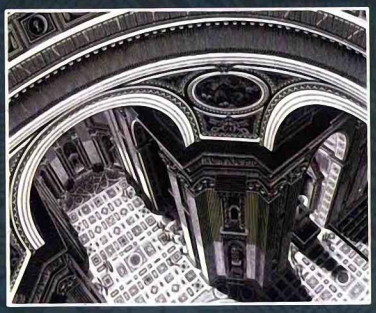
高等数学习题集
精品系列

基础数论例选
通过范例学技巧

朱尧辰 编著



朱尧辰，江苏镇江人，1942年生，1964年毕业于中国科学技术大学应用数学系，1992年任中国科学院应用数学研究所研究员，主要研究数论，曾任《数学进展》常务编委。1983年至1993年期间先后在法国Henri Poincaré研究所和IHES、德国Max-Planck数学研究所和Kōln大学、美国Southern Mississippi大学、中国香港浸会学院等科研机构或大学从事合作研究，迄今发表论文约100篇，出版专著5本，享受国务院政府特殊津贴。

哈爾濱工業大學出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS

SELECTED EXAMPLES OF BASIC NUMBER THEORY LEARNING SKILLS THROUGH EXAMPLES

基础数论例选
通过范例学技巧

● 朱尧辰　编著

哈爾濱工業大學出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS

内 容 简 介

本书选编了200个基础数论例题(题或题组)以及60个练习题,问题主要源自各种中外文数论书刊,以初等数论(整除性、同余、素数、数论函数、不定方程、连分数等)为主,并涉及与素数定理、整数列的密度、无理数、Diophantine逼近以及数的几何等有关的初步知识.问题有一定难度,解法也有启发性和参考价值.

本书可供数论爱好者阅读,也可作为大学数学系师生的教学辅助资料.

图书在版编目(CIP)数据

基础数论例选:通过范例学技巧/朱尧辰编著. —哈尔滨:哈尔滨工业大学出版社,2018.9

ISBN 978-7-5603-7602-8

Ⅰ.①基… Ⅱ.①朱… Ⅲ.①数论-自学参考资料 Ⅳ.①O156

中国版本图书馆CIP数据核字(2018)第183882号

策划编辑 刘培杰 张永芹
责任编辑 张永芹 李 欣
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 哈尔滨市工大节能印刷厂
开 本 787mm×1092mm 1/16 印张24.75 字数490千字
版 次 2018年9月第1版 2018年9月第1次印刷
书 号 ISBN 978-7-5603-7602-8
定 价 58.00元

前　言

编写本书的想法基本上与数年前出版的《数学分析例选——通过范例学技巧》及《高等代数例选——通过范例学技巧》类似,它通过解答一些经过特别挑选的例题来展示解基础数论习题的某些方法,以有助于具有一定解题基础的大学生“揣摩”和领会有关技巧,为有关师生提供一个教学辅导参考资料.虽然本书书名附以副标题“通过范例学技巧”,但是数论解题技巧算得上博大精深, 要全面给出绝非易事,本书所展示的,只不过是其若干侧面,实乃九牛之一毛而已.

本书问题的主题即所谓“基础数论”,看起来没有确切的范围界定,作者的理解是在初等数论的基础上按适当的深度扩张到数论的某些其他分支.本书含10章,以初等数论问题(整除性、同余、素数、数论函数、不定方程、连分数等)为主,但也包括少量初等数论范围以外的问题,它们涉及与素数定理的应用有关的一些简单解析方法、整数列的密度概念、无理数、Diophantine逼近,以及数的几何中的某些基本结果,等等.最后一章是供读者选做的练习题,没有提供解答(个别问题附提示).本书问题多数选自各种中外文书刊,有一定难度.由于当前各种类型的初等数论教材和习题集确实已经不少, 为减少重复,我们尽量略去某些标准例题(如与辗转相除和孙子定理有关的标准计算,一次不定方程和Pell方程的求解细节,等等);虽然本书证明题居多,但着重于“通用”解题方法,注意慎选具有奥数“血统”的问题,避免追求过于机巧的解法.本书所有问题的解答都是经过重新加工整理或改写的,多数包含必要的计算或推理的细节,有的附加若干注释或少许引申材料;有些问题或解法是作者自行设计的(但未必是新的).为便于读者参考,第1~9章标题之下都列出若干推荐问题的题号.

限于作者的水平和经验,本书在取材、编排和解题等方面难免存在不妥、疏漏甚至谬误,欢迎读者和同行批评指正.

朱尧辰

2018年1月于北京

符号说明

1° $\mathbb{N},\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$ (依次表示) 正整数集,整数集,有理数集,实数集,复数集.

$\mathbb{N}_0=\mathbb{N}\cup\{0\}$.

$\mathbb{R}_+$ 正实数集.

$\mathbb{Z}_m$ 模m剩余类环,$m=p$(素数)时$\mathbb{Z}_p$是域.

$|S|$ 有限集S所含元素的个数(也称S的规模).

2° $[a]$ 实数a的整数部分,即不超过a的最大整数.

$\{a\}=a-[a]$ 实数a的分数部分,也称小数部分.

$\lceil a\rceil$ 大于或等于a的最小整数.

$\lfloor a\rfloor$ 小于或等于a的最大整数(亦即a的整数部分$[a]$).

$((x))$ 距实数x最近的整数.

$\|x\|$ (实轴上)点x与距它最近的整数点间的距离.

$a\mid b$ ($a\nmid b$) 整数a整除(不整除)整数b.

$\gcd(a,b,\cdots,t)$ 整数$a,b,\cdots,t$的最大公因子, 不引起混淆时记为$(a,b,\cdots,t)$.

$\operatorname{lcm}(a,b,\cdots,t)$ 整数$a,b,\ldots,t$的最小公倍数, 不引起混淆时记为$[a,b,\cdots,t]$.

$\gcd\{\cdots\},\operatorname{lcm}\{\cdots\}$ 有限整数集合$\{\cdots\}$中的元素的最大公因子,最小公倍数.

$p^\alpha\|n$ 表示$p^\alpha\mid n$, 但$p^{\alpha+1}\nmid n$(其中$\alpha\geqslant 0$是整数,n是正整数,p是素数).

$\delta_{i,j}$ Kronecker符号,即当$i=j$时其值为1,否则为0.

3° $\log_b a$ 实数$a>0$的以b为底的对数.

$\log a$(与$\ln a$同义) 实数$a>0$的自然对数.

$\lg a$ 实数$a>0$的常用对数(即以10为底的对数).

$\exp(x)$ 指数函数e^x.

$a_n\,(n=1,2,\cdots)$, $a_n(n\geqslant 1)$ 数列,不引起混淆时记为a_n.

$\pi(x)$ 不超过$x(>0)$的素数个数.

4° $f(x)\sim g(x)\,(x\to a)$　函数$f(x)$和$g(x)$在$x\to a$时等价,即$\lim\limits_{x\to a}\dfrac{f(x)}{g(x)}=1$(此处$a$是实数或$\pm\infty$)(对于离散变量$n$类似,下同).

$f(x)=o\big(g(x)\big)\,(x\to a)$　指$\lim\limits_{x\to a}\dfrac{f(x)}{g(x)}=0$(此处$a$是实数或$\pm\infty$).

$f(x)=O\big(g(x)\big)\,(x\in A)$　指存在常数$C>0$使$|f(x)|\leqslant C|g(x)|$(对于所有$x\in A$,此处A为某个集合).

$f(x)=O\big(g(x)\big)\,(x\to a)$　指对于a的某个邻域中的所有x,$f(x)=O\big(g(x)\big)$(此处a是实数或$\pm\infty$).

$o(1)$和$O(1)$　分别表示无穷小量和有界量.

5° $\boldsymbol{M}_n$, $(a_{i,j})_n$　元素为$a_{i,j}$的n阶方阵,不引起混淆时记为$\boldsymbol{M}$或$(a_{i,j})$.

$\boldsymbol{A}^{\mathrm{T}}$, $\boldsymbol{x}^{\mathrm{T}}$　方阵$\boldsymbol{A}$和向量$\boldsymbol{x}$ 的转置.

$\det\boldsymbol{A}$, $\det(a_{i,j})$　方阵$\boldsymbol{A}$或$(a_{i,j})$的行列式.

6° $d(n)$　正整数n的(正)因子的个数(除数函数).

$\sigma_r(n)$　n的因子的r(实数)次方之和,即$\sum\limits_{d\,|\,n}d^r$;特别,$\sigma_1(n)=\sigma(n)$(n的因子之和);$\sigma_0(n)=d(n)=\sum\limits_{d\,|\,n}1$.

$\omega(n)$　n的不同素因子的个数,即$\omega(n)=\sum\limits_{p\,|\,n}1$ (p表示素数),并且约定$\omega(1)=0$.

$\Omega(n)$　n的素因子之总数,即计及素因子的重数:$\Omega(n)=\sum\limits_{p^\alpha\,\|\,n}\alpha$,并且约定$\Omega(1)=0$.

$\phi(n)$　Euler函数,即与n互素并且不超过n的正整数的个数,也就是模n 的不同既约剩余类的个数.

$\mu(n)$　Möbius函数,即

$$\mu(n)=\begin{cases}1 & \text{若}n=1,\\ (-1)^r & \text{若}n\text{为}r\text{个不同素数之积},\\ 0 & \text{若}n\text{有平方因子}.\end{cases}$$

$\lambda(n)$　Liouville函数,即$\lambda(n)=(-1)^{\Omega(n)}$.

$\Lambda(n)$　von Mangoldt函数,即

$$\Lambda(n)=\begin{cases}\log p & \text{若}n=p^{\alpha}\,(\alpha\in\mathbb{N}),\\ 0 & \text{其他情形.}\end{cases}$$

7° □　表示问题解答完毕.

目　　录

第1章 整除性

推荐问题: **1.5/1.6/1.7/1.12/1.14/1.16/1.20(1)-(3),(5).**

1.1 设a,b,c,d是整数,都与$m=ad-bc$互素,且x,y是整数.证明: $m\mid ax+by \Leftrightarrow m\mid cx+dy$.

解 下面是繁简不同的三种解法.解法1符合思维习惯(从定义出发),容易想到. 解法3基于一个简单的恒等式,并且自然地显示了题中的条件.

解法1 (i) 首先注意$(a,b)=1$.事实上,若$l=(a,b)$,则$l\mid a$和b,于是$l\mid m=ad-bc$,即l是a,b,m的一个公因子.因为a,b都与m互素,所以$l=1$.

(ii) 因为$m\mid ax+by$,所以存在整数k使得$ax+by=km=k(ad-bc)$,从而

$$a(x-kd)=-b(y+kc), \tag{1.1.1}$$

由此及a,b互素可知$a\mid y+kc$和$b\mid x-kd$,从而存在整数r和s,使得$y+kc=ar$和$x-kd=bs$,于是

$$x=kd+bs,\quad y=ar-kc, \tag{1.1.2}$$

从而

$$cx+dy=c(kd+bs)+d(ar-kc)=cbs+dar.$$

又将式(1.1.2)代入式(1.1.1)可知$s=-r$,因此由上式得到

$$cx+dy=-cbr+dar=r(ad-bc)=rm,$$

可见$m\mid cx+dy$.

也可以如下处理:由$a\mid y+kc$得到$y=ar-kc$,将此代入式(1.1.1)得到$x=kd-br$;由此也产生$cx+dy=rm$.

类似地,可由$m\mid cx+dy$推出$m\mid ax+by$.

解法 2 对于整数x,y,令$\alpha=ax+by,\beta=cx+dy$.若$m\mid ax+by$,则存在整数k使得$ax+by=km$.于是x,y满足方程组

$$ax+by=km,\quad cx+dy=\beta.$$

由此解出

$$x=\frac{kmd-b\beta}{ad-bc}=\frac{kmd-b\beta}{m}=kd-\frac{b\beta}{m}.$$

因为x,kd是整数,所以$b\beta/m$也是整数.又因为b,m互素,所以$m\mid\beta=cx+dy$.类似地,可证逆命题.

解法 3 我们有恒等式

$$c(ax+by)-a(cx+dy)=(cb-ad)y,$$

或

$$c(ax+by)-a(cx+dy)=-my.$$

若x,y是整数,$m\mid ax+by$,则$m\mid a(cx+dy)$.因为m,a互素,所以$m\mid(cx+dy)$.同理可证逆命题. □

1.2 (1) 证明:对于任何正整数$k,d=(9k^2+3k+1,6k+1)\neq 37$.

(2) 证明:对于任何正整数$k,d=(k^2+3k+2,6k^3+15k^2+3k-7)=1$.

(3) 设m,n,a是正整数,$m\neq n$.证明:

$$(a^{2^m}+1,a^{2^n}+1)=\begin{cases}1 & \text{若}a\text{是偶数},\\ 2 & \text{若}a\text{是奇数}.\end{cases}$$

(4) 设整数$n\geqslant 1$,求

$$\binom{2n}{k}\quad(k=1,3,\cdots,2n-1)\tag{1.2.1}$$

的最大公因子.

解 (1) 问题等价于证明同余方程组

$$9k^2+3k+1\equiv 0\pmod{37},\quad 6k+1\equiv 0\pmod{37}$$

无解.用反证法.若有解k,则由第二式得到$36k \equiv -6 \pmod{37}$,或$(37-1)k \equiv -6 \pmod{37}$,于是

$$k \equiv 6 \pmod{37}.$$

将此代入第一式,得到

$$9 \cdot 6^2 + 3 \cdot 6 + 1 \equiv 0 \pmod{37},$$

即$343 \equiv 0 \pmod{37}$,此不可能.于是本题得证.

或者,更简捷地:因为$4(9k^2+3k+1) = (6k+1)^2 + 3$,所以若结论不成立,则有$37 \mid 3$, 此不可能.

(2) 由d的定义可知,

$$d \mid 6k(k^2+3k+2) - (6k^3+15k^2+3k-7) = 3k^2+9k+7;$$

进而得到

$$d \mid (3k^2+9k+7) - 3(k^2+3k+2) = 1,$$

因此$d=1$.

(3) (i) 首先证明:若$m > n$,则$a^{2^n}+1 \mid a^{2^m}-1$.

这是因为,连续实施因式分解得到

$$\begin{aligned} a^{2^m}-1 &= (a^{2^{m-1}}+1)(a^{2^{m-1}}-1) \\ &= (a^{2^{m-1}}+1)(a^{2^{m-2}}+1)(a^{2^{m-2}}-1) \\ &= \cdots \\ &= (a^{2^{m-1}}+1)(a^{2^{m-2}}+1)\cdots(a^2+1)(a+1)(a-1). \end{aligned} \tag{1.2.2}$$

由此及$m > n$立得上述结论.

(ii) 因为

$$a^{2^m}-1 = (a^{2^m}+1) - 2,$$

且由式(1.2.2)右边每个因式都整除$a^{2^m}-1$,又因为$n < m$,所以$a^{2^n}+1$是这些因式中的一个,所以

$$a^{2^n}+1 \mid (a^{2^m}+1) - 2,$$

于是$d=(a^{2^n}+1,a^{2^m}+1)\mid 2$,从而$d=1$或2.显然,如果$a$是奇数,那么$a^{2^n}+1$和$a^{2^m}+1$都是偶数,于是$d=2$;如果$a$是偶数,那么$a^{2^n}+1$和$a^{2^m}+1$都是奇数, 于是$d=1$.

(4) (i) 设d是式(1.2.1)中各个数的最大公因子.那么d整除这些数之和

$$S=\sum_{k=1}^{2n-1}\binom{2n}{k}.$$

因为

$$\sum_{k=0}^{2n}\binom{2n}{k}=\sum_{k=0}^{2n}\binom{2n}{k}1^k\cdot 1^{2n-k}=(1+1)^{2n}=2^{2n},$$
$$\sum_{k=0}^{2n}(-1)^k\binom{2n}{k}=\sum_{k=0}^{2n}\binom{2n}{k}(-1)^k\cdot 1^{2n-k}=(1-1)^{2n}=0,$$

将此二式相减可得$2S=2^{2n}$,所以$S=2^{2n-1}$.于是$d\mid 2^{2n-1}$,可见$d=2^a$,其中a是非负整数,即或者$d=1$,或者d是偶数.

(ii) 设$n=2^m r$,其中r是奇数,m是非负整数.因为

$$\binom{2n}{1}=2n=2^{m+1}r,$$

所以

$$d\leqslant 2^{m+1}. \tag{1.2.3}$$

(iii) 对于$k=1,3,\cdots,2n-1$,有

$$\binom{2n}{k}=\binom{2^{m+1}r}{k}=\frac{2^{m+1}r}{k}\binom{2^{m+1}r-1}{k-1}=2^{m+1}\cdot\frac{r}{k}\binom{2^{m+1}r-1}{k-1}.$$

因为二项式系数是整数,并且k是奇数,所以$k\nmid 2^{m+1}$,从而由上式可知

$$M(k)=\frac{r}{k}\binom{2^{m+1}r-1}{k-1}\quad(k=1,3,\cdots,2n-1)$$

是一个整数.于是由

$$\binom{2n}{1}=2^{m+1}\cdot r,\quad \binom{2n}{k}=2^{m+1}\cdot M(k)\quad(k=3,\cdots,2n-1)$$

可推出$d \geqslant 2^{m+1}$.由此及不等式(1.2.3)立得$d = 2^{m+1}$,其中整数m由$2^m \parallel n$定义. □

1.3 求正整数n,使它可被所有不超过$\sqrt{n}$的整数整除.

解 我们首先证明下列命题:

命题 设k是一个正整数,如果正整数n可被$1, 2, 3, \cdots, [\sqrt[k]{n}]$整除,那么$n$只可能取有限多个不同的值.

证明 因为n可被$1, 2, 3, \cdots, [\sqrt[k]{n}]$整除,所以也可被这些数的最小公倍数$V$整除.用$p_\nu$表示第$\nu$个素数,并由下式定义下标$l$:

$$p_l \leqslant \sqrt[k]{n} < p_{l+1}, \tag{1.3.1}$$

于是可记

$$V = p_1^{\sigma_1} p_2^{\sigma_2} \cdots p_l^{\sigma_l}.$$

由最小公倍数的定义可知,p_s的指数σ_s是$1, 2, \cdots, [\sqrt[k]{n}]$ 的素因子分解式中p_s的指数的最大者,因此σ_s由不等式

$$p_s^{\sigma_s} \leqslant \sqrt[k]{n} < p_s^{\sigma_s+1} \quad (s = 1, \cdots, l) \tag{1.3.2}$$

确定.因为$p_s \leqslant p_l \leqslant \sqrt[k]{n}$,所以

$$\sigma_s \geqslant \left[\frac{[\sqrt[k]{n}]}{p_s}\right] \geqslant 1,$$

从而由式(1.3.2)得到

$$\sqrt[k]{n} < p_s^{2\sigma_s} \quad (s = 1, \cdots, l).$$

将这些不等式相乘,得到$n^{l/k} < V^2$;但由$V \mid n$可知$V \leqslant n$,所以$n^{l/k} < V^2 \leqslant n^2$,于是$l/k < 2$,或$l < 2k$,从而$l + 1 \leqslant 2k$.由此及式(1.3.1)推出

$$\sqrt[k]{n} < p_{l+1} < p_{2k},$$

于是$n < p_{2k}^k$.因为k是给定的,所以n有界.

现在取$k = 2$,则$p_{2k}^k = p_4^2 = 49$.直接计算得到$n = 24$. □

注 对于给定的$\alpha \in (0,1)$,存在整数$k>1$满足$\sqrt[k]{n} \leqslant n^{\alpha} < \sqrt[k-1]{n}$,从而$[n^{\alpha}] \geqslant [\sqrt[k]{n}]$,于是从上面的命题推出: 如果$0<\alpha<1$,那么只有有限多个正整数$n$可被$1,2,3,\cdots,[n^{\alpha}]$整除.

1.4 设a,b为整数,奇素数$p \mid a^2+b^2$.证明:

(1) 若a,b互素,则$p \equiv 1 \pmod 4$.

(2) 若$p \equiv 3 \pmod 4$,则$p \mid a, p \mid b$.

解 用反证法.

(1) 设$p=4m+3$.由$p \mid a^2+b^2$可知$a^2 \equiv -b^2 \pmod p$, 于是$(a^2)^{2m+1} \equiv (-b^2)^{2m+1} \pmod p$,即$a^{p-1} \equiv -b^{p-1} \pmod p$. 注意$a,b$互素,由此可知$p \nmid a$,并且$p \nmid b$.但由Fermat(小)定理有$a^{p-1} \equiv 1, -b^{p-1} \equiv -1 \pmod p$,从而$1 \equiv -1 \pmod p$,得到矛盾.于是奇素数$p \equiv 1 \pmod 4$.

(2) 设p,a互素,那么由$p \mid a^2+b^2$可知p,b也互素.于是由Fermat(小)定理推出$a^{p-1} \equiv 1, b^{p-1} \equiv 1 \pmod p$.又由$p \mid a^2+b^2$可知$a^2 \equiv -b^2 \pmod p$,于是由$p=4m+3$推出$(a^2)^{(p-1)/2} \equiv (-b^2)^{(p-1)/2} \pmod p$, 即

$$a^{p-1} \equiv -b^{p-1} \pmod p.$$

由此及Fermat(小)定理可知$1 \equiv -1 \pmod p$,再次得到矛盾.因此$p \mid a, p \mid b$. □

1.5 若p是奇素数,$(p,a)=1$,整数$k \geqslant 1$,则$p^k \parallel a-b \Rightarrow p^{k+1} \parallel a^p-b^p$.

解 由题设可知$a \neq b$,可记$b=a+cp^k$,其中$c \neq 0$是整数,$p \nmid c$. 于是

$$\begin{aligned} b^p &= (a+cp^k)^p = \sum_{i=0}^{p} \binom{p}{i} a^{p-i}(cp^k)^i \\ &= a^p + pa^{p-1}\cdot(cp^k) + \binom{p}{2} a^{p-2}(cp^k)^2 + \sum_{i=3}^{p} \binom{p}{i} a^{p-i}(cp^k)^i, \end{aligned}$$

从而

$$a^p - b^p + pa^{p-1}\cdot(cp^k) = -\binom{p}{2} a^{p-2}(cp^k)^2 - \sum_{i=3}^{p} \binom{p}{i} a^{p-i}(cp^k)^i. \quad (1.5.1)$$

因为$k \geqslant 1$,所以当$i \geqslant 3$时,$ki \geqslant k+2$;又因为p是奇素数,所以$p \mid \binom{p}{2}$,从而$p^{k+2} \mid \binom{p}{2} a^{p-2}(cp^k)^2$.于是

$$p^{k+2} \mid a^p - b^p + pa^{p-1} \cdot (cp^k).$$

特别,由此可知$p^{k+1} \mid a^p - b^p$.但因为$p \nmid a, p \nmid c$,所以$p^{k+2} \nmid pa^{p-1} \cdot (cp^k)$,可见$p^{k+2} \nmid a^p - b^p$.因此$p^{k+1} \parallel a^p - b^p$. □

注 由式(1.5.1)立知:设p是素数(不必是奇素数),k是正整数,则$a \equiv b \pmod{p^k} \Rightarrow a^p \equiv b^p \pmod{p^{k+1}}$.

1.6 (1) 设n是正整数,记$L_n = [1, 2, \cdots, n]$.证明:

$$L_n = \prod_{p \leqslant n} p^{[\log n / \log p]} \geqslant \prod_{p \leqslant n} p,$$

其中p表示素数.

(2) 设$n \geqslant 2$,正整数$a_1, \cdots, a_n$的最大公因子$(a_1, \cdots, a_n) = 1$.则存在$j \in \{2, \cdots, n\}$使得

$$(a_1, a_j) \leqslant a_1^{(n-2)/(n-1)}.$$

解 (1) 显然$L_n = [1, 2, \cdots, n]$的素因子不超过n.设它的标准素因子分解式是

$$L_n = \prod_{p \leqslant n} p^{\tau_p},$$

那么对于每个素因子p有

$$p^{\tau_p} \leqslant n < p^{\tau_p + 1},$$

于是

$$\tau_p \log p \leqslant \log n < (\tau_p + 1) \log p,$$

或者

$$\tau_p \leqslant \frac{\log n}{\log p} < \tau_p + 1,$$

因此

$$\tau_p = \left[\frac{\log n}{\log p}\right].$$

由此即得

$$L_n = \prod_{p \leqslant n} p^{[\log n/\log p]}.$$

注意$\tau_p \geqslant 1$,立得$L_n \geqslant \prod\limits_{p \leqslant n} p$.

(2) 记$d_i = (a_1, a_i)(i = 2, \cdots, n)$.由$(a_1, \cdots, a_n) = 1$可知

$$(d_2, d_3, \cdots, d_n) = 1$$

(不然将有素数p整除所有d_i,从而整除所有a_i).因为$d_2, d_3, \cdots, d_n$都整除a_1,所以它们的素因子都是a_1的素因子,从而a_1的每个素因子p不可能同时整除所有的$d_2, d_3, \cdots, d_n$,即至多可能同时整除$d_2, d_3, \cdots, d_n$中的$n-2$个数.设$p^\alpha \parallel a$,并且(不妨认为)p同时整除$d_3, \cdots, d_n$;若

$$p^{\alpha_3} \parallel d_3, \cdots, p^{\alpha_n} \parallel d_n,$$

则必$\alpha_3, \cdots, \alpha_n \leqslant \alpha$.于是在$d_2 \cdot d_3 \cdots d_n$的标准素因子分解式中$p$的幂为$p^{\alpha_3+\cdots+\alpha_n}$,其指数

$$\alpha_3 + \cdots + \alpha_n \leqslant (n-2)\alpha.$$

对于a_1的其他任何素因子都可进行类似推理得到与上式类似的不等式.因此

$$d_2 d_3 \cdots d_n \mid a_1^{n-2}.$$

设$d_j = \min\limits_{2 \leqslant i \leqslant n} d_i$,则

$$d_j^{n-1} \leqslant a_1^{n-2}.$$

于是$d_j = (a_1, a_j) \leqslant a_1^{(n-2)/(n-1)}$. □

1.7 设n是给定整数,正整数$a \leqslant n^2/4$,并且没有大于n的素因子,则$a \mid n!$.

解 下面给出两种解法,思路一致但略有差别.

解法 **1** 只需证明:若素数p适合$p^\alpha \parallel a$,则必有$p^\alpha \mid n!$(其中$\alpha \geqslant 1$是整数).

(i) 设$\alpha = 2s(s \geqslant 1)$,于是$p^{2s} \parallel a$.

我们有

$$p^{2s} \leqslant a \leqslant \frac{n^2}{4}, \quad \text{从而} \quad 2p^s \leqslant n,$$

于是$n!$的标准素因子分解式中p的幂指数等于

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots \geqslant \left[\frac{n}{p}\right] \geqslant \left[\frac{2p^s}{p}\right] = 2p^{s-1} \geqslant 2s$$

(关于最后一步,参见本题解后的注),从而$p^{2s} \mid n!$.

(ii) 设$\alpha = 2s+1(s \geqslant 0)$,于是$p^{2s+1} \parallel a$.

当$s = 0$时,即$p \parallel a$,因为a没有大于n的素因子,所以$p \leqslant n$,从而

$$\sum_{i \geqslant 1} \left[\frac{n}{p^i}\right] \geqslant \left[\frac{n}{p}\right] \geqslant 1,$$

于是$p \mid n!$.

当$s \geqslant 1$时,则有

$$p^{2s+1} \leqslant a \leqslant \frac{n^2}{4}, \quad \text{从而} \quad n \geqslant 2\sqrt{p}p^s. \tag{1.7.1}$$

区分两种情形:

(a) 若$n \leqslant 4p^s$,则有$2\sqrt{p}p^s \leqslant n \leqslant 4p^s$,可知$\sqrt{p} \leqslant 2$,所以$p = \sqrt{p} \cdot \sqrt{p} \leqslant 2\sqrt{p}$,从而由式(1.7.1) 得到$n \geqslant 2\sqrt{p}p^s \geqslant p \cdot p^s = p^{s+1}$,即知

$$\left[\frac{n}{p}\right] \geqslant p^s, \ \left[\frac{n}{p^2}\right] \geqslant p^{s-1}, \ \left[\frac{n}{p^3}\right] \geqslant p^{s-3}, \ \cdots,$$

于是$n!$的标准素因子分解式中p的幂指数等于

$$\begin{aligned} & \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots \\ \geqslant \ & p^s + p^{s-1} + \cdots + 1 \\ \geqslant \ & 2^s + 2^{s-1} + \cdots + 1 = 2^{s+1} - 1 = 4 \cdot 2^{s-1} - 1 \geqslant 4s - 1 \geqslant 2s + 1. \end{aligned}$$

因此$p^{2s+1} \mid n!$.