数论导引提要及习题解答

任承俊　编著

柯　召　审定

四川科学技术出版社

一九八六年·成都

责任编辑：赵　健
封面设计：陈加伟
版面设计：杨丽娜

数论导引提要及习题解答

任承俊 编著　柯 召 审定

出版：四川科学技术出版社
印刷：四川新华印刷厂
发行：四川省新华书店
开本：850×1168 毫米1/32
印张：15.5　　插页：4
字数：381千
印数：1—3,000
版次：1986年9月第一版
印次：1986年9月第一次印刷
书号：13298·66
定价：3.90 元

代　序

华罗庚教授的《数论导引》是写得很好的一部专著，而任承俊同志编写的这本《数论导引提要及习题解答》，对于学习《数论导引》的人将会很有帮助．不过，读者在做题时，首先还是应当独立思考、刻苦钻研，得出结果后再翻阅题解；只当确感困难时，才求助于本书．这样，则既可锻炼提高自己的解题能力，又不至于在障碍面前束手无策．

书此数语，不知读者以为然否？

柯　召

1985年5月

前　言

随着科学技术的不断发展，数论这一“古老”而又“年轻”的学科，在技术领域中得到了许多卓有成效的应用．这引起了人们对数论的瞩目，同时也激发了广大青少年的兴趣．要求学习、掌握数论知识的人越来越多了．

华罗庚教授所著《数论导引》是数论书籍中的一部名著．该书从一九五七年问世到一九七九年已经五次印刷，但是迄今国内还未曾出版过与之相配合的习题解答．而华先生在介绍维诺格拉托夫的《数论基础》时就曾说过：“如果读这本书而不看不做书后的习题，就好象入宝山而空返，把这书的最重要的部分忽略了！”可见，要学习好数论，必须做大量的习题．本着为学习数论的同志提供解题参考的目的，我不揣浅陋，编写了这本《数论导引提要及习题解答》．

本书各章均由提要和习题解答两部分组成，前者列出了相应于各章的定义、定理，而后者则给出了全部习题的解答．此外，还有对于习题及答案中一些疏漏的订正，以及对某些有关问题的介绍和讨论等．全书共二十章．原书部分章节无习题（如第十八章，第一章中的§2、§3、§4等），本书将这些章节略去了．但目录中仍列出了第十八章的章名．

应当着重指出的是，在编写本书初稿的过程中，我始终得到了著名数学家柯召教授的关怀与鼓励．脱稿后，柯老又在百忙中对全书进行了审阅，且为一些难度较大的题目提供了解题思路，

或亲自给予了详细解答。就是说，本书凝结着老一辈科学家的心血，体现了老一辈科学家的人梯精神。

尽管有柯老指教，但限于本人水平，本书仍难免疏谬之处，望读者批评指正。

任承俊

1985年3月13日

目　录

第一章　整数之分解

一、提　要

定义　a为一实数，命$[a]$表示不超过a的最大整数。又命$\{a\}=a-[a]$。$[a]$和$\{a\}$分别称为a的整数部分和小数部分。

定理1　任给二整数a及b（$b>0$），必有二整数q及r，使

$$a=qb+r,\quad 0\leqslant r<b.$$

定理2　若$b\neq 0$，$c\neq 0$，则

1）若$b|a$，$c|b$，则$c|a$；

2）若$b|a$，则$bc|ac$；

3）若$c|d$，$c|e$，则对任意的m、n有$c|dm+en$。

定理3　若b是a的真因数，则

$$1<|b|<|a|.$$

定理4　非1的自然数都可以分解为素数的乘积。

定义　称一整数集合M为模，是指M满足条件：若$m\in M$，$n\in M$，则$m\pm n\in M$。

定理5　任何模必包含0；若a、b在模中，则$am+bn$也在模中。m、n为任何整数。

定理6　任一非零模，必为一正整数的倍数所成的集合。

定义　命a、b为二整数，于定理6中取形如$am+bn$所成的模，其中最小的正整数d称为a、b的最大公因数，记为(a,b)。

定理 7　(a,b) 有如下性质：

1）有整数x、y，使 $(a,b)=ax+by$；

2）对任何整数x、y，必有 $(a,b)\mid ax+by$；

3）若$e\mid a$，$e\mid b$，则$e\mid(a,b)$。

定义　若$(a,b)=1$，则称a、b互素。

定理 8　若p为素数并且$p\mid ab$，则$p\mid a$或$p\mid b$。

定理 9　若$c>0$及$(a,b)=d$，则一定有 $(ac,bc)=dc$。

定理10　n的标准分解式是唯一的。即如果不计次序，则n仅能由唯一的方法表示为素数的乘积。

定理11　命a、b为二正整数，p_1，……，p为其素因数。记为

$$a=p_1^{a_1}\cdots\cdots p_s^{a_s},\qquad a_v\geqslant 0$$

$$b=p_1^{b_1}\cdots\cdots p_s^{b_s},\qquad b_v\geqslant 0$$

则 $(a,b)=p_1^{c_1}\cdots\cdots p_s^{c_s}$，$c_v=\min(a_v,b_v)$。符号$\min(x_1,\cdots\cdots,x)$表$x_1$，……，$x_n$中最小的一个。

定义　命a、b为正整数。a、b都能整除的数称为它们的公倍数，其中最小的一个正整数名为最小公倍数，记为$[a,b]$。

定理12　与定理11的假定相同。a、b的最小公倍数为

$[a,b]=p_1^{e_1}\cdots\cdots p_s^{e_s}$，$e_v=\max(a,b)$。符号$\max(x_1,\cdots\cdots,x)$表$x_1$，……，$x_n$中最大的一个。

定理13　a，b的任一公倍数必为其最小公倍数的倍数。

定理14　$[a,b]\cdot(a,b)=ab$

定理15　命

$$a_1=p_1^{e_{11}}\cdots\cdots p_s^{e_{1s}},\cdots\cdots,\ a_n=p_1^{e_{n1}}\cdots\cdots p_s^{e_{ns}},$$

且 $e_{\mu v}\geqslant 0$，则

$$(a_1,\cdots\cdots,a_n)=p_1^{e_1}\cdots\cdots p_s^{e_s},\ e_v=\min(e_{1v},\cdots\cdots,e_{nv}),$$

$$[a_1,\cdots\cdots,a_n]=p_1^{d_1}\cdots\cdots p_s^{d_s},\ d_v=\max(e_{1v},\cdots\cdots,e_{nv}).$$

其中 $(a_1,\cdots\cdots,a_n)=((a_1,\cdots\cdots,a_{n-1}),a_n)$，

$$[a_1,\cdots\cdots,\ a_n]=[[a_1,\cdots\cdots,a_{n-1}],\ a_n]\ .$$

它们分别表示$a_1,\cdots\cdots,\ a$ 的最大公因数和最小公倍数。

定理16 （逐步淘汰原则）设有N件事物，其中$N\alpha$件 有性质α，$N\beta$件有性质β，……，$N_{\alpha\beta}$ 件同时有性质α 及β，……，$N_{\alpha\beta\gamma}$件 同时有性质α，β及γ，……。则此事物中既无性质α，又无性质β，又无性质γ，……的件数为

$$N-N\alpha-N\beta-\cdots\cdots+N_{\alpha\beta}+\cdots\cdots-N_{\alpha\beta\gamma}-\cdots\cdots+\cdots\cdots$$

定理17 方程

$$ax+by=n$$

有整数解x、y的充分必要条件为 $(a,b)\mid n$。

定理18 若 $(a,b)=1$，且x_0、y_0为方程

$$ax+by=n$$

的一组解，则$ax+by=n$的所有解为

$$x=x_0+bt,\ \ y=y_0-at.$$

定理19 设 $(a,b)=1$，$a>0$，$b>0$。凡大于$ab-a-b$的数必可表示为$ax+by$的形式，但$ab-a-b$不能 表 示成此种形式，其中$x\geqslant 0$，$y\geqslant 0$。

定理20 命$\sigma(n)$为n的所有因数的和，如果

$$n=p_1^{a_1}\cdots\cdots p_s^{a_s}$$

则

$$\sigma(n)=\frac{p_1^{a_1+1}-1}{p_1-1}\cdots\cdots\frac{p_s^{a_s+1}-1}{p_s-1},$$

定理21 若 $(n,m)=1$，则

$$\sigma(mn)=\sigma(m)\sigma(n).$$

定义 若$\sigma(n)=2n$，则称n为完全数。

定理22 若$p=2^n-1$ 为素数，则

$$\frac{1}{2}p(p+1)=2^{n-1}(2^n-1)$$

是一个完全数，且无其它偶完全数存在。

定义 形如2^n-1的素数称为Merenne数。

定义 形如$2^{2^n}+1$的数称为Fermat数。

定理23 p为素数，在$n!$中p的方次数为

$$\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\left[\frac{n}{p^3}\right]+\cdots\cdots.$$

定理24 $\binom{n}{r}=\frac{n!}{r!(n-r)!}$为一整数。

定义 当变数x取整数时，如果多项式$f(x)$的值总是整数，则称$f(x)$为整值多项式。

定理25 设$\Delta f(x)=f(x+1)-f(x)$

则 $$\Delta\binom{x}{r}=\binom{x}{r-1}.$$

定理26 凡k次整值多项式必可表示成

$$a_k\binom{x}{k}+a_{k-1}\binom{x}{k-1}+\cdots\cdots+a_1\binom{x}{1}+a_0$$

上式中$a_k,\cdots\cdots,a_0$都是整数，且只要$a_k,\cdots\cdots,a_0$取整数，那么上式总是整值多项式。

定理27 对任意整数x，整值多项式$f(x)$是m的倍数的充分必要条件为

$$m\mid(a_k,\cdots\cdots,a_0).$$

此处$a_k,\cdots\cdots,a_0$定义同定理26。

定义 命$f(x)$为一有理系数多项式，若有二个非常数的有理系数多项式$q(x)$及$h(x)$使

$$f(x)=q(x)h(x)$$

则称$f(x)$可分解或可化，不然则称$f(x)$不可分解或不可化。

定理28 (Fisenstein) 命

$$f(x)=c_nx^n+\cdots+c_0$$

为一整系数多项式。若$p\nmid c_n$，$p\mid c_i$，$0\leqslant i<n$且$p^2\nmid c_0$，则$f(x)$不

可化。

二、题 解

§1 整除性

习题1　若n为正整数，则$\left[\frac{[n\alpha]}{n}\right]=[\alpha]$。

证：设　$[n\alpha]=nq+r$，$0\leqslant r<n$，那么

$$n\alpha=nq+r+\{n\alpha\}$$

$$\left[\frac{[n\alpha]}{n}\right]=\left[\frac{nq+r}{n}\right]=\left[q+\frac{r}{n}\right]=q$$

$$[\alpha]=\left[\frac{nq}{n}\right]=\left[\frac{nq+r+\{n\alpha\}}{n}\right]$$

$$=\left[q+\frac{r+\{n\alpha\}}{n}\right]=q$$

从而　$$\left[\frac{[n\alpha]}{n}\right]=[\alpha]。$$

习题2　若n为正整数，则

$$[\alpha]+\left[\alpha+\frac{1}{n}\right]+\cdots\cdots+\left[\alpha+\frac{n-1}{n}\right]=[n\alpha]。$$

证：设$[n\alpha]=nq+r$，$0\leqslant r<n$，那么

$$n\alpha=nq+r+\{n\alpha\}$$

$$\alpha=q+\frac{r+\{n\alpha\}}{n}$$

当$r=0$时结论显然成立。当$r\geqslant 1$时

$$[a]+\left[a+\frac{1}{n}\right]+\cdots\cdots+\left[a+\frac{n-1}{n}\right]$$

$$=\left[q+\frac{r+\{na\}}{n}\right]+\left[q+\frac{r+\{na\}+1}{n}\right]+\cdots\cdots$$

$$+\left[q+\frac{r+\{na\}+n-1}{n}\right]$$

$$=nq+\sum_{k=0}^{n-r-1}\left(\frac{r+\{na\}+k}{n}\right)+\sum_{k=n-r}^{n-1}\left[\frac{r+\{na\}+k}{n}\right]$$

$$=nq+0+((n-1)-(n-r)+1)$$

$$=nq+r=[na]\ .$$

习题 3　证明不等式

$$[2\alpha]+[2\beta]\geqslant[\alpha]+[\alpha+\beta]+[\beta]\ .$$

证：设$\alpha=m+a$，$\beta=n+b$，m、n为正整数，$0\leqslant a<1$，$0\leqslant b<1$．毫无损失，可设$a\geqslant b$，那么

$$[2\alpha]+[2\beta]=[2m+2a]+[2n+2b]$$

$$=2m+2n+[2a]+[2b]$$

$$\geqslant(m+n)+(m+n)+[a+b]$$

$$=[m+a]+[n+b]+[m+n+a+b]$$

$$=[\alpha]+[\beta]+[\alpha+\beta]\ .$$

§5　唯一分解定理

习题 1　证明以下各数非有理数(有理数者乃形如$\frac{a}{b}$之数)．

$$\log_{10}2,\ \sqrt{2}\ .$$

证：如果$\log_{10}2=\frac{a}{b}$，　　$(a,\ b)=1$，那么

$$2 = 10^{\frac{a}{b}},$$

$$2^b = 2^n \cdot 5^n.$$

由唯一分解定理可得$a = b = 0$，与题设矛盾.

如果$\sqrt{2} = \frac{a}{b}$，$(a, b) = 1$，那么

$$2 = \frac{a^2}{b^2}$$

$$2b^2 = a^2.$$

因此$2 \mid a^2$，$2 \mid a$. 设$a = 2a_1$就有

$$b^2 = 2a_1{}^2, \quad 2 \mid b^2, \quad 2 \mid b.$$

从而$(a, b) \geqslant 2$，与$(a, b) = 1$矛盾.

习题2 若已知

$$\log_{10}\frac{1025}{1024} = a, \qquad \log_{10}\frac{1024^2}{1023 \cdot 1025} = b,$$

$$\log_{10}\frac{81^2}{80 \cdot 82} = c, \qquad \log_{10}\frac{125^2}{1124 \cdot 126} = d,$$

$$\log_{10}\frac{99^2}{98 \cdot 100} = e,$$

则 $$196\log_{10}2 = 59 + 5a + 8b - 3c - 8d + 4e.$$

并试用a、b、c、d、e表出$\log_{10}3$及$\log_{10}41$；再用此法求$\log_{10}2$至小数第十位，以说明此法在实际计算上有用处(已知$\log_e 10 = 2.3025850930$).

证： $$a = \log_{10}\frac{1025}{1024} = \log_{10}\frac{5^2 \cdot 41}{2^{10}}$$

$$5a = 10\log_{10}5 + 5\log_{10}41 - 50\log_{10}2;$$

$$b = \log_{10}\frac{1024^2}{1023 \cdot 1025} = \log_{10}\frac{2^{20}}{3 \cdot 5^2 \cdot 11 \cdot 31 \cdot 41}$$

$$8b = 160\log_{10}2 - 8\log_{10}3 - 16\log_{10}5 - 8\log_{10}11 - 8\log_{10}31 - 8\log_{10}41;$$

$$c = \log_{10}\frac{81^2}{80\cdot 82} = \log_{10}\frac{3^8}{2^5\cdot 5\cdot 41}$$

$$-3c = 15\log_{10}2 + 3\log_{10}5 + 3\log_{10}41 - 24\log_{10}3;$$

$$d = \log_{10}\frac{125^2}{124\cdot 126} = \log_{10}\frac{5^6}{2^3\cdot 3^2\cdot 7\cdot 31}$$

$$-8d = 24\log_{10}2 + 16\log_{10}3 + 8\log_{10}7 + 8\log_{10}31 - 48\log_{10}5;$$

$$e = \log_{10}\frac{99^2}{98\cdot 100} = \log_{10}\frac{3^4\cdot 11^2}{2^3\cdot 5^2\cdot 72}$$

$$4e = 16\log_{10}3 + 8\log_{10}11 - 12\log_{10}2 - 8\log_{10}5 - 8\log_{10}7.$$

因此

$$\begin{aligned} &59 + 5a + 8b - 3c - 8d + 4e \\ &= 59 + 137\log_{10}2 - 59\log_{10}5 \\ &= 59 + 137\log_{10}2 - 59 + 59\log_{10}2 \\ &= 196\log_{10}2. \end{aligned} \qquad (1)$$

由（1）有

$$\begin{aligned} 588\log_{10}2 &= 3\times 196\log_{10}2 \\ &= 177 + 15a + 24b - 9c - 24d + 12e \end{aligned} \qquad (2)$$

又因为 $a = 2 - 12\log_{10}2 + \log_{10}41$

即 $12\log_{10}2 = 2 + \log_{10}41 - a$，从而又有

$$588\log_{10}2 = 49\times 12\log_{10}2 = 98 + 49\log_{10}41 - 49a \qquad (3)$$

由(2)、(3)有$43\log_{10}41 = 588\log_{10}2 + 49a - 98 = 177 + 15a + 24b - 9c - 24d + 12e + 49a - 98$

$$\begin{aligned} &= 177 + 15a + 24b - 9c - 24d + 12e + 49a - 98 \\ &= 79 + 64a + 24b - 9c - 24d + 12e \end{aligned} \qquad (4)$$

由 $c = \log_{10}\frac{81^2}{80\cdot 82} = 8\log_{10}3 - 5\log_{10}2 - \log_{10}5 - \log_{10}41$

有 $8\log_{10}3 = c + 4\log_{10}2 + \log_{10}41 + 1$

$$392\log_{10}3 = 49\times 8\log_{10}3$$
$$= 49c + 196\log_{10}2 + 49\log_{10}41 + 49 \qquad (5)$$

把（1）、（4）代入（5）得

$$392\log_{10}3 = 49c + 59 + 5a + 8b - 3c - 8d + 4e$$
$$+ 79 + 64a + 24b - 9c - 24d + 12e + 49$$
$$= 187 + 69a + 32b + 37c - 32d + 16e \qquad (6)$$

（1）、（4）、（6）即为所需的等式。下面用（1）式计算$\log_{10}2$至小数第十位。由（1）有

$$\log_{10}2 = \frac{59 + 5a + 8b - 3c - 8d + 4e}{196}$$
$$\approx \frac{59 + 2121475\times 10^{-9} - 2872\times 10^{-9} - 198597\times 10^{-9}}{196}$$
$$+ \frac{-222368\times 10^{-9} + 17726\times 10^{-8}}{196}$$
$$= \frac{59.00187489}{196}$$
$$\approx 0.3010299739.$$

§6 最大公因数及最小公倍数

习题1 证明下列二等式：

$$(a_1,\cdots\cdots,a_n) = ((a_1,\cdots\cdots,a_s),\ (a_{s+1},\cdots\cdots,a_n)),$$
$$[b_1,\cdots\cdots,a_n] = [[b_1,\cdots\cdots,b_s],\ [b_{s+1},\cdots\cdots,b_n]].$$

证：对s行归纳法，先证明第一个等式。当$s=1$时，由定义有

$$(a_1,\cdots\cdots,a_n) = (a_1,\ (a_2,\cdots\cdots,a_n)).$$

归纳假定$s=k(k<n)$时等式成立，即

$$(a_1,\cdots\cdots,a_k) = ((a_1,\cdots\cdots,a_k),(a_{k+1},\cdots\cdots,a_n)).$$

当$s=k+1$时

$$\begin{aligned}&((a_1,\cdots,a_k,\ a_{k+1}),\ (a_{k+2},\cdots,a_n))\\&=(((a_1,\cdots,a_k),\ a_{k+1}),\ (a_{k+2},\cdots,a_n))\\&=((a_1,\cdots,a_k),\ a_{k+1},\ (a_{k+2},\cdots,a_n))\\&=((a_1,\cdots,a_k),\ (a_{k+1},\ (a_{k+2},\cdots,a_n)))\\&=((a_1,\cdots,a_k),\ (a_{k+1},\ a_{k+2},\cdots,a_n))\\&=(a_1,\cdots\cdots,a_n)\end{aligned}$$

故等式对于$s=k+1$时也成立。同理可证第二个等式。

习题 2　证明下列二式：

$$(a_1,\cdots,a_n)=\frac{a_1a_2\cdots a_n}{[a_2\cdots a\ ,a_1a_3\cdots a_n,\cdots,a_1a_3\cdots a_{n-1}]},$$

$$[a_1,\cdots,a_n]=\frac{a_1a_2\cdots a}{(a_2\cdots a\ ,a_1a_3\cdots a_n,\cdots,a_1a_3\cdots a_{n-1})}.$$

证：先证明一个辅助等式：

$$[a_1b,\cdots,a\ b]=[a_1,\cdots,a_n]b.\qquad(1)$$

用归纳法。$n=2$时，由提要中定理14和定理 9 可得

$$[a_1b,a_2b]=\frac{a_1a_2b^2}{(a_1b,a_2b)}=\frac{a_1a_2b}{(a_1,a_2)}=[a_1,a_2]b,$$

即$n=2$时成立。归纳假定$n=k$时（1）成立，则当$n=k+1$时

$$\begin{aligned}&[a_1b,\cdots,a_kb,\ a_{k+1}b]=[[a_1b,\cdots,a_kb],\ a_{k+1}b]\\&=[[a_1,\cdots,a_k]b,\ a_{k+1}b]=[[a_1,\cdots,a_k],\ a_{k+1}]b\\&=[a_1,\cdots,a_k,a_{k+1}]b.\end{aligned}$$

因此（1）式在$n=k+1$时也成立。再证本题中第一个等式。仍用归纳法。$n=2$时，我们得到

$$(a_1,a_2)=\frac{a_1a_2}{[a_1,\ a_2]}$$

上式显然成立。设$n=k$时成立，即

$$[a_2\cdots a_k,\ a_1a_3\cdots a_{k-1},\cdots,a_1\cdots a_{k-1}]=\frac{a_1\cdots a_k}{(a_1,\cdots,a_k)}\qquad(2)$$

当$n=k+1$时，由（1）、（2）及提要中定理9立刻得到

$$\frac{a_1\cdots a_{k+1}}{[a_2\cdots a_{k+1},a_1a_3\cdots a_{k+1},\cdots,a_1\cdots a_k]}$$

$$=\frac{a_1\cdots a_{k+1}}{[[a_2\cdots a_{k+1},\cdots,a_1\cdots a_{k-1}a_{k+1}],\ a_1\cdots a_k]}$$

$$=\frac{a_1\cdots a_{k+1}}{[[a_2\cdots a_k,\cdots,a_1\cdots a_{k-1}]a_{k+1},a_1\cdots a_k]}$$

$$=\frac{a_1\cdots a_{k+1}}{\left[\frac{a_1\cdots a_k}{(a_1,\cdots,a_k)}\cdot a_{k+1},a_1\cdots a_k\right]}$$

$$=\frac{a_1\cdots a_{k+1}}{\left[\frac{a_1\cdots a_k}{(a_1,\cdots,a_k)}\cdot a_{k+1},a_1\cdots a_k\right]}\cdot\frac{a_1\cdots a_k}{(a_1,\cdots,a_k)}\cdot\frac{(a_1,\cdots,a_k)}{a_1\cdots a_k}$$

$$=\left(\frac{a_1\cdots a_k}{(a_1,\cdots,a_k)}\cdot a_{k+1},\ a_1\cdots a_k\right)\cdot\frac{(a_1,\cdots,a_k)}{a_1\cdots a_k}$$

$$=(a_{k+1},\ (a_1,\cdots,a_k))=(a_{k+1},a_1,\cdots,a_k)=(a_1,\cdots,a_{k+1})$$

故结论对于$n=k+1$时也成立。类似地可以证明本题中第二个等式。

习题3 命$a_1,\cdots,a_n$为n个整数，则$(a_1,\cdots,a_n)$为形如$a_1x_1+\cdots+a_nx_n$诸整数所成之模中之最小正整数。

证： 设$(a_1,\cdots,a_n)=d$，对于所给模中的任意正整数$d_1=a_1x_1+\cdots a_nx_n$，因为$d|a_1,\cdots,d|a_n$，所以$d|d_1$，$d\leqslant d_1$。下面我们只需要证明d形如$a_1x_1+\cdots+a_nx_n$就可以了。用归纳法证明如下：

当$n=2$时，$(a_1,a_2)=d$，由辗转相除法可得二整数x_1、x_2，使得$d=a_1x_1+a_2x_2$。设$n=k$时结论成立，则当$n=k+1$时