信息安全数学基础
整数理论(数论讲义第一章)

同济大学
杨礼珍

作业

- 阅读《数论讲义》上册第一章的1-6、8-9节。
- 阅读《密码学原理与实践》第5章中的欧几里得算法和扩展欧几里得算法的介绍。
- 作业：
  - 数论讲义第一章习题1、2、3、5、8、18、24、34。
  - k2.1：用欧几里得算法计算gcd(1245,233),gcd(189,211)
  - k2.2：用扩展欧几里得算法计算782^{-1}mod 1895

符号

- Z： 整数集合
- Z^+： 正整数集合

§1 整数性

- 定义： $\forall a,b\in Z$，其中$b\neq 0$，如果$\exists q\in Z$满足

$$a=bq \tag{1}$$

就说b整除a，记作$b|a$，此时把b叫做a的因数（或因子），把a叫做b的倍数。如果(1)中的整数q不存在，则说b不整数a，记作$b\nmid a$。

- 由整除的定义，容易证明以下性质.
  1. 传递性：如果$c|b, b|a$, 则$c|a$.
  2. 如果$b|a$，则$cb|ca$.
  3. 如果$c|a, c|b$，则对$\forall m,n\in Z$，有$c|ma+nb$
  4. 如果$b|a$且$a \neq 0$，则$|b|\leq|a|$.
  5. 如果$cb|ca$， $c\neq 0$，则$b|a$.
  6. 如果$b|a$，$a \neq 0$，则$a/b|a$.

- 由性质2、5得到：如果$c \neq 0$，则$b|a$当且仅当$cb|ca$.
- 由性质3可得到：$c|a+b, c|a$，则$c|b$（性质7）.
- 整除的基本性质的应用：
  - 后面的证明中反复应用到，需熟练应用。
  - 例：
    - 习题3. 证明：若$m-p|(mn+qp)$，则$m-p|(mq+np)$.（提示：应用性质3）
    - 习题4. 若$p|(10a-b)$和$p|(10c-d)$，则$p|(ad-bc)$.（提示：应用性质3）
    - 习题7. 证明：若方程$x^n+a_1x^{n-1}+\dots+a_n=0$($n>0$，$a_i$是整数，$i=1,\dots,n$)有有理数解，则此解必为整数.（提示：设$x=u/v$，u、v互素。应用性质7证明$v|u$）
    - 习题14.证明：对于同样的整数x和y，$17|2x+3y$的充分必要条件是$17|9x+5$7（提示：应用性质3）

- 定理1（带余除法） 设$a,b \in Z$，其中$b>0$，则唯一$\exists q,r \in Z$，满足下式

$$a=bq+r,\ 0 \le r<b \qquad (2)$$

证明：(1)存在性：作整数序列

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

则a必在上述序列的某两项之间，即$\exists q \in Z$使得$qb \le a<(q+1)b$成立.令$a-qb=r$，则(2)成立。

(2)唯一性：设q_1,r_1是满足(2)的另一对整数。

因为 $b q_1+r_1=bq+r$，

于是 $b(q-q_1)=r_1-r$，

故 $b|q-q_1|=|r_1-r|$。

因为$0 \le r_1,r<b$，所以$|r_1-r|<b$，必有$q-q_1=0$（否则$b|q-q_1|\ge b$，导出矛盾！）

- $a=bq+r,\ 0\leq r<b$ (2)

定义：把(2)中的q叫做a被b除得到的不完全商，r叫做a被b除所得到的余数（或非负最小剩余），记作**a mod b=r**（《数论讲义》中记为$\langle a\rangle_b=r$）

定理1的应用：

- 在证明中，对正整数k，对任意整数n可设 $n=km+r$， $0 \le r<k$，这对证明可能是便利的。
- 例：
  - 习题1：证明 $6|n(n+1)(2n+1)$，其中n是任何整数。（提示：设 $n=6q+r$，$r=0,1,2,3,4,5$）
  - 习题2：证明：任意n个连续整数中($n\ge1$)，有一个且只有一个数被n除尽.（提示：设第一个数是 $m=nq+r$， $0 \le r<n$）
  - 习题15. （提示：设 $m=5u+r$，则 $1 \le r \le 4$）

定理2 对$a_1,a_2,b \in Z$，其中$b>0$，有

$$(a_1+a_2)\bmod b = (a_1 \bmod b + a_2 \bmod b)\bmod b \quad (3)$$

$$(a_1-a_2)\bmod b = (a_1 \bmod b - a_2 \bmod b)\bmod b \quad (4)$$

$$(a_1a_2)\bmod b = (a_1 \bmod b \cdot a_2 \bmod b)\bmod b \quad (5)$$

证明：设$a_1=bq_1+a_1 \bmod b$, $a_2=bq_2+a_2 \bmod b$，

$a_1 \bmod b+a_2 \bmod b=bq_3+(a_1 \bmod b+a_2 \bmod b)\bmod b$.故

$$a_1+a_2=b(q_1+q_2)+a_1 \bmod b+ a_2 \bmod b$$

$$=b(q_1+q_2+q_3)+(a_1 \bmod b+ a_2 \bmod b)\bmod b$$

由定理1，即得到(3)式。类似地可证（4）和（5）.

定理2的应用：

- 用于提高计算速度。
- 例：
  - 计算：$(3\times 100+69)\bmod 5$
  - 解答：因为100mod5=0，69mod6=3。因此$(3\times 100+69)\bmod 5=(3\times 0+3)\bmod 5=3$

§2 最大公因式与辗转相除法(或欧几里得算法)

- 定义：设$a_1, a_2,\ldots,a_n \in Z$且不全为0. 若$d|a_1$, $d|a_2,\ldots,d|a_n$,那么d就叫做$a_1, a_2,\ldots,a_n$的一个**公因数(或公因子)**，它们的公因数中最大的一个叫做**最大公因数**，记作**$\gcd(a_1, a_2,\ldots,a_n)$，或$(a_1, a_2,\ldots,a_n)$**。若$(a_1, a_2,\ldots,a_n)=1$则称$a_1, a_2,\ldots,a_n$ **互素**。
- **性质*：** $(a/(a,b),b/(a,b))=1.$ （由定义可证明）
- **由性质*可设**$a=ku$，$b=kv$，其中$k=(a,b)$，$(u,v)=1$

- 应用例子：
  - 练习21. 证明：若$a>0,b>0$，$a'>0,b'>0$，$(a,b)=d,(a',b')=d'$，则$(aa',ab',ba',bb')=dd'$．(提示：设$a=du,b=dv$，$(u,v)=1$；$a'=d'u',b'=d'v'$，$(u',v')=1$）

- **定理1** 设a,b,c $\in$Z 且不全为0，且a=bq+c，q $\in$Z，则(a,b)=(b,c)。

证明： 因为(a,b)|a, (a,b)|b，所以有(a,b)|c，因而(a,b) ≤(b,c)。同法可证(b,c) ≤(a,b)。于是得到(a,b)=(b,c)。

- **辗转相除法（或欧几里得算法）、扩展欧几里得算法：** 见《密码学原理与实践》第五章.课件见《公钥密码学数学基础》
- 欧几里德算法是多项式时间算法，可见练习38.

- **欧几里德算法和扩展欧几里德算法的应用：**
  - 计算gcd(a,b)、a^{-1}modn
  - 证明两整数互素、两整数的最大公约数。例：
    - 习题：5、6、24、35、37
    - 本章第6节的引理和定理2的证明（课本对定理2的证明没有应用欧几里德算法）

例. §6 引理：设$a>0$，$b>0$，$s>1$，则$(s^a-1, s^b-1)=s^{(a,b)}-1$.

证明：自行看P14的证明。

例. §6 定理2：把$F_n={}_22^n+1$，$n \geqslant 0$，叫做费马数。任给两个费马数F_m，F_n，$m \neq n$，则

$$(F_m, F_n)=1.$$

证明：不失一般性，可设$m>n\geq 0$，$m=n+k$，$k>0$.如果令$x={}_22^n$，我们有

$$(F_{n+k}-2)/F_n=({}_22^{n+k}-1)/({}_22^n+1)$$

$$=({}_x2^k+1)/(x+1)={}_x(2^k-1)-{}_x(2^k-2)+\ldots-1,$$

故$F_{n+k}=({}_x(2^k-1)-{}_x(2^k-2)+\ldots-1)F_n+2$,

则$(F_{n+k},F_n)=(F_n,2)=1.$

由欧几里德算法立即得到：

定理3：若任给两不全为0的整数a,b，则$\exists m,n \in Z$使得

$$\gcd(a,b)=ma+nb.$$

另一非构造性证明（用带余除法证明）：设

$I=\{sa+tb|s,t\in Z\}$.则 $I\neq\{0\}$，令d为I中最小正整数，作为I的成员，有整数m和n使得$d=ma+nb$.

以下证明对任意$c=sa+tb$有$d|c$. 由带余除法，$c=qd+r$，其中$0 \leq r < d$. 如果$r\neq 0$，则$r=c-qd \in I$，与d是最小正整数相矛盾。因此$d|c$.

特别地$d|a$，$d|b$，则$d|(a,b)$.

另一方面$(a,b)|b,(a,b)|a$，因此$(a,b)|ma+nb=d$.

综上诉述，$(a,b)=d$.

- 由定理3的带余除法证明可得：$I=\{sa+tb|s,t\in Z\}=(d)$，$d=(a,b)$，(d)指d的一切倍数的集合。
- 以上结论的应用：
  - 练习18. 证明：若a,b是任意两个不全为0的整数，m为任一正整数，则$(am,bm)=(a,b)m$.
  - §8定理1：

§8 定理1：二元一次不定方程是指

$$a_1x+a_2y=n \qquad (1)$$

其中$a_1,a_2,n\in Z$，$a_1,a_2\neq 0$.

方程(1)有整数解x,y的充分必要条件是$(a_1,a_2)|n$.

由定理3得到以下2个推论：

推论1：a和b的公因数是(a,b)的因数.

定理4：若$a|bc$，$\gcd(a,b)=1$，则$a|c$.

证明：

（1）若$c\neq0$，由$\gcd(a,b)=1$知$\exists m,n\in Z$使得 $ma+nb=1$，故$mac+nbc=c$，由$a|bc$，知$a|c$。

（2）若$c=0$，结论显然成立。

- 定理4的应用：
  - 习题8.
  - 习题16. 提示：应用定理4及$(a/(a,b),b/(a,b))=1$
- 推论1的应用：
  - 习题11. 给定x和y，若$m=ax+by,n=cx+dy$，这里$ad-bc=\pm1$，证明$(m,n)=(x,y)$.
  - 习题19. 证明$(a_1,a_2,\ldots,a_n)=((a_1,\ldots,a_s),(a_{s+1},\ldots,a_n))$.
  - 下面的定理5

- **定理5**：设$a_1, a_2,\ldots,a_n \in Z^+$ (n>2)，且
$(a_1, a_2)=d_2$, $(d_2, a_3)=d_3$,…, $(d_{n-1},a_n)=d_n$, 则

$$(a_1, a_2,\ldots,a_n)= d_n$$

证明：（数学归纳法）n=3时，由$(a_1, a_2)=d_2$ 可得$d_2|a_1,d_2|a_2$。由 $(d_2, a_3)=d_3$可得$d_3|d_2$。根据整数的传递性有$d_3|a_1,d_3|a_2$。由$(d_2, a_3)=d_3$还可得$d_3|a_3$。综上所得d_3是a_1,a_2,a_3的因子，那么$d_3 \le (a_1, a_2,a_3)$。

另一方面，设$(a_1, a_2,a_3)=d$。则d是a_1,a_2的因数，又$(a_1, a_2)=d_2$，由推论1可得$d|d_2$。

由d的定义有d是a_3的因数，所以d是d_2,a_3的因数。又$(d_2, a_3)=d_3$,根据推论1同理可得$d|d_3$。故$d \le d_3$.

于是得到$(a_1, a_2,a_3)= d_3$.

假设n≥3时结论成立。用同样的方法可以证明n+1时也成立（略）。

定理5的课本证明：由$d_n|a_n$, $d_n|d_{n-1}$, $d_{n-1}|a_{n-1}$, $d_{n-1}|d_{n-2}$,可得$d_n|a_{n-1}$, $d_n|d_{n-2}$.

由此类推，最后得到

$$d_n|a_n,\ d_n|a_{n-1},\dots,\ d_n|a_1,$$

因此有$d_n \le (a_1, a_2,\dots,a_n)$.

另一方面，设$(a_1, a_2,\dots,a_n)=d$，由推论1可得

$$d|d_2,\ d|d_3,\dots,\ d|d_n,$$

故$d \le d_n$. 于是得到$(a_1, a_2,\dots,a_n)= d_n$

- 由定理5可推出

定理6：设$a_1, a_2,\ldots,a_n \in Z^+$ (n>2)，则∃ $x_1, x_2,\ldots,x_n \in Z$ 满足

$$(a_1, a_2,\ldots,a_n)=a_1 x_1+a_2x_2+,\ldots,a_nx_n$$

§3 最小公倍数

- **定义**：设$a_1, a_2,\ldots,a_n \in Z$，若m是这n个整数中的每一个数的倍数，则m称为这n个整数的一个公倍数。在$a_1, a_2,\ldots,a_n$的一切公倍数中最小的正整数叫做最小公倍数，记作$[a_1, a_2,\ldots,a_n]$（或者$\mathrm{lcm}(a_1, a_2,\ldots,a_n)$）

1. **最小公倍数存在**：$|a_1||a_2|\ldots|a_n|$是$a_1, a_2,\ldots,a_n$的一个公倍数，说明$a_1, a_2,\ldots,a_n$的公倍数集合不为空，根据非空自然数集合存在最小数的公理知道最小公倍数存在。
2. 显然$[a_1, a_2,\ldots,a_n]=[|a_1|,|a_2|,\ldots,|a_n|]$，**因此下面只限于讨论正整数的最小公倍数。**

定理1：设a,b $\in Z^+$，则

1. a,b的所有公倍数就是[a,b]的所有倍数。
2. [a,b]=ab/(a,b)

证明：设m是a,b的任一公倍数，m=ak=bk′，令 $a=a_1(a,b), b=b_1(a,b)$，代入ak=bk′得 $a_1k=b_1k'$，因为 $(a_1,b_1)=1$，故 $b_1|k$。因而存在整数t满足等式 $k=b_1t$。因此

$$m=ak=ab_1t=t\times ab/(a,b) \qquad (1)$$

反之，当t为任一整数时，t×ab/(a,b)为a,b的一个公倍数，故(1)可以表示a,b的一切公倍数。令t=1，即得到最小的正数，故[a,b]=ab/(a,b)，这便证明了定理1中的2。又由（1）式定理中的1也得证。

定理2：设$a_1, a_2,\dots,a_n \in Z^+$ (n>2)，且

$$[a_1, a_2]=m_2 ,[m_2, a_3]=m_3 ,\dots, [m_{n-1},a_n]=m_n, \quad (2)$$

则

$$[a_1, a_2,\dots,a_n]=m_n \quad (3)$$

证明：由(2)知$m_i \mid m_{i+1}$，i=2,3,...,n-1，且$a_1\mid m_2$，$a_i\mid m_i$，i=2,...,n，故m_n是$a_1, a_2,\dots,a_n$的一公倍数。

又设m是$a_1, a_2,\dots,a_n$的任一公倍数，则$a_1\mid m$，$a_2\mid m$，故由定理1知$m_2 \mid m$，又$a_3\mid m$，同理可得$m_3 \mid m$.依此类推，最后得$m_n \mid m$，因此$m_n\le|m|$，故(3)成立。

- 本节相关应用：
  - 习题20. 证明$[b_1,\ldots,b_n]=[[b_1,\ldots,b_s],[b_{s+1},\ldots,b_n]]$.

§4 素数、整数的惟一分解定理

- **定义**：一个大于1的整数，如果它的正因子只有1和它本身，就叫做**素数**，否则就叫做**合数**。

引理1：设a是任一大于1的整数，则a的除1以外的最小正因数q是素数，并且当a是合数时，

$$q \le \sqrt{a}$$

证明：假定q不是素数，由定义，q除1和它本身以外还有一正因数q_1，因而$1<q_1<q$，但q|a，所以有$q_1|a$，这与q是最小正因数矛盾，故q是素数。

当a是合数时，$a=a_1q$，且$q \le a_1$，故$q \le \sqrt{a}$

引理2：若p是素数，a是整数，则有p|a或(p,a)=1。

证明：因为(p,a)|p，故(p,a)=1或(p,a)=p，后者即p|a。

引理3：若p是素数，p|ab，则p|a或p|b.

证明：若p∤a，则由引理2，(p,a)=1，再由§2的定理4知p|b.

定理（**整数的惟一分解定理**）：任一大于1的整数能表成素数的乘积，即对于任一整数a>1，有

$$a=p_1p_2\ldots p_n\ ,\quad p_1 \le p_2 \le \ldots \le p_n \qquad (1)$$

其中$p_1, p_2, \ldots, p_n$是素数，并且若

$$a=q_1q_2\ldots q_m\ ,\quad q_1 \le q_2 \le \ldots \le q_m \qquad (2)$$

其中$q_1, q_2, \ldots, q_n$是素数，则$m=n$, $p_i=q_i$ $(i=1,2,\ldots,n)$.

证明：（1）存在性：用数学归纳法证明(1)式成立。当$a=2$时(1)式显然成立。假定对于一切小于a的正整数(1)式都成立。此时，若a是素数，则(1)式对a成立；若a是合数，则$\exists b,c\in Z^+$有$a=bc$，

$$1<b\le c<a,$$

由归纳假设，b, c分别能表示成素数的乘积，故a能表成素数的乘积，即(1)式成立。

定理（整数的惟一分解定理）：任一大于1的整数能表成素数的乘积，即对于任一整数a>1，有

$$a=p_1p_2\ldots p_n，\ p_1\le p_2\le\ldots\le p_n \qquad (1)$$

其中$p_1,p_2,\ldots,p_n$是素数，并且若

$$a=q_1q_2\ldots q_m，\ q_1\le q_2\le\ldots\le q_m \qquad (2)$$

其中$q_1,q_2,\ldots,q_n$是素数，则$m=n$, $p_i=q_i$ $(i=1,2,\ldots,n)$.

证明：（2）惟一性：若对a同时有(1)(2)式成立，则

$$p_1p_2\ldots p_n=q_1q_2\ldots q_m， \qquad (3)$$

由引理3知有p_k，q_j使得$p_1|q_j$，$q_1|p_k$，但p_k，q_j都是素数，所以$p_1=q_j$，$q_1=p_k$。又$p_k\ge p_1$，$q_j\ge q_1$，故同时有$q_1\ge p_1$，$p_1\ge q_1$，因而$p_1=q_1$，由(3)式得到$p_2\ldots p_n=q_2\ldots q_m$。同理可得$p_2=q_2$，$p_3=q_3$，依此类推，最后得$m=n$，$p_n=q_n$。

- 算数基本定理说明，$\forall a \in Z$，a>1能够惟一地写成

$$a=p_1^{\alpha_1}\ldots p_k^{\alpha_k},\ \alpha_i>0\ \ (i=1,\ldots,k), \qquad (8)$$

其中$p_1<p_k(i<j)$是素数。(8)式称为a的标准分解式。

- 标准分解式的应用：设a,b>0，且

$$a=p_1^{\alpha_1}\ldots p_k^{\alpha_k},\ \alpha_i\geq 0\ \ (i=1,\ldots,k),$$
$$b=p_1^{\beta_1}\ldots p_k^{\beta_k},\ \beta_i\geq 0\ \ (i=1,\ldots,k),$$

则

$$(a,b)=p_1^{\gamma_1}\ldots p_k^{\gamma_k},\ \gamma_i=\min(\alpha_i,\beta_i)\ (i=1,\ldots,k)$$
$$[a,b]=p_1^{\delta_1}\ldots p_k^{\delta_k},\ \delta_i=\max(\alpha_i,\beta_i)\ (i=1,\ldots,k)$$

标准分解式的应用例子

- 给出$[a,b]=ab/(a,b)$的另一证明.
- 习题25：证明：若$m>0$，$n>0$，$(m,n)=1$，方程$x^m=y^n$的全部解可以由$x=t^n$，$y=t^m$给出，其中t取任意整数。
- 习题9、10、12、13、17、29

素数定义改变后，惟一分解定理未必成立。

- 例：在自然数的子集

$$S=\{3k+1|k=0,1,2,...\}$$

中，如果定义其“素数”是恰有两个因子在S中

例如4,710,13,19,22,25,31,...都是S中的“素数”

那么S中的数100就有两种分解形式：

$$100=4\times25=10\times10$$

- 其它例子：习题28

§5 厄拉多塞筛法

- **厄拉多塞筛法**：
  - 古希腊数学家厄拉多塞提出的造出不超过N的素数表的方法。
  - 先列出不超过$\sqrt{N}$的全部素数，设为$2=p_1<p_2<\cdots<p_k\leq\sqrt{N}$，然后依此排列$2, 3, \cdots, N$，然后留下$p_1=2$，而把$p_1=2$的倍数删掉，再留下$p_2$，而把$p_2$的倍数删掉，…，留下$p_k$，而把$p_k$的倍数删掉

~~1~~	2	3	~~4~~	5	~~6~~	7	~~8~~	~~9~~	~~10~~
11	~~12~~	13	~~14~~	~~15~~	~~16~~	17	~~18~~	19	~~20~~
~~21~~	~~22~~	23	~~24~~	~~25~~	~~26~~	~~27~~	~~28~~	29	~~30~~
31	~~32~~	~~33~~	~~34~~	~~35~~	~~36~~	36	~~38~~	~~39~~	~~40~~
41	~~42~~	43	~~44~~	~~45~~	~~46~~	47	~~48~~	~~49~~	~~50~~
~~51~~	~~52~~	53	~~54~~	~~55~~	~~56~~	~~57~~	~~58~~	59	~~60~~
61	~~62~~	~~63~~	~~64~~	~~65~~	~~66~~	64	~~68~~	~~69~~	~~70~~
71	~~72~~	73	~~74~~	~~75~~	~~76~~	~~77~~	~~78~~	79	~~80~~
~~81~~	~~82~~	83	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	89	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	97	~~98~~	~~99~~	~~100~~

定理1（Euclid第二定理）： 素数的个数是无穷的.

证明1：反证法。如果素数的个数是有限的，那么设 $p_1=2, p_2=3\cdots p_k$是全体素数。再设

$P=p_1p_2\ldots p_k+1$，q是P的素因数，

则有$q\neq p_j(j=1,\cdots,k)$. 因为$(P,p_j)=1$，则$(q,p_j)=1$。于是与$p_1,p_2,\cdots,p_k$是全体素数矛盾。

证明2：我们在§2证明了§6的定理2：两个不同的费马数 $F_n=2^{2^n}+1$、 $F_m=2^{2^m}+1$互素。那么每个费马数的素因子互素，且有无穷个费马数，因此存在无穷多个素数。

- **定理2**：存在无穷个形如4n-1的素数

证明：类似定理1的证明1。反证法。假设这样的素数是有限的，设p是它们中的最大值。构造整数

$N=2^2\cdot3\cdot5\cdot\ldots\cdot p-1$，（$3\cdot5\cdot\ldots\cdot p$表示所有≤p的奇素数乘积）

1）N与所有≤p的素数互素，所以它的素因数>p。

2）N是4n-1形的。

3）N的素因数不是4n+1形的就是4n-1形的（因为其它形的整数4n形和4n+2形都不是素数）。如果N的素因数不包含4n-1形的，那么全部是4n+1形的，但任意两个4n+1形的整数的乘积仍然是4n+1形的，与N为4n-1形矛盾！因此N必然包含一个4n-1形的素因数。

使用Euclid第二定理的证明方法，可以证明以下练习，这里留给同学们思考。

例1(练习34)：证明若p_n表示第n个素数，则$p_n<2^{2^{\wedge}n.}$ (2^n表示2^n)

提示：用归纳法。由Euclid定理的证明可知$p_{n+1}\le p_1p_2\ldots p_n+1$.

例2：证明存在无穷个形如3n-1的素数

提示：类似于定理2的证明构造3n-1形的N.

- 一般地，设k>0,l>0那么形如kn+l的素数有无穷个（狄利克来定理）.
- 很难找到表示素数的一般公式。如以下定理给出了其中一个否定答案。

定理3：对于任意给定的整数x_0，不存在整系数多项式

$f(x)=a_nx^n+a_{n-1}x^{n-1}+\dots+a_1x+a_0(a_n\neq 0,n>0)$，

使得对∀整数 $x\geq x_0$，$f(x)$都表示素数。

证明：设$f(x_0)=p$是一个素数，对于整数y，有

$f(x_0+py)-f(x_0)=pM$(代入f的表达式展开可得)，

即 $f(x_0+py)=p(M+1)$，

当y充分大时，$|f(x_0+py)|$趋向于无穷大。因此对于充分大的y，$|M+1|>1$，这时$f(x_0+py)$不是素数。

§8 一次不定方程

- 二元一次不定方程是指

$$a_1x+a_2y=n \qquad (1)$$

其中$a_1,a_2,n \in Z$，$a_1,a_2 \neq 0$.

定理1：方程(1)有整数解x,y的充分必要条件是 $(a_1,a_2)|n$.

证明：由$I=\{sa+tb|s,t\in Z\}=(d)$易证，$d=(a,b)$，(d)指d的一切倍数的集合。

$$a_1x+a_2y=n \qquad (1)$$

其中$a_1,a_2,n\in Z$，$a_1,a_2\neq 0$.

定理2：设$(a_1,a_2)=1$，则(1)的全部解可表为

$$x=x_0+a_2t,\ y=y_0-a_1t\ , \qquad (3)$$

其中x_0, y_0为(1)的一组解，t为任意整数。

证明：必要性：设t为任意整数，把(3)代入(1)得

$$a_1(x_0+a_2t)+a_2(y_0-a_1t)=a_1x_0+a_2y_0=n,$$

故t为任意整数时，(3)均为(1)的解.

充分性：设x_1,y_1为(1)的任意一组解，由

$$a_1x_1+a_2y_1=n,\quad a_1x_0+a_2y_0=n$$

可得 $a_1(x_1-x_0)+a_2(y_1-y_0)=0$,

因$(a_1,a_2)=1$，所以$a_2|x_1-x_0$，可设$x_1-x_0=a_2t$，即$x_1=x_0+a_2t$，故得$y_1=y_0-a_1t$.

§8 一次不定方程

- 定理3 设s≥2，s元一次不定方程

$$a_1x_1+a_2x_2+\ldots+a_sx_s=n,\ a_1,\ldots,a_s\neq 0 \quad (4)$$

有整数解$x_1,\ldots,x_s$的充分必要条件是

$$(a_1,\ldots,a_s)|n. \quad (5)$$

证明：必要性：如果(4)有解，显然(5)成立.

充分性：如果(5)成立. 设$(a_1,\ldots,a_s)=d$，由§2定理5知存在整数$t_1,\ldots,t_s$有

$$a_1t_1+\ldots+a_st_s=d \quad (6)$$

令$x_1=t_1\cdot n/d,\ldots,x_s=t_s\cdot n/d$，由(6)知道是(4)的解.

注记

- 本节定理1等价于第二章§4的定理3：

设$(a,m)=d$，$m>0$，同余方程 $ax\equiv b \pmod m$有解的充分必要条件是$d|b$.

- 本节定理3等价于第二章§4的定理5：

设$k\geq 1$，同余式$a_1x_1+\ldots+a_kx_k+b\equiv 0 \pmod m$有解的充分必要条件是$(a_1,\ldots,a_k,m)|b$.

- 本节定理2给出了$(a_1,a_2)=1$时全体整数解。对一般情形，即$(a_1,a_2)=d$时，第二章§4的定理4的证明过程给出了所有整数解。

§9 抽屉原理

- 抽屉原理（又名鸽舍原理）：把n+1（或更多）个物体装入n个盒子里，那么一定有某个盒子至少装有2个物体。

证明：（反证法）如果每个盒子至多装有1个物体，那么盒子数量至多有n个，与有n+1（或更多）个相矛盾. 证毕.

抽屉原理在数论和组合论中有着许多应用，下面给出几个例子。

- 例1（定理1）：设$1\le a_1<a_2<\ldots<a_{n+1}\le 2n$，则有$1\le i<j\le n+1$，使得$a_i|a_j$.

证明：写$a_i=2^{\lambda_i}b_i$，$\lambda_i\ge 0$，$2\dagger b_i(i=1,\ldots,n+1)$，其中$b_i<2n$.

因为1,2,...,2n中恰有n个不同的奇数，由抽屉原理，在$b_1,\ldots,b_{n+1}$中至少有2个相同，设$b_i=b_j$, $1\le i<j\le n+1$，故$a_i|a_j$.

抽屉原理的应用:

- 例2（练习26）： 对于平面上任给的5个整点（即点的坐标都是整数的点）$A_i=(x_i,y_i)(i=1,2,\ldots,5)$，必有其中两点的连线的中点也是整点。

提示：5个整点的x的坐标至少有3个奇偶一致，这3个x坐标奇偶一致的整点中又至少有一对奇偶一致。

- 例3(练习41)：若$k>[(n+1)/2]$（[]为取整符号），则在k个整数$1\leq a_1<a_2<\ldots a_k\leq n$中存在$a_i,a_j(1\leq i<j\leq k)$满足$a_i+a_1=a_j$.

提示：考虑2k个整数$a_1,a_2,\ldots,a_k$, $a_1+a_1,a_2+a_1,\ldots,a_k+a_1$。这2k个整数在$[a_1,n+a_1]$之间，共有n个整取值。

总结

- 本章学习了整数的基本性质，是后面章节的基础。