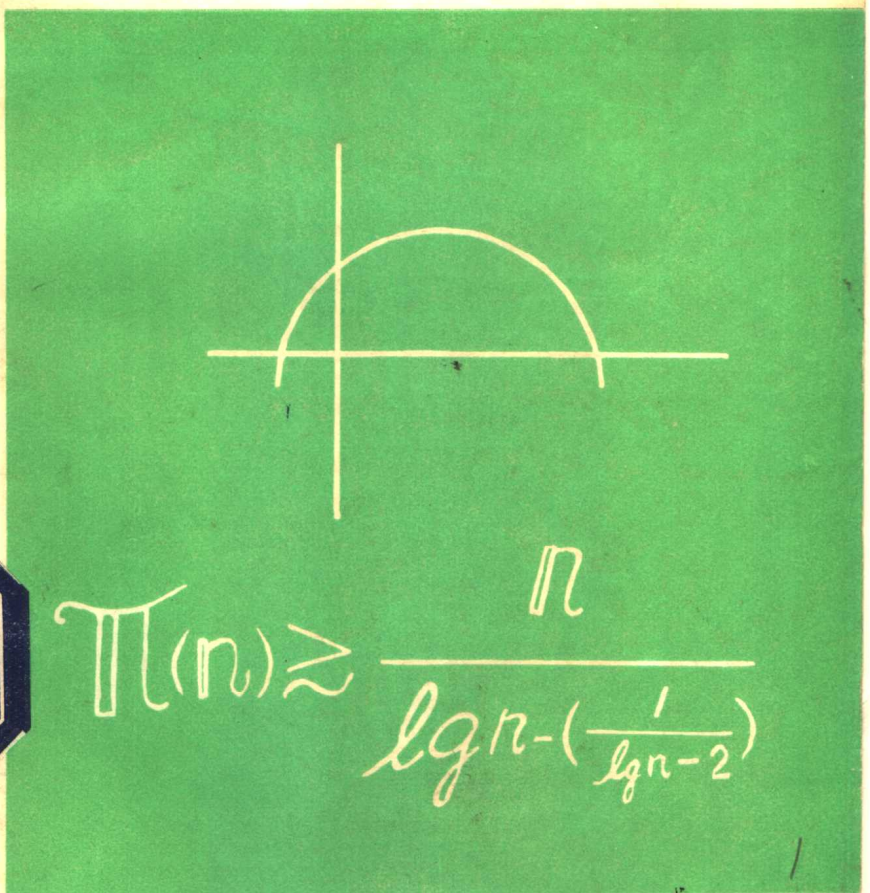
数论简易教程

郑格于著

郧阳师专学报丛书编委会编



序　言

我写这本书的目的是想用最浅显的叙述，把数论的基本知识介绍给读者，没有配备相应的习题，主要是想让读者把注意力放在弄懂基本概念和规律上，而不至于一开始就被一大堆习题耗费了精力，在懂透了道理之后，读者不仅可以自己编题，而且经过自己的刻苦探索可能会有新的发现。

至今为止，数论上仍有一大堆难题不能解决，甚至热爱数学的人也有对数论产生厌倦感的。其原因是解决数论问题的方法来得比较特殊，使初学者有不可捉摸之感。

数论的理论是比较严谨的。数学家总是这样认为，问题的解决中哪怕有一点不严密就不应当写到书本中来。我认为这样做对建立巩固的科学宝塔是必要的，但从教学和开发人的智力的角度来看，就不要把它做得太绝对了，否则会有碍于真理的发现。事物总是由不完善到完善的。一个正确的理论哪有一诞生就完美无缺的呢？

我所写的第三章质数的分布，是在质数分布密率函数存在的假定下展开的，因此这一章论证未达到完善的地步。但我仍然把它写出来，为的是想吸引读者用新的眼光来研究质数问题，唤醒人们注意过去的数学家库朗（*R.Courant*）、罗宾逊（*H.Robbins*）和赫兹（*Gustor Hertz*）曾经设想过的思想方法。

当今二十世纪数学思想中所出现的三大流派：经典数

学、统计数学和模糊数学既有矛盾也互相渗透，已经预示着在二十一世纪及其以后将会出现数学方法的重大变迁。展望到这一点，在遇到统计数学和模糊数学的观念多少和经典数学发生一些纠缠时，就会有必要的思想准备来对待它，对此不是格格不入，而是慢慢展开我们的研究，把一些没弄清楚的客观规律弄个清楚明白。

我正是本着这一观点来写这本书的，诚恳的希望这本书在发现真理的道路上能起到抛砖引玉的作用。

郑格于

1982年7月

勘 误 表

第11面第 7 行　a_0，a_2之间加上a_1

第13面倒数第 2 行　　$d|m$改正为$d|b$

第14面第13行　　$37\times27\times25$改正为 $3\times27\times25$

第15面$r_1\times t_2$，$r_2\times t_3$，$\cdots r_{n-1}\times t_n$ 均改为 $r_1'\times t_2$，$r_2'\times t_3$ $\cdots r_{n-1}'\times t$

第18面倒数第 2 行　$m_1, m_2, \cdots m_k$应改为$m_1 m_2 \cdots m_k$

第27面§ 4 之上　$\delta_1, \delta_2 \cdots \delta_k$应改为$\delta_1 \delta_2 \cdots \delta_k$

第28面第 2 行　-2，1之间加个-1

第31面*vii*所在的行　$\sum_{x-1}^{p_1}\left[\frac{2x}{p}\right]$改为 $\sum_{x-1}^{p_1}\left[\frac{ax}{p}\right]$

第39第10行　$N^{2h}a^{2h}$改为$N^{2h}a^h$

第43面倒数第 1 行　$x^{a_1b_1d}$应改为 $x^{a_1b_1d}{}_y{}^{a_1b_1d}$

第52面第 7 行$r_i\times0$改为$r_i\times10$，第 6 行再商r_i改为再商a_i

倒数第 6 行$o.a_1a_2\cdots a_{i-1}a_ia_{i+1}\cdots a_{i+k-1}$

改为$o.a_1\cdots\overset{\cdot}{a}_{i-1}\cdots a_{i-1}\overset{\circ}{a}_i\cdots\overset{\circ}{a}_{i+k-1}$

第54面倒数第 2 行$(b,10)=1$改为$(b_1,10)=1$

第55面第 1 行循环节等于改为循环节长等于

第 6 行$k_u\neq k_h$改为$k_u\neq c_h$

倒数第 1 行化成循环数改为化成纯循环小数

70

第57面第3行$\frac{5^{\alpha-\beta_\alpha}}{2b_1}$改为$\frac{5^{\alpha-\beta_\alpha}}{10b_1}$

第59面倒数第3行$\begin{pmatrix}1&1&1\\1&2&1\\1&1&2\end{pmatrix}\begin{pmatrix}i\\j\\k\end{pmatrix}$改为$\overline{\begin{pmatrix}1&1&1\\1&2&1\\1&1&2\end{pmatrix}\begin{pmatrix}i\\j\\k\end{pmatrix}}$

第63面第13行$x=3u+2t$改为$x=-3u+2t$

第64面第14行　$z=3$改为$z=-3$

第66面倒数第9行齐次不定方程的当然解。改为齐次不定方程的当然改有$(x,y,z)=(0,0,0)$

倒数第7行特别地无xyz的整数解改为$xyz\neq 0$的整数解

第86面(11)式改为$k^2+f^2=u^2$　Ⅱ$_1$及Ⅱ$_2$中的v改为u

第91面倒数第2行$z=K-1$改为$z=K+1$

第92面第5行无整数解改为无$xyz\neq 0$的整数解，定理的最末无整数解改为无x,y,z不全为0的整数解。

第102面〔推论〕改为若同余式 $C^t_{p-1}-(-1)^t\equiv 0(mod\,p)$对于$t=1,2\cdots(\sqrt{p})$都能成立则对于$t=1,2,\cdots p-1$也都成立。

第132面第3行$P>N$改为$g>N$.

目　录

第一章　基本概念

§1　整除、质数及同余

在小学算术中，人们就知道　$10=2\times5$，所以说10是2的倍数，也是5的倍数。

若用小写字母 a、b、m、x 等表示整数，则有

【定义1】若$a=bm$，就说a是b的倍数，或者说b整除a，a被b整除，b是a的约数，用符号$b\mid a$表之。

由定义1即得性质

【性质1】若$a_1+a_2+\cdots+a_k=0$，其中$k-1$项被b整除，则剩下的一项也必被b整除。

证：不失普遍性，可设$a_i=bm_i$，$i=1,2,\cdots,k-1$。

则　$$a_k=-\sum_{i=1}^{k-1}a_i=-\sum_{i=1}^{k-1}bm_i=b\left[-\sum_{i=1}^{k-1}m_i\right]$$

令　$m_k=-\sum_{i=1}^{k-1}m_i$，　则　$a_k=bm_k$

∴　a_k是b的倍数。即　$b\mid a_k$。

【性质2】给定正整数b，对于任一整数a，总可以写成　　$a=bq+r$　　$0\leqslant r<b$

且q，r是唯一确定的（当$a=bq$时，q叫做a除以b的商，当$r>0$时，q叫做不完全商，r叫做余数）。

证：设　$b=1$，则$a=ba+0$，∴$q=a$，$r=0$。若$b>1$，

4

则设 $a=bm$，此时 $q=m$，$r=0$。若a介于bm及$b(m+1)$之间，即 $bm<a<b(m+1)$，则$a=bm+(a-bm)$，此时$q=m$，$r=a-bm>0$，且$r<b(m+1)-bm=b$。 ∴ $0<r<b$。

再设 $a=bq_1+r_1=bq_2+r_2$，$0\leqslant r_i<b$，$i=1,2$。则 $b(q_1-q_2)=r_2-r_1$，于是有$b|r_2-r_1$。另一方面知$0\leqslant|r_2-r_1|<b$，∴只能 $r_2-r_1=0$，即 $r_1=r_2$，于是$q_1=q_2$，于是就证明了q及r的唯一性。

【定义 2】同时整除a_1、a_2、…、a_k的正整数a，叫做a_1、a_2、…、a_k的公约数，并用符号（a_1、a_2、…a_k）表这些公约数中的最大者。同时是a_1、a_2、…a_k的倍数的数b叫做a_1、a_2、…a_k的公倍数，用符号〔a_1、a_2、…，a_k〕表这些公倍数中的最小者。当$(a_1、a_2、\cdots、a_k)=1$时，叫a_1、a_2、…a_k是互质数，当$(a_i,a_j)=1, i\neq j$，则叫a_1、a_2、…a_k两两互质。

关于公约数，有性质

【性质 1】若 $a=bq+r$，用符号$H(a、b)$表a、b的公约数集，则有 $H(a、b)=H(b、r)$及$(a、b)=(b、r)$。

证：设 $d\in H(a、b)$，则 $d|a$，$d|b$，∴$d|bq$，∴ $d|a-bq$，∴$d|r$，∴$d\in H(b,r)$，∴$H(a,b)\subseteq H(b,r)$；反之设 $d\in H(b、r)$，则 $d|b$，$d|r$，则 $d|a$，∴$d\in H(a,b)$，∴ $H(b、r)\subseteq H(a、b)$，∴$H(a、b)=H(b、r)$。

特别地 $H(a、b)$中的最大的数与 $H(b、r)$中的最大的数相同，∴$(a、b)=(b、r)$。

【性质 2】当$b|a$时，$(a、b)=b$。

这是因为 $a=bm$，∴$(a、b)=(b、0)=b$。

【性质 3】$(a、b)$可以由下面的辗转相除法求得

设 a、b是正整数

$$
\begin{aligned}
a&=bq_1+r_0 && 0<r_0<b\\
b&=r_0q_2+r_1 && 0<r_1<r_0\\
r_0&=r_1q_3+r_2 && 0<r_2<r_1\\
&\cdots\cdots && \cdots\cdots\\
r_{n-1}&=r_nq_n+r_{n+1} && 0<r_n<r_{n-1}\\
& && r_{n+1}=0
\end{aligned}
$$

上面的过程是可以实现的，因$b>r_0>r_1>r_2>\cdots>r_n>0$是一个递降数列，必然出现$r_{n+1}=0$。于是由$H(a、b)=H(b、r_0)=H(r_0、r_1)=H(r_1、r_2)=\cdots=H(r_{n-1}、r_n)=H(r_n、r_{n+1})=H(r_n、0)=H(r_n)$，$H(r_n)$表示$r_n$的因数的集合，特别地有$(a、b)=(b、r_0)=(r_0、r_1)=\cdots=r_n$。

在实行上述辗转相除法时，最后一个不为0的余数就是$(a、b)$。

【性质4】 a、b的公约数就是a、b的最大公约数的约数。或者说a、b的公约数的集合与a、b的最大公约数的约数的集合重合。

证：上面已证得$H(a、b)=H(r_n)$

及 $r_n=(a、b)$

$\therefore$ $H(a、b)=H\big((a、b)\big)$。

以下各性质，没有证明的由读者自证。

【性质5】 $(am、bm)=(a、b)m$。

【性质6】 设c是a,b的公约数，则$\left(\frac{a}{c}、\frac{b}{c}\right)=\frac{(a、b)}{c}$。

【性质7】 $\left(\frac{a}{(a、b)}，\frac{b}{(a、b)}\right)=1$。

【性质8】 若 $(a、b)=1$，则 $(ac、b)=(c、b)$。

5

【性质9】若 $(a、b)=1$，$b|ac$，则 $b|c$。

【性质10】$(a_1a_2\cdots a_k,\ b_1b_2\cdots b_r)=1$的充要条件是 $(a_i,\ b_j)=1$，$1\leqslant i\leqslant k$，$1\leqslant j\leqslant r$。

【性质11】设d_i是a_1、a_2、…、a_i的最大公约数，则 $d_k=(d_{k-1}、a_k)$。

【性质12】$〔a、b〕(a、b)=ab$。

证：令 $(a、b)=d$，则 $a=a_1d$，$b=b_1d$。由 $\left(\frac{a}{d}、\frac{b}{d}\right)=1$，得 $(a_1、b_1)=1$。

又由 $\frac{ab}{(a、b)}=a_1b_1d=ab_1=a_1b$，∴ $\frac{ab}{(a、b)}$是a、b的公倍数；另一方面设R是a、b的公倍数，则 $R=at=bs$，于是 $\frac{a}{b}=\frac{s}{t}$，∴ $\frac{a_1d}{b_1d}=\frac{s}{t}$，∴ $\frac{a_1}{b_1}=\frac{s}{t}$。

∵ $(a_1、b_1)=1$，∴ $s=a_1k$，$t=b_1k$

∴ $R=ab_1k=a_1bk=\frac{ab}{(a、b)}k$ 是$\frac{ab}{(a、b)}$的倍数，所以R又是a、b的公倍数，在R中以 $\frac{ab}{(a、b)}$为最小，∴ $\frac{ab}{(a、b)}=〔a、b〕$，∴$〔a、b〕(a、b)=ab$。

【性质13】两个数的公倍数的集合与它们的最小公倍数的倍数的集合重合。

【性质14】n个数的公倍数的集合与它们的最小公倍数的倍数的集合重合。

【性质15】设 a_1，a_2，…，a_i的最小公倍数是d_i 则 $〔d_{k-1},\ a_k〕=d_k$。

【性质16】两两互质的数的最小公倍数等于它们的乘

积。

【定义 3 】只有 1 和本身是其约数的数叫做质数，也称素数。还有 1 和本身以外的数为其约数的数叫做合数。1 既非质数也非合数。

由定义可以推得质数的一些基本性质

【性质 1 】大于 1 的整数的约数中的 1 以外的最小约数是质数。（这可用反证法证之）

【性质 2 】合数a的不等于 1 的最小约数$\leqslant\sqrt{a}$。

证：设d是 1 以外的a的最小约数，则可写成

$$a=db \qquad 1<d\leqslant b$$

$$\therefore\ a\geqslant d^2, \qquad \therefore\ d\leqslant\sqrt{a}$$

【性质 3 】质数有无限多个。

证：设质数只有有限个p_1，p_2，…，p_k，则

$$N=p_1p_2\cdots p_k+1$$

就至少有一个p_1，p_2，…p_k以外的质约数。这显然发生矛盾。

【性质 4 】若$p|bc$，p是质数，则$p|b$或$p|c$，二者至少有其一。

证：因$(p,\ b)=1$或p，若$(p,\ b)=p$，则$p|b$。否则，必$(p,\ b)=1$，此时又推得$p|c$。

【性质 5 】每一个正整数$a>1$总可以写成唯一的标准的因子分解式

$$a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$$

其中$\alpha_i\geqslant 1$，p_i是质数，$p_1<p_2<p_3<\cdots<p_k$

证：设p_1表a的最小的质约数，$a=p_1a_1$，再依次设

6

$a_1=p_2a_2$，…，$a_i=p_{i+1}a_{i+1}$，p_{i+1}是a_{i+1}的最小质约数。由于$a>a_1>a_2>\cdots>a_i>a_{i+1}>\cdots\geqslant 1$，所以这个分解过程是有限的。∴设$a=p_1p_2\cdots p_k$。再设$a=q_1q_2\cdots q_t$，$q_i$是质数，$q_i<q_j$，$i<j$，则得$p_1p_2\cdots p_k=q_1q_2\cdots q_t$。因$p_1\mid q_1q_2\cdots q_t$，∴$p_1$必整除$q_1$，$q_2$，…$q_t$中之一，若$p_1\mid q_i$，则推出$p_1=q_i$，则$q_1$，$q_i$都是$a$的最小质约数，故必$q_i=q_1$，于是只能得出$p_1=q_1$，于是又有$p_2p_3\cdots p_k=q_2q_3\cdots q_t$，继续进行上述过程得$p_i=q_i$，且$k=t$。这就证明了分解的唯一性。再将$p_1p_2\cdots p_k$中的相同的质因子写成$p_1^{\alpha_1}$，…，最后就得标准分解式。

【性质6】设a的标准分解式为$p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$。$\alpha_i\geqslant 1$，则$a$的约数都可表成$p_1^{\beta_1}p_2^{\beta_2}\cdots p_k^{\beta_k}$，$0\leqslant\beta_i\leqslant\alpha_i$。

【性质7】设a，b是任意两个正整数，且

$$a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k},\quad b=p_1^{\beta_1}p_2^{\beta_2}\cdots p_k^{\beta_k}$$

其中 $max\{\alpha_i,\ \beta_i\}>0$，则

$$(a,\ b)=p_1^{\gamma_1}p_2^{\gamma_2}\cdots p_k^{\gamma_k},\quad [a,\ b]=p_1^{\delta_1}p_2^{\delta_2}\cdots p_k^{\delta_k}$$

$$\gamma_i=min\{\alpha_i,\ \beta_i\},\quad \delta_i=max\{\alpha_i,\ \beta_i\}$$

求一个正整数的标准分解式，必须借助于质数表，下面介绍质数表的制造。

【筛法】我们要造一个不超过N的质数表可如下进行，先划去1、2、3、4、…N中的1，第一个没有划去的数是2，故2是质数，再划去2的倍数（指4、6、8、…等），于是2后面没有划去的第一个数是3，3是质数，再划去3的倍数，位于3后未划去的第一个数是5，5是质数，再划去5的倍数，后面未划去的第一个数是7，7是质数，再划去7的倍数，位于7的后面第一个未划去的数是11。每划去一批倍数叫做过一次筛。若$\sqrt{N}$内有K个质数，在经过K

次筛选后，位于第K个质数后面第一个未划去的数必大于$\sqrt{N}$。若再进行第$K+1$次筛选，则在N内没有一个数是可以划去的，于是筛选过程就停止，所保留的数字就全是不超过N的质数，把这些数按顺序录于表中就是不超过N的质数表。

由此可见造一个较大的质数表是一个非常麻烦的工作，若在某一次筛选上出一点差错，则在以后的筛选中会带来一系列错误。

D. *N*. *Lehmer*曾造有1到10006721以内的质数表。

进一步研究不超过N的质数有多少个？也就是说经过前述的K次筛选还剩下多少个数没有筛去呢？

用〔x〕表不超过x的最大整数，如〔0.25〕$=0$，〔68.79〕$=68$，〔-4.8〕$=-5$。

用$\pi(N)$表不超过N的质数个数。

在不超过N的数中$2x$的数的个数有$\left[\frac{N}{2}\right]$个，但限定$x>1$，则此种筛去的个数为$\left[\frac{N}{2}\right]-1$，同样在$3x$的数中划去$\left[\frac{N}{3}\right]-1$个，设$\sqrt{N}$内有$K$个质数，$p_1$，$p_2$，$p_3$，…，$p_k$，则应共筛去$\sum_{i=1}^{k}\left[\frac{N}{p_i}\right]-K$个数。若某数是$2\cdot3$的倍数则划去了两次，还应补上一次，于是应补上$\left[\frac{N}{2\cdot3}\right]$个数，同理

应添上$\sum_{i\neq j}\left[\frac{N}{p_i p_j}\right]$个数，但当某一数是$p_i p_j p_t$的倍数时

(i, j, t, 互不相等)，则又应除去$\left[\frac{N}{p_i p_j p_t}\right]$个数，因

$$-C_k^1+C_k^2-C_k^3+\cdots+(-1)^r C_k^r+\cdots+(-1)^k C_k^k$$
$$=(1-1)^k-1=-1$$

所以 $$\pi(N)=N-\sum\left[\frac{N}{p_i}\right]+\sum\left[\frac{N}{p_i p_j}\right]-\sum\left[\frac{N}{p_i p_j p_t}\right]$$
$$+\cdots+(-1)^r\sum\left[\frac{N}{p_{i1}p_{i2}p_{i3}\cdots p_{ir}}\right]+K-1 \quad (1)$$

其中$K=\pi\left(\sqrt{N}\right)$。

在(1)中若假定$N=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$是$N$的标准分解式，则$\left[\frac{N}{p_i}\right]$, $\left[\frac{N}{p_i p_j}\right]$等项都可依次去掉外面的方括号，并且将后面的$K-1$去掉，则(1)的左端变成不超过$N$的且与$N$互质的数的个数。此时用$\varphi(N)$表示这一和数(人们称它为欧拉($Euler$)函数)。

即 $$\varphi(N)=N-\sum\frac{N}{p_i}+\sum\frac{N}{p_i p_j}-\cdots$$
$$+(-1)^r\sum\frac{N}{p_i p_j\cdots p_r}+\cdots+(-1)^k\frac{N}{p_1 p_2\cdots p_k}$$
$$=N\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\cdots\left(1-\frac{1}{p_k}\right)$$

欧拉函数的性质：若$(a,\ b)=1$，则 $\varphi(a,\ b)=\varphi(a)\varphi(b)$。

证：设 $a=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$，$b=q_1^{\beta_1}q_2^{\beta_2}\cdots q_t^{\beta_t}$

$\because$ $(a,\ b)=1$，故p_i与q_j没有相同的

$\therefore$ $ab=p_1^{\alpha_1}\cdots\cdots p_k^{\alpha_k}q_1^{\beta_1}\cdots\cdots q_t^{\beta_t}$

$$\therefore\quad \varphi(a,\ b)=p_1^{\alpha_1}\cdots p_k^{\alpha_k}q_1^{\beta_1}\cdots q_t^{\beta_t}\left(1-\frac{1}{p_1}\right)\cdots\cdots$$

$$\left(1-\frac{1}{p_k}\right)\cdot\left(1-\frac{1}{q_1}\right)\cdots\cdots\left(1-\frac{1}{q_t}\right)$$

$$=p_1^{\alpha_1}\cdots p_k^{\alpha_k}\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_k}\right)\cdot q_1^{\beta_1}\cdots q_t^{\beta_t}$$

$$\cdot\left(1-\frac{1}{q_1}\right)\cdots\cdots\left(1-\frac{1}{q_t}\right)$$

$$=\varphi(a)\varphi(b)$$

设$F(x)$对于所有的正数x都有定义，且至少对于一个这样的x它不等于0，在$(x,y)=1$时$F(xy)=F(x)F(y)$，这样的函数叫做可乘函数。所以欧拉函数是可乘函数。

【定义4】若$a-b$被m整除，则说a与b对模m同余，并写成$a\equiv b(\mathrm{mod}\,m)$，这种式子叫同余式，我们有定理

【定理】$a\equiv b(\mathrm{mod}\,m)$的充要条件为下列条件之一：

i) a可以写成 $a=mt+b$

ii) a与b被m除时，所得的余数相同。

证：由 $a\equiv b(\mathrm{mod}\,m)\rightleftarrows a-b=mt\rightleftarrows a=b+mt$。

又 $a\equiv b(\mathrm{mod}\,m)\rightleftarrows a-b=mt$

设 $a=mt_1+r_1$，$b=mt_2+r_2$，则有$m(t_1-t_2)+r_1-r_2$

$=mt$, $\therefore m|r_1-r_2$，由 $0\leq r_1<m$, $0\leq r_2<m$ 得 $r_1-r_2=0$。

$\therefore$ $r_1=r_2$；反之若 $r_1=r_2$，则 $a-b=m(i_1-t_2)$,

$\therefore$ $m|a-b$, $\therefore$ $a\equiv b(modm)$。

同余式有下列性质：

1、若 $a\equiv b(modm)$, $b\equiv c(modm)$, 则 $a\equiv c(modm)$。

2、若 $a_i\equiv b_i(modm)$, 则 $\sum a_i\equiv\sum b_i\ (modm)$。

3、若 $a\equiv b\ (modm)$, $c\equiv d\ (modm)$, 则 $ac\equiv bd\ (modm)$。

4、若 $S_1=\sum A_{\alpha_1\alpha_2\cdots\alpha_k}x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_k^{\alpha_k}$

$$S_2=\sum B_{\alpha_1\alpha_2\cdots\alpha_k}y_1^{\alpha_1}y_2^{\alpha_2}\cdots y_k^{\alpha_k}$$

其中 $x_i\equiv y_i$, $A_{\alpha_1\alpha_2\cdots\alpha_k}\equiv B_{\alpha_1\alpha_2\cdots\alpha_k}\ (modm)$

则 $S_1\equiv S_2\ (modm)$。

5、若 $a\equiv b\ (modm)$, $p|(a,\ b)$, $(p,\ m)=1$.

则 $\frac{a}{p}\equiv\frac{b}{p}(modm)$。

6、若 $a\equiv b\ (modm)$, 则 $ka\equiv kb\ \ (mod\ km)$

7、若 $a\equiv b\ (modm)$, $d|(a,\ b,\ m)$,

则 $\frac{a}{d}\equiv\frac{b}{d}\ \ \left(mod\ \frac{m}{d}\right)$。

8、若 $a\equiv b\ (mod\ m_i)\ i=1,\ 2,\ \cdots,\ k$

则 $a\equiv b\ \ (mod[m_1,\ m_2,\ \cdots,\ m_k])$。

9、若 $a\equiv b\ (mod\ m_1)$, $a\equiv b\ (mod\ m_2)$, $(m_1,\ m_2)=1$, 则 $a\equiv b\ \ (mod\ m_1m_2)$。

10、若 $a\equiv b\ (mod\ m_1m_2)$，则 $a\equiv b\ (mod\ m_i)$，$i=1,\ 2$。

11、若 $a\equiv b\ (mod m)$，$d|a$，$d|m$，则$d|b$。

12、若 $a\equiv b\ (mod m)$，则 $(a,\ m)=(b,\ m)$。

以上性质读者自证。

【定义5】 0，1，2，…，$m-1$叫做模m的最小完全剩余系，a_0，a_2，…，a_{m-1}叫做模m的完全剩余系，其中 $a_i\not\equiv a_j\ \ (i\neq j)\ (mod m)$。若又有$|a_i|\leqslant \frac{m}{2}$，则它叫做模$m$的绝对最小剩余系。

【定理】若$(a,\ m)=1$，x通过模m的完全剩余系，则 $ax+b$也通过模m的完全剩余系。

证：设 $ax_i+b\equiv ax_j+b\ \ (mod m)$

则 $a(x_i-x_j)\equiv 0\ \ \ (mod m)$

$\because\ \ (a,\ m)=1,\ \therefore\ \ m|x_i-x_j$

$\therefore\ \ x_i\equiv x_j\ (mod m)$

故 $x_i\not\equiv x_j(mod m)$时必有 $ax_i+b\not\equiv ax_j+b\ \ (mod m)$

$\therefore\ \ ax+b$ 当x通过模m的完全剩余系时也随着通过模m的完全剩余系。

【定义6】 b_1，$b_2\cdots$，$b_{\varphi(m)}$叫做模m的简化剩余系，其中 $b_i\not\equiv b_j\ (mod m)$ 且 $(b_i,\ m)=1$。

显然在 0，1，2，…，$m-1$中有且只有$\varphi(m)$个数是与模m互质的。这$\varphi(m)$个数组叫做模m的最小简化剩余系。

【定理】若 $(a,\ m)=1$，则当x通过模m的简化剩余系时，$ax+b$也通过模m的简化剩余系。

证：$\because\ (a,\ m)=1$，$(x,\ m)=1$，$\therefore\ (ax,\ m)=1$，