,\varphi(2k)\}$$

则