曾荣 王玉

# 基础数论典型题解300例

300

湖南科学技术出版社

高等学校理工科参考书

# 基础数论典型题解300例

曾荣　　王玉

湖南科学技术出版社

**基础数论典型题解300例**

曾 荣　　王 玉

责任编辑：胡海清

*

湖南科学技术出版社出版

（长沙市展览馆路14号）

湖南省新华书店发行　湖南省新华印刷二厂印刷

*

1982年4月第1版第1次印刷

开本：787×1092毫米 1/32　印张：11.125　字数：254,000

印数：1—25,700

统一书号：13204·49　　定价：1.20元

# 编 者 的 话

在和初次学习数论这门课程的青少年及大学低年级学生的接触中，编者不止一次地听到说："初等数论的书倒不太难读，但习题实在不好做."的确，数论的习题是很难做的。有人就曾这样说过："用以发现数学天才，在初等数学中再也没有比数论更好的课程了。任何学生，如能把当今一本数论教材中的练习做出，就应当受到鼓励，劝他将来去从事数学方面的工作."任何数论书的作者都要求把书中的习题作为教材的一部分看待。我国著名数学家华罗庚在介绍И. M. 维诺格拉陀夫的《数论基础》时就曾说："如果读这本书而不看不做书后的习题，就好像入宝山而空返，把这书的最重要的部分忽略了！"因此，要学好数论必需练习大量的习题。

近年来，由于对基础科学研究的重视，不少大学及师范院校又重新开设了数论课程。我国数学家在数论研究上的卓越贡献，大大激起了广大青少年对数论学习的浓厚兴趣。随着科学技术的不断发展，数论这门"古老"而又"年轻"的学科在技术领域中得到了很多卓有成效的应用，这也引起了许多从事技术工作的同志对数论的重视。总之，要求学习、掌握数论这一数学学科的人越来越多了。因此，编写一本解答基础数论习题的书，对于增强人们学习数论的信心，加深其对数论内容和方法的掌握，提高其解题能力，帮助教师节省备课时间，都是有益的。编者不揣浅陋，为此编写了这本题解。

本书共分四章，包括了基础数论的主要内容，全书共选了

166个例题和141个习题。这些问题有典型性，解题方法灵活、多样，有一定的广度和深度。每章分四部分：(一)提要部分列出了本章问题中所需要的定义、定理；(二)例题部分，写得比较详细，有时采用了一题多解的方法；(三)习题部分，有意安排一些与例题类似的题目，供读者自己练习；(四)习题解答部分，比较简要，有的只给出了主要步骤，但重要一点的或比较难的给出了详细解答。例题和习题都以理论题为主，计算题为辅。

本书尽量照顾到各方面的需要。一方面考虑到大专院校基础数论教学的需要，另一方面也考虑到学过一些初等数论知识的广大优秀中学生的需要。我们在某些章节中选用了一些国内外数学竞赛中有关数论部分的较好题目，供这些同学参考。

本书原稿由湖南师范学院王俊杰副教授审阅，提出了不少好的意见，在此谨表感谢。

本书难免有谬误之处，望读者批评指正。

编　者

1981.8.

# 目　录

# 第一章 整 除

## 提 要

### 1.1 整除和高斯(Gauss)符号

**定义** 正整数、零、负整数称为整数。

**定理1** 具有某种性质并且大于某给定整数的所有整数的集合具有最小整数。具有某种性质并且小于某给定整数的所有整数的集合具有最大整数。

**系** 具有某种性质的所有正整数的集合具有最小整数。

**定理2** 设$a$是非零的任意整数，$b$是任意整数，则可唯一确定整数$q$和$r$，使

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

$q$和$r$分别称为$a$除$b$的商及余数。

**定义** $b$被$a(\neq 0)$除时，如果余数是0，也就是存在整数$q$使$b = aq$，则称$a$整除$b$，或$b$可被$a$整除，记作$a|b$。$b$是$a$的**倍数**，$a$是$b$的**因数**。

**定理3** I. $a|a$;

II. 如果$a|b$，$b|a$，则$a = b$或$a = -b$;

III. 如果$a|b$，$b|c$，则$a|c$。

**定义** 设$x$是任意实数，用$[x]$表示不超过$x$的所有整数集合的最大整数，称$[x]$为**高斯符号**。当$x$是整数时，$[x] = x$；$x$不是

整数时，$[x]$表示小于$x$的最大整数。

**定理4** I. $[x]\leqslant x<[x]+1$；

II. 如果$x\geqslant y$，则$[x]\geqslant[y]$；

III. 如果$x$是实数，$a$是整数，则$[x+a]=[x]+a$。

**定理5** 正整数$a$除整数$b$的商等于$\left[\frac{b}{a}\right]$，且成立下式

$$\left[\frac{b}{a}\right]\leqslant\frac{b}{a}\leqslant\left[\frac{b}{a}\right]+1-\frac{1}{a}.$$

**定理6** 设$x$是正实数，$n$是正整数，则1到$x$的正整数中是$n$的倍数的个数等于$\left[\frac{x}{n}\right]$。

**定理7** 设$n$是大于1的整数，$a$是任意正整数，则可唯一的表作

$$a=c_0+c_1n+c_2n^2+\cdots+c_\lambda n^\lambda,\ (0\leqslant c_i<n,i=0,1,\cdots,\lambda)$$

其中$\lambda$由$n^\lambda\leqslant a<n^{\lambda+1}$确定。称此为$a$的**n进位**表示。

## 1.2 素数与复合数

**定义** 大于1且除了1和它自身外无其它因数的整数称为**素数**。1以外的非素数的正整数称为**复合数**。

**定理8** 整数$c$的因数的因数是$c$的因数。$c(\neq 0)$的因数的绝对值小于$|c|$或者等于$|c|$。

**定理9** 整数$a$是复合数的充要条件是$a$是两个大于1的正整数的乘积。

**定理10** 除0，1，-1外每一个整数至少有一个素因数。

**定理11** 复合数$a$一定具有不大于$\sqrt{a}$的素因数。

**定理12** 素数有无限多个。

## 1.3 素因数分解

**定义** 将整数表作一些素数的乘积称作**素因数分解**。

**定义** 设$p$是素数，若非零整数$a$可被$p^r$整除而不能被$p^{r+1}$整除，则称$a$恰被$p^r$整除。这时称$p^r$是$a$的**p成分**。用$p(a)$表$a$的$p$成分的幂指数。

〔注〕 0的$p$成分的幂指数以$\infty$表之。

**定理13** 如果不计素因数乘积的次序，整数的素因数分解是唯一的。

**定理14** 设$p$是素数，如果$p|ab$，则$p|a$或$p|b$。

**定理15** 设$a,b$是非零整数，则$a|b$的充要条件是对于一切素数$p$有$p(a)\leqslant p(b)$。

**系** 对于一切素数$p$，如果$p(a)=p(b)$，则$a=b$或者$a=-b$。

**定理16** $p(a_1a_2\cdots a_n)=p(a_1)+p(a_2)+\cdots+p(a_n)$。

**定理17** 设$p$是素数，如果$p^\lambda\leqslant n<p^{\lambda+1}$，则

$$p(n!)=\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\cdots+\left[\frac{n}{p^\lambda}\right].$$

### 1.4 最小公倍数和最大公因数

**定义** 整数$a_1,a_2,\cdots,a_n$的公共倍数称为$a_1,a_2,\cdots,a_n$的**公倍数**。最小的正公倍数称为**最小公倍数**。用符号$\{a_1,a_2,\cdots,a_n\}$表示。

**定义** 整数$a_1,a_2,\cdots,a_n$的公共因数称为$a_1a_{,2},\cdots,a_n$的**公因数**。最大的正公因数称为**最大公因数**。用符号$(a_1,a_2\cdots,a_n)$表示。

**定义** 当$(a,b)=1$时，称$a$和$b$**互素**。

**定理18** 设$p_1,p_2\cdots,p_r$是整数$a_1,a_2,\cdots,a_n$的全部素因数，$l_i=\max(p_i(a_1),p_i(a_2),\cdots,p_i(a_n)),i=1,2,\cdots,r$，则

$$\{a_1,a_2,\cdots,a_n\}=p_1^{l_1}p_2^{l_2}\cdots p_r^{l_r}.$$

**定理19** 设$p_1,p_2,\cdots,p_r$是整数$a_1,a_2,\cdots,a_n$的全部公共素因数，$f_i=\min(p_i(a_1),p_i(a_2),\cdots,p_i(a_n)),i=1,2,\cdots,r$，则

$$(a_1, a_2 \cdots, a_n) = p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r}.$$

**定理20** 公倍数是最小公倍数的倍数，公因数是最大公因数的因数。

**定理21** $$\left\{ \{a_1, a_2, \cdots, a_r\},\ \{a_{r+1}, \cdots, a_n\} \right\}$$

$$= \{a_1, \cdots, a_r, a_{r+1}, \cdots, a_n\},$$

$$\left( (a_1, a_2, \cdots, a_r), (a_{r+1}, \cdots, a_n) \right) = \left( a_1, \cdots, a_r, a_{r+1}, \cdots, a_n \right).$$

**定理22** 设$c \neq 0$，则

$$\{ca_1, ca_2, \cdots, ca_n\} = |c| \{a_1, a_2, \cdots, a_n\},$$

$$(ca_1, ca_2, \cdots, ca_n) = |c| (a_1, a_2, \cdots, a_n).$$

**定理23** $a$和$b$互素的充要条件是$a$和$b$没有公共的素因数。

**定理24** 设$a_1, a_2, \cdots, a_n$两两互素，则

$$\{a_1, a_2, \cdots a_n,\} = |a_1 a_2 \cdots a_n|.$$

**定理25** 设$a_1, a_2, \cdots, a_n$均与$b$互素，则乘积$a_1 a_2 \cdots a_n$也与$b$互素。

**定理26** 设$(a, c) = 1$，如果$a | bc$，则$a | b$。

**定理27** $(a, b) \cdot \{a, b\} = |ab|$.

**定理28** $(a_1, a_2 - a_1 q, a_3, \cdots, a_n) = (a_1, a_2, a_3, \cdots, a_n)$.

**系** 设$r$是$b$除$a$的余数，则$(a, b) = (b, r)$。

**定义** 用定理28求最大公因数的方法称为**欧几里得（Euclid）辗转相除法**。

**定义** 一整数如为另一整数的平方则称为**平方数**。

## 例 题

**1.** 证明 $[x] + [y] \leqslant [x + y] \leqslant [x] + [y] + 1$

【证】 由于 $[x]\leqslant x<[x]+1$，$[y]\leqslant y<[y]+1$。两边相加，有

$$[x]+[y]\leqslant x+y<[x]+[y]+2.$$

由于$[x+y]$是不超过$x+y$的最大整数，故

$$[x]+[y]\leqslant[x+y].$$

又因为$[x+y]\leqslant x+y$，故$[x+y]<[x]+[y]+2$，从而有

$$[x+y]\leqslant[x]+[y]+1.$$

因此，由上两不等式，便知

$$[x]+[y]\leqslant[x+y]\leqslant[x]+[y]+1.$$

**2.** 设$x$是实数，$n$是正整数，证明

$$[x]+\left[x+\frac{1}{n}\right]+\left[x+\frac{2}{n}\right]+\cdots+\left[x+\frac{n-1}{n}\right]=[nx].$$

【证】 由于$[nx]$是整数，用正整数$n$除$[nx]$，其商设为$q$，余数为$r(0\leqslant r<n)$，于是

$$[nx]=nq+r,\quad(0\leqslant r<n)$$

因此 $\quad q+\frac{r}{n}\leqslant x<q+\frac{r+1}{n}.$

由此有 $\quad q+\frac{r+i}{n}\leqslant x+\frac{i}{n}<q+\frac{r+i+1}{n},$

故当 $\quad 0\leqslant i\leqslant n-r-1$时，有

$$\left[x+\frac{i}{n}\right]=q,$$

当 $\quad n-r\leqslant i\leqslant n-1$时，有

$$\left[x+\frac{i}{n}\right]=q+1,$$

故 $$\sum_{i=0}^{n-1}\left[x+\frac{i}{n}\right]=(n-r)q+r(q+1)=nq+r=[nx].$$

3．(*a*) 证明$[5x]+[5y]\geqslant[3x+y]+[3y+x]$,其中$x\geqslant0$，$y\geqslant0$。

(*b*) 利用(*a*)证明对于一切正整数$m,n$

$$\frac{(5m)!(5n)!}{m!n!(3m+n)!(3n+m)!}$$

是整数。

**【证】** (*a*) 设 $x=[x]+x_0$，$y=[y]+y_0$，其中 $0\leqslant x_0$，$y_0<1$，$[x]$和$[y]$是非负整数．由定理6，所求证之不等式就成为

$$[x]+[y]+[5x_0]+[5y_0]\geqslant[3x_0+y_0]+[3y_0+x_0].$$

因此，如果能证明

$$[5x_0]+[5y_0]\geqslant[3x_0+y_0]+[3y_0+x_0],\quad 0\leqslant x_0,\ y_0<1.$$

命题(*a*)证完．由于$x_0=0$ 或 $y_0=0$时不等式显然成立，因此只需证明

$$[5x]+[5y]\geqslant[3x+y]+[3y+x],\quad 0<x,\ y<1.$$

不妨设$x\geqslant y$。上不等式可写作

$$[5x]-[3x+y]\geqslant[3y+x]-[5y],\quad 0<x,y<1.$$

当$3y+x\leqslant5y$，即$x\leqslant2y$时，上不等式显然成立(左边不小于0，右边不大于0)．因此，只需在$x>2y$，$0<x,y<1$，$x\geqslant y$下来证明

$$[5x]+[5y]\geqslant[3x+y]+[3y+x].$$

设 $5x=a+b$，$5y=c+d$，其中$0\leqslant b,d<1$,$a$和$c$是非负整数，不等式就成为

$$a+c\geqslant\left[\frac{3a+c}{5}+\frac{3b+d}{5}\right]+\left[\frac{3c+d}{5}+\frac{3d+b}{5}\right].\quad(1)$$

由$1>x>2y$，有$5>a+b>2c+2d$，故

$$4\geqslant a\geqslant2c.\qquad(2)$$

满足(2) 式的$a,c$的一切值为

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| $a$ | 4 | 4 | 4 | 3 | 3 | 2 | 2 | 1 | 0 |
| $c$ | 2 | 1 | 0 | 1 | 0 | 1 | 0 | 0 | 0 |

容易验证，除$a=2$，$c=0$和$a=1$，$c=0$两种情况外，其余情况均满足

$$a+c\geqslant\left[\frac{3a+c+4}{5}\right]+\left[\frac{3c+a+4}{5}\right]. \qquad (3)$$

又由$3b+d<4$，$3d+b<4$，故若(3)式成立，即有(1)式成立。当$a=2$，$c=0$时，由于$\frac{3b+d}{5}<1$，故$\left[\frac{6}{5}+\frac{3b+d}{5}\right]=1,\left[\frac{2}{5}+\frac{3d+b}{5}\right]=1$,所以这时 (1) 式成立．同样可以验证当$a=1$，$c=0$时，(1) 式也成立。

(b) 要证明 $\dfrac{(5m)!(5n)!}{m!n!(3m+n)!(3n+m)!}$

是整数，根据定理15，只需对于任意素数$p$，有

$$p[(5m)!(5n)!]\geqslant p[m!n!(3m+n)!(3n+m)!],$$

即证明 $p[(5m)!]+p[(5n)!]\geqslant p(m!)+p(n!)+p[(3m+n)!]+p[(3n+m)!]$.

由定理17，有

$$p(m!)=\left[\frac{m}{p}\right]+\left[\frac{m}{p^2}\right]+\left[\frac{m}{p^3}\right]+\cdots\cdots,$$

因此只需证明

$$\left[\frac{5m}{p^i}\right]+\left[\frac{5n}{p^i}\right]\geqslant\left[\frac{m}{p^i}\right]+\left[\frac{n}{p^i}\right]+\left[\frac{3m+n}{p^i}\right]$$

$$+\left[\frac{3n+m}{p^i}\right]. \qquad (i=1,2,3,\cdots)$$

事实上，对于任意整数$r\geqslant 2$，可以证明

$$\left[\frac{5m}{r}\right]+\left[\frac{5n}{r}\right]\geqslant\left[\frac{m}{r}\right]+\left[\frac{n}{r}\right]+\left[\frac{3m+n}{r}\right]$$

$$+\left[\frac{3n+m}{r}\right]. \tag{4}$$

为此，设

$m=rq_1+x$，$n=rq_2+y$，$q_1,q_2$是整数，$0\leqslant x,y<1$，

(4) 式就成为

$$\left[\frac{5x}{r}\right]+\left[\frac{5y}{r}\right]\geqslant\left[\frac{3x+y}{r}\right]+\left[\frac{3y+x}{r}\right].$$

此即$(a)$。

4．设$n$是正整数，证明

$$\left[\frac{[x]}{n}\right]=\left[\frac{x}{n}\right].$$

【证】 由于$[x]\leqslant x<[x]+1$，故

$$\left[\frac{[x]}{n}\right]\leqslant\frac{[x]}{n}\leqslant\frac{x}{n}<\frac{[x]}{n}+\frac{1}{n}.$$

由定理5有

$$\frac{[x]}{n}\leqslant\left[\frac{[x]}{n}\right]+1-\frac{1}{n},$$

故 $$\left[\frac{[x]}{n}\right]\leqslant\frac{x}{n}<\left[\frac{[x]}{n}\right]+1,$$

所以有 $$\left[\frac{[x]}{n}\right]=\left[\frac{x}{n}\right].$$

5．证明：对于同样的整数$x$和$y$，表达式

$$2x+3y,\quad 9x+5y$$

同时能被17整除。

**【证】** 设 $u=2x+3y,\ \nu=9x+5y.$ (1)

只要证明，对于能使$17|u$的整数$x,y$,也能使$17|\nu$，反之亦然。

由（1）式有

$$3v-5u=17x,$$

即
$$3v=5u+17x, \quad (2)$$
$$5u=3\nu-17x. \quad (3)$$

由（2）式知，如果整数$x,y$能使$17|u$，那么也能使$17|3v$.由于17是素数，$17\nmid 3$,故根据定理14，有$17|v$。同样，由(3)式知，如果整数$x,y$能使$17|\nu$，那么也能使$17|5u$,由于$17\nmid 5$,故$17|u$。

**【注】** 本题的一般情况，在问题3中研究。

6．当$n$是奇数时，证明16可整除

$$n^4+4n^2+11.$$

**【证】** 对于$n$，用数学归纳法证明。

当$n=1$时，$n^4+4n^2+11=16$,显然是16的倍数．设$n=2m+1$时，$n^4+4n^2+11$是16的倍数，则当$n=2m+3$时，有

$$\begin{aligned}n^4+4n^2+11&=[(2m+1)+2]^4+4[(2m+1)+2]^2+11\\&=\{(2m+1)^4+4(2m+1)^2+11]\\&\quad+16(2m+1)^2(m+2)+48(2m+1)+16.\end{aligned}$$

上式右边第二、三、四各项均是16的倍数，由假设第一项也是16的倍数．故当$n$是一切奇数时，有

$$16|n^4+4n^2+11.$$

**【另证】** 由于

$$\begin{aligned}n^4+4n^2+11&=n^4+4n^2-5+16\\&=(n^2+5)(n^2-1)+16.\end{aligned}$$

故当$n=2m+1$时，有

$$n^4+4n^2+11=[(2m+1)^2+5][(2m+1)^2-1]+16$$
$$=8m(m+1)(2m^2+2m+3)+16.$$

由于$2|m(m+1)$，故当$n$是一切奇数时，有

$$16|n^4+4n^2+11.$$

**7.** 证明：对于一切整数，$n^2+2n+12$均不是121的倍数。

**【证】** 用反证法，设$n^2+2n+12$是121的倍数，即存在整数$k$，使

$$n^2+2n+12=121k.$$

于是，有

$$(n+1)^2=11(11k-1).$$

上式右边可被11整除，故$11|(n+1)^2$. 由于11是素数，根据定理16，有$11|(n+1)$。于是$11^2|11(11k-1)$，即$11|11k-1$，从而有$11|-1$. 这显然是不可能的。

**8.** 证明：任给五个整数，必能从其中选出三个，使得它们之和能被3整除。

**【证】** 任意整数必可写作下列形式

$$3k,\ 3k+1,\ 3k+2$$

之一，其中$k$为整数。因此，如果给定的五个整数中有三个分别属于上述三种形式，那么这三个整数之和必可被3整除；如果给定的五个整数只属于上述三种形式之一种或两种，那么必有三个整数属于同一种形式，这三个整数之和便可被3整除。

因此，从给定的五个整数中，必可选出三个，它们之和被3整除。

**9.** 任给$n$个整数，证明必能从其中选出$k$个，使得它们之和能被$n$整除。

**【证】** 设$a_1, a_2, \cdots, a_n$是给定的$n$个整数。作和

$$s_1=a_1,$$