初等数论总复习题及知识点总结

初等数论学习总结

本课程只介绍初等数论的的基本内容。由于初等数论的基本知识和技巧与中学数学有着密切的关系， 因此初等数论对于中学的数学教师和数学系(特别是师范院校)的本科生来说，是一门有着重要意义的课程，在可能情况下学习数论的一些基础内容是有益的．一方面通过这些内容可加深对数的性质的了解，更深入地理解某些他邻近学科，另一方面，也许更重要的是可以加强他们的数学训练，这些训练在很多方面都是有益的．正因为如此，许多高等院校，特别是高等师范院校，都开设了数论课程。

最后，给大家提一点数论的学习方法，即一定不能忽略习题的作用，通过做习题来理解数论的方法和技巧，华罗庚教授曾经说过如果学习数论时只注意到它的内容而忽略习题的作用，则相当于只身来到宝库而空手返回而异。

数论有丰富的知识和悠久的历史，作为数论的学习者，应该懂得一点数论的常识，为此在辅导材料的最后给大家介绍数论中著名的“哥德巴赫猜想”和费马大定理的阅读材料。

初等数论自学安排

第一章：整数的可除性（6 学时）自学 18 学时

整除的定义、带余数除法

最大公因数和辗转相除法

整除的进一步性质和最小公倍数

素数、算术基本定理

[x]和{x}的性质及其在数论中的应用

习题要求 p_3：2，3 ； p_8：4 ； p_{12}：1； p_{17}：1，2，5； p_{20}：1。

第二章：不定方程（4 学时）自学 12 学时

二元一次不定方程 $ax+by=c$

多元一次不定方程 $a_1x_1+a_2x_2+\square\ a_nx_n=c$

勾股数

费尔马大定理。

习题要求 p_{29}：1，2，4； p_{31}：2，3。

第三章：同余（4 学时）自学 12 学时

同余的定义、性质

剩余类和完全剩余系

欧拉函数、简化剩余系

欧拉定理、费尔马小定理及在循环小数中的应用

习题要求 p_{43}：2，6； p_{46}：1； p_{49}：2，3； p_{53} 1，2。

第四章：同余式（方程）（4 学时）自学 12 学时

同余方程概念

孙子定理

高次同余方程的解数和解法

素数模的同余方程

威尔逊定理。

习题要求 p_{60}：1； p_{64}：1，2； p_{69}：1，2。

第五章：二次同余式和平方剩余（4 学时）自学 12 学时

二次同余式

单素数的平方剩余与平方非剩余

勒让德符号

二次互反律

雅可比符号、

素数模同余方程的解法

习题要求 p_{78}：2； p_{81}：1，2，3； p_{85}：1，2； p_{89}：2； p_{93}：1。

第一章：原根与指标（2 学时）自学 8 学时

指数的定义及基本性质

原根存在的条件

指标及 n 次乘余

模 2^{α} 及合数模指标组、

特征函数

习题要求 p_{123}：3。

➢ 第一章 整除

一、主要内容

整除的定义、带余除法定理、余数、最大公因数、最小公倍数、辗转相除法、互素、两两互素、素数、合数、算术基本定理、Eratosthesen 筛法、[x]和{x}的性质、n！的标准分解式。

二、基本要求

通过本章的学习，能了解引进整除概念的意义，熟练掌握整除 整除的定义以及它的基本性质，并能应用这些性质，了解解决整除问题的若干方法，熟练掌握本章中二个著名的定理：带余除法定理和算术基本定理。认真体会求二个数的最大公因数的求法的理论依据，掌握素数的定义以及证明素数有无穷多个的方法。能熟练求出二个整数的最大公因数和最小公倍数，掌握高斯函数[x]的性质及其应用。

三、重点和难点

（1）素数以及它有关的性质，判别正整数 a 为素数的方法，算术基本定理及其应用。

（2）素数有无穷多个的证明方法。

（3）整除性问题的若干解决方法。

（4）[x]的性质及其应用，n！的标准分解式。

四、自学指导

整除是初等数论中最基本的概念之一，b｜a 的意思是存在一个整数 q，使得等式 a=bq 成立。因此这一标准作为我们讨论整除性质的基础。也为我们提供了解决整除问题的方法。即当我们无法用整除语言来叙述或讨论整除问题时，可以将其转化为我们很熟悉的等号问题。

对于整除的若干性质，最主要的性质为传递性和线性组合性，即

（1） a｜b， b｜c，则有 a｜c

（2） a｜b， a｜c，则有 a｜mb+nc

读者要熟练掌握并能灵活应用。特别要注意，数论的研究对象是整数集合，比小学数学中非负整数集合要大。

本章中最重要的定理之一为带余除法定理，即为

设 a 是整数，b 是非零整数，则存在两个整数 q，r，使得

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

它可以重作是整除的推广。同时也可以用带余除法定理来定义整除性，（即当余数 r=0 时）。带余除法可以将全体整数进行分类，从而可将无限的问题转化为有限的问题。这是一种很重要的思想方法，它为我们解决整除问题提供了又一条常用的方法。同时也为我们建立同余理论建立了基础。读者应熟知常用的分类方法，例如把整数可分成奇数和偶数，特别对素数的分类方法。例全体奇素数可以分成 4k+1，4k+3；或 6k+1，6k+5 等类型。

和整除性一样，二个数的最大公约数实质上也是用等号来定义的，因此在解决此类问题时若有必要可化为等式问题，最大公因数的性质中最重要的性质之一为 a=bq+c，则一定有（a，b）=（b，c），就是求二个整数的最大公约数的理论根据。也是解决关于最大公约数问题的常用方法之一。读者应有尽有认真体会该定理的证明过程。

互素与两两互素是二个不同的概念，既有联系，又有区别。要认真体会这些相关的性质，例如，对于任意 a ,b∈Z，可设（a ,b）=d，则 $a=da_1$,$b=db_1$，则（a_1 ,b_1）=1，于是可对 a_1 ,b_1 使用相应的定理，要注意，相关定理及推论中互素的条件是经常出现的。读者必须注意定理成立的条件，也可以例举反例来进行说明以加深影响。顺便指出，若 a｜c，b｜c，（a ,b）=1，则 ab｜c 是我们解决当除数为合数时的一种方法。好处是不言而喻的。

最小公倍数实际上与最大公因数为对偶命题。特别要指出的是 a 和 b 的公倍数是有无穷多个。所以一般地在无穷多个数中寻找一个最小数是很困难的，为此在定义中所有公倍数中的最小的正整数。这一点实际上是应用自然数的最小自然数原理，即自然数的任何一个子集一定有一个最小自然数有在。最小公倍数的问题一般都可以通过以下式子转化为最大公因数的问题。两者的关系为

$a,b\in N$，　　$[a,b]=\dfrac{ab}{(a,b)}$

上述仅对二个正整数时成立。当个数大于 2 时，上述式子不再成立。证明这一式子的关键是寻找 a , b 的所有公倍数的形式，然后从中找一个最小的正整数。

解决了两个数的最小公倍数与最大公因数问题后，就可以求出 n 个数的最小公倍数与最大公因数问题，可以两个两个地求。即有下面定理

设 $a_1,a_2,\cdots\ a_n$ 是 n 个整数，$(a_1,a_2)=d_2,(d_2,a_3)=d_3,\cdots\ (d_{n-1},a_n)=d_n$，则（$a_1,a_2,\cdots\ a_n$）$=d_n$,

设 $[a_1,a_2]=m_2,(m_2,a_3)=m_3,\cdots\ (m_{n-1},a_n)=m_n$，则有 $[a_1,a_2,\cdots\ a_n]=m_n$,

素数是数论研究的核心，许多中外闻名的题目都与素数有关。除 1 外任何正整数不是质数即为合数。判断一个已知的正整数是否为质数可用判别定理去实现。判别定理又是证明素数无穷的关键。实际上，对于任何正整数 n>1，由判别定理一定知存在素数 p，使得 p｜n 。即任何大于 1 的整数一定存在一个素因数 p。素数有几个属于内在本身的性质，这些性质是在独有的，读者可以用反例来证明：素数这一条件必不可少。以加深对它们的理解。其中 p｜ab⇒p｜a 或 p｜b 也是常用的性质之一。也是证明算术基本定理的基础。

算术基本定理是整数理论中最重要的定理之一，即任何整数一定能分解成一些素数的乘积，而且分解是唯一的，不是任何数集都能满足算术基本定理的，算术基本定理为我们提供了解决其它问题的理论保障。它有许多应用，由算术基本定理我们可以得到自然数的标准分解问题。

设 $a=p_1^{\alpha_1}\cdots\ p_k^{\alpha_k}$，$b=p_1^{\beta_1}\cdots\ p_k^{\beta_k}$，$\alpha_i>0,\beta_i>0$ 则有

（a，b）$=p_1^{\gamma_1}\cdots\ p_k^{\gamma_k}$　　$\gamma_i=\min(\alpha_i,\beta_i)$

[a，b]$=p_1^{\delta_1}\cdots\ p_k^{\delta_k}$　　$\delta_i=\max(\alpha_i,\beta_i)$

例如可求最大公约数，正整数正约数的个数等方面问题，对具体的 n，真正去分解是件不容易的事。对于较特殊的 n，例如 n！分解还是容易的。应用[x]的性质，n！的标准分解式可由一个具体的公式表示出来，这一公式结合[x]

的性质又提供了解决带有乘除符号的整除问题的方法。

本章的许多问题都围绕着整除而展开，读者应对整除问题的解决方法作一简单的小结。

五、例子选讲

补充知识

①最小自然数原理：自然数的任意非空子集中一定存在最小自然数。

②抽屉原理：

（1）设 n 是一个自然数，有 n 个盒子，$n+1$ 个物体，把 $n+1$ 个物体放进 n 个盒子，至少有一个盒子放了两个或两个以上物体；

（2）$km+1$ 个元素，分成 k 组，至少有一组元素其个数大于或等于 $m+1$；

（3）无限个元素分成有限组，至少有一组其元素个数为无限。

③梅森数：形如 2^n-1 的数叫梅森数，记成 $M_n=2^n-1$。

④费尔马数：n 为非负整数，形如 $2^{2^n}+1$ 的数叫费尔马数，记成 $F_n=2^{2^n}+1$。

⑤设 $n=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$，设 n 的正因子个数为 $d(n)$，所有正因子之和为 $\sigma(n)$，则有

$$d(n)=(\alpha_1+1)\cdot(\alpha_2+1)\ldots(\alpha_k+1)$$

$$\sigma(n)=\frac{p_1^{\alpha_1+1}-1}{P_1-1}\cdot\frac{p_2^{\alpha_2+1}-1}{P_2-1}\cdots\frac{p_k^{\alpha_k+1}-1}{P_k-1}$$

⑥有关技巧

1. 整数表示 $a=a_0\times10^n+a_1\times10^{n-1}+\ldots+a_n$，

$a=2^kb$(b 为奇数)

2.整除的常用方法

a. 用定义

b. 对整数按被 n 除的余数分类讨论

c. 连续 n 个整数的积一定是 n 的倍数

d. 因式分解

$a^n-b^n=(a-b)M_1$,

$a^n+b_n=(a+b)M_2$, $2\nmid n$

e. 用数学归纳法

f. 要证明 $a|b$，只要证明对任意素数 p，a 中 p 的幂指数不超过 b 中 p 的幂指数即可，用 $p(a)$表示 a 中 p 的幂指数，则 $\boxed{a|b \Leftrightarrow p(a) \le p(b)}$

例题选讲

例 1.请写出 10 个连续正整数都是合数.

解: 11!+2，11!+3，……，11！+11。

例 2. 证明连续三个整数中，必有一个被 3 整除。

证：设三个连续正数为 a，a+1，a+2，而 a 只有 3k，3k+1，3k+2 三种情况，令 a=3k，显然成立，a=3k+1 时，a+2=3(k+1)，a=3k+2 时，a+1=3(k+1)。

例 3. 证明 lg2 是无理数。

证：假设 lg2 是有理数，则存在二个正整数 p，q，使得 $\lg 2=\frac{p}{q}$，由对数定义可得 $10^p=2^q$，

则有 $2^p \cdot 5^p = 2^q$,则同一个数左边含因子 5，右边不含因子 5，与算术基本定理矛盾。∴lg2 为无理数。

例 4. 求(21n+4，14n+3)

解：原式=(21n+4,14n+3)=(7n+1,14n+3)=(7n+1,7n+2)=(7n+1,1)=1

例 5. 求 2004!末尾零的个数。

解：因为 10=2×5，而 2 比 5 多，

所以只要考虑 2004！中 5 的幂指数，即

5（2004！）$=\left(\frac{2004}{5}\right)+\left(\frac{2004}{25}\right)+\left(\frac{2004}{125}\right)+\left(\frac{2004}{5^4}\right)+\left(\frac{2004}{5^5}\right)=499$

例 6.证明（n!）$^{(n-1)!}$|(n!)!

证：对任意素数 p,设（n!）$^{(n-1)!}$中素数 p 的指数为α，

（n!）!中 p 的指数 β，则

$\alpha=(n-1)!\sum_{k=1}^{\infty}\left(\frac{n}{p^k}\right)$，$\beta=(n-1)!\sum_{k=1}^{\infty}\left(\frac{n!}{p^k}\right)$，$(nx)\geq n(x)$

$$\therefore\sum_{k=1}^{\infty}\left(\frac{n!}{p^k}\right)=\sum_{k=1}^{\infty}\left(\frac{n(n-1)!}{p^k}\right)\geq\sum_{k=1}^{\infty}(n-1)!\left(\frac{n!}{p^k}\right)=(n-1)!\sum_{k=1}^{\infty}\left(\frac{n!}{p^k}\right)=\alpha$$

即 $\beta\geq\alpha$，即左边整除右边。

例 7. 证明 2003|（$2002^{2002}+2004^{2004}-2005$）

证：∵ $2002^{2002}=(2003-1)^{2002}=2003M_1+1$

$2004^{2004}=(2003+1)^{2002}=2003M_2+1$

∴$2002^{2002}+2004^{2004}-2005=2003(M_1+M_2-1)$

由定义 2003|（$2002^{2002}+2004^{2004}-2005$）

例 8. 设 $d(n)$为 n 的正因子的个数，$\sigma(n)$为 n 的所有正因子之和，求 $d(1000)$，$\sigma(1000)$。

解：∵ $1000=2^3\cdot5^3$

∴ $d(1000)=(3+1)(3+1)=16$，$\sigma(1000)=\frac{2^4-1}{2-1}\cdot\frac{5^4-1}{5-1}$

例 9. 设 c 不能被素数平方整除，若 $a^2|b^2c$，则 $a|b$

证：由已知 $p(c)\leqslant1$，且 $p(a^2)\leqslant p(b^2c)$

∴ $2p(a)\leqslant2p(b)+p(c)$ ， ∴ $p(a)\leqslant p(b)+\frac{p(c)}{2}$

即 $p(a)\leqslant p(b)$ ， ∴ $a|b$

例 10. 若 M_n 为素数，则 n 一定为素数。

证：若 n 为合数，则设 $n=ab$，（$1<a,b<n$）

∴ $2^{ab}-1=(2^a)^b-1=(2^a-1)M$ 为合数，与 M_n 为素数矛盾，

∴ n 为素数。

例 11. 证明对任意 m,n，$m\neq n$, $(F_n,F_m)=1$。

证：不妨设 $n>m$，则 $F_n-2=(2^{2^{n-1}}-1)(2^{2^{n-1}}+1)=(F_{n-1}-2)(2^{2^{n-1}}+1)$

$= F_{n-1}F_{n-2}\cdots\cdots F_m - F_0$

设（F_m,F_m）=d,则 $d|F_n$, $d|F_m \Rightarrow d|2$

但 F_n 为奇数，$\therefore d=1$, 即证。

例 12. 设 m,n 是正整数。证明

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

证 ： 不妨设 $m \geq n$ 。由带余数除法得

$$m = q_1 n + r_1, \qquad 0 \leq r_1 \leq n.$$

我们有

$$2^m - 1 = 2^{q_1 n + r_1} - 2^{r_1} + 2^{r_1} - 1 = 2^{r_1}\left(2^{q_1 n} - 1\right) + 2^{r_1} - 1$$

由此及 $2^n - 1 \mid 2^{q_1 n} - 1$ 得, $(2^m - 1, 2^n - 1) = (2^n - 1, 2^{r_1} - 1)$

注意到 $(m,n) = (n,r_1)$,若 $r_1 = 0$,则 $(m,n) = n$,结论成立.若 $r_1 > 0$,则继续对 $(2^n - 1, 2^{r_1} - 1)$ 作同样的讨论，由辗转相除法知，结论成立。显见，2 用任一大于 1 的自然 a 代替，结论都成立。

例 13. 证明：对任意的正整数 n ，成立如下不等式 $\lg n \geq k \lg 2$ 。

其中 $\lg n$ 是数 n 的以 10 为底的对数，k 是 n 的不同的素因数（正的）的个数。

证：设 n 是大于 1 的整数（如果 n =1，上述不等式显然成立，因 k =0），$p_1, p_2, \ldots, p_k$ 是 n 的 k 个相异的素因素。n 的素因数分解式为

$n = p_1^{l_1} p_2^{l_2} \ldots p_k^{l_k}$.$(l_i \geq 1, i = 1,2,\ldots,k)$ ，由于 $p_i \geq 2, (i = 1,2,\ldots,k)$，从而

$n = p_1^{l_1} p_2^{l_2} \ldots p_k^{l_k} \geq 2^{l_1} \cdot 2^{l_2} \cdot \ldots \cdot 2^{l_k} = 2^{l_1 + l_2 + \ldots + l_k}$ ，

而 $l_1 + l_2 + \ldots + l_k \geq k$，故 $n \geq 2^k$ 。

将上述不等式取对数（设底 $a > 1$ ）,则有 $\log_a n \geq k \log_a 2$ 。

特别有 $\lg n \geq k \lg 2$ 。

例 14. 试证明任意一个整数与它的数字和的差必能被 9

整除，并且它与它的数字作任意调后换后所成整数的差也能被 9 整除。

证： 设整数 m 的个位、十位、百位…的数字分别为a_1, a_2，…，a_n，则m可表作：

$$m = a_1 + 10a_2 + 100a_3 + ... + 10^{n-1}a_n$$

$$= (a_1 + a_2 + a_3 + ... + a_n) + (9a_2 + 99a_3 + ... + \underbrace{99...9}_{n-1}a_n)$$

$$= (a_1 + a_2 + a_3 + ... + a_n) + 9(a_2 + 11a_3 + ... + \underbrace{11...1}_{n-1}a_n)$$

所以$m - (a_1 + a_2 + a_3 + ... + a_n) = 9(a_2 + 11a_3 + ... + \underbrace{11...1}_{n-1}a_n)$

因为a_2， a_3,…， a_n都是整数，所以任一整数与其数字之和的差必能被 9 整除。

再设将a_1, a_2，…， a_n按任一种顺序排成a'_1, a'_2，…， a'_n，并令

$\sigma = a_1 + a_2 + ... + a_n$， $\sigma' = a'_1 + a'_2 + ... + a'_n$， $m = a_1 + 10a_2 + ... + 10^{n-1}a_n$，

$m' = a'_1 + 10a'_2 + ... + 10^{n-1}a'_n$。

根据前面证明的结果，知存在整数 A，B，使$m - \sigma = 9A, m' - \sigma' = 9B.$

因为$\sigma = \sigma'$，所以$m - m' = \sigma + 9A - \sigma' - 9B = 9(A - B)$。

由于 A-B 是整数，这就证明了$m - m'$能被 9 整除。

注：若对某个整数$k(1 \le k \le n)$，有$a'_k \ne 0$，但当$k < i \le n$时， $a'_i = 0$，则此时m'为整数：

$m' = a'_1 + 10a'_2 + ... + 10^{k-1}a'_k$, 即$m' = a'_k ... a'_2 a'_1$。

如前证，此时结论正确。又当m为负整数及零时，结论显然正确。

➢ 第二章 不定方程

一、 主要内容

一次不定方程有解的条件、解数、解法、通解表示，不定方程 $x^2+y^2=z^2$ 通解公式、无穷递降法、费尔马大定理。

二、 基本要求

1、 了解不定方程的概念，理解对“解”的认识，掌握一次不定方程$ax + by = c$有解的条件，能熟练求解一次不定方程的特解，正整数解及通解。了解多元一次不定方程

$a_1x_1 + a_2x_2 + \cdots a_nx_n = c$ 有解的条件，在有解的条件下的解法。

2、掌握不定方程 $x^2+y^2=z^2$ 在一定条件下的通解公式，并运用这个通解公式作简单的应用。

3、对费尔马大定理应有在常识性的了解，掌握无穷递降法求证不定方程 $x^4+y^4=z^2$ 无解的方法。

4、掌握证明不定方程无解的若干方法。

三、难点和重点

（1）重点为求解一次不定方程的方法

（2）掌握第二节中引证的应用。

（1） 费尔马无穷递降法。

四、自学指导

不定方程主要讲解以下几个问题

（i）给定一类不定方程，判别在什么条件下有解。

（ii）在有解的条件下，有多少解

（iii）在有解的条件下，求出所给的不定方程的所有解。

二元一次不定方程的一般形式为 ax+by=c 。若(a ,b)｜c，则该二元一次不定方程一定有解，若已知一个特解，则一切解可以用公式表示出来，因此求它的通解只要求出一个特解即可。求解二元一次不定方程的一个通解有好多种方法。读者应该总结一下，各种方法都有独到之处。特别要指出用最大公因数的方法。它的根据是求（a ,b）时所得的结果。由于注意通解公式 $x=x_0-b_1t$，$y=y_0+a_1t$ 中 a_1，b_1 的意义和位置。以免出错。

多元一次不定方程 $a_1x_1 + a_2x_2 + \cdots a_nx_n = c$ 也有类似的结果，但在求解的过程中将它转化二元一次不定方程组，从最后一个二元一次不定方程解起，可逐一解出 $x_1, x_2, \cdots\cdots x_n$ 。所用的方法一般选择最大公因数的方法。由于 n 元一次不定方程可转化为 n-1 个二元一次不定方程组，故在通解中依赖于 n-1 个任意常数。但不象二元一次不定方程那样有公式来表示。

$x^2+y^2=z^2$ 的正整数解称为勾股数，在考虑这个方程时，我们对（x ,y

）作了一些限制，而这些限制并不影响其一般性。在条件 x>0，y>0，z>0，（x, y）=1，2｜x 的条件可以给出 $x^2+y^2=z^2$ 的通解公式，x=2ab，$y=a^2-b^2$，$z^2=a^2+b^2$，a>b>0 , (a ,b)=1，a ,b 一奇一偶。若将 2｜x 限为 2｜y，则也有相应的一个通解公式。在证明这个通解公式的过程中，用到了引理 $uv=w^2$，u>0，v>0，（u ,v）=1，则 $u=a^2$，$v=b^2$，w=ab 。a>0，b>0，（a ,b）=1 。利用这个结论可以求解某些不定方程。特别当 w=1 或素数 p 。则由 uv=1 或 uv=P 可将原不定方程转化为不定方程组。从而获得一些不定方程的解。上述解不定方程的方法叫因子分解法。希望读者能掌握这种方法。

为了解决著名的费尔马大定理：$x^n+y^n=z^n$ ，n≥3 无正整数解时，当 n=4 时可以用较初等的方法给出证明。证明由费尔马本人给出的，一般称为费尔马无穷递降法。其基本思想为由一组解出发通过构造得出另一组解，使得两组解之间有某种特定的关系，而且这种构造可以无限重复的。从而可得到矛盾。因此无穷递降法常用来证明某些不定方程无整数解。

证明一类不定方程无解是研究不定方程邻域中常见的形式，一般的要求解不定方程比证明不定方程无解要容易些。证明不定方程无解的证明方法常采用以下形式：（反证法）

若 A 有解$\Rightarrow A_1$有解$\Rightarrow A_2$有解$\Rightarrow\cdots\cdots\Rightarrow A_n$有解，而 A_n 本身无解，这样来构造矛盾。从而说明原不定方程无解。

对于证明不定方程的无解性通常在几种方法，一般是总的几种方法交替使用。特别要求掌握：简单同余法、因子分解法、不等式法，以及中学数学中所涉及的判别式法。

五、例子选讲

例 1：利用整数分离系数法求得不定方程 $15x+10y+6z=61$。

解：注意到 z 的系数最小，把原方程化为

$$z=\frac{1}{6}(-15x-10y+61)=-2x-2y+10+\frac{1}{6}(-3x+2y+1)$$

令 $t_1=\frac{1}{6}(-3x+2y+1)\in z$，即 $-3x+2y-6t_1+1=0$

此时 y 系数最小，$\therefore y=\frac{1}{2}(3x++6t_1-1)=x+3t_1+\frac{1}{2}(x-1)$

令 $t_2=\frac{1}{2}(x-1)\in z$,即 $x=2t_2+1$,反推依次可解得

$y=x+3t_1+t_2=2t_2+1+3t_1+t_2=1+3t_1+3t_2$

$z=-2x-2y+10+t_1=6-5t_1+10t_2$

∴原不定方程解为 $\begin{cases} x = 1 + 2t_2 \\ y = 1 + 3t_1 + 3t_2 \\ z = 6 - 5t_1 - 10t_2 \end{cases}$ $t_1t_2 \in z$.

例 2:证明 $\sqrt{2}$ 是无理数

证：假设 $\sqrt{2}$ 是有理数，则存在自数数 a,b 使得满足 $x^2 = 2y^2$ 即 $a^2 = 2b^2$，容易知道 a 是偶数，

设 $a=2a_1$，代入得 $b^2 = 2a_1^2$,又得到 b 为偶数，$a_1 < b < a$，设 $b = 2b_1$，则 $a_1^2 = 2b_1^2$,这里 $b_2 < a_1$

这样可以进一步求得 a_2，b_2…且有 $a>b>a_1>b_1> a_2>b_2>\cdots$

但是自然数无穷递降是不可能的，于是产生了矛盾，∴ $\sqrt{2}$ 为无理数。

例 3：证明：整数勾股形的勾股中至少一个是 3 的倍数。

证：设 $N=3m\pm1$(m 为整数) ， ∴$N^2=9m^2\pm6m+1=3(3m^2\pm2m)+1$

即一个整数若不是 3 的倍数，则其平方为 $3k+1$,或者说 $3k+2$ 不可能是平方数，设 x,y 为勾股整数，且 x,y 都不是 3 的倍数，则 x^2,y^2 都是 $3k+1$，但 $z^2=x^2+y^2=3k+2$ 形，这是不可能，∴勾股数中至少有一个是 3 的倍数。

例 4：求 $x^2+y^2=328$ 的正整数解

解：∵ 328 为偶数，∴x,y 奇偶性相同，即 $x\pm y$ 为偶数，设 $x+y=2u$, $x-y=2$v，代入原方程即为

$u^2+v^2=164$,同理令 $u+v=2u_1$,$u-v=2v_1$ 有

$u_1^2 + v_1^2 = 82, u_1 + v_1 = 2u_2, u_1 - v_1 = 2v_2$

$u_2^2 + v_2^2 = 41,\ u_2, v_2$ 为一偶一奇，且 $0<u_2<6$

u_2=1，2，3，4，5 代方程，有解（4，5）（5，4）

∴原方程解 $x=18,y=2$,或 $x=2,y=18$。

例 5：求 $x^2+xy-6=0$ 的正整数解。

解：原方程等价于 $x(x+y)=2\cdot3$,故有

∴ $\begin{cases} x = 2, \\ x + y = 3, \end{cases}$ $\begin{cases} x = 3, \\ x + y = 2, \end{cases}$ $\begin{cases} x = 1, \\ x + y = 6, \end{cases}$ $\begin{cases} x = 6, \\ x + y = 1. \end{cases}$ ， ∴ 即有 $x=2,y=1$; $x=1,y=5$.

例 6：证明不定方程 $x^2-2xy^2+5z+3=0$ 无整数解。

解：若不定方程有解，则 $x=y^2\pm\sqrt{y^4-5z-3}$

但 $y^4\equiv 0,1(\mathrm{mod}5)$，∴ 对 y,z ，$y^4-5z-3\equiv 2,3(\mathrm{mod}5)$

而一个平方数≡0，1，4（mod 5）

∴ y^4-5z-3 不可能为完全平方，即 $\sqrt{y^4-5z-3}$ 不是整数，所以原不定方程无解。

例 7：证明：$x^2+y^2+z^2=8a+7$ 无整数解

证：若原方程有解，则有 $x^2+y^2+z^2\equiv 8a+7(\mathrm{mod}8)$

注意到对于模 8，有

$0^2\equiv 0,1^2\equiv 1,2^2\equiv 4,3^2\equiv 1,4^2\equiv 0,5^2\equiv 1,6^2\equiv 4,7^2\equiv 1,$

因而每一个整数对于模 8，必同余于 0，1，4 这三个数。

不论 x^2,y^2,z^2 如何变化，只能有 $x^2+y^2+z^2\equiv 0,1,2,3,4,5,6(\mathrm{mod}8)$

而 $8a+7\equiv 7(\mathrm{mod}8)$，故 $8a+7$ 不同余于 $x^2+y^2+z^2$ 关于模 8，所以假设错误，即 $8a+7\neq x^2+y^2+z^2$，从而证明了原方程无解。

例 8:某人到银行去兑换一张 d 元和 c 分的支票，出纳员出错，给了他 c 元和 d 元，此人直到用去 23 分后才发觉其错误，此时他发现还有 $2d$ 元和 $2c$ 分，问该支票原为多少钱？

解：由题意立式得：$100c+d-23=100\times 2d+2c$

即 $98c-199d=23.$

令 $u=c-2d$ 得 $98u-3d=23,$

令 $v=33u-d$ 得 $3v-u=23.$

所以 $u=3v-23$（v 为任意整数），代入得：

$d=33u-v=98v-33\times 23,$ （1）

$c=u+2d=199v-67\times 23,$

其中 v 是任意整数。又根据题意要求：$d>0,0<c<100$.

根据(1)，仅当 $y=8$ 时满足此要求，从而 $d=25, c=51.$

因此该支票原为 25 元 51 分.

➢ 第三章　同余

一、　主要内容

同余的定义、性质、剩余类和完全剩余系、欧拉函数、简化剩余系、欧拉定理、费尔马小定理、循环小数、特殊数 2，3，4，5，6，7，8，9，11，13 的整除规律

二、　基本要求

通过本章的学习，能够掌握同余的定义和性质，区别符号：“三”和=”之间的差异。能利用同余的一些基本性质进行一些计算，深刻理解完全剩余系，简化剩余系的定义、性质及构造。能判断一组数是否构成模 m 的一个完全剩余系或一个简化剩余系。能计算欧拉函数的值，掌握欧拉定理、费尔马小定理的内容以及证明方法。能应用这二个定理证明有关的整除问题和求余数问题。能进行循环小数与分数的互化。

三、难点和重点

（1）同余的概念及基本性质

（2）完全剩余系和简化剩余系的构造、判别

（3）欧拉函数计算、欧拉定理、费尔马小定理的证明及应用

（4）循环小数与分数的互化

（5）特殊数的整除规律。

四、自学指导

同余理论是初等数论中最核心的内容之一，由同余定义可知，若 a≡b(mod m)，则 a 和 b 被 m 除后有相同的余数。这里 m 为正整数，一般要求 m 大于 1，称为模，同余这一思想本质上是将整数按模 m 分类，然后讨论每一个类中整数所具有的共性及不同类之间的差异。第一章中用带余除法定理将整数分类解决一些问题的方法只不过是同余理论中的一个特殊例子。从同余的定理上看，同余和整除实际上是同一回事，故同余还有二个等价的定义：①

用整除来定义即 m | a-b 。②用等号来定义 a=b+mt 。值得注意 a 和 b 关于 m 同余是个相对概念。即它是相对于模 m 来讲，二个整数 a 和 b 关于一个整数模 m 同余。则对于另一个整数模 m_1，a 和 b 未必会同余。

从定义上看，同余和整除是同一个事情，但引进了新的符号“三”后，无论从问题的叙述上，还是解决问题的方法上都有了显著的变化，同时也带来了一些新的知识和方法。在引进了同余的代数性质和自身性质后，同余符号“三”和等号“=”相比，在形式上有几乎一致的性质，这便于我们记忆。事实上在所有等号成立的运算中，只有除法运算是个例外，即除法的消去律不成立。为此对于同余的除法运算我们有二种除法：

（i）模不改变的除法，若 ak≡bk(mod m) ，(k,m)=1，则 a≡b(mod m)

(ii)模改变的除法， 若 ak≡bk(mod m) (k,m)=d,则 $a\equiv b\left(\mathrm{mod}\frac{m}{a}\right)$

这一点读者要特别注意。

完全剩余系和简化剩余系是二个全新的概念，读者只要搞清引成这些概念的过程。因为同余关系是一个等价关系，利用等价关系可以进行将全体整数进行分类，弄清来胧去脉，对于更深刻理解其本质是很有好处的。完全剩余系或简化剩余系是一个以整数为元素的集合，在每个剩余类各取一个数组成的 m 个不同数的集合，故一组完全剩余系包含 m 个整数，由于二个不同的剩余类中的数关于 m 两两不同余，故可得判别一组数是否为模 m 的一个完全剩余系的条件有二条为

（1） 个数=m

（2） 关于 m 两两不同余

另外要能用已知完全剩余系构造新的完全剩余系。即有定理

设（a，m）=1，x 为 m 的完全剩余系，则 ax+b 也是 m 的完全剩余系。

当 $(m_1,m_2)=1$ 时，能由 m_1 的完全剩余系和 m_2 的完全剩余系，构造 m_1m_2 完全剩余系。

为讨论简化剩余系，需要引进欧拉函数 $\phi(m)$，欧拉函数 $\phi(m)$ 定义为不超过 m 且与 m 互素的正整数的个数，记为 $\phi(m)$，要掌握 $\phi(m)$ 的计算公式，了解它的性质。这些性质最主要的是当（a ,b）=1 时， $\phi(ab)=\phi(a)\ \phi(b)$，和 $\phi(p^{\alpha})=p^{\alpha}-p^{\alpha-1}$

现在在剩余类中把与 m 互素的集合分出来，从中可在各个集合中任取一个数即可构造模 m 的一个简化剩余系。另一方面，简化剩余数也可从模 m 的一个完全剩余系中得到简化剩余系，一组完全剩余系中与 m 互素的的数组成的 $\phi(m)$ 个不同数的集合称为 m 简化剩余系。同样简化剩余系也有一个判别条件。

判别一组整数是否为模 m 的简化剩余系的条件为

（2） 个数= $\phi(m)$

（3） 关于 m 两两不同余

（3） 每个数与 m 互素

关于 m 的简化剩余系也能用已知完全剩余系构造新的简化剩余系。

设（a，m）=1，x 为 m 的简化剩余系，则 ax 也是 m 的简化剩余系。

当 $(m_1, m_2) = 1$ 时，能由 m_1 的简化剩余系和 m_2 的简化剩余系，构造 $m_1 m_2$ 简化剩余系。

欧拉定理、费尔马小定理是同余理论非常重要的定理之一。要注意欧拉定理和费尔马定理的条件和结论。

欧拉定理：设 m 为大于 1 的整数，（a，m）=1，则有

$$a^{\varphi(m)} \equiv 1 (\mathrm{mod}\, m)$$

费尔马小定理：若 p 是素数，则有

$$a^{p} \equiv a (\mathrm{mod}\, p)$$

除此以外，欧拉定理的证明的思想是非常好的，在各个地方都有应用。就欧拉定理、费尔马小定理来讲，它在某些形如 a^n 数的整除问题应用起来显得非常方便。同余方法也是解决整除问题的方法之一。

另外同余方法在证明不定方程时也非常有用，即要掌握同余“三”和相等“=”的关系：相等必同余，同余未必相等，不同余肯定不相等。

对于特殊数的整除规律要求能掌握其一般定理的证明，并熟记一些特殊数的整除规律

1、 一个整数被 2 整除的充要条件是它的末位为偶数。

2、