基础数论

U. 杜德利 著

上海科学技术出版社

ELEMENTARY NUMBER THEORY
U. Dudley
W. H. Freeman and Co., 1969

基 础 数 论

U. 杜德利 著
周仲良 译
俞文鈜 校
上海科学技术出版社出版
（上海瑞金二路450号）
新华书店上海发行所发行 江苏泗阳印刷厂印刷
开本787×1092 1/32 印张9.25 字数202,000
1980年9月第1版 1980年9月第1次印刷
印数 1—14,500

书号：13119·859 定价：(科四) 0.87元

前　言

如今，在开设数论课的时候，通常只有数学专业高年级学生才学它．我认为，对未来的数学教师来说，数论显然是很有价值的，因此完全应该向更多的人讲授这门课．本书是作为一学期的数论教材编写的，需要的预备知识很少，除了实数的性质和初等代数外，不要求读者懂得其它数学．（在§21和§22中，稍有数学分析的知识是有益的，但也不是非有不可．）然而，由于一般程度的学生认为数论并不容易，因此我把证明写得较为详细，并插进了许多数字例子．这些例子的目的在于说明定理，并力图表明对数进行研究是件多么有趣的事，许多定理就源出于此．

在本书中，我至少已对初等数论的大多数论题进行了介绍．§1～§5中，推导了整数和同余式的基本性质，§6给出了费马定理和威尔逊定理的证明，§7～§9介绍了数论函数d, σ和ϕ，在§10～§12中，推出了重要的二次互反性定理．接下去是多少有点互不相关的三部分材料：关于数的表示式（§13～§15），丢番图方程（§16～§20）和素数（§21～§22）．我认为，在数论中，习题和练习特别重要，也很有趣，因此，在§23中收进了105道杂题，它们大致上是按照难度而未考虑论题排列起来的．

对于由初学数论的学生组成的普通班级来说，本书作为一学期的材料已绰绰有余，上面提及的最后三部分材料均可略去．甚至§10～§12（它们包含了本书最困难的内容）也可

以删掉，因为在这几节里证明的、且后来又要用到的唯一结论是：-1 是奇素数 p 的二次剩余还是二次非剩余取决于 $p\equiv 1$ 还是 $p\equiv 3 \pmod 4$.

书中一些定理的证明，往往既不是最简短的证明，也不是人们已经知道的最优美的证明，不过，在我看来，它们是最自然的证明. 例如，§22 中关于 $\pi(x)$ 的界限的切比雪夫定理的处理相当长，但这样做有其优点，即可以介绍在数论其它地方也要用到的函数和技巧，而且，当学生以后看到定理的更优美的证明后，印象就会更深刻.

学习数学的唯一路径是动手去做. 出于这一想法，我收进了一千多道练习和习题. 练习插在课文(和一些证明)中，习题则附在各节末尾. 四篇附录中有三篇也附有练习和习题. 可以有好几种方式来运用这些练习：学生可以在第一次阅读教材时就做，以后再回到这些练习以检查自己对已学内容的理解程度，教师也可用它们来作讲解.

有些练习和习题是计算题，有些是传统的习题，有些则多少有点新颖. 还有几道题可算得上是令人惊奇的. 由于在数论中，攻下一道题往往有多种方法，而最有成效的方法却可能不那么明显，因此，我给许多习题作了些提示，它们附在书末一节中(有些提示几乎就是完整的解答). 不用提示而得之解答当然要比依靠提示而得之解答更值得赞许，但解决某些习题需要许多巧妙的想法，这却不是轻易可得的. 数论习题可以非常难，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，就应受到鼓励，劝他将来去从事数学方面的工作."在本书末，我还为部分习题和练习逐节提供了答案. 尽管题目很多，一个学生在一学期里难以做完，但

希望他能把这些题目及其提示当作教材的一部分来看待，在阅读时对它们应同样重视. 可以发现，这些题目往往比作为其基础的那些内容更为有趣.

本书还有四篇附录. 前两篇(附录一，归纳法证明；附录二，记号)供学生需要时阅读. 收进附录三(模为合数的二次同余式)，是为了使对二次同余式的解的研究更臻完整，它也可放在§11后使用. 附录四包括了三张表，这些表不但本身使人感到兴趣，而且对解答数字习题也有用处. 表A可以简化10^5以内的正整数的因子分解，表B给出了开头447个平方数，表C是因子分解表的一部分.

课文和习题中无疑都会有些错误，欢迎大家指正.

U. 杜德利

1969年2月

目　录

§1 整　数

整数是这样一些数：…，−2，−1，0，1，2，…．数论的很大一部分内容就是研究整数的性质．整数通常只用来提供数据(如3个苹果，32元，$17x^2+9$等)，人们并不考虑它们的性质．3有多少个因子？32是否为素数？17能不能写为两个整数的平方和？我们在给苹果、钞票或x^2计数时，这些问题都是无关紧要的．但是，整数是数学中非常基本的内容，人们认为它们本身就值得加以研究．

从本节开始，除非另有说明，小写字母总表示整数．整数的加法、减法、乘法和除法的通常性质以及整数的有序性，我们认为大家已经知道，并将随时应用．本节中，我们还要用到整数的一个重要性质，由于它不象某些性质(如乘法结合律)那样经常地明确表出，因此你也许还未认真地加以注意．此性质叫做**最小整数原理**：一个下有界的非空整数集合总包含有它的最小元．也可以说，一个上有界的非空整数集合总包含有它的最大元．

当且仅当存在一个整数d使$ad=b$时，我们称a整除b，记为$a|b$．例如，$2|6$，$12|60$，$17|17$，$-5|50$，$8|-24$．如a不能整除b，我们写作$a\nmid b$．例如，$4\nmid 2$，$3\nmid 4$．

【练习1】　哪些整数整除零？

【练习2】　证明：若$a|b$，$b|c$，则$a|c$．

为了说明整除具有怎样的性质，我们证明下列引理：

引理1　若$d|a$，$d|b$，则$d|(a+b)$．

证明 根据整除的定义，我们知道存在整数 q 和 r，使

$$dq=a,\ dr=b.$$

因此

$$a+b=d(q+r).$$

故再由定义，$d|(a+b)$.

引理 2 若 $d|a$，则对任何整数 c，$d|ca$.

引理 3 若 $d|a_1$，$d|a_2$，$\cdots$，$d|a_n$，则对任何整数 c_1，c_2，$\cdots$，c_n，有 $d|(c_1a_1+c_2a_2+\cdots+c_na_n)$.

这两个引理的证明是很容易的.

【练习 3】 证明引理 2 和引理 3.

作为引理 3 的应用，我们知道，若 d 整除一个方程一端的所有项，则它也整除此方程另一端. 因此，若 $a+b=c$，且 $d|a$，$d|c$，则 $d|b$. 又若

$$3x+81y+6z+363=w,$$

则 $3|w$，因为 3 整除该方程左端所有项（记住：所有小写字母，包括 x，y，z，w 在内，除非另有说明，均表示整数）. 类似地，若

$$3x^2+15xy+5y^2=0,$$

则 $3|5y^2$，$5|3x^2$.

本节的其余部分将用以研究最大公因子及其性质，这些性质我们以后要经常用到. 我们称 d 是 a 和 b 的最大公因子（记为 $d=(a,\ b)$），当且仅当：

(i) $d|a$，$d|b$；

(ii) 若 $c|a$，$c|b$，则 $c\leqslant d$.

条件(i)说明，d 是 a 和 b 的公因子；条件(ii)说明，它是这种因子中最大的一个. 注意，若 a 和 b 不同时为零，那么 a 和 b 的公因子集合是以 a，b，$-a$ 和 $-b$ 中最大者为其上界的整数集. 因此，根据整数的良序原理，该集合有最大元，故 a 和

b 的最大公因子存在，而且是唯一的. 注意，$(0, 0)$没有定义；而如(a, b)有意义，则它是正数. 事实上，必成立$(a, b) \geqslant 1$，因为对任何 a 和 b，$1 \mid a$，$1 \mid b$.

【练习 4】 $(4, 14)$，$(5, 15)$，$(6, 16)$各是什么？

【练习 5】 设 n 为任意正整数，$(n, 1)$是什么？$(n, 0)$是什么？

【练习 6】 若 d 为正整数，(d, nd)是什么？

作为使用最大公因子的定义的一个练习，我们将证明下列定理，它在以后要常用到.

定理 1 若$(a, b) = d$，则$(a/d, b/d) = 1$.

证明 设 $c = (a/d, b/d)$. 我们需证 $c = 1$. 为此，我们证明，$c \leqslant 1$ 且 $c \geqslant 1$. 由于 c 是两个整数的最大公因子，我们已注意到，每个最大公因子都大于或等于 1，故得后一不等式. 为了说明 $c \leqslant 1$，我们利用 $c \mid (a/d)$ 和 $c \mid (b/d)$，即知存在 q 和 r，使 $cq = a/d$，$cr = b/d$，或 $(cd)q = a$，$(cd)r = b$. 这两个式子表明，cd 是 a 和 b 的一个公因子，因此它不大于 a 和 b 的最大公因子 d，故有 $cd \leqslant d$. 又因 d 是正数，可得 $c \leqslant 1$. 因此，$c = 1$，乃所欲证.

若$(a, b) = 1$，我们就称 a 和 b *互素*. 其道理在学习因子分解唯一性这一节时即可明白.

当(a, b)较小时，常可用观察法看出(a, b). 当 a 和 b 很大时，就不大容易看出了. 如：$(31415926, 5358979)$是什么？现在我们介绍一种求最大公因子的有效方法：欧几里得(Euclid)算法. 这种算法在证明我们后面需要的一些定理时也是有用的.

定理 2(除法算式) 给定正整数 a 和 b，$b \neq 0$，存在唯一的整数 q 和 r(其中 $0 \leqslant r < b$)，使

$$a=bq+r.$$

证明 如将 $a=bq+r$ 写为

$$\frac{a}{b}=q+\frac{r}{b},$$

我们就可看到，此定理只是说明了我们用 b 除 a 具体是怎么做的罢了：求出一个商 q 和一个余数 r. 我们可将此写得更为正式一些. 考虑整数 $a-bt$ 构成的集合 S，其中 $t=0, \pm1, \pm2, \cdots$. 因为 S 中有非负元(如 a, $a+b$ 等)，由最小整数原理，我们知道 S 有一个最小的非负元，把它叫做 r，并设 q 是相应的 t 值，则 $a-bq=r$，且 $r\geqslant0$. 为了完成定理的证明，我们尚需证 $r<b$. 假若不然，则有 $r=b+r_1$，且 $r_1\geqslant0$. 因而，

$$r_1=r-b=a-bq-b=a-b(q+1).$$

这就说明，r_1 在集合 S 中. 但

$$0\leqslant r_1=r-b<r,$$

这是不可能的，因为 r 是集合 S 中的最小非负元.

上述作法给出了 q 和 r，剩下来要证明，它们是唯一确定的. 假定我们找到了 q, r 和 q_1, r_1，使

$$a=bq+r=bq_1+r_1,$$

其中 $0\leqslant r<b$, $0\leqslant r_1<b$. 两式相减，我们有

$$0=b(q-q_1)+(r-r_1). \tag{1}$$

由于 b 整除此式左端以及右端第一项，它也整除右端另一项：$b\mid(r-r_1)$. 但因 $0\leqslant r<b$, $0\leqslant r_1<b$，我们有

$$-b<r-r_1<b.$$

$-b$ 和 b 之间的 b 的倍数只有零，因而 $r-r_1=0$. 由(1)又得 $q-q_1=0$. 因此，定理中的数 q 和 r 是唯一确定的.

虽然此定理只是对正整数 a 和 b 而言的(因为它最经常

地用于正整数)，但在证明过程中，我们始终不必要求 a 是正数. 此外，若 b 为负数，只要将 $0\leqslant r<b$ 换成 $0\leqslant r<-b$，定理也一样成立. 请你将上述证明再读一遍，进而验证这一点.

【练习 7】 当 $a=75$，$b=24$ 时，q 和 r 是多少？当 $a=75$，$b=25$ 时，q 和 r 又是多少？

定理 2 连同下一引理即可推出欧几里得算法.

引理 4 若 $a=bq+r$，则 $(a, b)=(b, r)$.

证明 设 $d=(a,b)$. 我们知道，因 $d|a$，$d|b$，由 $a=bq+r$ 即可得 $d|r$，故 d 是 b 和 r 的一个公因子. 假定 c 是 b 和 r 的任一公因子，我们知 $c|b$，$c|r$，由 $a=bq+r$，可得 $c|a$. 因而 c 是 a 和 b 的公因子，故 $c\leqslant d$. d 满足最大公因子定义中的两个条件，故我们有 $d=(b, r)$.

【练习 8】 当 $a=16$，$b=6$ 时，验证此引理的正确性.

根据引理 4，我们对 a 和 b 用除法算式，可得

$$(a, b)=(b, r);$$

最大公因子相同，但右端括号中有了更小的数. 我们可继续对 b 和 r 用除法算式而得更小的数，但最大公因子仍然相同. 除法算式用了相当次数后，这些数终将变得较小，以致我们能用观察法看出最大公因子来. 例如，我们来算一算 (5767, 4453). 用除法算式，我们有

$$5767=4453\cdot 1+1314.$$

由引理 4，我们知 (5767, 4453) = (4453, 1314). 除非你非常善于观察，否则要看出其最大公因子，这两个整数仍嫌太大. 我们再次相除：

$$4453=1314\cdot 3+511.$$

现在我们知道，(5767, 4453) = (1314, 511). 我们继续相除：

$$1314=511\cdot 2+292,$$

$$511=292\cdot1+219,$$
$$292=219\cdot1+73,$$
$$219=73\cdot3.$$

上面一系列余数中，最后一个为零(必然如此，因为一个非负整数的递降序列决不能无限地写下去)，而由引理 4，我们就知道，

$$(5767,\ 4453)=(4453,\ 1314)=\cdots=(219,\ 73)$$
$$=(73,\ 0)=73.$$

将上面这一特殊例子中所用的方法正式写出来，就是欧几里得算法.

定理 3(欧几里得算法)　若 a 和 b 为正整数，$b\neq0$，且

$$a=bq+r,\quad 0\leqslant r<b,$$
$$b=rq_1+r_1,\quad 0\leqslant r_1<r,$$
$$r=r_1q_2+r_2,\quad 0\leqslant r_2<r_1,$$
$$\cdots\qquad\cdots$$
$$r_{k-1}=r_kq_{k+1}+r_{k+1},\quad 0\leqslant r_{k+1}<r_k,$$

则对足够大的 k，比如 $k=t$，我们有

$$r_{t-1}=r_tq_{t+1},$$

且 $(a,\ b)=r_t$.

证明　下列非负整数序列必有终点：

$$b>r>r_1>r_2>\cdots.$$

所以，这些余数中最后必出现零，假定就是 $r_{t+1}=0$，那么

$$r_{t-1}=r_tq_{t+1}.$$

反复应用引理 4，可得

$$(a,\ b)=(b,\ r)=(r,\ r_1)=(r_1,\ r_2)=\cdots$$
$$=(r_{t-1},\ r_t)=r_t.$$

若 a 和 b 中有一个为负数，我们可利用

$$(a, b)=(\pm a, b)=(a, -b)=(-a, -b).$$

【练习 9】 计算(299, 247)和(578, 442).

下面是欧几里得算法的一个推论，以后要多次用到.

定理 4 若$(a, b)=d$, 则有 x 和 y 使 $ax+by=d$.

证明 其想法是：将欧几里得算法倒推上去. 以(5767, 4453)=73 这一计算为例. 算法中倒数第二行给出

$$73=292-219.$$

我们用它前面一行将 73 表为 511 和 292 的一个组合：

$$73=292-(511-292)=2\cdot 292-511.$$

再用更前面一行来消去 292：

$$73=2(1314-511\cdot 2)-511=2\cdot 1314-5\cdot 511.$$

依此类推：

$$73=2\cdot 1314-5(4453-3\cdot 1314)=17\cdot 1314-5\cdot 4453.$$

最后，我们可把 1314 用 4453 和 5767 表出，从而求得所要之表示式：

$$73=17(5767-4453)-5\cdot 4453=17\cdot 5767-22\cdot 4453.$$

一般地，我们有

$$d=(a, b)=r_t=r_{t-2}-r_{t-1}q_t,$$

它将 d 表成了 r_{t-1} 和 r_{t-2} 的具有整系数的一个组合. 从算法中在其前面的一行

$$r_{t-3}=r_{t-2}q_{t-1}+r_{t-1},$$

我们可得 $$d=r_{t-2}-(r_{t-3}-r_{t-2}q_{t-1})q_t,$$

它将 d 表成了 r_{t-2} 和 r_{t-3} 的具有整系数的一个组合：

$$d=(q_{t-1}q_t+1)r_{t-2}-q_tr_{t-3}.$$

然后我们可用

$$r_{t-4}=r_{t-3}q_{t-2}+r_{t-2}$$

消去 r_{t-2}, 得

$$d=(\text{整数})\cdot r_{t-3}+(\text{整数})\cdot r_{t-2},$$

若我们依此继续做下去，最后将求得 x 和 y，使

$$d=ax+by.$$

【练习 10】 求出 $299x+247y=13$ 的一组解.

定理 4 有许多应用，现在我们介绍后面将要用到的两个.

定理 5 若 $d|ab$, $(d, a)=1$, 则 $d|b$.

证明 由于 d 和 a 互素，由定理 4 我们知，存在整数 x 和 y，使

$$dx+ay=1.$$

两端乘以 b，我们有

$$d(bx)+(ab)y=b.$$

上式左端第一项当然可被 d 整除，由于 $d|ab$，d 也整除左端第二项，因此 d 也整除右端，这就是我们所要证明的.

注意，在定理 5 中，若 d 与 a 不互素，那么结论未必成立. 例如，$6|8\cdot 9$，但 $6\nmid 8$，$6\nmid 9$.

定理 6 令 $(a, b)=d$，且设 $c|a$, $c|b$，则 $c|d$.

证明 此定理说起来就是，两个整数的任一公因子也是它们的最大公因子的因子. 证明非常简短：我们知，存在整数 x 和 y，使

$$ax+by=d.$$

由于 c 整除此式左端的两项，c 也整除右端.

习 题

1. 计算：(a) (314, 159)；　(b) (3141, 1592)；
   (c) (4144, 7696)；　(d) (10,001, 100,083).
2. 证明：若 $a|b$, $b|a$，则 $a=b$ 或 $a=-b$.
3. 证明：若 $a|b$, $a>0$，则 $(a, b)=a$.
4. 证明：$((a, b), b)=(a, b)$.

5. 说明"$a>b$ 蕴涵 $a\nmid b$"这一命题不真.

6. (a) 证明：对所有 $n>0$，有 $(n, n+1)=1$；

(b) 当 $n>0$ 时，$(n, n+2)$可取什么值？

(c) 当 $n>0$ 时，$(n, n+k)$可取什么值？

7. 若 $N=n_1n_2\cdots n_k+1$，证明：对于 $i=1, 2, \cdots, k$，有 $(n_i, N)=1$.

8. 证明：若 $(a, b)=1$，$c\mid a$，则 $(c, b)=1$.

9. 求 x 和 y，使

(a) $314x+159y=1$；　　(b) $3141x+1592y=1$；

(c) $4144x+7696y=592$；　　(d) $10001x+100083y=73$.

10. (a) 证明：当且仅当 $(k, n)=1$ 时，成立 $(k, n+k)=1$；

(b) "当且仅当 $(k, n)=d$ 时，成立 $(k, n+k)=d$"，这一说法对不对？

(c) "当且仅当 $(k, n)=d$ 时，对所有整数 r，有 $(k, n+rk)=d$"，这一说法对不对？

11. (a) 证明：$(299, 247)=13$；

(b) 求出 $299x+247y=13$ 的两组解；

(c) 求出 $299x+247y=52$ 的两组解.

12. (a) 若 $x^2+ax+b=0$ 有一整数根，证明此根整除 b；

(b) 若 $x^2+ax+b=0$ 有一有理数根，证明此根实际上是一整数.

13. 证明：若 $a\mid b$，$c\mid d$，则 $ac\mid bd$.

14. 证明：若 $d\mid a$，$d\mid b$，则 $d^2\mid ab$.

15. 证明：若 $c\mid ab$，$(c, a)=d$，则 $c\mid db$.

16. 证明：若 d 为奇数，$d\mid(a+b)$，$d\mid(a-b)$，则 $d\mid(a, b)$.

17. 证明："若 $a\nmid b$，则 $(a, b)=1$"未必成立.

18. 证明：由 $p\mid(10a-b)$ 和 $p\mid(10c-d)$，可得 $p\mid(ad-bc)$.

19. 证明：对所有 $n>0$，有 $6\mid(n^3-n)$.

20. (a) 证明：若对某一 m 有 $10\mid(3^m+1)$，则对所有 $n>0$，有 $10\mid(3^{m+4n}+1)$；

(b) 当 m 是怎样的数时，有 $10\mid(3^m+1)$？

§2 因子分解的唯一性

本节的目的是介绍素数，它是数论研究的主要对象之一；同时还要证明正整数因子分解的唯一性定理，它对于以后的内容也是十分重要的．本节中，小写字母总是代表正整数．

大于1、且除了1和它自身外没有其它正因子的整数称为*素数*．大于1而又不是素数的整数叫做*合数*．这样，2，3，5，7等都是素数，4，6，8，9等都是合数．还存在着很大的素数，如

170，141，183，460，469，231，731，687，303，715，884，105，727

就是一个素数．合数显然可以任意大．注意，我们称1既非素数，也非合数．虽然1除了1和它自身外，没有其它正因子，但如把它包括在素数内，有些定理（特别是因子分解唯一性定理）会变得非常麻烦．我们将把1称为*单位元*．这样，正整数集合就被分成了三类：素数、合数和单位元．

【练习1】 偶素数有多少个？末位数为5的素数有多少个？

我们的目标是要证明，每一正整数都能写为素数之积，而且这种写法是唯一的．若两个乘积只是其因子的次序不相同，我们将不把它们看作为不同的分解式．因此，

$$2^2\cdot 3\cdot 7,\ 2\cdot 3\cdot 7\cdot 2,\ 7\cdot 3\cdot 2\cdot 2$$

中每一个我们都看作是84的同一分解式．这样，整个正整数系统就可通过素数的乘法建立起来．以下，起先的两个引理