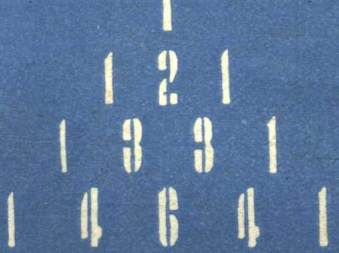
# 初等数论

王锋




中国人民解放军工程技术学院

# 编　者　的　话

初等数论是我院应用数学系的一门基础课，为进一步学习近世代数、群论、移位寄存器等课提供必要的基础知识。

初等数论对数学分析、近世代数、概率论等学科的发展都起过重要作用。初等数论在计算技术、通信技术、信息理论中也得到广泛的应用。

《初等数论》一书是编者对六期本科生和两期电专业研究生讲课中逐渐形成的。该书力求由浅入深、深入浅出地讲解本学科的内容。由于初等数论习题较难，除编印了《初等数论习题解》外，在讲义中还注意了讲解典型例题，以引导学生较快提高解题能力。

编者水平有限，缺点错误一定很多，恳请批评、指正。

郑州工学院印刷厂为本书的排印付出了艰苦的劳动，谨向印刷厂领导和工人师付表示衷心地感谢。

王　锋　　1986年2月

# 目　录

# 第一章　整数的基本性质

## 第 1 节　奇偶数的性质

可以表为$2m+1$的整数称为奇数，可表为$2m$的整数称为偶数，其中$m=0, 1, 2, \cdots\cdots$。

奇偶数的基本性质如下：

1、两个奇数的和（或差）是偶数，两个偶数的和（或差）是偶数，即

$$\text{奇数} \pm \text{奇数} = \text{偶数}$$

$$\text{偶数} \pm \text{偶数} = \text{偶数}$$

反之，两个整数的和或差是偶数，则这两个数或者同为奇数，或者同为偶数。

2、一个奇数与一个偶数的和（或差）是奇数，即

$$\text{奇数} \pm \text{偶数} = \text{奇数}$$

反之，两个整数的和（或差）为奇数，则这两个数一个为奇数，一个为偶数。

3、任意有限个奇数的积仍是奇数，即

$$\text{奇数} \times \text{奇数} \times \cdots \times \text{奇数} = \text{奇数}$$

反之，若有限个整数的积是奇数，则这有限个整数都是奇数。

特别，一个奇数的$n$次幂（$n$为正整数）是奇数，反之，若一个整数的$n$次幂是奇数，则这个整数是奇数。

4、若有限多个整数中至少有一个偶数，它们的积是偶数，即

$$\text{整数} \times \text{整数} \times \cdots\cdots \times \text{偶数} = \text{偶数}$$

反之，若有限多个整数的积是偶数，则这些因数中至少有一个是偶数。

以上四条性质皆可由奇偶数定义直接推出，读者自证之，下面证明第五条性质：

5、两个整数的和与差或者同为奇数，或者同为偶数。

〔证〕 设两个整数为a和b

若a、b都为奇数，由性质1知a＋b和a－b都是偶数。若a、b都是偶数，亦由性质1知a＋b和a－b都是偶数。若a、b为一奇一偶，由性质2知a＋b和a－b都是奇数。

利用奇偶数的简单性质可以解决一些看起来不是很容易的问题。

例、证明在空间中不可能有这样的多面体存在，它有奇数个面，而每个面又都有奇数个边。（北京市一九六二年中学数学竞赛题）

〔证〕 假设此多面体有k个面（k为奇数），每个面的边数分别为：$x_1$，$x_2$，……，$x_K$（$x_i$皆为奇数，i＝1，2，3，……k）

由假设知，此多面体的棱数为：

$$\frac{x_1 + x_2 + \cdots\cdots + x_K}{2}$$

因奇数个奇数的和仍为奇数，则上式不可能为整数，而多面体的棱数只能为整数，产生矛盾。

## 第 2 节　整数整除的定义和性质·带余除法定理

### 一、整除的定义

人类从古老的年代就认识了自然数集合：

$$N=\{1,\ 2,\ 3,\ \cdots,\ n,\ \cdots\}$$

显然，在自然数集合内对加法、乘法封闭。为了能做减法运算，扩充了零和负整数，从而产生整数集合：

$$Z=\{\cdots -3,\ -2,\ -1,\ 0,\ 1,\ 2,\ 3,\ \cdots\}$$

在整数集合内，可做加法、减法和乘法，即：

整数 ± 整数 = 整数

整数 × 整数 = 整数

但在Z 内不能做除法，即：

整数除整数不一定为整数

上式如果等于一个整数就叫整除，不等于一个整数就叫不能整除。研究整除的问题，例如什么是整除？整除有什么性质？整除的判别？……就成为本门学科首先遇到的一个基本问题。

整除定义如下：对于$a$，$b\in z$，$b\neq 0$，若存在$q\in z$，使$a=bq$成立，则称b整除a或a能被b 整除，记作$b\mid a$。否则，上述q不存在，称b不整除a或a不能被b整除，记作$b\nmid a$。当$b\mid a$时，b称作a的因数或约数，a称作b的倍数。

## 二、整数的性质

整数的整除有一系列性质：

1、±1 是任何整数的因数，除此再没有其它整数有此性质。0是任何整数的倍数，除此再没有其它整数有此性质。

〔证〕 $\because\ a=1\cdot a \qquad a=(-1)\cdot(-a)$

$\therefore\ \pm 1$是$a\in z$的因数

又$\because\ 0=a\cdot 0 \qquad \therefore\ 0$是任何整数的倍数。

2 、对$a\in z$，a既是它本身的因数，又是它本身的倍数（反身律）。

〔证〕 ∵ $a=1\cdot a$ ∴ 命题显然。

3、若$c|b$，$b|a$，则$c|a$（传递律）。

〔证〕 ∵ $c|b$ ∴ $b=cq_1$，（$q_1\in z$）

又∵ $b|a$ ∴ $a=bq_2$，（$q_2\in z$）∴ $a=cq_1q_2$

∴ $c|a$

利用整除的定义，还可证明：

4、若$b|a$，则$-b|a$，$b|-a$，$-b|-a$，$|b|\ |a|$

5、若$b|a$，当$a\neq0$时，则$|b|\leqslant|a|$，当 $a=0$时 则$|b|>|a|$，（可比较律）。此性质说明，任何不为零 的整数，只能有有限多个因数。

6 、若$b|a$，$c\neq0$，则$bc|ac$。对$c\in z$， 则$b|ac$。（倍律）。反之，若$bc|ac$，$c\neq0$，则$b|a$。（消去率）

7 、若$a|b$，$b|a$，则$b=\pm a$。特别当a，$b\in N$时$b=a$

8 、若$b|a$，则 $\frac{a}{b}|a$， $\frac{a}{b}$称为b的共轭因子。该性质给出了整数的一种分解式。

9 、若$b_1|a_1$，$b_2|a_2$，…，$b_n|a_n$，则 $\prod_{i=1}^{n} b_i|\prod_{i=1}^{n} a_i$。

10、若$b|a_1$，$b|a_2$，…，$b|a_n$（$n>1$），对$k_1$，$k_2$，…，$k_n\in z$，则$b|\sum_{i=1}^{n}\pm k_ia_i$（线性律）。由该性质易得：

若$a_1$，$a_2$，…$a_n$中只有一个不是b的倍数，则$b\nmid\sum_{i=1}^{n}\pm a_i$。

若 $\sum_{i=1}^{m} a_i = \sum_{j=1}^{n} b_j$，当$m+n-1$项都是整数d的倍数时，所余一项也是d的倍数。当有一项不是d的倍数时，则至少还有一项也不是d的倍数。

## 三、带余除法定理

对于a，$b\in z$，有整除关系是特殊情况。更为一般的情况是不能整除，这时a，b的关系由带余除法定理决定。

带余除法定理：设a，$b\in z$，且$b\neq 0$，则存在$q,r\in z$，使$a=bq+r$成立，其中$0\leqslant r<|b|$。这样的q、r是唯一的。q称为不完全商，简称商，r称作余数。

〔证〕 若$b>0$，b的倍数按小到大的顺序为

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

若$b<0$，则b的倍数按由小到大的次序为

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

在上两列数中：(1)a等于b的某一个倍数，即$a=qb$，此时$r=0$。(2)a介于相邻的两个倍数之间，即

$$0<a-qb=r<|b|。$$

综上可得 $a=bq+r$ 其中$0\leqslant r<|b|$

再证唯一性：设另有$q_1$，$r_1\in z$，使

$$a=bq_1+r_1 \quad 其中 0\leqslant r_1<|b|$$

$\therefore\ 0=b(q-q_1)+(r-r_1)$

$\therefore\ b|r-r_1 \quad \therefore\ |b|\leqslant|r-r_1|$

但 $0\leqslant r<|b|$，$0\leqslant r_1<|b|$

$$\therefore\ |r-r_1|=\begin{cases} r-r_1\leqslant r<|b| & 当 r\geqslant r_1 \\ r_1-r\leqslant r_1<|b| & 当 r\leqslant r_1 \end{cases}$$

$\therefore\ r-r_1=0$ 即 $r=r_1$

$\therefore q - q_1 = 0$　　即 $q = q_1$

带余除法定理的另一表达形式为：若$a, b \in z$，且 $b \neq 0$，则存在 $q, r \in z$，使 $a = bq + r$，其中$|r| \leqslant \frac{|b|}{2}$。当b是奇数时，q、r是唯一的；当b是偶数时，q、r不唯一。该命题的证明留给读者。

## 第 3 节　整数整除的判别

对于给定的两个整数，怎样判别它们有没有整除关系呢？最容易想到的办法就是除一下，除得尽就是整除，除不尽就是不能整除，对于很大的整数，这个办法显然比较麻烦。

有没有比较简单的办法去判别它们的整除关系呢？整数的整除判别有什么应用？这就是本节课所讨论的内容。

### 一、一些特殊数的整除判别

1、若一个自然数的末位数能被2（或5）整除，则此数是2（或5）的倍数。

〔证〕 ∵ $a = 10q + r$　　$0 \leqslant r < 10$

$2|10q$，$5|10q$

$\therefore$ 当$2|r$时，$2|a$；$5|r$时，$5|a$

末位数能被2除尽的有2，4，6，8，0共五类，被5除尽的有5，0两类。

2、若自然数a的末两位数能被4（或25）除尽，则此数是4（或25）的倍数。

证法同上。末两位数被4除尽的有04，08，12，…，96，00共25类，末两位数被25除尽的有25，50，75，00共四类。

3、末三位数被8（或125）除尽，则此数是8（或125）的倍数。

被8除得尽的有$\frac{1000}{8}=125$类，被125除尽的有8类。

4、奇位数的和与偶位数的和的差是11的倍数，则该数可以被11整除。

〔证〕 设 $A=a_{2K}a_{2K-1}\cdots a_2a_1a_0$

$$=a_{2K}10^{2k}+a_{2K-1}10^{2k-1}+\cdots+a_2\cdot10^2+a_1\cdot10+a_0$$

将偶位数项减去它的系数，奇位数项加上它的系数，则上式变为：

$$A=[(a_{2K}10^{2k}-a_{2K})+(a_{2k-1}10^{2k-1}+a_{2k-1})+\cdots+(a_1\cdot10+a)+(a_0-a_0)]+[(a_2+a_{2k-2}+\cdots a_2+a_0)-(a_{2k-1}+a_{2k-3}+\cdots+a_1)]$$

分析上式：先看偶数项

$$a_{2i}10^{2i}-a_{2i}=a_{2i}(10^{2i}-1)\quad 其中i=0,1,2,\cdots k$$

$$=a_{2i}\cdot\underbrace{99\cdots9}_{2i个}$$

显然被11整除。

再看奇数项：

$$a_{2i-1}10^{2i-1}+a_{2i-1}=a_{2i-1}(10^{2i-1}+1)$$

其中$i=1,2,\cdots,k$

而$10^{2i-1}+1=(10+1)(\cdots\cdots)$，显然被11整除。

∴当第二个中括号能被11整除时，则A能被11整除。

按类似方法还可证明：

5、整数a的各位数字和被3（或9）整除时，则该数是3（或9）的倍数。

## 二、截去末位数法

对于9，还有没有别的判断法呢？

例$252=25\times10+2=25\times9+(25+2)$，末位数去掉就是25，若25＋2能是9的倍数，则该数就是9的倍数。

这样，就得到另一个判别方法：截去末位数法。

1.一个整数a，其末位数截去后，加末位数的n倍，它的和能被10n－1整除时，则该数a能被10n－1整除。

［证］ 设 $a=10q+r \quad 0\leqslant r<10$

$\because a=10q+r+10nr-10nr$

$=10(q+nr)-(10n-1)r$

$\therefore$ 当$10n-1\mid q+nr$时有$10n-1\mid a$

应用这个方法可以判别一个数能否被9，19，29，39，49，……等数整除

例 判断708296能否被29整除？

［解］ 对29，n＝3

$$
\begin{array}{r}
70829\mid 6\\
+\quad 18\\
\hline
7084\mid 7\\
+\quad 21\\
\hline
710\mid 5\\
+\quad 15\\
\hline
72\mid 5\\
+15\\
\hline
8\mid 7\\
+21\\
\hline
29
\end{array}
$$

$\therefore$可被29整除。

按此证法还可得到：

2.一个整数a，截去末位数后，再减去末位数字的n倍，它

的差能被10n＋1整除时，这个数能被10n＋1整除。

用这个方法可以判别一个数能否被11，21，31，……整除。

3.一个正整数a，截去末位数后，减去这个末位数的2倍，其差能被7整除时，这个自然数能被7整除。

4.一个正整数a，截去末位数后，并加上末位数的4倍，其和能被13整除时，这个自然数能被13整除。

综上，截去末位数的方法，对于判断一个整数A能否被数P整除是一个行之有效的方法，可列表如下：

| 数A | 数P | 能被P整除的判别方法 |
|---|---|---|
| 10x＋y | 2 | y是偶数 |
| | 3 | x＋y能被3整除 |
| | 5 | y＝0或5 |
| | 7 | x－2y被7整除 |
| | 9 | x＋y被9整除 |
| | 11 | x－y被11整除 |
| | 13 | x＋4y被13整除 |
| | 17 | x－5y被17整除 |
| | 19 | x＋2y被19整除 |
| | … | …… |
| | 10n－1 | x＋ny被10n－1整除 |
| | 10n＋1 | x－ny被10n＋1整除 |

利用整除别判法，可以解决一些有趣的问题。

例若62xy427是99的倍数，求x，y？

〔解〕 由已知

$$6+2+x+y+4+2+7=9q_1$$

$$(6+x+4+7)-(2+y+2)=11q_2$$

$$\therefore \quad x+y=9q_1-21$$

$$x-y=11q_2-13$$

$$\because \quad 0\leqslant x\leqslant 9,\ 0\leqslant y\leqslant 9 \qquad \therefore \quad \begin{matrix}0\leqslant 9q_1-21\leqslant 18\\ -9\leqslant 11q_2-13\leqslant 9\end{matrix}$$

解得 $q_1=3$或4，　　$q_2=1$或2

$$\therefore \quad x+y=6\text{或}15 \qquad x-y=-2\text{或}9$$

组成四个方程

$$\begin{cases}x+y=6\\ x-y=-2\end{cases}\text{解得}\begin{cases}x=2\\ y=4,\end{cases}\qquad \begin{cases}x+y=6\\ x-y=9\end{cases}\text{解得}\begin{cases}x=\frac{15}{2}\\ y=-\frac{3}{2}\end{cases}$$

$$\begin{cases}x+y=15\\ x-y=-2\end{cases}\text{解得}\begin{cases}x=\frac{13}{2}\\ y=\frac{17}{2}\end{cases}\qquad \begin{cases}x+y=15\\ x-y=9\end{cases}\text{解得}\begin{cases}x=12\\ y=3\end{cases}$$

$\because x$，$y$皆为0～9的整数，$\therefore$仅有一组解 $\begin{cases}x=2\\ y=4\end{cases}$ 满足题意

# 第 4 节　最大公因数

第二节是研究两个整数之间的关系，当研究三个或更多个整数之间的关系时，引入了最大公因数的概念。

## 一、最大公因数定义

设$n\geqslant 2$，若$a_1$，$a_2$，…，$a_n$是不都为零的整数，当$d|a_1$，$d|a_2$，…，$d|a_n$时，d称作$a_1$，$a_2$，…，$a_n$的公因数，公因数最大者叫最大公因数，记作

$$(a_1, a_2, \cdots a_n) = d$$

## 二、最大公因数性质

最大公因数有一系列性质：

1、因为$a_1$，$a_2$，…，$a_n$的公因数也就是$|a_1|$，$|a_2|$，…，$|a_n|$的公因数，反之亦成立，所以可得性质1：若$a_1$，$a_2$，…，$a_n$是n个不全为零的整数，则〈1〉$a_1$，$a_2$，…，$a_n$和$|a_1|$，$|a_2|$，…，$|a_n|$的公因数相同。〈2〉$(a_1, a_2, \cdots, a_n) = (|a_1|, |a_2|, \cdots, |a_n|)$

有了这条性质，我们就可以只在正整数集合N中研究最大公因数。

2、若$a, b\in N$，且$a = bq + r$（$0\leqslant r < |b|$），则a，b的公因数和b，r的公因数相同，其中$q\in Z$。

〔证〕设d是a，b的公因数，则$d|a$，$d|b$，因q是整数，所以$d|bq$。由整除性质可知$d|r$，

∴　d是b，r的公因数

同理可证b，r的公因数亦为a，b的公因数

推论1：若有$a=bq+r$，则$(a, b)=(b, r)$。

推论2：

若有$a=bq+r$，则$(a\pm nb, b)=(a, b)$，其中$n\in z$。

这是一条非常重要的性质，由它可得到求最大公因数的最常用方法。

推论3，辗转相除法（Enclid除法）

设$a, b\in N$，$a>b$，则一定有

$$a=bq_1+r_1\ (0<r_1<b) \quad \cdots\ (1)$$

$$b=r_1q_2+r_2\ (0<r_2<r_1) \quad \cdots\ (2)$$

$$r_1=r_2q_3+r_3\ (0<r_3<r_2) \quad \cdots\ (3)$$

……

……

$$r_{n-3}=r_{n-2}q_{n-1}+r_{n-1}\ (0<r_{n-1}<r_{n-2}) \quad \cdots\cdots (n-1)$$

$$r_{n-2}=r_{n-1}q_n+r_n\ (r_n=0) \quad \cdots\cdots (n)$$

则$(a, b)=r_{n-1}$

〔证〕由(1)式得$(a,b)=(b,r_1)$

由(2)式得$(b,r_1)=(r_1,r_2)$

由(3)式得$(r_1,r_2)=(r_2,r_3)$

……

由$(n-1)$式得$(r_{n-3},r_{n-2})=(r_{n-2},r_{n-1})$

由$(n)$式得$(r_{n-2},r_{n-1})=r_{n-1}$

$\therefore\ (a, b)=r_{n-1}$

推论4　若$a, b\in N$，则a，b的公因数与$(a, b)$的因数相同。