当代数论引论

刘弘泉　著

哈爾濱工業大學出版社

当代数论引论

刘弘泉　著

哈爾濱工業大學出版社

内 容 简 介

作者是一位训练有素的数学家，长期从事数论方面的研究工作. 本书涵盖初等数论的主要内容以及使用实分析的广义初等数论的一些内容，同时将超越数论和代数数论的一些重要内容也吸收进去了(它们需要引入虚单位 i，但并不使用复变函数理论)，特别是对 Fermat 问题、Goldbach 问题、Kloosterman 和估计问题、算术级数中的 Dirichlet 除数问题这些著名问题指出了迄今为止的最佳结果(澄清了许多历史错误)，并给予详细证明. 本书包含的技术性强而深的非正统内容，有的取材于国内外一些数论名著，有的取材于作者已发表或尚待发表的研究论文，有的则取材于作者近年来对数学一些重要的基础理论与问题的探究.

本书适合具有大学以上数学学历的数论研究者阅读.

图书在版编目(CIP)数据

当代数论引论/刘弘泉著. —哈尔滨：哈尔滨工业大学出版社，2015.5

ISBN 978-7-5603-5372-2

Ⅰ.①当… Ⅱ.①刘… Ⅲ.①数论 Ⅳ.①O156

中国版本图书馆 CIP 数据核字(2015)第 091353 号

责任编辑 蒋东翔
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 哈尔滨工业大学印刷厂
开 本 787mm×960mm 1/16 印张 15.75 字数 266 千字
版 次 2015 年 5 月第 1 版 2015 年 5 月第 1 次印刷
书 号 ISBN 978-7-5603-5372-2
印 数 1～1 000 册
定 价 68.00 元

前　言

数论，顾名思义，是研究数的学问，是一门古老的数学学科. 使用复分析工具的研究称为解析数论，本书中没有使用复分析. 数的概念，按其发展历史看，有整数、有理数和无理数（包括代数数与超越数）. 整数是数的基础. 早在古希腊时代，写出《几何原本》一书的数学家欧几里德（Euclid）就证明过存在无穷多个素数. 中国古代的数学家对数论的贡献是举世公认的，他们曾提出“勾广三，股修四，径隅五”作为一组特殊的勾股数. 著名的孙子定理（外国称为“中国剩余定理”）提出了如何解相当于现在的联立一次同余式组的问题. 明代学者程大位所写的一首诗

三人同行七十稀
五树梅花廿一枝
七子团圆整半月
除百零伍便得知

便生动而形象地指出了用孙子定理解同余式组（其中 a,b,c 为整数）

$$x\equiv a(\mathrm{mod}\ 3)$$
$$x\equiv b(\mathrm{mod}\ 5)$$
$$x\equiv c(\mathrm{mod}\ 7)$$

所得的解是

$$x\equiv 70a+21b+15c(\mathrm{mod}\ 105).$$

刘徽发明了所谓“割圆术”，精确地计算出圆周率的值约为 3.14159，祖冲之更精确地计算出圆周率的大小介于 3.1415926 和 3.1415927 之间，杨辉则发明了相当于现在的“二项式定理”，等等.

近代（十七世纪以后）对于数论的研究，则要归功于费马（Fermat）、欧拉（Euler）、拉格朗日（Lagrange）、勒让德（Legendre）以及高斯（Gauss），他们对于同余式以及不定方程求解进行过许多高深的研究. 其中高斯证明了关于 Legendre 记号的二次互反律，欧拉的方法经过改进后能证明费马猜想指数为 3 的情形. 进入二十世纪则产生了象前苏联的 I. M. Vinogradov、匈牙利的 P. Erdös 等著名的数论研究学者，特别地后者曾给出著名的素数定理的第一个正确的不用复分析工具的证明（当时 A. Selberg 认为根本不可能得到这种证明，在看了 Erdös 的证明后，他很快给出另一

个较为简洁的证明). 由于复分析用到虚单位($i=\sqrt{-1}$),它在现实中并不存在,因此凡用了复分析工具得到的结果,其价值大大贬值. 特别要指出的是,许多涉及整数的结果(例如 §1.4 的定理 2),虽没有用到复分析,但却要用到虚单位 i,因此实际上也是一些有条件的结果,并不能算作完全初等的.

本书起源于我于 2003 年上半年为哈工大的大学生和研究生所开设的一门选修课的讲义,这次出版之前我又添加了一些较深入的内容,有的取材于我发表过的数论方面的论文,有的取材于我近年来对数论中一些基本理论的研究和发现,有的是未发表的新结果,特别是我结合 Davenport方法和 Estermann 方法给出 Kloosterman 和的正确估计,指出了哥德巴赫问题最佳无条件结果为 Estermann 的结果"6+6"(并且我对他的结果进行推广,超过了 Halberstam 与 Richert 的经典结果),给出迄今为止关于算术级数的 Dirichlet 除数问题的最好结果(Heath-Brown 和 Hooley 等人用复分析工具获得的结果,都有错误). 这些内容(见于第八、九、十章),以及第三章中关于不定方程 $x^3+y^3=z^3$ 以及用二次域的性质研究一些不定方程的论述,在国内其他同类书中一般是没有的. 有的人早在中学时代就对于与"整除"、"素数"有关的问题感兴趣,那么学习本书就可以使他们能够系统地掌握有关的内容,初学者开始可能觉得有些枯燥,但坚持学习则对于训练逻辑思维能力有好处,并且能够增长对数论乃至数学的理解与兴趣,也能够对其他学科的学习有所帮助. 我本人对于数论的兴趣始于初中,当时颇费脑筋地自学了陈景润的书,以后上大学则自学了华罗庚和闵嗣鹤的一些名著,并开始探索从事这方面的研究,早在大学期间就曾在数学系学生会主办的油印刊物《蛙鸣》上发表十多篇论文,深入掌握了指数和估计的 van der Corput 方法的指数对理论,并在《湖南数学通讯》上发表过两篇简短的研究论文,在《中国科学技术大学学报》上发表的论文里则解决了印度数学家 Suryanarayana 在《美国数学会会报》(Bull. Amer. Math. Soc.)上提出的一个问题. 我后来将主要兴趣转向指数和估计方面,前不久已经出版了《指数和估计与数论问题》一书(46 万多字),其中对我新近的许多研究给出详细论述. 当然我的许多观点是会引起争议的,对此我本人要负全部责任,同时我希望有关专家能够提出有价值的改进建议,以便再版时加以更正.

哈工大数学系资助了出版费用.

哈工大　刘弘泉

2015 年 5 月

目　录

第一章　整数的基本性质

§1.1　辗转相除法

定义 1　任给两个整数 a 与 b，$b \neq 0$，如果存在一个整数 q，使得 $a = bq$，则称 b 能整除 a，b 是 a 的因子，a 是 b 的倍数，并记为 $b \mid a$. 否则，若不存在这样的 q，则称 b 不能整除 a，并记为 $b \nmid a$.

例如，我们有 $3 \mid 6$，$2 \mid 0$，但 $3 \nmid 7$. 显然，若 a，b 与 c 为整数，$bc \neq 0$，$bc \mid ac$，则 $b \mid a$，并且反之亦然.

定义 2　设 a，b 与 q 为整数，a 与 b 不全为零，$q \neq 0$ 并且 $q \mid a$，$q \mid b$，则称 q 为 a 与 b 的公因子. 设 q 是 a 与 b 的正的公因子，且对任一 a 与 b 的正的公因子 q'，都有 $q' \leqslant q$，则称 q 为 a 与 b 的最大公因子，并记为 $q = (a, b)$. 显然，$(a, b) = (|a|, |b|)$，这里 $|a|$ 与 $|b|$ 分别表示 a 与 b 的绝对值. 若 $(a, b) = 1$，且 $ab \neq 0$，则称 a 与 b 互素.

由定义，可知 $(3, 6) = 3$，$(10, 6) = 2$，$(7, 3) = 1$. 显然，若 a 与 b 是不全为零的整数，则 a 与 b 的最大公因子 (a, b) 必存在，这是因为 a 与 b 至少有公因子 1，而若 $a \neq 0$，则由于 $|a|$ 仅有有限个因子，并且 a 与 b 的公因子也是 $|a|$ 的因子，因此 a 与 b 的正的公因子中必有最大者. 如何求任意两个非零整数的最大公因子呢？对此，我们有

定理 1　(ⅰ)(带余除法) 设 a 与 b 为整数，$b > 0$，则在唯一一组整数 (q, r)，$0 \leqslant r < b$，使得 $a = bq + r$.

(ⅱ) 设 a，b 与 r 为任意的整数，$b \neq 0$，并存在整数 q 使得 $a = bq + r$，则 $(a, b) = (b, r)$.

(ⅲ) 设 a 与 b 为不全为零的整数，则存在整数 x 与 y，使得

$$ax + by = (a, b).$$

证明　(ⅰ) 任取一个正整数 Q，满足 $Q > \dfrac{|a|}{b}$ 则显然

$$-bQ < a < bQ$$

于是，若以$[bn,b(n+1))$表示左闭右开的区间，$-Q \leqslant n \leqslant Q$，$n$为整数，则

$$a \in \bigcup_{n=-Q}^{Q} [bn,b(n+1)).$$

由于这些区间互不相交，所以存在某个整数q，$-Q \leqslant q \leqslant Q$，使得

$$a \in [bq,b(q+1)),$$

即

$$bq \leqslant a < b(q+1).$$

令$r=a-bq$，则$0 \leqslant r < q$，$a=bq+r$. 若还有一组整数(q',r')，使得$a=bq'+r'$，$0 \leqslant r' < q'$，则

$$b(q-q')=r'-r.$$

若$q \neq q'$，则$|q-q'| \geqslant 1$，

$$b \leqslant |b(q-q')| = |r'-r| \leqslant \max(r',r) < b,$$

矛盾. 这说明必然有$q=q'$，从而$r=r'$. 因此满足$a=bq+r$以及$0 \leqslant r < b$的整数对(q,r)是唯一的.

（ⅱ）由于

$$r=a-bq=(a,b)\left\{\frac{a}{(a,b)}-\frac{b}{(a,b)}q\right\}$$

所以$(a,b) \mid r$，又$(a,b) \mid b$. 因此(a,b)为b与r的正的公因子，由定义可知$(a,b) \leqslant (b,r)$. 类似地，可知(b,r)为a与b的公因子，所以又有$(b,r) \leqslant (a,b)$. 因此$(a,b)=(b,r)$.

（ⅲ）无妨设$b>0$. 由（ⅰ）可知存在整数q及r，$0 \leqslant r < b$，使得

$$a=bq+r. \tag{1}$$

若$r=0$，则$a=bq$，$(a,b)=b$. 若$b>1$，$1 \leqslant r < b$，则对b及r应用（ⅰ），可知存在整数q_1及r_1，使得

$$b=rq_1+r_1, \quad 0 \leqslant r_1 < r. \tag{2}$$

若$r_1=0$，则由（ⅱ），(1)及(2)，可知$(a,b)=(b,r)=r$. 若$r_1>0$，则类似于(2)可得

$$r=r_1q_2+r_2, \quad 0 \leqslant r_2 < r_1, \tag{3}$$

其中q_2及r_2为整数. 若$r_2=0$，则由（ⅱ）、(1)、(2)及(3)，可知$(a,b)=(b,r)=(r,r_1)=r_1$. 若$r_2>0$，则可类似于(2)及(3)，应用（ⅰ）得到

$$r_1=r_2q_3+r_3, 0 \leqslant r_3 < r_2, \tag{4}$$

这里 q_2 及 r_3 为整数，若 $r_3=0$，则由(ⅱ)，(1)、(2)、(3)及(4)可知 $(a,b)=(b,r)=(r,r_1)=(r_1,r_2)=r_2$. 若 $r_3>0$，则我们可以与(4)类似地讨论下去，即得

$$r_2=r_3q_4+r_4,\quad 0<r_4<r_3,$$
$$\vdots$$
$$r_n=r_{n+1}q_{n+2}+r_{n+2},\quad 0<r_{n+2}<r_{n+1},$$
$$\vdots$$

由于 $b>r>r_1>\cdots>r_n>r_{n+1}>r_{n+2}\cdots$，因此经过有限步后，必定有某个整数 $k,k\geqslant 2$，使得

$$r_i=r_{i+1}q_{i+2}+r_{i+2},\quad 0<r_{i+2}<r_{i+1},\quad 1\leqslant i\leqslant k-1,r_k=r_{k+1}q_{k+2}. \tag{5}$$

于是，由(ⅱ)可得

$$r_{k+1}=(r_k,r_{k+1})=(r_{k-1},r_k)=\cdots=(r_1,r_2)=(r,r_1)=(b,r)=(a,b). \tag{6}$$

现在，由(1)，(2)，(5)及(6)可得(设 $r_0=r$)

$$\begin{aligned}(a,b)=r_{k+1}&=r_{k-1}-r_kq_{k+1}=r_{k-1}-(r_{k-2}-r_{k-1}q_k)q_{k+1}\\&=r_{k-1}(1+q_kq_{k+1})-r_{k-2}q_{k+1}=\cdots=r_1c_k-r_0d_{k+1}\\&=(b-r_0q_1)c_k-r_0d_{k+1}=bc_k-r_0(qc_k+d_{k+1})\\&=bc_k-(a-bq)(qc_k+d_{k+1})\\&=b(c_k+q^2c_k+qd_{k+1})-a(qc_k+d_{k+1}),\end{aligned}$$

其中 c_k 和 d_{k+1} 是可能与 $q_{k+1},q_k,\cdots,q_2$ 有关的整数. 于是，我们证明了存在整数 x 与 y，使得

$$ax+by=(a,b). \tag{7}$$

若在(4)中 $r_3=0$，或在(3)中 $r_2=0$，或在(2)中 $r_1=0$，或在(1)中 $r=0$，则可以用类似的“反推”手法证明(7). 若 $b<0$，则由于 $(a,b)=(a,|b|)$，我们可先找到一组整数 (x_0,y_0)，满足

$$ax_0+|b|y_0=(a,|b|),$$

然后令 $x=x_0,y=-y_0$，即仍得到(7). **证毕.**

在定理1的(ⅲ)的证明中所给出的求两个整数最大公因子的方法被称为辗转相除法，又称为欧几里德算法(Euclid's algorithm). 下面我们具体举例说明如何用辗转相除法求两个正整数的最大公因子.

例 1　(ⅰ)求(788,231). (ⅱ)求一组整数 (x,y)，满足 $788x+231y=(788,231)$.

解 （ⅰ）由于

$$788=231\times 3+95,$$
$$231=95\times 2+41,$$
$$95=41\times 2+13,$$
$$41=13\times 3+2,$$
$$13=2\times 6+1,$$
$$2=2\times 1,$$

所以反复应用定理 1 的（ⅱ），可得

$$(788,231)=(231,95)=(95,41)=(41,13)=(13,2)=(2,1)=1.$$

按定义 2，这说明 788 与 231 是互素的.

（ⅱ）将（ⅰ）中的运算步骤倒过来，可得

$$\begin{aligned}1&=13-6\times 2=13-6(41-13\times 3)=19\times 13-6\times 41\\&=19(95-41\times 21)-6\times 41=19\times 95-44\times 41\\&=19\times 95-44\times(231-95\times 2)=107\times 95-44\times 231\\&=107\times 788-365\times 231.\end{aligned}$$

所以，若取

$$x=107,\quad y=365,$$

则得

$$788x+231y=1=(788,231).$$

解毕.

由定理 1 的（ⅲ）可得如下推论：

推论 1 设 a,b 及 c 为整数，$bc\neq 0$

（ⅰ）若 $c>0$，则 $(ca,cb)=c(a,b)$.

（ⅱ）若 $a\mid bc$，且 $(a,b)=1$ 则 $a\mid c$.

（ⅲ）若 $(b,c)=1$，则 $(a,bc)=(a,b)(a,c)$.

证明 （ⅰ）由定理 1 的（ⅲ），可知存在整数 x 及 y，使得

$$(a,b)=ax+by.$$

所以

$$c(a,b)=cax+cby=(ca,cb)m,$$

其中 $m=\dfrac{ca}{(ca,cb)}x+\dfrac{cb}{(ca,cb)}y$，$m$ 为正整数，由此可得，

$$(ca,cb)\mid(c(a,b)),(ca,cb)\leqslant c(a,b). \tag{8}$$

又由于存在整数 u 及 v 使得

$$(ca,cb)=cau+cbv,$$

所以

$$(ca,cb)=c(ax+by)=c(a,b),$$

其中 $n=\frac{a}{(a,b)}x+\frac{b}{(a,b)}y$，$n$ 为正整数. 由此又可得

$$(c(a,b))\mid(ca,cb),c(a,b)\leqslant(ca,cb). \tag{9}$$

由(8)与(9)得(ⅰ).

(ⅱ) 由于$(a,b)=1$，由定理 1 的(ⅲ)可知存在整数 x 及 y，使得

$$1=(a,b)=ax+by.$$

于是

$$c=cax+bcy.$$

因为 $a\mid bc$，所以 $a\mid c$.

(ⅲ) 一方面，由定理 1 的(ⅲ)，可知存在整数对(x,y)及(u,v)，使得

$$(a,b)=ax+by,\quad (a,c)=au+cv,$$

于是，

$$(a,b)(a,c)=a(axu+cxv+byu)+bcyv+(a,bc)M,$$

其中 $M=\frac{a}{(a,bc)}(axu+cxv+byu)+\frac{bc}{(a,bc)}yv$，$M$ 为正整数. 由此可知

$$(a,b)(a,c)\geqslant(a,bc). \tag{10}$$

另一方面，由$(b,c)=1$容易看出$((a,b),(a,c))=1$. 于是，根据

$$(a,b)\mid a,\quad a=(a,c)\frac{a}{(a,c)},$$

以及本推论的(ⅱ)，可得$(a,b)\left|\frac{a}{(a,c)}\right.$，即$\frac{a}{(a,b)(a,c)}$为整数，则由本推论的(ⅰ)即可得

$$\begin{aligned}(a,bc)&=((a,b)(a,c)m,(a,b)(a,c)n)\\&=(a,b)(a,c)(m,n)\geqslant(a,b)(a,c),\end{aligned} \tag{11}$$

其中 $m=\frac{a}{(a,b)(a,c)}$，$n=\frac{a}{(a,b)}\cdot\frac{c}{(a,c)}$. 由(10)及(11)可得

$$(a,bc)=(a,b)(a,c).$$

证毕.

我们来研究两个与求最大公因子有关的问题.

例 2　设 a 与 b 为全不为零的整数，且$(a,b)=1$，求证

$$(a^2-ab+b^2,a+b)=1\text{ 或 }3.$$

证明 应用定理 1 的(ⅲ),容易证明:若 A,B 与 C 为整数,且 $(A,B)=1,BC\neq 0$,则

$$(A,BC)=(A,C). \tag{12}$$

(见练习).我们将应用这个结果.另外,(12) 显然也可由(10) 直接经过论导出.显然

$$a^2-ab+b^2=(a+b)a+b^2-2ab. \tag{13}$$

若 $a+b=0$,则 $b=-a,(a,b)=|a|=1$,此时

$$(a^2-ab+b^2,a+b)=(3a^2,0)=(3,0)=3. \tag{14}$$

若 $a+b\neq 0$,则由(13) 以及定理 1 的(ⅱ) 可得

$$(a^2-ab+b^2,a+b)=(a+b,b^2-2ab). \tag{15}$$

若 $b=2a$,则因 $(a,b)=1$,可得 $|a|=1$,此时

$$(a^2-ab+b^2,a+b)=(3a^2,3a)=3. \tag{16}$$

若 $b\neq 2a$,则 $b^2-2ab\neq 0$.由

$$a+b-a=b,$$

定理 1 的(ⅱ) 及假设可知

$$(a+b,a)=(a,b)=1. \tag{17}$$

所以由(12) 及(15) 可得

$$(a^2-ab+b^2,a+b)=(a+b,b(b-2a))=(a+b,b-2a). \tag{18}$$

由于

$$b-2a-(a+b)=-3a,$$

$b\neq -a,2a$,由定理 1 的(ⅱ),(12) 及(17) 可得

$$(a+b,b-2a)=(a+b,-3a)=(a+b,3).$$

由于 $(a+b,3)$ 必为 3 的因子,因此只能为 1 或 3.因此,由(18) 可知所需结论成立. **证毕.**

例 3 设 m 与 n 为大于 1 的正整数,求证

$$(2^m-1,2^n-1)=2^{(m,n)}-1.$$

证明 不妨设 $m>n$.由定理 1 的(ⅰ),我们有

$$m=nq+r,\quad 0\leqslant r<n,$$

其中 q 及 r 为正整数.若 $r=0$,则

$$(m,n)=n \tag{19}$$

显然成立.设 $1\leqslant r<n$,我们可以证明

$$(2^m-1,2^n-1)=(2^n-1,2^r-1). \tag{20}$$

事实上,由于(应用等比级数求和)

$$2^{m-1}-1=(2^{n-1}-1)(2^{m-n}+2^{m-2n}+\cdots+2^{m-qn})+2^{m-qn}-1,$$

所以由定理 1 的(ⅱ)可得

$$(2^m-1,2^n-1)=(2^n-1,2^{m-qn}-1)=(2^n-1,2^r-1).$$

利用(20),以及我们在证明定理 1 的(ⅲ)中采用的求最大公因子的步骤(1) ~ (6),可得

$$(2^m-1,2^n-1)=(2^n-1,2^r-1)=(2^r-1,2^{r_1}-1)=\cdots$$
$$=(2^{r_k}-1,2^{r_{k+1}}-1)=2^{r_{k+1}}-1=2^{(m,n)}-1. \quad (21)$$

若求最大公因子的步骤停止于(1) ~ (4)中的某一步,则(21)中相应的步骤会简单些. **证毕.**

对于多于 2 个的整数,我们也可以定义最大公因子.

定义 3　设 $n\geqslant 3,a_1,\cdots,a_n$ 是不全为零的整数,$q\neq 0$,q 为整数,并且 $q\mid a_1,\cdots q\mid a_n$,则 q 称为 $a_1,\cdots,a_n$ 的一个公因子. $a_1,\cdots,a_n$ 所有正的公因子中最大者称为他们的最大公因子.

关于多于 2 个整数的最大公因子,我们有

定理 2　设 $n\geqslant 3,a_1,\cdots a_n$ 为整数,$a_1\neq 0$. 归纳地定义

$$(a_1,\cdots,a_k)=((a_1,\cdots,a_{k-1}),a_k),\quad 3\leqslant k\leqslant n.$$

则

(ⅰ)存在整数 $x_1,\cdots,x_n$ 使得

$$a_1x_1+\cdots+a_nx_n=(a_1\cdots a_n).$$

(ⅱ)$(a_1,\cdots,a_n)$ 是 $a_1,\cdots,a_n$ 的最大公因子.

证明　(ⅰ)对 n 用归纳法. 若 $n=3$,则由定义可知

$$(a_1,a_2,a_3)=((a_1,a_2),a_3),(a_1,a_2)\geqslant 1.$$

由定理 1 的(ⅲ),可知存在整数 u 及 v,使得

$$(a_1,a_2)u+a_3v=((a_1,a_2),a_3)=(a_1,a_2,a_3),$$

又存在整数 u_1 及 v_1,使得

$$a_1u_1+a_2v=(a_1,a_2).$$

因此

$$a_1x_1+a_2x_2+a_3x_3=(a_1,a_2,a_3),$$

其中 $x_1=uu_1,x_2=uv_1,x_3=v$. 若当 $n=m$ 时,已证明了所需结论,则由定义可知

$$(a_1,\cdots,a_m,a_{m+1})=((a_1,\cdots,a_m),a_{m+1}).$$

由定理 1 的(ⅲ)及归纳假设,可知存在整数 $u,v,u_1,\cdots,u_m$,使得

$$(a_1\cdots,a_m)u+a_{m+1}v=(a_1,\cdots,a_m,a_{m+1}),$$

$$a_1u_1+\cdots+a_mu_m=(a_1,\cdots,a_m).$$

于是

$$a_1x_1+\cdots+a_mx_m+a_{m+1}x_{m+1}=(a_1,\cdots,a_m,a_{m+1}).$$

其中 $x_1=u_1u,\cdots,x_m=u_mu,x_{m+1}=v$. 这说明命题对 $n=m+1$ 也成立. 归纳法完成. (ⅰ) 的结论成立.

(ⅱ) 由定义, 显然 $(a_1,\cdots,a_n)$ 是 $a_1,\cdots,a_n$ 的正的公因子. 若 q 是 $a_1,\cdots,a_n$ 的任一正的公因子, 则由于存在整数 $x_1,\cdots,x_n$, 使得

$$a_1x_1+\cdots+a_nx_n=(a_1,\cdots,a_n),$$

可得

$$(a_1,\cdots,a_n)=qM,\quad M=\sum_{i=1}^{n}a_ix_iq^{-1}.$$

由于 M 为整数, 所以 $(a_1,\cdots,a_n)\geqslant q$. 按定义, $(a_1,\cdots,a_n)$ 就是 $a_1,\cdots,a_n$ 的最大公因子. **证毕.**

例如, 我们有 $(2,3,6,)=((2,3),6)=(1,6)=1$, 即 2,3, 与 6 的最大公因子为 1.

练　　习

1. 求 $(732,286)$, 并找出一组整数 x 及 y, 使得

$$732x+286y=(732,286).$$

2. 求 $(26,143,77)$, 并找出一组整数 x,y 及 z, 使得

$$26x+143y+77z=(26,143,77).$$

(提示: 由定理 2 的 (ⅱ), 可知这样一组 (x,y,z) 必存在, 并应用那里的证法具体地构造一组数).

3. 设 n 为任意整数, 证明 $6\mid n(n+1)(2n+1)$.

4. 设 a,b,c 整数, $bc\neq 0$ 且 $(a,b)=1$. 应用定理 1 的 (ⅲ), 证明 $(a,bc)=(a,c)$.

5. 若 a 与 b 为互素的整数 (a 与 b 不全为零), 且 $|a|\neq 1$, 求证 $(a+b,a-b)$ 等于 1 或者 2.

6. 设 x,y,a,b,c 及 d 都是整数, 并且 x 与 y 不全为零. 设 $m=ax+by$, $n=cx+dy$, $|ad-bc|=1$, 证明: m 与 n 不全为零, 并且 $(m,n)=(x,y)$.

7. 设 x 与 y 为整数, 证明: $17\mid(2x+3y)$ 当且仅当 $17\mid(9x+5y)$.

8. 一个分子与分母互素的分数被称为既约分数. 证明：对于任何自然数 n，

$$\frac{21n+4}{14n+3}$$

为既约分数.

9. 若 m 和 n 为正整数，m 为奇数，求证 $(2^m-1,2^n+1)=1$. (提示：应用例 3 的结论，推论 1 的(ⅲ)，以及 $(2^n+1)\mid(2^{2n}-1)$).

§1.2　算术基本定理

定义 1　设 n 为一个正整数(即自然数)，$n>1$. 若 n 仅以 1 和 n 为正因子，则称 n 为素数(prime)，若 n 有不同于 1 和 n 的正因子，则称 n 为复合数，一个复合数的素数因子被称为素因子. 于是，按照这个定义，全体正整数被分成了 1，全体素数，以及全体复合数三类. 素数通常用字母 p 表示.

按定义，显然可知 2,3,5,7,11,13,17,19,23,29,31,37,… 都是素数. 两个不相等的素数必定互素. 关于复合数，我们有

引理 1　每个(大于 1) 的复合数 n 都被分解成若干素数的乘积.

证明　对全体复合数应用数学归纳法. 显然，4 是最小的复合数，而 $4=2\times2$，2 是素数. 假设 n 是一个复合数，并且对于所有小于 n 的复合数命题成立. 因为 n 是复合数，则有正整数 d，$d\mid n$，$1<d<n$，于是 $n=du$，u 为正整数，$1<u<n$. 由归纳假设，可得(考虑到了 d 或 u 本身即为素数的情况)

$$d=q_1\cdots q_r,\quad r\geqslant 1,\quad q_1,\cdots,q_r \text{ 为素数},$$
$$u=q_1\cdots q_s,\quad s\geqslant 1,\quad q_1,\cdots,q_s \text{ 为素数}.$$

于是，

$$n=p_1\cdots p_rq_1\cdots q_s,$$

即 n 也可分解成若干素数之积，归纳法完成. 命题成立.　**证毕.**

例如，$39=13\times3$，$176=2^4\times11$. 读者不禁会问，素数是否有有限多个呢？下面的定理回答了这个问题.

定理 1　存在无穷多个素数，

证明　用反证法. 若仅有有限个不同的素数，记为 $p_1,\cdots,p_n$，并令