初等数论及其应用

阎满富　王朝霞　　编著

中国铁道出版社

初等数论及其应用

[illegible]

[illegible]

初等数论及其应用

阎满富　王朝霞　编著

中国铁道出版社

1999年·北京

(京)新登字 063 号

内 容 简 介

数论是研究数的性质的一门学科，有其广泛的应用。本书主要阐述了数论的基本内容和方法，包括整除性理论、不定方程、同余式及同余方程、连分数、分数与小数的互化、数论函数及数论知识的应用等。

本书条理清楚，层次分明，深入浅出，例题丰富，适用范围广泛，并重点阐述了应用。每章均配备了习题，书后附有解答，可作为师范院校和中学教师继续教育的教材。

图书在版编目(CIP)数据

初等数论及其应用/阎满富，王朝霞编著．—北京：中国铁道出版社，1999

ISBN 7-113-03318-0

Ⅰ．初… Ⅱ．①阎… ②王… Ⅲ．初等数论 Ⅳ．O156.1

中国版本图书馆 CIP 数据核字(1999)第 10685 号

书　　名：**初等数论及其应用**

著作责任者：阎满富　王朝霞编著

出版·发行：中国铁道出版社(100054，北京市宣武区右安门西街 8 号)

责任编辑：任　军

印　　刷：河北省遵化市印刷厂

开　　本：850×1168　1/32　印张：8.75　字数：229 千

版　　本：1999 年 4 月第 1 版　　1999 年 4 月第 1 次印刷

印　　数：1～3000 册

书　　号：ISBN7-113-03318-0/O·65

定　　价：14.00 元

前　言

初等数论是研究整数性质和方程(组)整数解的一门学科,也是一个古老的数学分支。作为大学数学专业的基础课程,不仅师范院校普遍开设,也是综合大学数学专业及计算机科学等许多相关专业所需的课程。近两年来,教育部颁发的《中小学教师继续教育课程开发指南》已把《初等数论》列入数学专业教师继续教育课程。中学生(甚至小学生)课外数学兴趣小组及数学竞赛的许多内容也是属于初等数论的。

为了适应本专科师范院校数学专业的教学需要,特别是中学教师继续教育教学的需要,我们编写了此书。编写这本教材,力求从我国社会发展的客观要求和师范教育的特点出发,体现时代的先进性和创新性;知识体系的科学性和系统性;师范教育的专业性和综合性;教材内容的应用性和针对性。编写时尽可能把最新的研究成果吸收并渗透到教材内容中去。考虑到师范专业在校生及在职中学数学教师学完本门课程后,要应用到中学数学教学中,所以本书特别安排了初等数论在中学数学中的应用,因而使本书更具实用性。

我们深知要写好一本初等数论的教材绝非易事,虽然我们从事数论教学和研究工作数十年,但一直未敢动笔。现在为了适应教学需要,把我们多年所积累的讲稿进行挑选、补充和进一步加工整理,编写成这一本不够成熟、我们也仍不满意的教材,其中疏漏不当以至错误之处在所难免,切望同行和读者不吝赐教。

编　者

1999 年 3 月

目　录

第一章　整除性理论

数论是研究整数性质的一个数学分支. 整数是我们天天接触的数,它们是那样平凡无奇,但是几千年来全世界无数的数学家绞尽脑汁,探索着整数间的一个又一个的规律. 遗憾的是至今仍有许多规律尚未被人类所证明. 像中外闻名的哥德巴赫猜想,它被称作"数学皇冠上闪闪发光的明珠"(以后将介绍这个猜想),数学家陈景润致力于这个猜想的证明,他已取得了目前在世界上处于领先地位的结果. 但可惜的是距离这个问题的最终结果还差一步. 为了认识和解决一些数论问题,我们还必须从基础理论学起.

§1.1　整除的概念及基本性质

全体整数的集合用 $\mathbf{Z}$ 来表示,其中有正整数,负整数和零.

定义 1.1.1　设 $a,b\in\mathbf{Z}$,若$\exists\ q\in\mathbf{Z}$,使得

$$a=bq \tag{1.1.1}$$

则称 b 整除 a,记作 $b\mid a$,并把 a 叫做 b 的倍数,b 叫做 a 的因数.

若 $b\mid a$ 且 $b\neq\pm a, b\neq\pm 1$,b 叫做 a 的真因数.

显然,b 是 a 的真因数的充要条件是:$b\mid a$ 且 $1<|b|<|a|$.

若使(1.1.1)成立的整数 q 不存在,则称 b 不整除 a,记作 $b\nmid a$.

下面为整除的基本性质.

定理 1.1.1　若 $a,b\in\mathbf{Z}, b\mid a$,则 $(-b)\mid a, b\mid(-a), |b|\mid|a|$, $(-b)\mid(-a)$.

定理 1.1.2　若 $c\mid b, b\mid a$,则 $c\mid a$,其中 $a,b,c\in\mathbf{Z}$.

定理 1.1.3　若 $a,b,c\in\mathbf{Z}$,且 $b\mid a$,则 $bc\mid ac$.

定理 1.1.4 若 $a,b,c\in\mathbf{Z}$，且 $c\mid a$，$c\mid b$，则$\forall\ m,n\in\mathbf{Z}$，有 $c\mid(ma+nb)$.

定理 1.1.5 如果在全是整数的等式中

$$k+l+\cdots+m=p+q+\cdots+r$$

除一项外，其余各项都能被 b 整除，则这项也能被 b 整除.

这些定理的证明都不难，留给读者练习.

定理 1.1.6 设 $b\in\mathbf{Z}$，$b\neq0$，则任意整数 a 可唯一地表示为下面形式

$$a=bq+r$$

其中 $q,r\in\mathbf{Z}$，且 $0\leqslant r<|b|$.

证明 只就 $b>0$ 的情形证明，在以下数列

$$\cdots,-3b,-2b,-b,0,b,2b,3b,\cdots$$

中总存在 $q\in\mathbf{Z}$，使

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

于是 $0\leqslant a-bq<b$. 令 $r=a-bq$，则 $a=bq+r$，　$0\leqslant r<b$.

假如另有表示式 $a=bq_1+r_1$　$0\leqslant r_1<b$，

则　$0=b(q-q_1)+r-r_1$，$b\mid(r-r_1)$.

但 $|r-r_1|<b$，于是只有 $r-r_1=0$，即 $r=r_1$.

从而

$$q=q_1.$$

这个定理叫带余除法定理，q 叫 a 除以 b 所得的商，r 叫 a 除以 b 的余数.

例如，$b=14$，$a=177$ 时，$177=14\times12+9$，$0<9<14$.

$b=14$，$a=-64$ 时，$-64=14\times(-5)+6$，$0<6<14$.

$b=14$，$a=154$ 时，$154=14\times11+0$，$0=0<14$.

习题 1.1

1. 证明：$6\mid a(a-1)(2a-1)$，其中 $a\in\mathbf{Z}$.

2. 若 $a,b\in\mathbf{Z}$，$|b|\mid|a|$，$|a|<|b|$，求证 $a=0$.

3. 证明：$\forall\ n\in\mathbf{Z}$，一元二次方程

$$x^2-16nx+75=0$$

没有整数解.

4. n 个整数 $a_1,a_2,\cdots,a_n$ 满足关系式：

$$a_1a_2\cdots a_n=n,\quad a_1+a_2+\cdots+a_n=0,$$

求证：$4\mid n$.

5. 设 a 为有理数，b 是使 ba 为整数的最小正整数，如果 c 和 ca 都是整数，则 $b\mid c$.

§1.2 最大公因数

定义 1.2.1 若 $a,b,c\in\mathbf{Z}$，且 $c\mid a,c\mid b$，则称 c 是 a 与 b 的公因数.

定义 1.2.2 若 $a,b,d\in\mathbf{Z}$，且 d 是 a,b 的公因数，并且对于 a,b 的任一公因数 c 都有 $c\mid d$，则称 d 是 a 与 b 的最大公因数.

例 1.2.1 0 与 0 的最大公因数是 0.

例 1.2.2 若 d 是 a 与 b 的最大公因数，则 $-d$ 也是 a 与 b 的最大公因数.

证明 因 d 是 a 与 b 的最大公因数，所以 $d\mid a,d\mid b$，从而 $-d\mid a$，$-d\mid b$.

对于 a,b 的任一个公因数 c，即 $c\mid a,c\mid b$ 有 $c\mid d$，从而 $c\mid -d$.

所以 $-d$ 是 a 与 b 的最大公因数.

约定：用 (a,b) 表示 a,b 的非负的最大公因数.

定理 1.2.1 若 $b=aq+r,a\neq 0,a,b,q,r\in\mathbf{Z}$，则 $(a,b)=(a,r)$.

证明 令 $d=(a,b)$，则 $d\mid a,d\mid b$，由

$$b=aq+r$$

有 $d\mid r$，所以 d 是 a 和 r 的公因数.

$\forall\ c\in\mathbf{Z}$，且 $c\mid a,c\mid r$，由 $b=aq+r$，则 $c\mid b$，即 c 是 a 与 b 的公因数，而 $d=(a,b)$，则 $c\mid d$，所以 $d=(a,r)$.

定理 1.2.2 任意两个整数都有最大公因数.

证明 设 a,b 是任意两个整数.

若 $a=b=0$，显然 $(0,0)=0$.

若 a,b 不全为 0，不妨设 $b\neq 0$，由带余除法，$\exists\ q_1,r_1\in\mathbf{Z}$，使

$$a=bq_1+r_1,0\leqslant r_1<|b|.$$

若 $r_1\neq 0$，则 $b=r_1q_2+r_2,0\leqslant r_2<r_1$；若 $r_2\neq 0$，则 $r_1=r_2q_3+r_3$，$0\leqslant r_3<r_2$.

因为 $|b|$ 是一个有限正整数，且

$$|b|>r_1>r_2>r_3>\cdots$$

于是经过有限次带余除法后，得到

$$(*)\begin{cases} a=bq_1+r_1, & 0<r_1<|b| \\ b=r_1q_2+r_2, & 0<r_2<r_1 \\ r_1=r_2q_3+r_3, & 0<r_3<r_2 \\ \quad\vdots & \quad\vdots \\ r_{k-3}=r_{k-2}q_{k-1}+r_{k-1}, & 0<r_{k-1}<r_{k-2} \\ r_{k-2}=r_{k-1}q_k+r_k, & 0<r_k<r_{k-1} \\ r_{k-1}=r_kq_{k+1}+0, & r_{k+1}=0 \end{cases}$$

由定理 1.2.1

$$r_k=(r_{k-1},r_k)=(r_{k-2},r_{k-1})=\cdots=(r_1,r_2)=(b,r_1)=(b,a),$$

即 a 与 b 的最大公因数存在.

注 上述除法过程，称为辗转除法，也叫 Eucilid 除法.

例 1.2.3 求(6 731,2 809).

解

$q_2=2$	6 731	2 809	$2=q_1$
	5 618	2 226	
$q_4=1$	1 113	583	$1=q_3$
	583	530	
	530	53	$10=q_5$
	530		
	0		

所以(6 731,2 809)=53.

定理 1.2.3 设 a,b 是正整数,且 $a>b$,设求(a,b)时,所用的除法次数为 k,b 在十进制中的位数是 l,则 $k\leqslant 5l$.

证明 考察裴波那契数列$\{u_n\}$:

$$u_1=1,u_2=1,u_{n+2}=u_{n+1}+u_n,n=1,2,\cdots \tag{1.2.1}$$

首先证明(1.2.1)的一个性质:

$$u_{n+5}>10u_n,n\geqslant 2. \tag{1.2.2}$$

当 $n=2$ 时,$u_2=1,u_7=13,u_7>10u_2$;

设 $n\geqslant 3$,

$$u_{n+5}=u_{n+4}+u_{n+3}=2u_{n+3}+u_{n+2}=3u_{n+2}+2u_{n+1}=$$
$$5u_{n+1}+3u_n=8u_n+5u_{n-1}.$$

因为 $u_n=u_{n-1}+u_{n-2}\leqslant 2u_{n-1}$,故 $2u_n\leqslant 4u_{n-1}$,这样:

$$u_{n+5}=8u_n+5u_{n-1}>8u_n+4u_{n-1}\geqslant 10u_n,$$

即(1.2.2)成立.

由(1.2.2)可得:

$$u_{n+5t}>10^tu_n,n=2,3,\cdots,t=1,2,\cdots \tag{1.2.3}$$

(对 t 用归纳法可得).

设 $a=n_0,b=n_1$,用辗转除法得:

$$\begin{cases} n_0=n_1q_1+n_2, & 0<n_2<n_1 \\ n_1=n_2q_2+n_3, & 0<n_3<n_2 \\ \quad\vdots & \quad\vdots \\ n_{k-2}=n_{k-1}q_{k-1}+n_k, & 0<n_k<n_{k-1} \\ n_{k-1}=q_kn_k, \end{cases} \tag{1.2.4}$$

由(1.2.4)及 $q_k\geqslant 2$ 知:

$n_{k-1}=n_kq_k\geqslant 2n_k\geqslant 2=u_3$,

$n_{k-2}\geqslant n_{k-1}+n_k\geqslant u_3+u_2=u_4$(因为 $n_k\geqslant 1=u_2$),

$n_{k-3}\geqslant n_{k-2}+n_{k-1}\geqslant u_3+u_4=u_5$,

$\vdots$

$n_1 \geqslant n_2 + n_3 \geqslant u_k + u_{k-1} = u_{k+1}$.

如果 $k > 5l$，即 $k \geqslant 5l+1$，那么 $n_1 \geqslant u_{k+1} \geqslant u_{5l+2}$.

由(1.2.3)，$u_{5l+2} \geqslant 10^l \cdot u_2 = 10^l$，所以 $n_1 \geqslant 10^l$.

又 $n_1 = b$ 的位数是 l，故 $n_1 < 10^l$ 矛盾，所以 $k \leqslant 5l$.

注 存在正整数 a, b 使 $k = 5l$.

例如：$a = 144, b = 89$，

$144 = 89 + 55$，

$89 = 55 + 34$，

$55 = 34 + 21$，

$34 = 21 + 13$，

$21 = 13 + 8$，

$13 = 8 + 5$，

$8 = 5 + 3$，

$5 = 3 + 2$，

$3 = 2 + 1$，

$2 = 1 \times 2$.

以上作了 10 次除法，而 b 是二位数，故 $k = 5l (k = 10, l = 2)$.

定理 1.2.4 设 a, b 的最大公因数是 d. 则$\exists\ \lambda, \mu \in \mathbf{Z}$ 使

$$d = a\lambda + b\mu$$

证明 由于 $a = 1 \cdot a + 0 \cdot b = \lambda_{-1} a + \mu_{-1} b$，

$$b = 0 \cdot a + 1 \cdot b = \lambda_0 a + \mu_0 b,$$

其中 $\lambda_{-1} = 1, \mu_{-1} = 0, \lambda_0 = 0, \mu_0 = 1$.

由定理 1.2.2 的证明中的(*)式：

$$r_1 = a - bq_1 = (\lambda_{-1} a + \mu_{-1} b) - q_1(\lambda_0 a + \mu_0 b) =$$
$$(\lambda_{-1} - \lambda_0 q_1) a + (\mu_{-1} - \mu_0 q_1) b =$$
$$\lambda_1 a + \mu_1 b$$

其中 $\lambda_1 = \lambda_{-1} - \lambda_0 q_1, \mu_1 = \mu_{-1} - \mu_0 q_1$.

$$r_2 = b - q_2 r_1 = (\lambda_0 a + \mu_0 b) - q_2(\lambda_1 a + \mu_1 b) =$$
$$(\lambda_0 - \lambda_1 q_2) a + (\mu_0 - \mu_1 q_2) b =$$

$$\lambda_2 a+\mu_2 b$$

其中 $\lambda_2=\lambda_0-\lambda_1 q_2$，$\mu_2=\mu_0-\mu_1 q_2$.

同理 $r_3=\lambda_3 a+\mu_3 b$，其中 $\lambda_3=\lambda_1-\lambda_2 q_3$，$\mu_3=\mu_1-\mu_2 q_3$.

由此可见，一般有：

$$r_k=\lambda_k a+\mu_k b,$$

其中 $\lambda_k=\lambda_{k-2}-\lambda_{k-1}q_k$，$\mu_k=\mu_{k-2}-\mu_{k-1}q_k$，

其中 λ_k,μ_k 为整数，r_k 为 a,b 的最大公因数.

注 上述 λ_k,μ_k 可由下表求得：

k	-1	0	1	2	3	…	k
q			q_1	q_2	q_3	…	q_k
λ	1	0	1	$-q_2$	$1+q_2q_3$	…	λ_k
μ	0	1	$-q_1$	$1+q_1q_2$	$-q_1-q_3-q_1q_2q_3$	…	μ_k

例 1.2.4 求(24 871,3 468)，并求 λ,μ 使

$$(24\ 871,3\ 468)=\lambda\cdot 2\ 4871+\mu\cdot 3\ 468.$$

解 由辗转除法：

$q_2=5$	24 871	3 468	$7=q_1$
	24 276	2 975	
$q_4=4$	595	493	$1=q_3$
	493	408	
$q_6=5$	102	85	$1=q_5$
	85	85	
	17	0	

所以(24 871,3 468)=17.

k	-1	0	1	2	3	4	5
q			$q_1=7$	$q_2=5$	$q_3=1$	$q_4=4$	$q_5=1$
λ	1	0	1	-5	6	-29	35
μ	0	1	-7	36	-43	208	-251

所以当 $\lambda=35,\mu=-251$ 时

$$(24\ 871,3\ 468)=\lambda\cdot 2\ 4871+\mu\cdot 3\ 468.$$

注 ①此定理的逆命题不成立，即如果 $d=a\lambda+b\mu,d$ 不一定是 a,b 的最大公因数.

例如：$3=2\times1+1\times1$. 但 3 不是 2 和 1 的最大公因数.

②如果 $d=a\lambda+b\mu$，且 $d|a,d|b$，那么 d 是 a 和 b 的最大公因数.

证明：因为 $d|a,d|b$，所以 d 是 a 、的公因数，

设 c 是 a 和 b 的任一公因数，即 $c|a,c|b$，又 $d=a\lambda+b\mu$，则 $c|d$.

所以 d 是 a 和 b 的最大公因数.

定理 1.2.5 (i)设 m 为任一正整数，那么 $(am,bm)=(a,b)m$；

(ii)设 $\delta|a,\delta|b,\delta>0$，则

$$\left(\frac{a}{\delta},\frac{b}{\delta}\right)=\frac{(a,b)}{\delta}.$$

证明 (i)由定理 1.2.4，$\exists\ \lambda,\mu\in\mathbf{Z}$，使

$$(a,b)=\lambda a+\mu b,$$

$$(a,b)m=\lambda(am)+\mu(bm).$$

又显然 $(a,b)m|am,(a,b)m|bm$，则有：

$$(a,b)m=(am,bm).$$

(ii)由(i)

$$\left(\frac{a}{\delta}\cdot\delta,\frac{b}{\delta}\cdot\delta\right)=\left(\frac{a}{\delta},\frac{b}{\delta}\right)\cdot\delta,$$

即

$$(a,b)=\left(\frac{a}{\delta},\frac{b}{\delta}\right)\cdot\delta,$$

所以

$$\left(\frac{a}{\delta},\frac{b}{\delta}\right)=\frac{(a,b)}{\delta}.$$

定义 1.2.3 若两个整数 a,b 的公因数只有 ±1，则称 a 与 b 互素，即，若 $(a,b)=1$，则称 a,b 互素.

显然，$(a,b)=1$ 的充要条件是 $\exists\ \lambda,\mu\in\mathbf{Z}$，使 $\lambda a+\mu b=1$.

下面讨论互素的几条基本性质.

定理 1.2.6 (i)若 $(a,b)=1,(a,c)=1$，则有 $(a,bc)=1$；

(ii)若$(a,b)=1$，且$a|bc$，则$a|c$；

(iii)若$a|b,c|b,(a,c)=1$，则$ac|b$.

证明 (i)因为$(a,b)=1$，$\exists\ \lambda_1,\mu_1\in\mathbf{Z}$，使$\lambda_1 a+\mu_1 b=1$，

又因为$(a,c)=1$，$\exists\ \lambda_2,\mu_2\in\mathbf{Z}$，使$a\lambda_2+c\mu_2=1$，

从而
$$(a\lambda_1+b\mu_1)(a\lambda_2+c\mu_2)=1,$$
$$a(a\lambda_1\lambda_2+c\lambda_1\mu_2+b\lambda_2\mu_1)+bc(\mu_1\mu_2)=1,$$

因此，$(a,bc)=1$.

(ii)因为$(a,b)=1$，$\exists\ \lambda,\mu\in\mathbf{Z}$，使$a\lambda+b\mu=1$，

则
$$a\lambda c+b\mu c=c,$$

又
$$a|a\lambda c,a|bc\mu,$$

所以$a|c$.

(iii)因为$a|b$，$\exists\ q_1\in\mathbf{Z}$，使$b=aq_1$，又$c|b$，$\exists\ q_2\in\mathbf{Z}$，使得$b=cq_2$，则$aq_1=cq_2$，而$a|aq_1$，则$a|cq_2$，又$(a,c)=1$，则$a|q_2$，从而$\exists\ q_3\in\mathbf{Z}$，使$q_2=aq_3$，因此，$b=acq_3$，即$ac|b$.

以上我们讨论的是两个数的最大公因数，下面把这一概念推广.

定义 1.2.4 设$h|a_i,i=1,2,\cdots,n$，则称h是$a_1,a_2,\cdots,a_n$的公因数.

定义 1.2.5 设d是$a_1,a_2,\cdots,a_n$的公因数，如果对于$a_1,a_2,\cdots,a_n$的任何一个公因数c，都有$c|d$，则称d是$a_1,a_2,\cdots,a_n$的最大公因数.

用$(a_1,a_2,\cdots,a_n)$表示$a_1,a_2,\cdots,a_n$的非负的最大公因数.

定理 1.2.7 设$(a_1,a_2)=d_2,(d_2,a_3)=d_3,\cdots,(d_{n-1},a_n)=d_n$

则
$$(a_1,a_2,\cdots,a_n)=d_n.$$

证明 因$(a_1,a_2,\cdots,a_n)|a_1,(a_1,a_2,\cdots,a_n)|a_2$，

则$(a_1,a_2,\cdots,a_n)|d_2$，又$(a_1,a_2,\cdots,a_n)|a_3$，则$(a_1,a_2,\cdots,a_n)|d_3$，继续下去，…

$$(a_1,a_2,\cdots,a_n)|d_n,$$

又 $d_n|a_n,d_{n-1},a_{n-1},d_{n-2},\cdots,d_3,a_3,d_2,a_2,a_1,$

则
$$d_n|(a_1,a_2,\cdots,a_n),$$

所以 $$d_n=(a_1,a_2,\cdots,a_n).$$

习题 1.2

1. 求 λ,μ 使 $(325,214)=325\lambda+214\mu$.

2. 设 $(a,b)=1$，求证：$(ac,b)=(c,b)$.

3. 设 $(a,b)\neq 0$，证明 (a,b) 为 $ax+by$ 形式的数中的最小正数.（其中 $x,y\in\mathbf{Z}$）.

4. 设 n,A 是正整数，且 $\sqrt[n]{A}$ 不是整数，证明 $\sqrt[n]{A}$ 一定不是有理数.

5. 有一间长方形屋子，长 525 cm，宽 325 cm，现用方砖铺地，要恰好铺满整个屋子，问所用方砖的最大边长应为多少？

6. 设 $m>0,n>0$，且 m 是奇数，求证：$(2^m-1,2^n+1)=1$.

7. 对任何自然数 n，证明分数 $\frac{21n+4}{14n+3}$ 不能约分.

§1.3 最小公倍数

定义 1.3.1 设 $a_1,a_2,\cdots,a_n$ 及 m 是整数，如果 $a_i\mid m,i=1,2,\cdots,n$，则称 m 是 $a_1,a_2,\cdots,a_n$ 的公倍数.

定义 1.3.2 若 m 是 $a_1,a_2,\cdots,a_n$ 的公倍数，且对它们的任一公倍数 k，都有 $m\mid k$，则称 m 是 $a_1,a_2,\cdots,a_n$ 的最小公倍数.

用 $[a_1,a_2,\cdots,a_n]$ 表示 $a_1,a_2,\cdots,a_n$ 的非负的最小公倍数.

如：$[3,6,9]=18$.

显然 $[a_1,a_2,\cdots,a_n]=[|a_1|,|a_2|,\cdots,|a_n|]$，故只须讨论正数的最小公倍数.

下面讨论两个数的最小公倍数.

定理 1.3.1 设 $d=(a,b)\neq 0$，则 $ab=[a,b](a,b)$.

证明 因 $d\mid a,d\mid b$，显然 $\frac{ab}{d}$ 是 a,b 的公倍数.

设 M 是 a,b 的任一公倍数，则 $M=ak,k\in\mathbf{Z}$，又 $b\mid M$，则 $b\mid ak$，