普通高中课程标准实验教科书

数学 选修 4－6

初等数论初步

教师教学用书

人民教育出版社 课程教材研究所
中学数学教材实验研究组 编著

人民教育出版社
B版

ISBN 7-107-19115-2

9 787107 191152 >

ISBN 7-107-19115-2
G · 12205（课）

定价：3.60 元

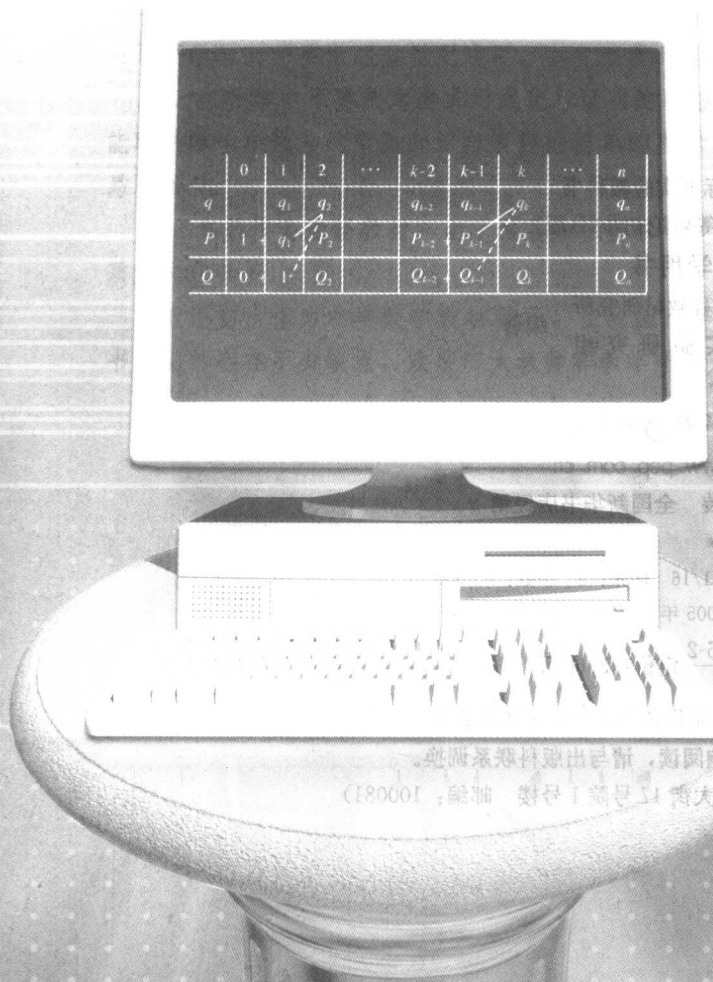
普通高中课程标准实验教科书

数学

选修 4-6　初等数论初步

教师教学用书

人民教育出版社　课程教材研究所
中学数学教材实验研究组　编著



人民教育出版社
B版

主　　编　　高存明

编　　者　　罗声雄　曹惠中
责任编辑　　王旭刚
美术编辑　　王　喆
封面设计　　李宏庆

普通高中课程标准实验教科书
数学选修 4-6　初等数论初步(B 版)
教师教学用书
人民教育出版社　课程教材研究所
中学数学教材实验研究组　编著
*
人民教育出版社 出版发行
网址:http://www.pep.com.cn
北京天宇星印刷厂印装　全国新华书店经销
*
开本:890 毫米×1 240 毫米　1/16　印张:3　字数:65 000
2005 年 9 月第 1 版　2005 年 12 月第 1 次印刷
ISBN 7-107-19115-2
G·12205(课)　定价:3.60 元

(联系地址:北京市海淀区中关村南大街 17 号院 1 号楼　邮编:100081)

说　明

本书是配合全国中小学教材审定委员会2004年初审通过的《普通高中课程标准实验教科书·数学选修4-6初等数论初步（B版）》的使用编写的教师用书.

本套教师教学用书编写的原则是：

1. 努力体现普通高中数学课程标准实验教科书（B版）编写的指导思想. 帮助教师钻研教材，理解教材的编写意图.

2. 明确各章的教学要求及要达到的教学目标. 帮助教师完成“课标”中规定的教学任务.

3. 对相关内容进行分析，并提出一些教法建议，帮助教师克服教学中的一些困难.

本册教师教学用书每章包括四部分：Ⅰ教学要求，Ⅱ本章的重点、难点与课时分配，Ⅲ教材分析与教学建议，Ⅳ习题参考答案.

教材的课程目标的确定，主要依据是教育部2003年颁布的《普通高中数学课程标准》中的系列4的相关内容的教学要求进行编写.

在教科书中，我们已对全套教材的结构、编写特点和指导思想作了阐述，下面再对这册教科书作如下说明，以帮助老师理解教材.

1. 这册书教学的主要目的是，提供初等数论的一般理论与方法. 主要涉及整除、素数、同余和不定方程，所用的方法是初等的，主要是算术方法.

2. 学习数论虽然有一定的难度，但初等数论问题具有浓厚的兴味. 所需数学预备知识较少，而且提法简练，往往为中学生所喜闻乐见. 教学中主要是启发学生学习数论的兴趣.

3. 数论问题中有些表面上很简单，但它们是极其艰难的，仅用初等方法是无法解决的，教学中要引导同学暂时不要做这些世纪难题，以免浪费时光.

4. 在教学中不要刻意追求形式化与证明的严格性，把重点放在对相关内容本质的理解上，要尽可能联系学生所熟知的整除知识与有趣的简单的整除问题. 有些定理可以采取举例说明的方式，使学生易于接受.

5. 本册作为选修教材，由于预备知识要求不多，所以高一入学后就可选修，以提高学生的数学素质及文化素养.

数论初步作为中学数学教材编写，在我国还是首次，有些内容的编排没有经验，又由于时间紧，书中必然存在不少缺点，欢迎广大教师和教学研究人员指正.

中学数学教材实验研究组

2005年9月

目录

第一章 整数的整除性

Ⅰ 教学要求

1. 掌握整除的基本性质，并会运用这些性质求解一些整除问题.

2. 了解寻找素数的厄拉多塞方法.

3. 掌握带余除法的表达形式，会用辗转相除法求最大公约数. 理解裴蜀恒等式，掌握两数 a、b 互素的充要条件是存在函数 x，y，使得 $ax+by=1$. 掌握最大公约数与最小公倍数的关系.

4. 理解算术基本定理，并通过基本定理计算一个整数的正约数个数.

5. 会解二元一次不定方程.

Ⅱ 本章重点、难点与课时分配

本章重点是：整除性质、辗转相除法、二元一次不定方程的解法.

本章难点是：求余数的算法、两数互素的充分必要条件、二元一次不定方程的通解.

本章全部课时为 7 学时，原则上每一节 1 学时，但可作必要调整. 1.4、1.7 节可用 1.5 学时，其余节可适当减少.

Ⅲ 教材分析与教学建议

1.1 整　　除

本节的核心内容是整除的四条简单性质. 这些性质是研究整除的理论基础和基本工具. 全节围绕这些性质展开：整除概念——整除符号——性质的验证（或证明）——性质的应用. 建议：

1. 从有趣的实际问题入手，让学生了解整除的重要性；从学生所熟悉的除法与乘法互为逆运算，引出整除概念与符号；

2. 引导学生用整除概念证明整除的四条性质，并用实际数字加以检验；

3. 让学生理解一个整数的正约数成对出现，并用实际例子检验. 认清一个正整数 n 的约数，若从小到大排列 q_1，q_2，…，q_k，则 $\frac{n}{q_k}$，$\frac{n}{q_{k-1}}$，…，$\frac{n}{q_1}$ 与其对应相等.

4. 为使学生更好地掌握整除性质，可补充一些例习题，例如

(1) 若 $7|n^2+3n-5$，求 n.

解：若 $7|n^2+3n-5$，则存在 k 使 $n^2+3n-5=7k\Rightarrow(n+1)(n+2)=7(k+1)\Rightarrow 7|n+1$ 或 $7|n+2\Rightarrow n+1=7p$ 或 $n+2=7q\Rightarrow n=7p-1$ 或 $n=7q-2$，p，q 为整数.

(2) 设 n 为正的奇数，则 $2^{2n}-2^n-2$ 是 9 的倍数.

证明：当 $n=1$ 时，$2^{2n}-2^n-2=0$ 是 9 的倍数. 假设 $2^{2n}-2^n-2$ 是 9 的倍数，由 n 为奇数，

$2^{2(n+2)}-2^{n+2}-2=2^4(2^{2n}-2^n-2)+12\cdot 2^n+30=2^4(2^{2n}-2^n-2)+9\cdot 2^n+27+3(2^n+1)$.

右边前三项是 9 的倍数. 当 n 为奇数时，$2^n+1=(2+1)\cdot k$，故 $3(2^n+1)$ 是 9 的倍数. 因此 $2^{2(n+2)}-2^{n+2}-2$（n 为奇数）为 9 的倍数，于是得证.

1.2 素数与合数

本节讲授素数有无穷多个，在自然数中分布很不规则，为找出不超过 N 的所有素数，给出一种方法，叫做厄拉多塞筛法. 建议：

1. 讲清素数概念. 要特别强调 1 不是素数、2 是最小的素数、也是唯一的偶素数，其余素数都是奇数，但奇数不一定是素数.

2. 可用 100 以内的素数 2、3、5、7、11、13、17、19、23、29、41、43、47、53、59、61、67、71、73、79、83、89、97 让同学们感受素数分布很不规则. 找出一定范围内的所有素数是一件很艰难的工作. 但有人编制了一本素数表格，厚达 276 页，印有二百万以内的全部素数，从 2 到 1 999 993 共有 148 933 个素数. 18 世纪，人类知道的最大素数是 $2^{31}-1$，19 世纪的记录是 $2^{127}-1$，20 世纪是 $2^{1\,398\,269}-1$. 新世纪这个纪录又有新的突破.

3. 了解厄拉多塞筛法，知其原理，并会用此法找出不超过 N 的素数.

厄拉多塞筛法的基本原理是一个整数大于 1 的最小约数必为素数，这是容易理解的. 因为大于 1 的最小正约数若能分解，便得到一个更小的约数，得到矛盾.

显然合数 a 的大于 1 的最小约数不超过 $\sqrt{a}$（如 $a=pq$，$p\leqslant q$，则 $p\leqslant\sqrt{a}$）.

为把不超过 N 的素数全部列出，只须在 2 到 N 的全部正数中，将 2，3，5，7，…，直至不超过 $\sqrt{N}$ 的素数全部留下，划去它们的倍数就完成了. 原因是在 $2\sim N$ 的整数中，不是合数，就是素数. 如果是合数，必会有不超过 $\sqrt{N}$ 的素因数. 把这些素因数的倍数都划去了，也就是把合数都划去了，剩下的都是素数.

4. 判断正整数 N 是否素数，原则上要用不超过 $\sqrt{N}$ 的素数逐个试除. 例如，

$N=299$，$17<\sqrt{N}<18$，原则上要用 2、3、5、7、11、13、17 逐个试除，但这里容易看出 $13\mid 299$，知 299 不是素数.

$N=293$，$16<\sqrt{N}<17$，易知，293 不是 2、3、5、7、11、13 的倍数，因此 293 是素数.

5. 要求学生知道素数无穷，并能给出证明. 同时让学生感知，素数很稀疏，例如，

$$(n+1)!+2,\ (n+1)!+3,\ \cdots,\ (n+1)!+n,\ (n+1)!+(n+1)$$

是 n 个连续的合数，由此可见，有的相邻两素数相隔遥远.

6. 可补充如下例习题.

(1) 若 $p>1$，$p\mid(p-1)!+1$，则 p 为素数.

证明：假设 p 是合数. 可令 $p=p_1p_2$，$1<p_1<p$. 由 $p\mid(p-1)!+1$，知 $p_1\mid(p-1)!+1$，而 $p_1\mid(p-1)!\Rightarrow p_1\mid 1$. 矛盾.

(2) 有人证明了当 $n=0$，1，2，…，11 000 时，$n^2+n+72\ 491$ 都是素数. 证明：永远找不到整系数多项式 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$，当 x 为整数时，$f(x)$都是素数.

证明：假设 $f(x)$当 $x=m$ 时是素数. 令 $f(m)=p$，将 $x=m+kp$ 代入，得

$$\begin{aligned}f(m+kp)&=a_n(m+kp)^n+\cdots+a_1(m+kp)+a_0\\&=f(m)+lp=p+lp=p(1+l)，\text{其中 } l \text{ 为整数.}\end{aligned}$$

可见 $f(m+kp)$是合数.

1.3 带余除法

整数的带余除法是研究整除的出发点，也是初等数论的基础. 本节首先讲解带余除法定理，然后，把数的进制作为带余除法的应用予以介绍，建议：

1. 首先引导同学从熟知的整数除法，总结出两整数相除，商和余数是唯一存在的. 然后把此结论写成带余除法表达式（或定理）：

设 a、b 为整数，$b>0$，则存在唯一一对整数 q、r，使

$$a=bq+r,\ 0\leqslant r<b,$$

再给出严格证明. 注意此定理中，对 a、q 只要求是整数，可以为正，也可以为 0 或负；对 b 要求为正；对 r 的要求是很明确的：$0\leqslant r<b$，即 r 只能取 0，1，2，…，$b-1$ 这 b 个值. 例如，$a=-7$，$b=3$，$-7=3\times(-3)+2$ 是正确的带余除法表达式，而 $-7=3\times(-2)+(-1)$则是不正确带余除法表达式.

注意 a 可以小于 b. 例如，$a=8$，$b=14$，则 $a=14\cdot 0+8$；又如 $a=-12$，$b=14$，则 $-12=14\cdot(-1)+2$.

2. 如果将除数 $b>0$ 改成 $b\neq 0$，则带余除法表示为：设 a、b 为整数，$b\neq 0$，则存在唯一一对 q、r，使

$$a=bq+r,\ 0\leqslant r<|b|.$$

例如，$a=8$，$b=-3$，则

$$8=(-3)\times(-2)+2$$

是正确的带余除法表达式，而 $8=(-3)\times(-3)+(-1)$不是带余除法表达式，原因是 $r<0$；$8=(-3)\times(-1)+5$ 也不是带余除法表达式，原因是 $r>|b|$.

3. 用带余除法认识数的进制.

设 b 是大于 1 的整数，对任一整数 N，都可唯一表为

$$N=a_nb^n+a_{n-1}b^{n-1}+\cdots+a_1b+a_0.$$

其中 a_k 在 0，1，2，…，$b-1$ 中取值. 这就是 N 的 b 进制表达式，b 称为基数，可简记为

$$N=(a_na_{n-1}\cdots a_0)_N.$$

证明如下：由带余除法知存在唯一一对数 N_1，a_0 使

$$N=N_1b+a_0,\ 0\leqslant a_0<b.$$

继而存在唯一一对整数 N_2，a_1 使

$$N_1=N_2b+a_1,\ 0\leqslant a_1<b.$$

于是 $N=(N_2b+a_1)b+a_0=N_2b^2+a_1b+a_0$. 继续对 N_2 做带余除法，最终得到存在唯一一组数 a_0，a_1，…，a_n 使

$$N=a_nb^n+a_{n-1}^{n-1}b^{n-1}+\cdots+a_1b+a_0,\ 0\leqslant a_1<b.$$

这个证明还给出了 N 的 b 进制的求法.

由 N 的 b 进制表达式很容易换成十进制表达式，直接计算 b 的多项式的值就完成了. 反过来，对十进制数 N，可反复用带余除法求出其 b 进制表达式. 例如用 3 进制表示 10 进制数 101，算法如下：

$101=33\cdot 3+2$

$33=11\cdot 3+0$

$11=3\cdot 3+2\ \Rightarrow\ (101)_{10}=(10202)_3.$

$3=1\cdot 3+0$

$1=0\cdot 3+1$

如何将 b 进制换成 c 进制呢？一个行之有效的方法是将 b 进制换成 10 进制，再把 10 进制换成 c 进制. 例如，将$(1100101)_2$ 换成 8 进制和 5 进制，算法如下：

$(1100101)_2=2^6+2^5+2^2+1=101,$

$101=8^2+4\cdot 8+5=(145)_8,$

$101=4\times 5^2+1=(401)_5.$

4. 可补充例习题，如

(1) $3\times 5=13$ 是什么进制的乘法口诀？

解：$3\times 5=13$ 表明基数 $b>5$. 可见符号 1、3、5 在 b 进制与 10 进制中所表示的数值是相同的.

$(13)_b=b+3$，$b+3$ 是 10 进制数，在 10 进制中，$3\times 5=15$，3×5 在 b 进制与 10 进制中所表示的数值应该相同，于是

$$b+3=15.$$

由此 $b=12$.

(2) $22\times 31=1232$ 是什么进制的乘法？并将其化为 10 进制乘法，看结果是否一致？

解：设基数为 b，由 $22\times 31=1232$ 可知

$$(2b+2)(3b+1)=b^3+2b^2+3b+2,$$

$\Rightarrow b^3-4b^2-5b=0$，因 $b>1$，约去 b 可得

$$b^2-4b-5=0.$$

解得 $b=5$.

$(22)_5\times(31)_5=(1232)_5.$

换成 10 进制：$(22)_5=12$，$(31)_5=16$，$(1232)_5=192.$

上述乘法等式换成 10 进制便是

$$12\times16=192.$$

这个结果与 10 进制乘法是一致的.

1.4 辗转相除法与最大公约数

辗转相除法是带余除法的延伸. 它对两数相除的除数和余数反复做带余除法，直至余数为 0 时截止. 本节的核心内容是就如何求出辗转相除法中各级余数，给出了一个行之有效的算法. 本节还讲清了如何用辗转相除法求最大公约数及最大公约数的若干性质.

建议：

1. 首先对具体数字反复做带余除法. 例如，对 704 与 108，351 与 201 作如下运算：

$$\begin{aligned} 704&=108\times6+56 & 351&=201\times1+150\\ 108&=56\times1+52 & 201&=150\times1+51\\ 56&=52\times1+4 & 150&=51\times2+48\\ 52&=4\times13+0 & 51&=48\times1+3\\ & & 48&=3\times16+0 \end{aligned}$$

这种反复将前式的除数作被除数，余数作除的带余除法，一直做到余数为 0 的算法叫做辗转相除法. 由于余数（非负）越来越小，做了若干次带余除法后，最终总可以使余数为 0.

辗转相除法写成一般的表达式就是：设有整数 a、b $(a,\ b>0)$，

$$\begin{aligned} &a=bq_1+r_1,\ 0<r_1<b,\\ &b=r_1q_2+r_2,\ 0<r_2<r_1,\\ &r_1=r_2q_3+r_3,\ 0<r_3<r_2,\\ &\quad\vdots\\ &r_{n-2}=r_{n-1}q_n+r_n,\ 0<r_n<r_{n-1},\\ &r_{n-1}=r_nq_{n+1}+r_{n+1},\ r_{n+1}=0. \end{aligned}$$

2. 由辗转相除法的表达式，可以给出各余数的关于 a、b 的表达式：

$$\begin{aligned} r_1&=a-q_1b,\\ r_2&=b-r_1q_2=b-(a-q_1b)q_2=-q_2a+(1+q_1q_2)b.\\ r_3&=r_1-r_2q_3=(a-q_1b)-[-q_2a+(1+q_1q_2)b]q_3\\ &=(1+q_2q_3)a-(q_1+q_3+q_1q_2q_3)b. \end{aligned}$$

这样算下去非常麻烦，本节定理 1 给出了一种逆推算法，不要求学生严格证明定理 1，可用 r_1，r_2，r_3 的表达式来验证公式

$$(-1)^{k-1}r_k=Q_ka-P_kb,$$

令 $Q_0=0$，$Q_1=1$，有 $Q_2=q_2Q_1+Q_0=q_2$，$Q_3=q_3Q_2+Q_1=q_3q_2+1$，

$P_0=1$，$P_1=q_1$，有 $P_2=q_2P_1+P_0=q_1q_2+1$，$P_3=q_3P_2+P_1=q_3(1+q_1q_2)+q_1=q_1+q_3+q_1q_2q_3$. 这和以上直接算出的 r_2，r_3 的表达式完全一致.

3. 要求学生掌握 $(a,\ b)=r_n$ 的来源，r_n 是辗转相除的倒数第二个余数，而 $r_{n+1}=0$ 是最后一个余

数. 并通过若干实例让学生掌握最大公约数的求法.

要求学生知道 (a, b) 可表为 $ma+nb$，并且知道如果 a，b 的公约数 d 可以表为 $d=ma+nb$，则 d 为最大公约数. 理由如下：

设 d 为 a，b 的公约数，并设存在 m，n 使 $d=ma+nb$. 又设 d_1 是 a，b 的任一公约数，则有 $a=d_1m_1$，$b=d_1n_1$. 代入 d 的表达式 $d=mm_1d_1+nn_1d_1$，$\Rightarrow d_1 \mid d$，可见 $d \geqslant d_1$.

由此可见，a，b 互素的充分必要条件是存在 m，n 使 $ma+nb=1$. 例如

由 $3\times5-2\times7=1$ 可知 $(5, 7)=1$；

$3\times12-5\times7=1$ 可知 $(12, 7)=1$.

又如，相邻两正整数互素，可用 $(n+1)-n=1$ 来证明.

4. 可补充如下例习题.

(1) 证明 $21n+2$ 与 $28n+3$ 互素，其中 n 为正整数.

证明：容易看出

$$-4(21n+2)+3(28n+3)=1,$$

所以 $21n+2$ 与 $28n+3$ 互素.

(2) $2^{23}-1$ 与 $2^{22}+1$ 互素，试证之.

证明：做辗转相除，

$2^{23}-1=(2^{22}+1)\cdot1+(2^{22}-2)$，

$2^{22}+1=(2^{22}-2)\cdot1+3$，

$2^{22}-2=3\cdot\left(\dfrac{2^{22}-1}{3}-1\right)+2$（其中 $2^{22}-1=(3+1)^{11}-1$ 被 3 整除）或 $2^{22}-2=3\cdot(2^{20}+2^{18}+\cdots+2^2)+2$，

$3=2\cdot1+1$.

于是，$(2^{23}-1, 2^{22}+1)=1$.

1.5 最小公倍数

本节内容比较简单，给出了最小公倍数的定义及其四条性质. 建议强调以下几点：

1. 由实际问题引出研究最小公倍数的必要性，可补充实例，如“六十花甲子”.

甲 乙 丙 丁 戊 己 庚 辛 壬 癸

子 丑 寅 卯 辰 巳 午 未 申 酉 戌 亥

上行 10 个字与下行 12 个字依次两两搭配，形成年号：甲子、乙丑、丙寅、丁卯……正好 60 年一个轮回. 60 是 10 与 12 的最小公倍数.

2. 理解最小公倍数是正整数；在最小公倍数的定义中，要求每一个数非零，原因是如果有一个数为 0，则任何正整数都不是它们的公倍数.

3. 掌握最小公倍数的四条性质，特别是

$$[a\cdot b]=\frac{ab}{(a, b)}.$$

此公式给出了最小公倍数的算法，并由此可知互素两数的最小公倍数就是该两数之积.

1.6 算术基本定理

算术基本定理是算术与数论中最重要、最基本的定理之一，它和代数基本定理、微积分基本定理同样重要. 算术基本定理是说任何一个整数的素数分解式不仅存在，而且是唯一的. 这样对整数 N 的研究可归结到对 N 的分解式的研究，或者说归结到对 N 的素因子的研究.

本节先讲解该定理所需的预备知识，然后给出基本定理的证明，再列举该定理的若干应用.

建议：

1. 在证明基本定理之前，给出素数作除数的三条性质，务必要求学生掌握.

2. 要求学生理解并记住算术基本定理，对证明过程不要求学生掌握. 通过算术基本定理，让学生理解 1 不算作素数的原因，因为否则分解式就不唯一.

3. 掌握计算一个整数的正约数个数的计算公式，并用实例加以验证. 如

$\tau(36)=\tau(2^2\cdot 3^2)=(2+1)(2+1)=9.$

事实上，36 的正约数有 1、2、3、4、6、9、12、18、36，一共 9 个.

4. 运用算术基本定理求最大公约数与最小公倍数. 例如，

设 $a=2^3\cdot 3^2\cdot 5^4$，$b=2^2\cdot 3^4\cdot 5\cdot 7^2$，则

$(a,\ b)=2^2\cdot 3^2\cdot 5$，$[a,\ b]=2^3\cdot 3^4\cdot 5^4\cdot 7^2.$

5. 可补充例题.

设 n 是正整数，证明 $\lg n$ 不是整数就是无理数.

证明：令 $\lg n=a$，则 $n=10^a$. 假设 a 是分数，$a=\dfrac{q}{p}$，p 与 q 互素. $\Rightarrow n^p=10^q=2^q\cdot 5^q.$

由算术基本定理，n 可唯一表为 $n=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$. $n^p=p_1^{p\alpha_1}p_2^{p\alpha_2}\cdots p_k^{p\alpha_k}$. 由唯一性可知 $k=2$，$p_1=2$，$p_2=5$，$\Rightarrow 2^{p\alpha_1}\cdot 5^{p\alpha_2}=2^q\cdot 5^q$. $\Rightarrow p\alpha_1=q$，$p\alpha_2=q$. $\Rightarrow p\mid q$，这与假设矛盾.

1.7 二元一次不定方程

本节比较完整地讲述了求解二次一元不定方程的理论与方法. 首先给出二元一次不定方程有解的充分必要条件，然后给出了通解公式（通解与特解的关系），最后是求特解的算法. 用辗转相除法求特解是本节的核心，也是落脚点，要求学生不仅知道怎样计算，而且要理解其中的道理. 建议：

1. 由简单的实际问题引出二元一次方程，并用试算的方法给出解答，让学生体会不定方程及其解的意义. 例如，用票面为 2 元与 5 元的人民币支付 30 元，有哪些支付方案?

解：列不定方程，设 5 元票用 x 张，2 元票用 y 张.

$$5x+2y=30.$$

易知，用奇数张 5 元票，方程无解，令 $x=0$，2，4，6，则相应的 $y=15$，10，5，0. 问题的全部解答是（5 元票张数，2 元票张数）$=(0,\ 15)$，$(2,\ 10)$，$(4,\ 5)$，$(6,\ 0)$.

2. 要求学生掌握二元一次不定方程 $ax+by=c$ 有解的充分必要条件是 $(a, b)|c$，并用实例检验. 例如，

$12x+9y=124$，$(12, 9)\nmid 124$，无解.

$12x+9y=126$，$(12, 9)|126$，有解.

3. 要求学生掌握通解公式：设 x_0，y_0 是 $ax+by=c$ 的一个特解，则通解为

$$\begin{cases} x=x_0+\dfrac{b}{(a, b)}t, \\ y=y_0-\dfrac{a}{(a, b)}t. \end{cases} \quad t \text{ 为任意整数.}$$

可用代入法检验：$a\left(x_0+\dfrac{b}{(a, b)}t\right)+b\left(y_0-\dfrac{a}{(a, b)}t\right)=ax_0+by_0=c.$

4. 特解的求法.

既然有了用特解求通解的公式，那么求一个特解便成了解不定方程的关键.

在不定方程 $ax+by=c$ 中，不妨设 $(a, b)=1$，否则方程可化为 $\dfrac{a}{(a, b)}x+\dfrac{b}{(a, b)}y=\dfrac{c}{(a, b)}$. 因为原方程有解的充要条件是 $(a, b)|c$，所以，如果原不定方程有解，$\dfrac{c}{(a, b)}$ 必为整数，这种变化是合理的.

由 1.4 节定理 1，

$$Q_na-P_nb=(-1)^{n-1}r_n.$$

因为 $r_n=(a, b)=1$，所以

$$Q_na-P_nb=(-1)^{n-1},$$

$\Rightarrow Q_na\cdot c-P_nb\cdot c=(-1)^{n-1}c,$

$\Rightarrow a[(-1)^{n-1}Q_nc]+b[(-1)^nP_nc]=c.$

于是不定方程有特解

$$x_0=(-1)^{n-1}Q_nc,\ y_0=(-1)^nP_nc.$$

再由 1.4 定理 1 中的逆推公式算出 Q_n 与 P_n.

用实例来体会上述求特解的方法.

例 1　求不定方程 $7x+4y=100$ 的整数解.

解：作辗转相除

$$\begin{array}{l} 7=4\times1+3, \\ 4=3\times1+1 \end{array} \Rightarrow \begin{array}{l} q_1=1, \\ q_2=1, \end{array} \Rightarrow \begin{array}{l} Q_0=0,\ P_0=1, \\ Q_1=1,\ P_1=q_1=1 \end{array} \Rightarrow \begin{array}{l} Q_2=q_2Q_1+Q_0=1\cdot1+0=1, \\ P_2=q_2P_1+P_0=1\cdot1+1=2. \end{array}$$

$x_0=(-1)^{n-1}Q_nc=-100$，$y_0=(-1)^nP_nc=200$，这里 $n=2$.

通解为 $x=-100+4t$，$y=200-7t$，t 为整数.

例 2　求整数解：$12x+31y=135$.

解：作辗转相除

$$\begin{array}{ll} 31=12\times2+7, & q_1=2, \\ 12=7\times1+5, & q_2=1, \\ 7=5\times1+2, & q_3=1, \\ 5=2\times2+1, & q_4=2, \end{array} \Rightarrow \text{令} \quad \begin{array}{l} Q_0=0, \\ Q_1=1, \\ P_0=1, \\ P_1=2, \end{array}$$

$Q_2=q_2Q_1+Q_0=1$，$P_2=q_2P_1+P_0=3$，

$\Rightarrow Q_3=q_3Q_2+Q_1=2$，$P_3=q_3P_2+P_1=5$，

$Q_4=q_4Q_3+Q_2=5$，$P_4=q_4P_3+P_2=13$.

特解为

$x_0=(-1)^4\cdot 13\cdot 135$

$y_0=(-1)^3\cdot 5\cdot 135$ （因为作辗转相除时，12 与 31 交换了位置，相应的 x 与 y 要交换位置.）

通解为

$x=13\cdot 135+31t$，

$y=-5\cdot 135-12t$，t 为整数.

注意，如果 x，y 不交换位置，作辗转相除，第一式为 $12=31\times 0+12$，以下步骤与前面完全相同. 商依次为 $q_1=0$，$q_2=2$，$q_3=1$，$q_4=1$，$q_5=2$.

$Q_0=1$，$Q_1=1$，$Q_2=2$，$Q_3=3$，$Q_4=5$，$Q_5=13$，

$P_0=1$，$P_1=0$，$P_2=1$，$P_3=1$，$P_4=2$，$P_5=5$.

$r_n=(12,\ 31)$，$n=5$. 特解为

$x_0=(-1)^{5-1}Q_5\cdot 135=13\cdot 135$，

$y_0=(-1)^5P_5\cdot 135=-5\cdot 135$.

结果完全一致，但多做了一步除法，计算 Q_n，P_n 多一个步骤.

第二章

同　余

Ⅰ 教学要求

1. 掌握同余概念及其性质，熟悉同余符号，学会运用同余处理一些整除问题.

2. 掌握剩余类概念及剩余类的加法乘法运算，体会剩余类运算的特点，要特别注意非零 $\bar{a}$，$\bar{b}$，其积可能为 $\bar{0}$.

3. 理解完全剩余系与简化剩余系概念. 了解如下结论：

(1) 当 $(k, m)=1$ 时，如果 x 遍历 m 的一个完全剩余系，则 $kx+l$ 也遍历模 m 的一个完全剩余系；

(2) 当 $(k, m)=1$ 时，如果 x 遍历 m 的一个简化剩余系，则 kx 也遍历模 m 的一个简化剩余系；

4. 掌握欧拉函数概念，并会用如下公式求欧拉函数的值：

(1) 设 $(m_1, m_2)=1$，则 $\varphi(m_1m_2)=\varphi(m_1)\varphi(m_2)$；

(2) 若 n 的全部素因数为 p_1，p_2，…，p_k，则

$$\varphi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right).$$

5. 掌握欧拉定理及费马小定理，并学会运用这两个定理解决一些整除问题.

6. 会用同余性质作出一些不定方程无解的结论.

Ⅱ 本章重点、难点与课时分配

本章重点是：(1) 同余及其性质、剩余类及其运算；(2) 完全剩余系和简化剩余系概念；
(3) 欧拉函数及其求法；(4) 欧拉定理及其应用.

本章难点是：(1) 同余符号的掌握，对剩余类运算的理解；
(2) 对剩余系性质的理解，对剩余系性质证明的理解；
(3) 欧拉定理的证明与运用.

课时分配：本章共用 6 学时，3.1 节与 3.2 节合用 1 学时，3.3 节用 1 学时，3.4 节用 2 学时，3.5 节用 1 学时，3.6 节用 1 学时.

2.1 同余及其基本性质

同余是数论中的基本概念，也是研究整除问题的基本工具. 本节基本内容是同余概念、同余符号与同余性质，务必要求学生掌握. 建议：

1. 弄清“模 m”的含义. “模 m”相当于“除以 m”，m 必须是正整数. 说 a，b 模 m 同余时，a，b 可为正、负整数或 0. 例如，$-2\equiv5(\mathrm{mod}\ 7)$，$-14\equiv0(\mathrm{mod}\ 7)$.

在记 $a\equiv b$ 时，千万不能忘记 $(\mathrm{mod}\ m)$，一定要写成

$$a\equiv b(\mathrm{mod}\ m).$$

在写连续的同余等式时，在出现 $a=b$ 的情形，可仍然用符号“$\equiv$”，写成 $a\equiv b(\mathrm{mod}\ m)$，但不能把 $a\equiv b(\mathrm{mod}\ m)$ 写成 $a=b$. 例如，

$8+2+(-2)+1=8+1\equiv4(\mathrm{mod}\ 5)$，

可以写成

$8+2+(-2)+1\equiv8+1\equiv4(\mathrm{mod}\ 5)$.

2. 掌握 a，b 模 m 同余的充分必要条件是 $m\mid(a-b)$，并会灵活运用这个结论.

3. 在教学同余性质 1、2、3 时，可先用具体数字让学生领悟. 例如，

性质 1　$3\equiv-4(\mathrm{mod}\ 7)$，$9\equiv2(\mathrm{mod}\ 7)$，则有

(1) $3+9\equiv-4+2(\mathrm{mod}\ 7)$，即 $12\equiv-2(\mathrm{mod}\ 7)$；(2) $3\times9\equiv-4\times2(\mathrm{mod}\ 7)$，即 $27\equiv-8(\mathrm{mod}\ 7)$.

性质 2　若 $ac\equiv bc(\mathrm{mod}\ m)$，且 $(c,\ m)=d$，则 $a\equiv b\left(\mathrm{mod}\ \frac{m}{d}\right)$.

这个性质告诉我们如下事实：

(1) 当 $(c,\ m)=1$ 时，在 $ac\equiv bc(\mathrm{mod}\ m)$ 中，可以约去 c：$a\equiv b(\mathrm{mod}\ m)$. 没有 c，m 互素这个条件不能约去 c，例如

$3\times7\equiv-2\times7(\mathrm{mod}\ 5)$，因为 $(c,\ m)=1$，所以 $3\equiv-2(\mathrm{mod}\ 5)$.

$3\times10\equiv-4\times10(\mathrm{mod}\ 5)$，$(c,\ m)=5$，不能约去 10. 事实上，

$3\not\equiv-4(\mathrm{mod}\ 5)$.

(2) 注意 $ac\equiv bc(\mathrm{mod}\ m)$，$(c,\ m)=d$，要约去 c，必须同时约去模 m 中的因数 d.

由 $5\times3\equiv7\times3(\mathrm{mod}\ 6)$，可得 $5\equiv7(\mathrm{mod}\ 2)$.

性质 3　若 $a\equiv b(\mathrm{mod}\ m_i)$，$i=1,\ 2,\ \cdots,\ n$. 则

$a\equiv b(\mathrm{mod}[m_1,\ m_2,\ \cdots,\ m_n])$.

以 $n=2$ 为例，

$$\begin{cases}123\equiv63(\mathrm{mod}\ 12)\\123\equiv63(\mathrm{mod}\ 15)\end{cases}\Rightarrow123\equiv63(\mathrm{mod}\ 60).$$

$$\begin{cases}56\equiv 38(\bmod 9)\\ 56\equiv 38(\bmod 6)\end{cases}\Rightarrow 56\equiv 38(\bmod 18).$$

4. 学会用同余符号和同余性质解决一些整除问题. 可补充

例 1　证明：若 n 不是 4 的倍数，则 $5\mid(1^n+2^n+3^n+4^n)$.

证明：令 $n=4k+r$，$r=1$，2 或 3.

$$1^n+2^n+3^n+4^n\equiv 1+16^k\cdot 2^r+81^k\cdot 3^r+16^{2k}4^r$$
$$\equiv 1+2^r+3^r+4^r\equiv 1+2^r+(-2)^r+(-1)^r(\bmod 5).$$

当 $r=1$ 时，$1^n+2^n+3^n+4^n\equiv 1+2+(-2)+(-1)\equiv 0(\bmod 5)$，

当 $r=2$ 时，$1^n+2^n+3^n+4^n=1+4+4+1\equiv 0(\bmod 5)$，

当 $r=3$ 时，$1^n+2^n+3^n+4^n=1+8-8-1\equiv 0(\bmod 5)$.

例 2　求 14^{14} 的末两位数字.

解：$14^{14}\equiv(14^2)^7\equiv(196)^7\equiv(\quad 4)^7\equiv(-4)^4(-4)^3\equiv 56\cdot(-64)$

$$\equiv -3584\equiv -84=16(\bmod 100).$$

14^{14} 的末两位数是 16.

2.2　特殊数的整除特征

本节内容比较简单，只是讨论被 3、9 与 7、11、13 整除的整数的特征. 理论不必多讲，重点在实际判断一个数是否被这些数整除. 建议补充：

1. 一个数被 3、9 整除的充要条件是各位数字之和被 3、9 整除，更进一步有如下结论：

若数 $n=\overline{n_1n_2\cdots n_k}$ 是 10 进制数，则

$$n\equiv n_1+n_2+\cdots+n_k(\bmod 9)\ 或(\bmod 3).$$

例 1　证明 2 357 844 不是完全平方数.

证明：$n=2\ 357\ 844\equiv 2+3+5+7+8+4+4\equiv 33\equiv 6(\bmod 9)$.

假设 n 是完全平方数，$n=p^2\equiv(9k+r)^2\equiv r^2$，$0\leqslant r\leqslant 8$. 但 $r^2\not\equiv 6(\bmod 9)$，矛盾.

例 2　设 $n=2\ 007^{2\ 008}$ 各位数字之和为 A，A 的各位数字之和为 B，B 的各位数字之和是多少？

解：容易看出 $n\equiv 0(\bmod 9)$.

$$\lg n=2\ 008\lg 2\ 007<2\ 008\times 4=8\ 032.$$

可见 n 的位数不超过 8 032. 所以 $A<8\ 032\times 9=72\ 288$. $B<7+4\times 9=43$. B 的各数字之和 C 小于 $4+9=13$. 由于 $n\equiv C(\bmod 9)$，n 是 9 的倍数，C 也是 9 的倍数，在小于 13 的正整数中，只有 9 被 9 整除，所以 B 的各位数字之和是 9.

2. 判断正整数 n 是否被 7、11、13 整除是将 n 按三位数分段，右起第一段取正号，以下各段正负相间，求各段的代数和，看其是否被 7、11、13 整除.

例如，$n=4\ 657\ 842$，先计算代数和

$$842-657+4=189$$

易知 $7\mid 189$，$11\nmid 189$，$13\nmid 189$，因此 n 是 7 的倍数，而不是 11 和 13 的倍数.

判断 n 是否是 11 的倍数是将各位数字隔位相加，所得两数之差是否为 11 的倍数，或者说，各位数

字正负相间，看其代数和是否为 11 的倍数.

理由如下：当 m 为奇数时，$11\mid 10^m+1$；当 m 为偶数时，$11\mid 10^m-1$.

设 $n=a_k10^k+a_{k-1}10^{k-1}+\cdots+a_1 10+a_0$，令

$p=a_1+a_3+a_5+\cdots$，

$q=a_0+a_2+a_4+\cdots$，

$n+p-q=a_1(10+1)+a_2(10^2-1)+a_3(10^3+1)+a_4(10^4-1)+\cdots$.

上式右边被 11 整除，n 能否被 11 整除，取决于 $p-q$ 能否被 11 整除.

例如 39578，$(3+5+8)-(9+7)\equiv 0(\mathrm{mod}\ 11)$，可见 39578 是 11 的倍数.

3. 建议补充以下例习题

1. 证明对任何自然数 n，$7\nmid(2^n+1)$.

证明：令 $n=3k+r$，$r=0$，1 或 2.

$2^n+1\equiv 2^{3k}\cdot 2^r+1\equiv 8^k\cdot 2^r+1\equiv(7+1)^k\cdot 2^r+1\equiv 2^r+1(\mathrm{mod}\ 7)$.

而当 $r=0$，1 或 2 时，$7\nmid(2^r+1)$. 故 $7\nmid(2^n+1)$.

2. 设 $17\mid 2^n+1$，求 n.

解：设 $n=4k+r$，$r=0$，1，2 或 3.

$2^n+1\equiv 2^{4k}\cdot 2^r+1\equiv 16^k\cdot 2^r+1\equiv(-1)^k\cdot 2^r+1(\mathrm{mod}\ 17)$.

当 $r=1$，2，3 时，$17\nmid(-1)^k2^r+1$.

当 $r=0$ 时，

$2^n+1\equiv(-1)^k+1(\mathrm{mod}\ 17)$.

可见当 k 为奇数时，$2^n+1\equiv 2^{4k}+1\equiv 0(\mathrm{mod}\ 17)$.

故当 $n=4(2m+1)=8m+4$ 时，$17\mid 2^n+1$，其中 m 为自然数.

例如 $2^{12}+1=4\ 096+1=4\ 097=17\times 241$.

2.3 剩余类及其运算

剩余类是数论中基本概念之一. 剩余类的运算是学生没有接触过的新运算，但它仍以数的运算为基础. 本节教学应注意以下几点：

1. 掌握剩余类的意义. 设 $m>0$，模 m 的剩余类是将全体整数分类，把模 m 余数相同的整数分在一类. 这样，模 m 的剩余类共有如下 m 个：

$$K_r=\{qm+r\},\ r=0,\ 1,\ 2,\ \cdots,\ m-1.\ \text{其中 } q \text{ 为整数.}$$

记号 $\bar{a}$ 表示 a 所属的剩余类，a 称作代表元，那么 $K_r=\bar{r}=\overline{qm+r}$. K_r 中任何一个元素都可以作代表元. 例如，模 7，-5，2，9 都可以作为 K_2 的代表元，即 $\overline{-5}=\bar{2}=\bar{9}(\mathrm{mod}\ 7)$.

Z_m 表示模 m 的所有剩余类组成的集合. 这样

$$Z_m=\{K_0,\ K_1,\ K_2,\ \cdots,\ K_{m-1}\}=\{\bar{0},\ \bar{1},\ \bar{2},\ \cdots,\ \overline{m-1}\}.$$

例如模 7，

$$Z_7=\{\bar{0},\ \bar{1},\ \bar{2},\ \cdots,\ \bar{6}\}.$$

例 1　把以下整数按模 7 分类：-10，-9，-8，$\cdots$，0，1，2，$\cdots$，10.

解：0，7，$-7\in K_0$；1，8，$-6\in K_1$；2，9，$-5\in K_2$；3，10，$-4\in K_3$；

4，-3，$-10\in K_4$；5，-2，$-9\in K_5$，6，-1，$-8\in K_6$.

2. 理解剩余类加法与乘法意义：

设$\bar{a}$，$\bar{b}\in Z_m$，定义

$$\bar{a}+\bar{b}=\overline{a+b},\ \bar{a}\cdot\bar{b}=\overline{a\cdot b}.$$

应注意以下两点：(1) 同一模的剩余类才能进行运算；(2) 剩余类的运算与数的运算、集合的运算是不同的，不能混为一谈. 比如，集合的交集运算结果是两集合的公共部分，而两剩余的积可能是另一个剩余类.

例如 (1) 在Z_7中，

$\bar{1}+\bar{5}=\bar{6}$，$\bar{3}+\bar{4}=\bar{0}$，$\bar{4}+\bar{5}=\bar{2}$，

$\bar{1}\cdot\bar{5}=\bar{5}$，$\bar{3}\cdot\bar{4}=\bar{5}$，$\bar{4}\cdot\bar{5}=\bar{6}$；

(2) 在Z_6中，

$\bar{1}+\bar{5}=\bar{0}$，$\bar{3}+\bar{4}=\bar{1}$，$\bar{4}+\bar{5}=\bar{3}$，

$\bar{2}\cdot\bar{5}=\bar{4}$，$\bar{3}\cdot\bar{4}=\bar{0}$，$\bar{4}\cdot\bar{5}=\bar{2}$.

3. 因为剩余类的运算基于数的运算，因此剩余类加法、乘法运算满足交换律、结合律，乘法对加法满足分配律，仅以分配律为例说明之.

$\bar{a}(\bar{b}+\bar{c})=\bar{a}\cdot\overline{\bar{b}+\bar{c}}=\overline{a(b+c)}=\overline{ab+ac}=\overline{ab}+\overline{ac}=\bar{a}\cdot\bar{b}+\bar{a}\cdot\bar{c}$.

4. 对环的定义只作了解，说明Z_m（对所定义的加法与乘法）构成一个环.

5. 了解零因子概念：如果a，b非零，而$ab=0$，则称a、b为零因子. 在数的乘法中，若$ab=0$，则a、b中至少有一个为0，因此在实数集与复数集中，没有零因子. 在解多项式的方程时，如果$f(x)=g(x)\cdot h(x)=0$，则可通过$g(x)=0$，$h(x)=0$求解，原因是在多项式集合中没有零因子. 但在Z_m中，可能有零因子存在. 例如，在Z_6中，$\bar{2}\cdot\bar{3}=\bar{0}$，$\bar{2}$，$\bar{3}$是零因子；在$Z_{12}$中，$\bar{2}\cdot\bar{6}=\bar{0}$，$\bar{3}\cdot\bar{4}=\bar{0}$，$\bar{2}$，$\bar{3}$，$\bar{4}$，$\bar{6}$是零因子.

可补充下列例习题：

(1) 说明Z_7中没有零因子；(2) 找出Z_{36}中的零因子；

(3) 编制Z_{11}中乘法表.

2.4 剩余系和欧拉函数

本节是为下一节证明欧拉定理作准备的，非常重要. 首先引入欧拉函数和剩余系的概念，然后给出剩余系的两条性质，最后得出欧拉函数的计算公式，在本节教学时，建议注意以下几点：

1. 欧拉函数是重要的数论函数，所谓数论函数是定义域和值域都是整数集的函数. 例如，表示n的正约数的个数$\tau(n)$是数论函数. 欧拉函数的定义域和值域都是正整数集. 在交待了定义以后，让学生写出$\varphi(1)$，$\varphi(2)$，…，$\varphi(20)$及$\varphi(p^2)$，p为素数，以体会欧拉函数的意义.

2. 理解互素剩余类的意义，我们知道模m的所有剩余类集合Z_m有m个元素，模m的互素剩余类只是其中一部分. 例如，模12的互素剩余类有$\bar{1}$，$\bar{5}$，$\bar{7}$，$\overline{11}$，共4个，模13的互素剩余类有12个. —

般地，模 m 的互素剩余类有 $\varphi(m)$ 个.

理解完全剩余系与简化剩余系的意义. 剩余系是整数的集合，模 m 的一个完全剩余系是从模 m 的所有剩余类中，各取一个代表元（数）所构成的集合，其中最典型的一个是 $\{0, 1, 2, \cdots, m-1\}$. 其余的模 m 的完全剩余系都可表为 $\{k_0 m, k_1 m+1, k_2 m+2, \cdots, k_{m-1} m+m-1\}$，其中 k_i 是整数.

简化剩余系是完全剩余系的真子集，它由模 m 的所有互素剩余类中各取一个代表元（数）组成. 模 m 的简化剩余系共有 $\varphi(m)$ 个元素. 例如，$\{1, 5, 7, 11\}$ 是模 12 的一个简化剩余系. 模 12 的其余简化剩余系都可表为 $\{k_1 m+1, k_2 m+5, k_3 m+7, k_4 m+11\}$，其中 k_i 为整数.

3. 对本节定理 1 与定理 2 的含义要交待清楚.

定理 1 是说，(1) 当 k 与 m 互素时，如果 $\{x_0, x_1, \cdots, x_{m-1}\}$ 是模 m 的一个完全剩余系，那么，$\{kx_0+l, kx_1+l, \cdots, kx_{m-1}+l\}$ 也是模 m 的一个完全剩余系；(2) 当 k 与 m 互素时，如果 $\{x_1, x_2, \cdots, x_{\varphi(m)}\}$ 是模 m 的一个简化剩余系，则 $\{kx_1, kx_2, \cdots, kx_{\varphi(m)}\}$ 也是模 m 的一个简化剩余系.

以模 $m=12$ 为例，$\{0, 1, 2, \cdots, 11\}$ 是一个完全剩余系，取 $k=5$，$l=4$，那么

$$\{4, 9, 14, 19, 24, 29, 34, 39, 44, 49, 54, 59\}$$

也是模 12 的一个完全剩余系.

$\{1, 5, 7, 11\}$ 是模 12 的一个简化剩余系，那么 $\{5, 25, 35, 55\}$，$\{7, 35, 49, 77\}$ 也是模 12 的简化剩余系. 其中 k 分别取 5 和 7.

定理 2 比较复杂，涉及两个模. 意思是说，(1) 当 m_1 与 m_2 互素时，如果 $\{x_0, x_1, \cdots, x_{m_1-1}\}$，$\{y_0, y_1, \cdots, y_{m_2-1}\}$ 分别是模 m_1、模 m_2 的一个完全剩余系时，则

$$\{m_2 x+m_1 y \mid x=x_0, x_1, \cdots, x_{m_1-1}, y=y_0, y_1, \cdots, y_{m_2-1}\}$$

是模 $m_1 m_2$ 的一个完全剩余系，其中 x_i 与 y_i 两两搭配，共有 $m_1 m_2$ 个元素；(2) 的意义和 (1) 类似.

例如，$\{0, 1, 2\}$ 是模 3 的一个完全剩余系，$\{0, 1, 2, 3\}$ 是模 4 的一个完全剩余系，$(3, 4)=1$.

$\{4x+3y \mid x=0, 1, 2, y=0, 1, 2, 3\}$

$=\{0, 3, 6, 9, 4, 7, 10, 13, 8, 11, 14, 17\}$

是模 12 的一个完全剩余系.

$\{1, 2\}$ 是模 3 的一个简化剩余系，$\{1, 3\}$ 是模 4 的一个简化剩余系，则

$\{4x+3y \mid x=1, 2, y=1, 3\}$

$=\{7, 13, 11, 17\}$

是模 12 的一个简化剩余系.

4. 检验 m 个数是否构成模 m 的一个完全剩余系，只需检验这 m 个数是否两两不同余.

检验 $\varphi(m)$ 个数是否构成模 m 的一个简化剩余系，需检验这 $\varphi(m)$ 个数是否两两不同余，还需检验每一个数是否与 m 互素.

5. 由定理 2 立得公式

(1) $\varphi(m_1 m_2)=\varphi(m_1)\varphi(m_2)$，$(m_1, m_2)=1$；

(2) $\varphi(p^\alpha)=p^\alpha-p^{\alpha-1}$（$p$ 为素数）；

(3) $\varphi(n)=n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right)$，其中 $p_1, \cdots, p_k$ 是 n 的不同的素因数.

公式 (1) 的来源只需说明：由定理 2，模 $m_1 m_2$ 的简化剩余系有 $\varphi(m_1)\cdot\varphi(m_2)$ 个元素，因此 $\varphi(m_1 m_2)=\varphi(m_1)\varphi(m_2)$.

在应用公式（1）时，要特别注意 $(m_1, m_2)=1$ 这个条件. 例如，

$\varphi(12)=\varphi(3)\varphi(4)=2\cdot 2=4$，

$\varphi(12)\neq\varphi(2)\varphi(6)=1\cdot 2=2$.

可补充例习题，以熟悉上述公式.

例 1　$\varphi(64)=\varphi(2^6)=2^6-2^5=32$ 或 $\varphi(64)=64\cdot\left(1-\frac{1}{2}\right)=32$.

$\varphi(1\,000)=\varphi(2^3\cdot 5^3)=\varphi(2^3)\varphi(5^3)=(2^3-2^2)(5^3-5^2)=400$，

或 $\varphi(1\,000)=1\,000\left(1-\frac{1}{2}\right)\left(1-\frac{1}{5}\right)=400$.

例 2　$\varphi(1\,001)=\varphi(7\cdot 11\cdot 13)=\varphi(7)\varphi(11)\varphi(13)=6\times 10\times 12=720$.

或 $\varphi(1\,001)=1\,001\cdot\frac{6}{7}\cdot\frac{10}{11}\cdot\frac{12}{13}=720$.

2.5　欧拉定理

欧拉定理是数论中最重要的定理之一. 其证明以上节定理 1 为基础，非常容易，本节中心内容为该定理及其推论——费马小定理的应用.

1. 在研究整除时，欧拉定理与费马小定理起着重要作用. 在研究高次幂的整除性时，可用欧拉定理将幂降低，这是因为 $a^{\varphi(m)}\equiv 1(\mathrm{mod}\ m)$，$(a, m)=1$. 这样从 a 的高次幂中模去 $a^{\varphi(m)}$，余数不变. 进而只需研究 a 的低次幂模 m 的余数.

例如，求 27^{22} 的个位数字，由于 $(27, 10)=1$，$\varphi(10)=4$，$\Rightarrow 27^4\equiv 1(\mathrm{mod}\ 10)$，$27^{22}\equiv(27^4)^5\cdot 27^2\equiv 27^2\equiv 9(\mathrm{mod}\ 10)$.

求 23^{42} 的末两位数字，由于 $(23, 100)=1$，$\varphi(100)=40$，$\Rightarrow 23^{40}\equiv 1(\mathrm{mod}\ 100)$，$23^{42}\equiv 23^2\equiv 29(\mathrm{mod}\ 100)$.

2. 在应用欧拉定理与费马小定理时一定要注意幂的底与模 m 互素. 例如，

$$21^{12}=21^{\varphi(36)}\neq 1(\mathrm{mod}\ 36).$$

但对素数中 $a^p\equiv a(\mathrm{mod}\ p)$ 总是成立. 这是因为如果 a，p 不互素，则有 $a=kp$，因此 $a^p\equiv 0\equiv a(\mathrm{mod}\ p)$. 如果 a，p 互素，则由费马小定理，$a^{p-1}\equiv 1(\mathrm{mod}\ p)$，$\rightarrow a^p\equiv a(\mathrm{mod}\ p)$.

3. 可补充例习题：

（1）证明 $546\mid n^{13}-n$.

证明：$546=2\times 3\times 7\times 13$，首先 $n^{13}-n$ 为偶数，$2\mid n^{13}-n$

$n^{13}-n\equiv(n^3)^4\cdot n-n\equiv n^4\cdot n-n\equiv n^3\cdot n^2-n=n^3-n\equiv 0(\mathrm{mod}\ 3)$

$n^{13}-n\equiv n^7\cdot n^6-n\equiv n\cdot n^6-n\equiv n^7-n\equiv 0(\mathrm{mod}\ 7)$

$n^{13}-n\equiv 0(\mathrm{mod}\ 13)$.

由 2，3，7，13 两两互素，知 $546\mid n^{13}-n$.

（2）求 $2\,007^{2\,008}$ 的末两位数.

解：$\varphi(100)=40$，$2\,007^{2\,008}\equiv 2\,007^{50\times\varphi(100)}\,2\,007^8\equiv 2\,007^8\equiv 7^8\equiv[(50-1)^2]^2\equiv 1(\mathrm{mod}\ 100)$.

故所求末两位数是 01.

(3) 设 $n>1$，证明 $n\nmid 2^n-1$.

证明：不妨设 n 不含素因子 2（否则必有 $n\nmid 2^n-1$）. 设 p 是 n 的最小素因子，$(p,2)=1$. 由费马小定理，$p\mid 2^{p-1}-1$. 令 q 是使得 $p\mid 2^m-1$ 的正整数 m 的最小值. 于是，

$$1<q\leqslant p-1,\ 2^q\equiv 1(\mathrm{mod}\ p).$$

因为 p 是 n 的最小素因子，所以 q 不是 n 的约数，即 $q\nmid n$. 可令

$$n=kq+r,\ 0<r<q,$$

$$2^n-1=2^{kq+r}-1=(2^q)^k\cdot 2^r-1\equiv 2^r-1(\mathrm{mod}\ p).$$

假设 $n\mid 2^n-1$，则有 $p\mid 2^n-1$. 由上式知 $p\mid 2^r-1$，$r<q$，这与 q 是 $p\mid 2^m-1$ 的 m 的最小值矛盾. 因此，$n\nmid 2^n-1$.

2.6 不定方程与同余

本节介绍同余的一种应用，用同余来判定某些不定方程无解. 讲授本节时，建议注意以下几点：

1. 如果不定方程 $f(x,y,\cdots)=0$ 有整数解 $(x,y,\cdots)$. 那么对任意正整数 m，必有 $f(x,y,\cdots)\equiv 0(\mathrm{mod}\ m)$. 那么，如果对任一正整数 m，$f(x,y,\cdots)\not\equiv 0(\mathrm{mod}\ m)$，则不定方程 $f(x,y,\cdots)=0$ 无解.

如果 $f(x,y,\cdots)\equiv 0(\mathrm{mod}\ m)$，则不能断定不定方程 $f(x,y,\cdots)=0$ 一定有解.

2. 一般的做法是取方程中绝对值最大的系数为模 m，使方程简化，然后判断方程两边对模 m 是否同余. 这种做法有局限性，一是当系数较大时，工作量较大. 二是得不到方程有解的判断.

3. 本节例 5 有一定难度，可讲可不讲，现作如下说明.

求方程 $(x-1)!=x^y-1$ 的所有正整数解，是很难直接求解的. 一般说来，这类方程的解可能不是很多，不妨先对指数 y 较小的值试一试.

令 $y=1$，则 $(x-1)!=x-1$，$\Rightarrow(x-2)!=1$. 解得 $x=2$，3.

令 $y=2$，则 $(x-1)!=x^2-1\Rightarrow(x-2)!=x+1$. 易知 $x=2$，3，4 不是解，$x=5$ 是其一解. 若 $x>5$，使 $(x-2)!=x+1$，令 $v=x-2$，则 $v>3$，$v!=v+3$. 左边被 v 整除，右边也应被 v 整除，但 $v\nmid 3$. 所以，$(x-1)!=x^2-1$ 没有大于 5 的整数解.

由以上试验，可猜想原方程当 $x>5$ 时，没有整数解.

由 $(x-1)!\equiv -1(\mathrm{mod}\ x)$ 可知 x 必为素数. 因此只需对 x 为大于 5 的素数来讨论. 以下证明步骤见课本.

第三章 同余方程

Ⅰ 教学要求

1. 掌握同余方程及其解的意义. 知道同余方程解的个数与次数无关. 但解的个数不超过模 m. 理解不能用因式分解求解同余方程. 其原因是在 Z_m 中可能有零因子. 由 $f(x)g(x)\equiv 0(\mathrm{mod}\ m)$ 不能导出 $f(x)\equiv 0$ 或 $g(x)\equiv 0(\mathrm{mod}\ m)$. 会用试算方法解同余方程.

2. 掌握一次同余方程有解的充分必要条件；如果一次同余方程 $ax\equiv b(\mathrm{mod}\ m)$ 有解，则解的个数为 (a, m). 并会求解一次同余方程.

3. 了解形式分数法，会用此种方法求解一次同余方程.

4. 了解孙子定理，会用该定理求解一次同余方程组与多项式的插值公式.

5. 了解公开密钥码，学会编码与译码.

Ⅱ 本章重点、难点与课时分配

1. 本章重点是

(1) 同余方程及其解的意义；(2) 一次同余方程有解的充分必要条件及解的个数；(3) 一次同余方程及方程组的求解方法；(4) 孙子定理的应用.

2. 本章难点是

(1) 同余方程解的个数；(2) 一次同余方程组特解的求法；(3) 对形式分数法的理解.

3. 课时分配

本章共 5 学时，建议 3.1 节与 3.2 节合用 2 学时，3.3 节与 3.4 节合用 2 学时，3.5 节 1 学时.

3.1 同余方程的概念

1. 正确理解同余方程的有关概念.

(1) 元即表示未知数，元数即未知数的个数；未知数只代表整数.

(2) 模 m，方程中的等号“$\equiv$”对模 m 成立. 括号$(\bmod m)$必须写上. 注意要求 $m>1$.

(3) 系数都是整数. 若系数 $a_k\equiv 0(\bmod m)$，则可去掉项 a_kx^k. 若 $a_k\equiv r(\bmod m)$，则可用 r 代替 a_k. 如 $7x^4+6x^3+5x^2+4x+8\equiv 0(\bmod 3)$ 可改写成 $x^4+2x^2+x+2\equiv 0(\bmod 3)$.

(4) 次数：方程中系数不被 m 整除的最高次项的次数. 如 $6x^3+2x^2+5x+4\equiv 0(\bmod 3)$的次数是 2，而不是 3.

2. 掌握同余方程解的意义.

设有同余方程 $f(x)\equiv 0(\bmod m)$，如果整数 c 使 $f(c)\equiv 0(\bmod m)$，则称 c 是其解. 由于 c 是其解，$c+km(k$ 为整数$)$也是其解. 这些解统一表为 $x\equiv c(\bmod m)$，并称 $x\equiv c(\bmod m)$ 是同余方程 $f(x)\equiv 0(\bmod m)$的一个解. 这就是说同余方程的一个解是模 m 的一个剩余类.

例如，$x^2-3x+2\equiv 0(\bmod 5)$，将 $x=1$，2 代入，可知左边$\equiv 0$，则 $x=5k+1$，$5x+2$ 也满足该同余方程. $x\equiv 1$，$2(\bmod 5)$ 称为该同余方程两个不同的解.

通过实例了解同余方程解的个数与次数没有必然联系，但与模 m 有关. 模 m 的同余方程解的个数不超过 m.

例如，

$x^5+x+1\equiv 0(\bmod 7)$ 有两个解 $x\equiv 2$，$4(\bmod 7)$；

$x^2+1\equiv 0(\bmod 3)$ 无解；

$x^2+1\equiv 0(\bmod 5)$ 有两个解 $x\equiv 2$，$3(\bmod 5)$；

$x^3-x\equiv 0(\bmod 6)$ 有 6 个解 $x\equiv 0$，1，2，3，4，$5(\bmod 6)$；

$x^3-x\equiv 0(\bmod 7)$ 有 3 个解 $x\equiv 0$，1，$6(\bmod 7)$.

3. 学会用试算方法解同余方程. 例如

$$32x^3+49x^2+6x+48\equiv 0(\bmod 7)$$

先将方程化简为

$$4x^3-x-1\equiv 0(\bmod 7)$$

分别将 $x\equiv 0$，1，…，6 代入试算. 易知 $x\equiv 0$，1 不是解；

将 $x\equiv 2$ 代入，$4\times 1-2-1\not\equiv 0$；将 $x\equiv 3$ 代入，$4\times(-1)-3-1\not\equiv 0(\bmod 7)$；将 $x\equiv 4$ 代入，$4\times 1-4-1\not\equiv 0(\bmod 7)$；将 $x\equiv 5$ 代入，$4\times(-1)-5-1\not\equiv 0(\bmod 7)$；将 $x\equiv 6$ 代入，$4\times(-1)-6-1\not\equiv 0(\bmod 7)$. 因此原方程无解.

4. 注意一般不能用因式分解求解同余方程. 例如

$$x^3-x\equiv 0(\bmod 6)$$

用因式分解 $x^3-x=x(x-1)(x+1)\equiv 0(\bmod 6)$，得解 $x\equiv 0$，1，$-1(\bmod 6)$，而实际上 $x\equiv 0$，1，2，…，$5(\bmod 6)$都是原方程的解. 原因是 $f(x)=f_1(x)f_2(x)\equiv 0(\bmod m)$，如果 $x\equiv c$ 是 $f_1(x)\equiv 0(\bmod m)$或 $f_2(x)\equiv 0(\bmod m)$的解，则 $x\equiv c$ 是 $f(x)\equiv 0(\bmod m)$的解；反之，如果 $x\equiv c$ 是 $f(x)\equiv 0(\bmod m)$的解，不能得出 $x\equiv c$ 是 $f_1(x)\equiv 0(\bmod m)$或 $f_2(x)\equiv 0(\bmod m)$的解. 这是因为 Z_m 中可能有零因子. 当 $f_1(x)\not\equiv 0$，$f_2(x)\not\equiv 0(\bmod m)$时，可能有 $f_1(x)f_2(x)\equiv 0(\bmod m)$.

对同余方程，$f(x)\equiv 0(\bmod m)$，如果有解 $x\equiv a(\bmod m)$，则必有

$$f(x)\equiv(x-a)f_1(x)(\bmod m).$$

由多项式除法，总存在 $f_1(x)$与 r，使

$$f(x)=(x-a)f_1(x)+r.$$

由于 $f(a)\equiv 0(\bmod m)$，所以 $r\equiv 0(\bmod m)$. 例如 $x^3-x\equiv 0(\bmod 6)$有解 $x\equiv 5(\bmod 6)$，$x^3-x\equiv(x-5)(x^2+5x+24)+120\equiv(x-5)(x^2+5x+24)(\bmod 6)$.

设 p 为素数，$f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\equiv 0(\bmod p)$，$p\nmid a_n$，则此同余方程解的个数不超过 n.

理由大致如下：设 $f(x)\equiv 0(\bmod p)$有解 $x\equiv a(\bmod p)$则有

$$f(x)\equiv(x-a)f_1(x)(\bmod p)$$

设另有一解 $x\equiv b(\bmod p)$，则 $0\equiv f(b)=(b-a)f_1(b)(\bmod p)$，由于 p 是素数，$p\nmid a-b$，$\Rightarrow p\mid f_1(b)$. $x\equiv b(\bmod p)$是 $f_1(x)\equiv 0(\bmod p)$的解. 因此，

$$f(x)\equiv(x-a)(x-b)f_2(x)(\bmod p).$$

如此继续，可知 $f(x)\equiv 0(\bmod p)$解的个数不超过 n. 对于模 m，m 是合数，则没有这个结论. 例如，$x^3-x\equiv 0(\bmod 6)$有六个解. 而当模 m 是素数时，解的个数不超过次数. 例如，

$x^3-x\equiv 0(\bmod 7)$有解 $x\equiv 0$，1，6，恰有三个解；

$x^3-x^2+x\equiv 0(\bmod 7)$有解 $x=0$，5，只有两个解.

威尔逊定理：如果 p 是素数，则$(p-1)!+1\equiv 0(\bmod p)$.

证明：由费马小定理，$x^{p-1}\equiv 1(\bmod p)$，这里要求$(x,\ p)=1$.

当 $x\equiv 1$，2，…，$p-1(\bmod p)$时，$(x,\ p)=1$. 所以 $x\equiv 1$，2，…，$p-1$ 是 $x^{p-1}\equiv 1(\bmod p)$的解，此外没有别的解（因解的个数不超过 $p-1$）. 因此有

$$x^{p-1}-1\equiv(x-1)(x-2)\cdots(x-p+1)(\bmod p).$$

令 $x=0$，则有

$$-1\equiv(-1)^{p-1}(p-1)!(\bmod p).$$

$\Rightarrow(p-1)!+1\equiv 0(\bmod p)$.

3.2 一次同余方程

本节讨论一次同余方程有解的条件及其求解方法. 内容虽然单纯，但有一定难度，必须让学生对本节内容有准确的理解. 建议注意以下几方面：

1. 一次同余方程 $ax\equiv b(\bmod m)$，当$(a,\ m)=1$ 时，有唯一解. 可用例子检验上述结论.

$5x\equiv 4(\bmod 6)$，$(5,\ 6)=1$. 恰有一解 $x\equiv 2(\bmod 6)$.

$5x\equiv4(\mathrm{mod}\ 10)$，$(5,\ 10)=5$. 无解.

$2x\equiv4(\mathrm{mod}\ 6)$，$(2,\ 6)=2$，有两解 $x\equiv2,\ 5(\mathrm{mod}\ 6)$.

2. 对定理：$ax=b(\mathrm{mod}\ m)$有解的充分必要条件是$(a,\ m)|b$;如方程有解，则解的个数是$(a,\ m)$的证明的补充.

(1) $ax\equiv b(\mathrm{mod}\ m)$有解的充要条件是 $ax-my=b$ 有解.

若 $ax-my=b$ 有解$(x_0,\ y_0)$，即 $ax_0-my_0=b$，$\Rightarrow ax_0\equiv b(\mathrm{mod}\ m)$. 这表明 $ax\equiv b(\mathrm{mod}\ m)$有解 $x\equiv x_0(\mathrm{mod}\ m)$.

若 $ax\equiv b(\mathrm{mod}\ m)$有解 $x\equiv x_0(\mathrm{mod}\ m)$，则有 $ax_0=km+b$，$\Rightarrow ax_0-mk=b$. 此式表明 $ax-my=b$ 有解$(x_0,\ k)$.

(2) $ax\equiv b(\mathrm{mod}\ m)$与$\frac{a}{d}x\equiv\frac{b}{d}\left(\mathrm{mod}\ \frac{m}{d}\right)$的解相同. 这里 $d=(a,\ m)$.

设 $x\equiv x_0(\mathrm{mod}\ m)$满足 $ax_0\equiv b(\mathrm{mod}\ m)$. $\Rightarrow d\cdot\frac{a}{d}x_0\equiv d\cdot\frac{b}{d}(\mathrm{mod}\ m)$.

而$(d,\ m)=d$，由 2.1 节性质 2 知$\frac{a}{d}x_0\equiv\frac{b}{d}\left(\mathrm{mod}\ \frac{m}{d}\right)$.

设 $x\equiv x_0\left(\mathrm{mod}\ \frac{m}{d}\right)$满足 $\frac{a}{d}x_0\equiv\frac{b}{d}\left(\mathrm{mod}\ \frac{m}{d}\right)$，$\Rightarrow\frac{m}{d}\left|\left(\frac{a}{d}x_0-\frac{b}{d}\right)\right.$，$\Rightarrow d\ \frac{m}{d}\left|d\left(\frac{a}{d}x_0-\frac{b}{d}\right)\right.$，$\Rightarrow m|(ax_0-b)$，$\Rightarrow ax_0\equiv b(\mathrm{mod}\ m)$.

(3) 设 $x=t_0\left(\mathrm{mod}\ \frac{m}{d}\right)$，$0\leqslant t_0<\frac{m}{d}$，是$\frac{a}{d}x\equiv\frac{b}{d}\left(\mathrm{mod}\ \frac{m}{d}\right)$的唯一解. 则 $ax\equiv b(\mathrm{mod}\ m)$的全部解可表为 $x=t_0+k\frac{m}{d}$，其中互不同余的解恰有 d 个.

理由如下：设 $x\equiv x_0$ 是 $ax\equiv b(\mathrm{mod}\ m)$的解. x_0 也是$\frac{a}{d}x_0\equiv\frac{b}{d}\left(\mathrm{mod}\ \frac{m}{d}\right)$的解. 后一方程的解是 $t_0+k\frac{m}{d}$（对模$\frac{m}{d}$是唯一的），因此 x_0 可表为 $x_0=t_0+k\frac{m}{d}$，对模 m，x_0 有多少个不同的值呢？考虑 k 取 0，1，2，…，$d-1$ 这 d 个数，它们对模 m，相应的 x_0 两两互不同余. 这 d 个数都是原方程不同的解. 这样 $x\equiv t_0+k\frac{m}{d}(\mathrm{mod}\ m)$，$k=0,\ 1,\ 2,\ \cdots,\ d-1$ 是原方程的 d 不同个解.

若原方程有解 $x\equiv t_0+k\frac{m}{d}(\mathrm{mod}\ m)$，$k\geqslant d$，则可令 $k=qd+r$，$0\leqslant r<d$，则

$$x\equiv t_0+(qd+r)\frac{m}{d}\equiv t_0+r\frac{m}{d},$$

由于 $0\leqslant r<d$，此解必在前述 d 个解之中.

掌握了这三个关键，对定理的证明就容易理解了.

可以用一些例子帮助理解这个定理. 比如，

(1) $4x\equiv6(\mathrm{mod}\ 18)$，$(4,\ 18)=2$，$2|6$. 方程有两个解.

(2) $4x\equiv6(\mathrm{mod}\ 18)$与 $2x\equiv3(\mathrm{mod}\ 9)$的解相同.

(3) $x\equiv6$ 是 $2x\equiv3(\mathrm{mod}\ 9)$的唯一解.

(4) $4x\equiv6(\mathrm{mod}\ 18)$全部解可表为

$$x=6+9k,\ k\text{ 为整数.}$$

(5) 取 $k=0$，1，得到 $4x\equiv 6 \pmod m$ 的两个解 $x\equiv 6$，$15 \pmod{18}$.

3. 对形式分数法的理解.

(1) 设 $(a, m)=1$，可将方程 $ax\equiv b \pmod m$ 改写成 $x\equiv \frac{b}{a} \pmod m$，分子分母同乘以与 m 互素的正整数 n，再分别对分子、分母模 m，使等式右边变成整数，便得到方程的唯一解.

过程如下：

$$ax\equiv b \pmod m \Rightarrow x\equiv \frac{b}{a}\equiv \frac{b\times n}{a\times n}, \text{ 令 } b\times n\equiv q \pmod m,\ a\times n\equiv p \pmod m,$$

则 $x\equiv \frac{q}{p} \pmod m$，$\frac{q}{p}$ 是整数.（如果 $\frac{p}{q}$ 不是整数，可继续类似步骤.）

合理性如下：如果 $x_0\equiv \frac{q}{p} \pmod m$，则 $px_0\equiv q \pmod m$. 由 $b\times n\equiv q$，$a\times n\equiv p \pmod m$ 知

$$q=bn-km,\ p=an-lm,\ (n, m)=1.$$

$\Rightarrow (an-lm)x_0=b\times n-km$，$\Rightarrow anx_0=bn \pmod m$，

因为 n 与 m 互素，由 2.1 节性质 2，$ax_0=b \pmod m$.

例如，$7x\equiv 8 \pmod{10}$，解：$x\equiv \frac{8}{7}\equiv \frac{8\times 3}{7\times 3}\equiv \frac{4}{1}\equiv 4 \pmod{10}$；

$12x\equiv 8 \pmod{13}$，解：$x\equiv \frac{8}{12}\equiv \frac{8\times 12}{12\times 12}\equiv \frac{5}{1}\equiv 5 \pmod{13}$.

(2) 设 $(a, m)=1$，可将方程 $ax\equiv b \pmod m$ 改写成 $x\equiv \frac{b}{a} \pmod m$. 将分子加上 m 的 k 倍，使新分子和分母有公约数 d，再约去 d. 使等式右边变成整数. 便得解.

理由如下：令 $(a, b+km)=d$，$a=qd$，$b+km=pd$. 方程化为 $x\equiv \frac{p}{q} \pmod m$.

假设 $\frac{p}{q}$ 为整数，则 $x_0=\frac{p}{q} \pmod m$ 便是原方程的唯一解. 这是因为

$$qx_0\equiv p \pmod m,\ \Rightarrow qdx_0\equiv pd \pmod m$$

$\Rightarrow ax_0\equiv b+km \pmod m$，$\Rightarrow ax_0\equiv b \pmod m$.

例如，$7x=8 \pmod{10}$，$\Rightarrow x\equiv \frac{8}{7}\equiv \frac{8+20}{7}\equiv 4 \pmod{10}$；

$12x\equiv 8 \pmod{13}$，$\Rightarrow x\equiv \frac{8}{12}\equiv \frac{8+13}{12}\equiv \frac{7}{4}\equiv \frac{7+13}{4}\equiv 5 \pmod{13}$.

例　设数列 $a_n=6n+8$，$n=1$，2，3，…. 问末两位数都是 0 的是哪些项？

解：问题化为求解 $6n+8\equiv 0 \pmod{100}$. 方程化为 $3n+4\equiv 0 \pmod{50}$，

$$n\equiv \frac{-4}{3}\equiv \frac{-4+100}{3}=32 \pmod{50}, \text{ 原方程有两解 } n\equiv 32,\ 82 \pmod{100}.$$

即 $n=32+100k$，$82+100k$（$k=0$，1，2，…）的项 a_n 末两位数是 0.

3.3　孙子定理

本节主要内容是一次同余方程组的解法. 我国古代的孙子定理给出了这类方程的通用解法. 本节由

“物不知数”问题引出同余方程组，并给出具体的解法. 这种解法体现了两种重要的数学思想. 一是把复杂的问题分解为几个简单的问题；二是把几个简单的问题标准化，并给出标准的解答. 在教学时，要充分展现这种思想方法.

1. “物不知数”问题化为同余方程组

$$\begin{cases} x\equiv 2(\bmod 3) \\ x\equiv 3(\bmod 5) \\ x\equiv 2(\bmod 7) \end{cases} \tag{1}$$

这种同余方程组与普通的一次方程不同，它只有一个未知数，但有多个不同的模，要求几个模两两互素. 若 $x\equiv x_0$ 是（1）的解，则 $x\equiv x_0+3\times5\times7k$ 也是方程的解. 这些解可表为 $x\equiv x_0(\bmod 3\times5\times7)$.

2. 如何求解方程组（1）呢？一步求出 $x\equiv x_0(\bmod 105)$是困难的. 我们把问题分解为 3 个子问题. 分别求出三个数 l_1，l_2，l_3，各满足如下标准条件：

$l_1\equiv1(\bmod 3)$，$l_1\equiv0(\bmod 5)$，$l_1\equiv0(\bmod 7)$；

$l_2\equiv0(\bmod 3)$，$l_2\equiv1(\bmod 5)$，$l_2\equiv0(\bmod 7)$；

$l_3\equiv0(\bmod 3)$，$l_3\equiv0(\bmod 5)$，$l_3\equiv1(\bmod 7)$.

横 / l_i	3	5	7
l_1	1	0	0
l_2	0	1	0
l_3	0	0	1

那么 $x\equiv2l_1+3l_2+2l_3(\bmod 105)$就是（1）的解.

现在的问题是怎样求出 l_1，l_2，l_3.

由于 l_1 被 5、7 整除，可令 $l_1=35k$，找出 k，使 $l_1\equiv1(\bmod 3)$. 可取 $k=2$，$l_1=70$. 同样，令 $l_2=21k$，取 $k=1$；令 $l_3=15k$，取 $k=1$；这样 $l_1=70$，$l_2=21$，$l_3=15$ 满足如上条件.

$$x=2\times70+3\times21+2\times15=233\equiv23(\bmod 105).$$

$x=23$ 就是“物不知数”问题的最小正整数解.

上述 l_1，l_2，l_3 的求法可统一表为：设 $m_1=3$，$m_2=5$，$m_3=7$. 令 $M_i=\dfrac{m_1m_2m_3}{m_i}$，$i=1$，2，3. 求出 M_i'使

$l_i=M_iM_i'\equiv1(\bmod m_i)$，$i=1$，2，3. 这里 $M_1=35$，$M_1'=2$，$M_2=21$，$M_2'=1$，$M_3=15$，$M_3'=1$.

3. 把上述问题及其解法一般化，便得到孙子定理：

设 m_1，m_2，…，m_n 两两互素，记 $m=m_1m_2\cdots m_n$. 令 $M_i=\dfrac{m}{m_i}$，$i=1$，2，…，n.

则同余方程组

$$\begin{cases} x\equiv b_1(\bmod m_1) \\ x\equiv b_2(\bmod m_2) \\ \quad\vdots\qquad\vdots \\ x\equiv b_n(\bmod m_n) \end{cases} \tag{2}$$

有唯一解 $x\equiv b_1M_1'M_1+b_2M_2'M_2+\cdots+b_nM_n'M_n(\bmod m)$，其中 M_i'满足

$$M_i'M_i\equiv1(\bmod m_i),\quad i=1,\ 2,\ \cdots,\ n. \tag{3}$$

定理证明的关键是：要证明对每一个 M_i 及 m_i，都存在 M_i'使（3）成立；证明如下：由$(M_i,\ m_i)=1$，知存在 M_i'与 c 使

$$M_i'M_i+cm_i=1,\ \Rightarrow M_i'M_i\equiv1(\bmod m_i).$$

又知 $M_i \equiv 0 (\mathrm{mod}\ m_j)$，$i \neq j$. 将上述 x 的表达式代入（2），便知其是（2）的解. 这里只是证明了 M_i' 的存在性，并没有给出具体的求法.

4. M_i'的求法. 求 M_i'使 $M_i' M_i \equiv 1 (\mathrm{mod}\ m)$，即求解（2）的辅助方程

$$M_i x \equiv 1 (\mathrm{mod}\ m_i),\ i=1,\ 2,\ \cdots,\ n.$$

由辗转相除法求最大公约数知

$$1=(M_i, m_i)=[(-1)^{n-1} Q_n] M_i + [(-1)^n P_n] m_i,$$

$$\Rightarrow M_i [(-1)^{n-1} Q_n] \equiv 1 (\mathrm{mod}\ m_i),$$

取 $M_i' = (-1)^{n-1} Q_n$. Q_n 由对 M_i，m_i 实施辗转相除而求得. 但用辗转相除法求 Q_n 比较麻烦，对于简单的同余方程组，可用形式分数法直接求解辅助方程 $M_i x \equiv 1 (\mathrm{mod}\ m_i)$.

例如，对“物不知数”问题可用形式分数法求解辅助方程：

$$35x \equiv 1 (\mathrm{mod}\ 3),\ \Rightarrow x \equiv \frac{1}{35} \equiv \frac{1+3\times 3}{35} \equiv \frac{10}{35} \equiv \frac{2}{7} \equiv \frac{2+3\times 4}{7} = 2 (\mathrm{mod}\ 3),$$

$$21x \equiv 1 (\mathrm{mod}\ 3),\ \Rightarrow x \equiv \frac{1}{21} \equiv \frac{1+5\times 4}{21} \equiv 1 (\mathrm{mod}\ 5),$$

$$15x \equiv 1 (\mathrm{mod}\ 7),\ \Rightarrow x \equiv \frac{1}{15} \equiv \frac{1+7\times 2}{15} \equiv 1 (\mathrm{mod}\ 7).$$

故原方程的唯一解是

$$\begin{aligned} x &\equiv b_1 M_1' M_1 + b_2 M_2' M_2 + b_3 M_3' M_3 \\ &\equiv 2\times 2\times 35 + 3\times 1\times 21 + 2\times 1\times 15 \equiv 23 (\mathrm{mod}\ 105). \end{aligned}$$

3.4 拉格朗日插值公式

本节用《孙子定理》所揭示的数学方法求多项式插值公式. 所谓多项式插值是已知 n 组数值 $(x_i,\ y_i)$，$i=1,\ 2,\ \cdots,\ n$，求一个多项式 $f(x)$，使 $f(x_i)=y_i$，$i=1,\ 2,\ \cdots,\ n$.

1. 预备知识

（1）余式定理：设有多项式 $f(x)$，$x-a$ 除 $f(x)$的余式(数)是 $f(a)$.

[做多项式除法：$f(x)=g(x)(x-a)+r$，$\Rightarrow f(a)=r$.]

因式定理：$x-a$ 整除 $f(x)$的充分必要条件是 $f(a)=0$. 即 $f(x)$含有因式$(x-a)$的充要条件是 $f(a)=0$.

（2）一个 n 次多项式方程 $f(x)=0$ 解的个数不超过 n. 这可由因式定理直接导出.

一个 n 次多项式 $f(x)$被其在 $n+1$ 的值唯一确定. 证明如下：设有 n 次多项式 $f(x)$，

已知 $f(x_i)=y_i$，$i=1,\ 2,\ \cdots,\ n+1$. 如果有 n 次多项式 $g(x)$满足 $g(x_i)=y_i$，$i=1,\ 2,\ \cdots,\ n+1$.

令 $h(x)=f(x)-g(x)$，$h(x)$的次数不超过 n. 假设 $h(x) \neq 0$($h(x)$不恒等于 0)

$$h(x_i)=f(x_i)-g(x_i)=y_i-y_i=0.\ \ i=1,\ 2,\ \cdots,\ n+1.$$

这样 $h(x)=0$ 有 $n+1$ 个根，矛盾. 因此 $h(x) \equiv 0$，$\Rightarrow g(x) \equiv f(x)$（这里“$\equiv$”是恒等符号）.

2. 已知 n 组值$(x_i,\ y_i)$，$i=1,\ 2,\ \cdots,\ n$，我们应用孙子定理来求一个多项式 $f(x)$，使$f(x_i)=y_i$，$i=1,\ 2,\ \cdots,\ n$.

如果能求出多项式

$$L_i(x_j)=\begin{cases}1, & j=i\\ 0, & j\neq i\end{cases}\quad i,\ j=1,\ 2,\ \cdots,\ n \tag{1}$$

那么，$f(x)=y_1L_1(x)+y_2L_2(x)+\cdots+y_nL_n(x)$为所求.

设 $m(x)=(x-x_1)(x-x_2)\cdots(x-x_n)$，令 $M_i(x)=\dfrac{m(x)}{x-x_i}$，$=(x-x_1)\cdots(x-x_{i-1})(x-x_{i+1})\cdots(x-x_n)$，$i=1,\ 2,\ \cdots,\ n$.

易知 $L_i(x)=\dfrac{M_i(x)}{M_i(x_i)}$满足 (1). $L_i(x)$可表为

$$L_i(x)=\frac{(x-x_1)\cdots(x-x_{i-1})(x-x_{i+1})\cdots(x-x_n)}{(x_i-x_1)\cdots(x_i-x_{i-1})(x_i-x_{i+1})\cdots(x_i-x_n)}.$$

3. 应用举例

例 1　求和 $1\cdot2+2\cdot3+3\cdot4+\cdots+n(n+1)$.

解：令$S(n)=0\cdot1+1\cdot2+2\cdot3+\cdots+(n+1)n$，$n$ 表示项数，$S(n)$不超过 3 次（易见其和$<n^2(n+1)$）.

$$S(0)=0,\ S(1)=0,\ S(2)=2,\ S(3)=8.$$

由插值公式

$$S(n)=2\cdot\frac{n(n-1)(n-3)}{2(2-1)(2-3)}+8\,\frac{n(n-1)(n-2)}{3\cdot(3-1)(3-2)}=\frac{1}{3}(n-1)n(n+1).$$

所以 $1\cdot2+2\cdot3+\cdots+n(n+1)=\dfrac{1}{3}n(n+1)(n+2)$.

例 2　求一个多项式 $f(x)$，使 $f(k)=\dfrac{k}{k+1}$，$k=0,\ 1,\ 2,\ 3$.

解：用插值公式

$$\begin{aligned}f(x)&=\frac{1}{2}\frac{x(x-2)(x-3)}{1\cdot(1-2)(1-3)}+\frac{2}{3}\frac{x(x-1)(x-3)}{2(2-1)(2-3)}+\frac{3}{4}\frac{x(x-1)(x-2)}{3(3-1)(3-2)}\\&=\frac{1}{4}x(x-2)(x-3)-\frac{1}{3}x(x-1)(x-3)+\frac{1}{8}x(x-1)(x-2)\\&=\frac{1}{24}(x^3-7x^2+18x).\end{aligned}$$

另解：由$(k+1)f(k)=k$，$k=0,\ 1,\ 2,\ 3$ 可知，$x=0,\ 1,\ 2,\ 3$ 是方程

$$(x+1)f(x)-x=0$$

的解. 因此可令

$$(x+1)f(x)-x=\lambda x(x-1)(x-2)(x-3).$$

将 $x=-1$ 代入上式，可得 $\lambda=\dfrac{1}{24}$. 于是，

$$\begin{aligned}f(x)&=\frac{1}{24(x+1)}[x(x-1)(x-2)(x-3)+24x]\\&=\frac{x}{24(x+1)}[(x+1)(x-2)(x-3)-2(x-2)(x-3)+24x]\\&=\frac{x}{24(x+1)}[(x+1)(x-2)(x-3)-2(x+1)(x-6)]\end{aligned}$$

$$=\frac{x}{24}(x^2-7x+18).$$

3.5 公开密钥码

本节作为同余方程的应用，介绍一种公开密钥码——RSA 码.

1. 1978 年，三位美国工程师 Rivest、Shamir 和 Adleman 创造了一种新颖的编码方法，后来称之为 RSA 体制. 它的特点是公开密钥，很难被别人破译.

通常，通讯双方为了保密，彼此有某种秘密约定，称为密钥. 最早的密钥是将明文的字母按字母表顺序后移 n 格，得到密文，接收者把所收到的密文前移 n 格便得明文，n 就是密钥. 例如，$n=3$.

明文：G O O D M O R N I N G

密文：J R R G P R U Q L Q J

这种密码不难破译，只要分析一下各字母在某些文献中出现的频率便可大致猜出密文中的字母代表明文中的哪一个字母. 后来出现了产生随机数序列的机器. 用随机数序列来加密和解密. 将明文编成 0、1 两个数字形成的序列，然后将明文与随机数对齐，上下两行数字两两做模 2 加法，形成密文. 例如，

明文　1 0 0 1 1 0 1 0 1 0 0 0 1 1 1

随机数　0 1 0 1 0 0 1 1 0 1 1 0 0 0 1

密文　1 1 0 0 1 0 0 1 1 1 1 1 0 1 1 0

当接收者收到密文后，将密文与随机数作模 2 加法便得明文. 这种编码译码方法虽然比前一种好得多，但也常常被第三方破译.

2. 通讯者 A 可以选取两个大素数(比如 100 位)p，g，令 $N=pg$. 那么

$$\varphi(N)=(p-1)(q-1).$$

再找一个正整数 e，使$(e,\ \varphi(N))=1$. 令 d 满足

$$ed\equiv 1(\mathrm{mod}\ \varphi(N)),\ \Rightarrow d=\frac{k\varphi(N)+1}{e},\ k \text{ 为正整数}.$$

此人将自己所选的加密密钥$(N,\ e)$公开，d 作为解密密钥严格保密. 由于 N 很难分解，别人无从知道 d. 通讯者 B 与 A 没有任何秘密约定，B 可按 A 公开的密钥$(N,\ e)$向 A 发送信息，操作规程如下：设明文是 M，$M^e\equiv C(\mathrm{mod}\ N)$，$C$ 作为密文发给 A，A 收到 B 的密文 C 后，作运算 $C^d(\mathrm{mod}\ N)$便得明文 M. 为什么 $C^d\equiv M(\mathrm{mod}\ N)$呢?

$$C^d\equiv(M^e)^d=M^{ed}\equiv M^{1+k\varphi(N)}\equiv M\cdot[M^{\varphi(N)}]^k\equiv M(\mathrm{mod}\ N)\ \text{(欧拉定理)}.$$

习题参考答案

习题 1—1

1. (1) 证明：$a|b \Rightarrow b=ka$，$\Rightarrow mb=kma$，$\Rightarrow ma|mb$.

   (2) 证明：由 $a|b \Rightarrow b \geqslant a$，由 $b|a \Rightarrow a \geqslant b$. 于是 $a=b$.

2. 证明：设连续三个正整数为 $n-1$，n，$n+1$，三位之和为 $3n$，$3|3n$.

3. 证明：$a^3+b^3=(a+b)(a^2-ab+b^2)$，由 $6|a+b$，$\Rightarrow 6|a^3+b^3$.

4. 证明：$n(n+1)(2n+1)=n(n+1)[(n+2)+(n-1)]=n(n+1)(n+2)+(n-1)n(n+1)$.
   由连续三个正整数中必有一个是偶数，也必有一个是 3 的倍数，因此连续三个正整数之积必为 6 的倍数. 因此，$6|n(n+1)(2n+1)$.

5. 解：两人握手，握手次数应为 2 人次. 总握手次数应为偶数. 但 15 人每人握手 5 次，总共次数为 75，与偶数次矛盾. 因此不可能每人都握手 5 次.

6. 解：由 $n-1|n+11$，$\Rightarrow n+11=k(n-1)$，$\Rightarrow (n-1)+12=k(n-1)$，
   $\Rightarrow (k-1)(n-1)=12$，
   12 有约数 1，2，3，4，6，12$\Rightarrow n-1=1$，2，3，4，6，12$\Rightarrow n=2$，3，4，5，7，13.
   另解：$n+11=k(n-1) \Rightarrow (k-1)n=11+k \Rightarrow n=\dfrac{k+11}{k-1}=1+\dfrac{12}{k-1}$，
   $k-1$ 只能取 1，2，3，4，6，12，相应的 $n=13$，7，5，4，3，2.

习题 1—2

1. 解：$\sqrt{359}<19$，易知 2，3，5，7，11，13，17 $\nmid 359$. 所以 359 是素数.

2. 略.

3. 解：如 24，25，26，27，28.

4. 证明：如果 $n>11$，n 为奇数，则 $n=9+m$，m 为大于 2 的偶数. 如果 n 为偶数，$n=4+l$，l 为大于 2 的偶数. 故大于 11 的自然数都可以表为两合数之和.

习题 1—3

1. 解：$-1\ 999=17\times(-118)+7$.

2. 解：设所添三数从左至右依次为 a，b，c. 则所得 6 位数是 $N=503\ 000+100a+10b+c$，$0 \leqslant a$，b，$c \leqslant 9$. 由 N 被 7，9，11 整除，$\Rightarrow 7\times 9\times 11|N$，$\Rightarrow 693|-118+100a+10b+c$. 由此

$$100a+10b+c=118,$$

$$\text{或 } 100a+10b+c=118+693=811,$$

   解得 $a=1$，$b=1$，$c=8$ 或 $a=8$，$b=1$，$c=1$.

3. 解：由 $101=3^4+2\cdot 3^2+2\cdot 3^0$，得

$$101=(10\ 202)_3.$$

习题 1—4

1. $(198, 252)=18$，$(1\,008, 1\,260)=252$

2. 解：$(1\,008, 1\,260)=252$，$(252, 882)=126$，$(126, 1\,134)=126$. $(1\,008, 1\,260, 882, 1\,134)=126$.

3. 证明：设 d 是 a_1 与 a_2 的一个公约数，则有 $a_1=qd$，$a_2=pd$. $a_2+a_1x=pd+qxd$，因此 d 也是 a_1 与 a_2+a_1x 的公约数. 反之，若 d 是 a_1 与 a_2+a_1x 的公约数，则有 $a_1=qd$，$a_2+a_1x=pd$，$\Rightarrow a_2+qdx=pd$，$\Rightarrow d\mid a_2$，因此，d 是 a_1 与 a_2 的公约数. 这就是说 a_1 与 a_2，a_1 与 a_2+a_1x 公约数相同. 最大公约数必相等. 同理可证 $(a_1, a_2)=(a_1+a_2y, a_2)$.

4. 证明：易知 (c, b) 是 c 与 ab 的一个公约数，令 $(c, ab)=k$. 若 k 含有素因数 p，p 是 c 与 ab 的一个公约数. 则 $p\mid c$，$p\mid ab$. 由 $p\mid ab$ 知 $p\mid a$ 或 $p\mid b$. 由 $(a, c)=1$，及 $p\mid c$ 知 $p\nmid a$，所以 $p\mid b$.
由 $p\mid c$ 及 $p\mid b$，知 p 是 c，b 的一个公约数. 因此 c 与 ab 的公约数也是 c 与 b 的公约数. 于是，
$$(c, ab)=(c, b).$$

5. 证明：令 $(c, ab)=d$，易知 $(c, a)\mid d$ 及 $(c, b)\mid d$，而 $((c, a), (c, b))=1$（因为 $(a, b)=1$）.
$\Rightarrow (c, a)(c, b)\mid d$. 设 p 为 d 的任一素因数. 则 $p\mid c$，$p\mid ab$，$\Rightarrow p\mid c$，$p\mid a$ 或 $p\mid b$.
$\Rightarrow p$ 是 c 与 a 或 p 是 c 与 b 的一个公约数. 因此，$p\mid (c, a)$ 或 $p\mid (c, b)$，$\Rightarrow p\mid (c, a)(c, b)$. 进而知 $d\mid (c, a)(c, b)$. 于是 $(c, ab)=(c, a)(c, b)$.

6. 证明：令 $(a, b)=d$，则存在 x，y 使 $ax+by=d$，$\Rightarrow \frac{a}{d}x+\frac{b}{d}y=1$，$\frac{a}{d}$，$\frac{b}{d}$ 是整数，根据两数互素的充分必要条件可知 $\left(\frac{a}{d}, \frac{b}{d}\right)=1$.

7. 解：由 $-2(21n+4)+3(14n+3)=1$，可知 $21n+4$ 与 $14n+3$ 互素.

习题 1—5

1. 略.

2. 解：$24\,871=3\,468\times 7+595$，$3\,468=595\times 5+493$，$595=493\times 1+102$，$493=102\times 4+85$，$102=85\times 1+17$，$85=17\times 5+0$.

$$[24\,871, 3\,468]=\frac{24\,871\times 3\,468}{17}=24\,871\times 204=5\,073\,684.$$

3. 解：设 $a=7k$，$b=7m$，$(k, m)=1$. $105=\frac{49km}{7}$，$\Rightarrow 15=km$，$\Rightarrow k=1$，$m=15$ 或 $k=3$，$m=5$
$\Rightarrow a=7$，$b=105$ 或 $a=21$，$b=35$. 注意 a，b 是对称的，可以互换.

4. 证明：由 $[a, b]=\frac{ab}{(a, b)}$ 和 $[a, b]=(a, b)$ 得 $(a, b)^2=ab$，$\Rightarrow \frac{a}{(a, b)}\cdot\frac{b}{(a, b)}=1$，$\Rightarrow \frac{a}{(a, b)}=1$，$\frac{b}{(a, b)}=1$，$\Rightarrow a=(a, b)$，$b=(a, b)$，$\Rightarrow a=b$.

5. 证明：由算术基本定理，设
$a=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$，$b=p_1^{\beta_1}\cdots p_k^{\beta_k}$，则
$(a, b)=p_1^{\gamma_1}\cdots p_k^{\gamma_k}$，$\gamma_i=\min(\alpha_i, \beta_i)$.
$a^3=p_1^{3\alpha_1}\cdots p_k^{3\alpha_k}$，$b^3=p_1^{3\beta_1}\cdots p_k^{3\beta_k}$，

$(a^3,\ b^3)=p_1^{3\gamma_1}\cdots p_k^{3\gamma_k}=(p_1^{\gamma_1}\cdots p_k^{\gamma_k})^3=(a,\ b)^3.$

$[a^3,\ b^3]=\dfrac{a^3b^3}{(a^3,\ b^3)}=\dfrac{a^3b^3}{(a,\ b)^3}=\left[\dfrac{ab}{(a,\ b)}\right]^3=[a,\ b]^3.$

6. 证明：$[a,\ b,\ c]=[[a,\ b],\ c]=\left[\dfrac{ab}{(a,\ b)},\ c\right]=\dfrac{\dfrac{ab}{(a,\ b)}\cdot c}{\left(\dfrac{ab}{(a,\ b)},\ c\right)}=\dfrac{abc}{(ab,\ c(a,\ b))}$

$(ab,\ ac,\ bc)=(ab,\ (ac,\ bc))=(ab,\ c(a,\ b)).$

两式相乘便得证.

习题 1—6

1. (1) $(4\ 712,\ 4\ 978,\ 5\ 890)=(38,\ 5\ 890)=38$；

(2) $\dfrac{4\ 712\times4\ 978\times5\ 890}{38\times38}=124\times131\times5\ 890=95\ 677\ 160$

2. 解：$300\ 000=3\times2^5\times5^5$，$\tau(300\ 000)=(1+1)(5+1)(5+1)=72.$

3. (1) 证明：假设$\sqrt{6}=\dfrac{q}{p}$，$(p,\ q)=1.$ $\Rightarrow6p^2=q^2$，$\Rightarrow q$ 含有因数 2^k，q^2 含有 2^{2k}，$k\geqslant1$，而 p 不含素因数 2. $6p^2$ 只含因数 2. 由算术基本定理，$2k=1$，这是不可能的.

(2) 证明：假设 $\lg7=\dfrac{q}{p}$，$(q,\ p)=1$，则 $7=10^{\frac{q}{p}}$，$\Rightarrow7^p=10^q=2^q\cdot5^q$. 根据算术基本定理，这是不可能的.

习题 1—7

1. 解：$107=37\times2+33$，$37=33\times1+4$，$33=4\times8+1$，

$q_1=2$，q_2-1，$q_3=8.$

$Q_0=0$，$Q_1=1$，$Q_2=q_2Q_1+Q_0=1$，$Q_3=q_3Q_2+Q_1=9.$

$P_0=1$，$P_1=2$，$P_2=q_2P_1+P_0=3$，$P_3=q_3P_2+P_1=26.$

$x_0=-26\cdot25$，$y_0=-9\cdot25$（因方程中 y 的系数为负）.

$x=-650-107t$，$y=-225-37t$，t 为整数.

2. 解：$7=19\times0+7$，$19=7\times2+5$，$7=5\times1+2$，$5=2\times2+1.$

$q_1=0$，$q_2=2$，$q_3=1$，$q_4=2.$

$Q_0=0$，$Q_1=1$，$Q_2=2$，$Q_3=3$，$Q_4=8.$

$P_0=1$，$P_1=0$，$P_2=1$，$P_3=1$，$P_4=3.$

$x=(-1)^3\cdot8\cdot213+19t$，$y=(-1)^2\cdot3\cdot213-7t.$

正整数解要求 $19t-8\cdot213>0$，$3\cdot213-7t>0$，

$$\frac{8\cdot213}{19}<t<\frac{3\cdot213}{7},\ \Rightarrow90\leqslant t\leqslant91.\ t=90\text{ 或 }91.$$

$$\begin{cases}x=-1\ 704+19\times90\\y=639-7\times90\end{cases}\text{ 或 }\begin{cases}x=-1\ 704+19\times91\\y=639-7\times91\end{cases}\text{ 即 }\begin{cases}x=6\\y=9\end{cases}\text{ 或 }\begin{cases}x=25\\y=2\end{cases}$$

3. 解：设年号为$\overline{2abc}$，依题意，

(*)2 000+100a+10b+c−22=495(a+b+c)，易知 $a+b+c<7$(∵(*)式右边之积<3 000)

因为(*)两边为 5 的倍数，所以 $c=2$ 或 7. 但 $a+b+c<7$，故 $c=2$.

因为(*)两边为 9 的倍数，所以 $2+a+b+c-4$ 是 9 的倍数，即 $a+b$ 是 9 的倍数. 由于 $a+b+c<7$，所以 $a+b=0$，由此 $a=b=0$. 所求年号为 2002 年.

4. 解：设大牛 x 头，小牛 y 头，牛犊 z 头，依题意，

$$\begin{cases}10x+5y+0.5z=100\\x+y+z=100\end{cases}\Rightarrow\begin{cases}20x+10y+z=200\\x+y+z=100\end{cases}\Rightarrow 19x+9y=100.$$

$19=9\times2+1$，$Q_1=1$，$P_1=2$，

$$\begin{cases}x=100+9t\\y=-200-19t\end{cases}$$

题中要求 $\begin{cases}0\leqslant 100+9t\leqslant 100\\0\leqslant -200-19t\leqslant 100\end{cases}\Rightarrow\begin{cases}-\frac{100}{9}\leqslant t\leqslant 0\\-\frac{300}{19}\leqslant t\leqslant -\frac{200}{19}\end{cases}$ 因 t 为整数，$\begin{cases}-11\leqslant t\leqslant 0\\-15\leqslant t\leqslant -11\end{cases}$

$\Rightarrow t=-11$，

$$\Rightarrow\begin{cases}x=1\\y=9\\z=90\end{cases}$$

或者直接从 $19x+9y=100$ 看出有特解 $x_0=1$，$y_0=9$. 通解为

$\begin{cases}x=1+9t\\y=9-19t\end{cases}$ 只有 $t=0$ 才能使 x，y 同时非负，所以问题只有一解 $\begin{cases}x=1\\y=9\\z=90.\end{cases}$

习题第一章巩固与提高

1. 证明：设 $a=p_1^{\alpha_1}\cdots p_k^{\alpha_k}$，$b=p_1^{\beta_1}\cdots p_k^{\beta_k}$，$\alpha_i$，$\beta_i\geqslant 0$.

由 $a^n\mid b^n$，$\Rightarrow\alpha_i n\leqslant\beta_i n$，$\Rightarrow\alpha_i\leqslant\beta_i$，$\Rightarrow a\mid b$.

2. 证明：若 n 含奇素因数 p，$n=kp$.

$$2^n+1=2^{kp}+1=(2^k)^p+1=(2^k+1)(2^{k(p-1)}-2^{k(p-2)}+\cdots+1)$$

可见 2^n+1 不是素数. 因此 n 只含偶素因数 2. 即 $n=2^m$.

3. 证明：设 $p=3k+r$，$r=0$，1 或 2. 因为 p 是素数，$r\neq 0$. 因为 $2p+1=6k+2r+1$ 是素数，$r\neq 1$. 由此 $r=2$. $4p+1=12k+4r+1=12k+9=3(4k+3)$是合数.

4. 证明：因 n 为奇数，$1+\frac{1}{2}+\cdots+\frac{1}{n-1}$两两配对相加：$\frac{1}{k}+\frac{1}{n-k}=\frac{n}{k(n-k)}$.

$$\left(1+\frac{1}{2}+\cdots+\frac{1}{n-1}\right)(n-1)!=n\left[\frac{(n-1)!}{1\cdot(n-1)}+\frac{(n-1)!}{2(n-2)}+\cdots+\frac{(n-1)!}{\frac{n-1}{2}\left(n-\frac{n-1}{2}\right)}\right],$$

括号内各项都是整数. 所以 $n\mid\left(1+\frac{1}{2}+\cdots+\frac{1}{n-1}\right)(n-1)!$

5. 证明：设$(a,b)=d$，$b\mid ma\Leftrightarrow\frac{b}{d}\,\Big|\,m\,\frac{a}{d}\Leftrightarrow\frac{b}{d}\,\Big|\,m\Leftrightarrow m=k\cdot\frac{b}{d}$. 题中 $m\leqslant b$，因此 $k\leqslant d$. 当$m=\frac{b}{d}$，

$\frac{2b}{d}$，…$\frac{(d-1)\ b}{d}$，$\frac{db}{d}$时，$\frac{b}{a}\Big|m$. 可见，a，$2a$，…，ba 中能被 b 整除的数恰有 d 个.

6. 证明：由习题 1-4 第 5 题知

$(a,[b,c])=\left(a,\frac{bc}{(b,c)}\right)=\left(a,\frac{b}{(b,c)}\right)(a,c)\left(因\frac{b}{(b,c)}与c互素\right)$

$[(a,b),(a,c)]=\left[\left(a,\frac{b}{(b,c)}\right),(a,c)\right]$(因 c 中含因数(b,c)，约去 b 中的(b,c)不改变此最小公倍数的值).

$$=\frac{\left(a,\frac{b}{(b,c)}\right)(a,c)}{\left(\left(a,\frac{b}{(b,c)}\right),(a,c)\right)}=\left(a,\frac{b}{(b,c)}\right)(a,c).\left(因\frac{b}{(b,c)}与c互素，\left(\left(a,\frac{b}{(b,c)}\right),(a,c)\right)=1.\right)$$

7. 略.

8. 证明：假设 $4n+3$ 型素数个数有限，不妨设为 p_1，p_2，…，p_k. 令 $q=4p_1p_2\cdots p_k-1=4(p_1p_2\cdots p_k-1)+3$. q 的素因数不是 $4n+1$ 型便是 $4n+3$ 型. 但 q 的素因数不能都是 $4n+1$ 型，否则与 q 是 $4n+3$ 型矛盾（两个 $4n+1$ 型数之积仍然是 $4n+1$ 型），因此 q 必有 $4n+3$ 型素因数，但 $4n+3$ 型素数 p_1，…，$p_k\nmid q$，于是存在与 p_1，…，p_k 不同的 $4n+3$ 型素数，这与假设矛盾. 从而证明了 $4n+3$ 型素数无限.

习题第一章自测与评估

1. $1\ 000\ 027=7\times19\times7\ 519$.

2. $(198,252)=18$.

3. 解：方程化为 $37x-107y=25$. 作辗转相除

$$-107=37\times(-3)+4,$$
$$37=4\times9+1,$$

$q_1=-3$，$q_2=9$. $Q_0=0$，$Q_1=1$，$Q_2=q_2Q_1+Q_0=9$.

$P_0=1$，$P_1=q_1=-3$，$P_2=q_2P_1+P_0=9\times(-3)+1=-26$.

特解：$x_0=(-1)^2P_2c=-26\times25=-650$，

$y_0=(-1)Q_2c=-9\times25=-225$.

通解：$\begin{cases}x=-650-107t\\y=-225-37t\end{cases}$ 都取正值，要求 $t<-6$.

4. 证明：$mq+np-(mn+pq)=(m-p)q+n(p-m)\equiv0(\mathrm{mod}(m-p))$

$\Rightarrow mq+np\equiv0(\mathrm{mod}\ (m-p))$.

5. 证明：设$(a+b,a^2+b^2)=d$，

$$\begin{cases}d\mid a+b\\d\mid a^2+b^2\end{cases}\Rightarrow d\mid2ab.$$

若 a，b 同为奇数，则 2，a，b 两两互素，$\Rightarrow d\mid2$，或 $d\mid a$，或 $d\mid b$. 若 $d\mid2$，则 $d=1$，2；若 $d\mid a$，又 $d\mid a+b$，$\Rightarrow d\mid b$，$\Rightarrow d=1$（因$(a,b)=1$）. 同理若 $d\mid b$，$\Rightarrow d\mid a$，$\Rightarrow d=1$.

若 a，b 一奇一偶，则 d 为奇数，若 $d>1$，则 $d\nmid2$，$\Rightarrow d\mid ab\Rightarrow d\mid a$ 或 $d\mid b$，$\Rightarrow d=1$（同上理）.

a，b 不可能同为偶数. 综上所述，$d=1$ 或 2.

习题 2—1

1. 证明：由 $a\equiv b(\mathrm{mod}\ m)$，$\Rightarrow m\mid a-b$，又 $d\mid m$，$\Rightarrow d\mid a-b$，$\Rightarrow a\equiv b(\mathrm{mod}\ d)$.

2. 证明：由 $a\equiv b(\mathrm{mod}\ m)$，$\Rightarrow a-b=lm(l$ 为整数$)$，$\Rightarrow |d|(a-b)=|d|lm$，
   $\Rightarrow$由于 l 为任意整数，上式可写为 $d(a-b)=l|d|m$，
   $\Rightarrow |d|m|ad-bd$，$\Rightarrow ad\equiv bd(\mathrm{mod}\ |d|m)$.

3. 证明：$a\equiv b(\mathrm{mod}\ m)\Rightarrow a-b=lm$，$\Rightarrow \frac{a}{d}-\frac{b}{d}=l\frac{m}{d}$，$\Rightarrow \frac{m}{d}\left|\frac{a}{d}-\frac{b}{d}\right.$，

   $$\Rightarrow \frac{a}{d}\equiv\frac{b}{d}\left(\mathrm{mod}\ \frac{m}{d}\right).$$

4. 16.

5. 解：$\varphi(10)=4$，$3^{406}=(3^4)^{101}\cdot 3^2\equiv 9(\mathrm{mod}\ 10)$，个位数是 9.

6. 解：$6^{48}=(6^{12})^4\equiv 1^4\equiv 1(\mathrm{mod}\ 13)$.

7. 证明：$168=3\cdot 7\cdot 8$，3，7，8 两两互素.

   $$13^{6n}-1=(13^2)^{3n}-1\equiv 1^{3n}-1\equiv 0(\mathrm{mod}\ 3),$$
   $$13^{6n}-1=(13^6)^n-1\equiv 1^n-1\equiv 0(\mathrm{mod}\ 7),$$
   $$13^{6n}-1=(169)^{3n}-1\equiv 1^{3n}-1\equiv 0(\mathrm{mod}\ 8)$$

   所以 $168\mid 13^{6n}-1$.

习题 2—2

1. 略.

2. 解：$(8+6+5+8+7)-(2+7+9+5)=11$，所以该数是 11 的倍数.

3. 证明：$1\ 001\equiv 0(\mathrm{mod}\ 7)$，即 $1\ 000=-1(\mathrm{mod}\ 7)$.
   设 $a=b\times 1\ 000+c$，c 是 a 的末三位数，b 是 a 的在 c 之后的各位数字所表示的数.

   $$a\equiv b\times(-1)+c\equiv b-c(\mathrm{mod}\ 7).$$

   由此可见若 $b-c$ 被 7 整除，则 a 被 7 整除. 对 11、13 也是一样.

4. 第一个数是 7 的倍数，第二个数是 13 的倍数，第三个数是 11 的倍数.

习题 2—3

1.

	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

2. $\overline{2}$、$\overline{3}$、$\overline{4}$、$\overline{6}$、$\overline{8}$.

3. 证明：模 11 的剩余类共有 11 个. 将 101 个按模 11 同余分类，至少有一类数字个数不少于 11，从此类中选 11 个数. 记为 a_1，a_2，…，a_{11}，$a_i\equiv r$，$i=1$，2，…，11. $a_1+a_2+\cdots+a_{11}\equiv 11\cdot r\equiv 0\pmod{11}$.

习题 2—4

1. 证明：设$\{a_0, a_1, \cdots, a_{m-1}\}$是模 m 的一个完全剩余系. 不妨设

$$a_0\equiv 0,\ a_1\equiv 1,\ \cdots,\ a_{m-1}\equiv m-1\pmod m,$$

$\Rightarrow a_0=k_0m,\ a_1=k_1m+1,\ a_2=k_2m+2,\ \cdots,\ a_{m-1}=k_{m-1}+m-1.$

易知 a_0，a_2，…，a_{m-2}为偶数. 其余一半为奇数.

2. 证明：$\{1, 2, \cdots, 10\}$是模 11 的一个简化剩余系. $\{2\times 1, 2\times 2, \cdots, 2\times 11\}$也是模 11 的一个简化剩余系.

这两个简化剩余系中的数，两两对应模 11 同余. 故

$$1^5+2^5+\cdots+10^5\equiv(2\times 1)^5+(2\times 2)^5+\cdots+(2\times 10)^5\pmod{11},$$

$\Rightarrow(2^5-1)(1^5+2^5+\cdots+10^5)\equiv 0\pmod{11}$.

因为 $11\nmid 2^5-1$，所以 $11\mid 1^5+2^5+\cdots+10^5$.

3. 解：10 080 只含素因子 2，3，5，7，

$$\varphi(10\ 080)=10\ 080\left(\frac{1}{2}\cdot\frac{2}{3}\cdot\frac{4}{5}\cdot\frac{6}{7}\right)=2\ 304.$$

4. 证明：(1) 设 n 只含素因子 2，则 $n=2^k$. 因 $n>2$，所以 $k>1$，$\varphi(n)=2^k\cdot\left(1-\frac{1}{2}\right)=2^{k-1}$，因 $k>1$，$\varphi(n)$为偶数.

(2) 设 n 含有素因子 $p>2$，p 为奇数. $\varphi(n)$含因子 $\varphi(p^\alpha)=p^\alpha-p^{\alpha-1}$，$p^\alpha-p^{\alpha-1}$为偶数. $\varphi(n)$为偶数.

5. 解：$\varphi(p^{100})+\varphi(p^{99})+\cdots+\varphi(p^2)+\varphi(p)$

$$=(p^{100}-p^{99})+(p^{99}-p^{98})+\cdots+(p^2-p)+p-1=p^{100}-1.$$

习题 2—5

1. 解：$\varphi(10)=4$，$7^{355}=(7^4)^{88}\cdot 7^3\equiv 3\pmod{10}$，个位数是 3.

2. 解：$\varphi(100)=40$，$3^{400}\equiv(3^{40})^{10}\equiv 1\pmod{100}$，末两位数是 01.

3. 解：$8^{4\,964}=8^{12\times 413+8}\equiv 8^8\equiv 64^4=(-1)^4\equiv 1\pmod{13}$.

4. 解：$10^{10}\equiv 4^{10}\equiv 16^5\equiv(-2)^5=-32\equiv 4\pmod 6$，

$10^{10^{10}}=10^{6k+4}\equiv 10^4\equiv 3^4\equiv 4\pmod 7$，是星期天.

5. 略.

习题 2—6

1. 证明：若方程有整数解 x，y，z，则 $x^2+y^2\equiv 3\pmod 4$，而 x^2，$y^2\equiv 0$ 或 $1\pmod 4$，矛盾. 所以方程无解.

2. 证明：若方程有整数解 x，y，z，则 $x^3+y^3+z^3\equiv-4\equiv5(\mathrm{mod}\ 9)$. 而对任何 x，$x^3\equiv-1$，0 或 $1(\mathrm{mod}\ 9)$. 由此 $x^3+y^3+z^3\not\equiv5(\mathrm{mod}\ 9)$，矛盾.

3. 证明：易知 $x=y=z=0$ 是方程的解.

(1) 若 $x\neq0$，$y\neq0$，则 $x^2\equiv y^2\equiv1(\mathrm{mod}\ 3)$. 原方程式左边$\equiv x^2+y^2\equiv2(\mathrm{mod}\ 3)$，右边$\equiv0(\mathrm{mod}\ 3)$，矛盾.

(2) 若 x，y 中有一个是 3 的倍数，例如 $x\equiv0(\mathrm{mod}\ 3)$，则由原方程可知 $y\equiv0(\mathrm{mod}\ 3)$.

因此可令 $x=3^{k_1}d_1$，$y=3^{k_2}d_2$，假设 d_1，$d_2\neq0$，$(d_1,3)=(d_2,3)=1$. k_1，$k_2\geqslant1$.

代入原方程$(3a+1)3^{2k_1}d_1^2+(3b+1)3^{2k_2}d_2=3z^2$，$\Rightarrow z$ 是 3 的倍数，可令 $z=3^{k_3}d_3$，

$\Rightarrow(3a+1)3^{2k_1}d_1^2+(3b+1)3^{2k_2}d_2=3^{2k_3+1}d_3^2$.

上式约去 3^{2k_1}，3^{2k_2}，3^{2k_3+1} 中的较小者，则一边是 3 的倍数，另一边不是 3 的倍数，矛盾. 因此假设 d_1，$d_2\neq0$ 不成立. 即 d_1，d_2 中至少有一个为 0. 不妨设 $d_1=0$，$d_2\neq0$，则 $d_3\neq0$，

$$(3b+1)3^{2k_2}d_2^2=3^{2k_3+1}d_3^2,$$

约去 3^{2k_2} 与 3^{2k_2+1} 中的较小者，得到矛盾. 因此 $d_1=d_2=0$，$\Rightarrow d_3=0$. 故方程只有解 $x=y=z=0$.

4. 证明：由 $y^2=x^3+7$，$\Rightarrow y^2\equiv x+1(\mathrm{mod}\ 3)$. 有下列三种情况：

(1) $y\equiv0$，则 $x\equiv-1$；(2) $y\equiv1$，则 $x\equiv0$；(3) $y\equiv-1$，则 $x\equiv0$. $(\mathrm{mod}\ 3)$

(1) 可令 $y=3k$，$x=3k-1$，代入原方程

$$9k^2=(3k-1)^3+7,\ \Rightarrow9k^2=27k^3-27k^2+9k-1+7,\ \text{模 9 便得矛盾.}$$

(2) 可令 $y=3k+1$，$x=3l$，$\Rightarrow9k^2+6k+1=27l^3+7\Rightarrow3k^2+2k-2=9l^3$，

$\Rightarrow3k^2+2k-2\equiv0(\mathrm{mod}\ 9)$. 将 $k\equiv0$，1，2，…，8 代入试算，得到矛盾.

(3) 可令 $y=3k-1$，$x=3l$，结果与 (2) 相同.

因此方程无整数解.

习题第二章巩固与提高

1. 证明：$70!=61!\times62\times63\times\cdots\times70\equiv61!(-9)\times(-8)\times\cdots\times(-1)$

$$\equiv61!\times72\times(-210)\times24\equiv61!\times(+3)\times24\equiv61!(\mathrm{mod}\ 71)$$

2. 证明：$240=2^4\times3\times5$，$p\geqslant7$，

$p^4-1=p^{\varphi(5)}-1\equiv0(\mathrm{mod}\ 5)$，

$p^4-1=p^{2\varphi(3)}-1\equiv0(\mathrm{mod}\ 3)$，

令 $p=4k+r$，$r=1$，3.

$$p^4-1=(4k+r)^2(4k+r)^2-1$$

$$\equiv(8kr+r^2)^2-1\equiv r^4-1\equiv0(\mathrm{mod}\ 16),$$

故 $16\times3\times5\mid p^4-1$.

3. 证明：$91=13\times7$，$(a,91)=(b,91)=1$，

$$a^{12}-b^{12}=a^{2\varphi(7)}-b^{2\varphi(7)}\equiv1-1\equiv0(\mathrm{mod}\ 7),$$

$$a^{12}-b^{12}=a^{\varphi(13)}-b^{\varphi(13)}\equiv1-1\equiv0(\mathrm{mod}\ 13),$$

所以 $91\mid a^{12}-b^{12}$.

4. 证明：$2^{6k+1}+3^{6k+1}+5^{6k}+1\equiv2+3+1+1\equiv0(\mathrm{mod}\ 7)$，

所以此数被 7 整除.

5. 证明：

由 $m^p+n^p\equiv 0(\mathrm{mod}\ p)$，$\Rightarrow m+n\equiv 0(\mathrm{mod}\ 7)$.

$$m^p+n^p=(m+n)(m^{p-1}-m^{p-2}n+\cdots-mn^{p-2}+n^{p-1})$$

$p\mid m+n$，又因为 $n\equiv -m(\mathrm{mod}\ p)$

$$m^{p-1}-m^{p-2}n+\cdots-mn^{p-2}+n^{p-1}$$
$$\equiv m^{p-1}+m^{p-1}+\cdots+m^{p-1}+m^{p-1}$$
$$\equiv pm^{p-1}\equiv 0(\mathrm{mod}\ p)$$

所以 $p^2\mid m^p+n^p$.

6. 证明：令 $\varphi(m)=kd+r$，$0\leqslant r<d$.

$$1\equiv a^{\varphi(m)}\equiv a^{kd+r}\equiv (a^d)^k a^r\equiv a^r(\mathrm{mod}\ m).$$

$\Rightarrow r=0$.（否则因 $0<r<d$，导致与 d 是使 $a^x\equiv 1$ 的 x 的最小正整数矛盾.）

习题第二章自测与评估

1. $3^{406}\equiv 3^{404}\cdot 3^2\equiv 9(\mathrm{mod}\ 10)$.

2. 证明：$504=7\times 8\times 9$.

不妨设$(n,\ 7)=1$（否则 n^9-n^3 被 7 整除），

$$n^9-n^3=n^{\varphi(7)}n^3-n^3\equiv n^3-n^3\equiv 0(\mathrm{mod}\ 7).$$

不妨设$(n,\ 9)=1$（否则 n^9-n^3 被 9 整除），

$$n^9-n^3=n^{\varphi(9)}\cdot n^3-n^3\equiv 0(\mathrm{mod}\ 9).$$

不妨设$(n,\ 8)=1$，

$$n^9-n^3\equiv n^{2\varphi(8)}n-n^3\equiv n-n^3\equiv n(n^2-1)(\mathrm{mod}\ 8).$$

令 $n=4k\pm 1$，

$$n^2-1=(4k\pm 1)^2-1\equiv 0(\mathrm{mod}\ 8).$$

故 $504\mid n^9-n^3$.

3. 由 $a^p\equiv b^p\Rightarrow a\equiv b(\mathrm{mod}\ p)$，

$$a^p-b^p=(a-b)(a^{p-1}+a^{p-2}b+\cdots+b^{p-1}).$$

$p\mid a-b$，$a^{p-1}+a^{p-2}b+\cdots+b^{p-1}=pa^{p-1}\equiv 0(\mathrm{mod}\ p)$.

所以 $p^2\mid a^p-b^p$.

4. 证明：当 $l=3$ 时，

$5^{2^{l-2}}=5^2\equiv 1(\mathrm{mod}\ 2^3)$.

假设 $5^{2^{l-2}}\equiv 1(\mathrm{mod}\ 2^l)$. 即假设 $5^{2^{l-2}}=k\cdot 2^l+1$，

$$5^{2^{l+1-2}}\equiv (5^{2^{l-2}})^2$$
$$\equiv (k\,2^l+1)^2$$
$$\equiv k^2 2^{2l}+k2^{l+1}+1\equiv 1(\mathrm{mod}\ 2^{l+1}).$$

故当 $l\geqslant 3$ 时，$5^{2^{l-2}}\equiv 1(\mathrm{mod}\ 2^l)$.

5. 因为 $(a^{\frac{p-1}{2}})^2=a^{p-1}\equiv 1(\mathrm{mod}\ p)$.

$a^{\frac{p-1}{2}}$ 的取值就是同余方程 $x^2\equiv 1(\mathrm{mod}\ p)$ 的解.

易知 $x\equiv 1$，$p-1 \pmod p$ 是 $x^2\equiv 1 \pmod p$ 的解.

假设有解 $x\equiv k \pmod p$，$1<k<p-1$，则 $k^2-1\equiv 0 \pmod p$.

$\Rightarrow p\mid k^2-1$，$\Rightarrow p\mid k+1$ 或 $p\mid k-1$ 这是不可能的.

故 $a^{\frac{p-1}{2}}$ 取值为 1、$p-1 \pmod p$.

例如，$p=7$，$a^3\equiv 1$，$6 \pmod 7$，

$p=11$，$a^5\equiv 1$，$10 \pmod{11}$.

6. 证明：设 mn 的素因子为 p_1，p_2，…，p_k，则 $[m, n]$ 的素因子也是 p_1，p_2，…，p_k.

$$\varphi(mn)=mn\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_k}\right),$$

$$\varphi([m, n])=[m, n]\left(1-\frac{1}{p_1}\right)\cdots\left(1-\frac{1}{p_k}\right),$$

$$\Rightarrow\frac{\varphi(mn)}{\varphi([m, n])}=\frac{mn}{[m, n]}=(m, n),$$

$$\Rightarrow\varphi(mn)=(m, n)\varphi([m, n]).$$

习题 3—1

1. 无解.
2. 解：方程化为 $(x-1)^2\equiv p(x-1) \pmod{p^2}$，$x$ 是方程的解 $\Leftrightarrow p\mid x-1$. 此方程的解为 $x\equiv kp+1 \pmod{p^2}$. x 在 0 至 p^2-1 内，k 取 0，1，2，…，$p-1$，共 p 个解.
3. 解：$x^2+2x+2\equiv 0 \pmod 5$，有解 $x\equiv 2 \pmod 5$.

习题 3—2

1. 证明：设 $x\equiv x_0 \pmod m$ 是 $ax\equiv b \pmod m$ 的解，$ax_0\equiv b \pmod m$. 由同余性质 2 得 $a^{\varphi(m)}x_0=ba^{\varphi(m)-1}$，由欧拉定理，$x_0\equiv ba^{\varphi(m)-1} \pmod m$.
2. 设 $m=p_1^{\alpha_1}\cdots p_i^{\alpha_i}$，$m+1=q_1^{\beta_1}\cdots q_l^{\beta_l}$. 由 $(m, m+1)=1$. q_i，p_i 全不同.

   假设 $m(m+1)=n^k$，由算术基本定理，n 的全部素因子是 p_1，…，p_m，q_1，…，q_l，$n^k=p_1^{\alpha_1 k}\cdots p_i^{\alpha_i}\cdots q_1^{\beta_1 k}\cdots q_l^{\beta_l k}$.

   于是，$p_1^{\alpha_1}\cdots p_i^{\alpha_i}\cdot q_1^{\beta_1}\cdots q_l^{\beta_l}=p_1^{\alpha_1 k}\cdots q_l^{\beta_l k}$，由分解的唯一性，知 $k=1$.
3. 解：$(111, 321)=3$，$3\mid 75$. 原方程有 3 个解. 方程 $37x\equiv 25 \pmod{107}$ 有唯一解.

$$x\equiv\frac{25}{37}\equiv\frac{25\times 3}{37\times 3}\equiv\frac{75}{4}\equiv\frac{75+107\times 3}{4}=99 \pmod{107}$$

   原方程解 $x_1\equiv 99 \pmod{321}$，$x_2\equiv 99+107=206$，$\pmod{321}$，$x_3\equiv 99+2\times 107=313 \pmod{321}$.
4. 解：$(15, 6)\equiv 3$，$3\mid 9$. 原方程有 3 个解. 方程 $5x\equiv 3 \pmod 2$ 有唯一解 $x\equiv 1 \pmod 2$.

   原方程的解为 $x\equiv 1$，3，$5 \pmod 6$
5. 解：$(258, 348)=6$，$6\nmid 131$，方程无解.
6. 解：$(20, 53)=1$，方程有唯一解.

$$x\equiv\frac{7}{20}\equiv\frac{7+53}{20}\equiv 3 \pmod{53}.$$

习题 3—3

1.（1）问题化为求解同余方程组

$$\begin{cases} x\equiv 1(\bmod 7) \\ x\equiv 1(\bmod 8) \\ x\equiv 3(\bmod 9) \end{cases}$$

$x\equiv M_1'M_1+M_2'M_2+3M_3'M_3(\bmod 7\times 8\times 9)$.

其中$M_1=72$，$72M_1'\equiv 1(\bmod 7)$，$\Rightarrow 2M_1'\equiv 1(\bmod 7)$，$\Rightarrow M_1'\equiv 4(\bmod 7)$.

$M_2=63$，$63M_2'\equiv 1(\bmod 8)$，$\Rightarrow -M_2'\equiv 1(\bmod 8)$，$\Rightarrow M_2'\equiv -1(\bmod 8)$.

$M_3=56$，$56M_3'\equiv 1(\bmod 9)$，$\Rightarrow 2M_3'\equiv 1(\bmod 9)$，$\Rightarrow M_3'\equiv 5(\bmod 9)$.

$x\equiv 4\times 72+(-1)\times 63+3\times 5\times 56\equiv 57(\bmod 7\times 8\times 9)$.

（2）问题化为求解同余方程组

$$\begin{cases} x\equiv 3(\bmod 11) \\ x\equiv 2(\bmod 12) \\ x\equiv 1(\bmod 13) \end{cases}$$

解辅助方程

$$156x\equiv 1(\bmod 11)\Rightarrow x\equiv\frac{1}{156}\equiv\frac{1}{2}\equiv\frac{1+11}{2}\equiv 6(\bmod 11),$$

$$143x\equiv 1(\bmod 12)\Rightarrow x\equiv\frac{1}{143}\equiv -1(\bmod 12),$$

$$132x\equiv 1(\bmod 13)\Rightarrow x\equiv\frac{1}{132}\equiv\frac{1}{2}\equiv\frac{1+13}{2}\equiv 7(\bmod 13).$$

$x=3\times 156\times 6-2\times 143+132\times 7\equiv 14(\bmod 11\times 12\times 13)$.

（3）问题化为解同余方程组

$$\begin{aligned} x&\equiv 1(\bmod 2) \\ x&\equiv 2(\bmod 5) \\ x&\equiv 3(\bmod 7) \\ x&\equiv 4(\bmod 9) \end{aligned}$$

解辅助方程

$$315x\equiv 1(\bmod 2)\Rightarrow x\equiv\frac{1}{315}\equiv 1(\bmod 2)$$

$$126x\equiv 1(\bmod 5)\Rightarrow x\equiv\frac{1}{126}\equiv 1(\bmod 5)$$

$$90x\equiv 1(\bmod 7)\Rightarrow x\equiv\frac{1}{90}\equiv\frac{1}{-1}\equiv -1(\bmod 7)$$

$$70x\equiv 1(\bmod 9)\Rightarrow x\equiv\frac{1}{70}\equiv\frac{1}{7}\equiv\frac{1+9\times 3}{7}\equiv 4(\bmod 9)$$

原方程解为 $x\equiv 1\times 315\times 1+2\times 126\times 1+3\times 90\times(-1)+4\times 70\times 4\equiv 157(\bmod 2\times 5\times 7\times 9)$.

2. 解辅助方程

$$385x\equiv 1(\bmod 3)\Rightarrow x\equiv\frac{1}{385}\equiv 1(\bmod 3),$$

$231x\equiv 1(\bmod 5)\Rightarrow x\equiv\frac{1}{231}\equiv 1(\bmod 5)$,

$165x\equiv 1(\bmod 7)\Rightarrow x\equiv\frac{1}{165}\equiv\frac{1}{4}\equiv\frac{1+7}{4}\equiv 2(\bmod 7)$,

$105x\equiv 1(\bmod 11)\Rightarrow x\equiv\frac{1}{105}\equiv\frac{1}{6}\equiv\frac{1+11}{6}\equiv 2(\bmod 11)$.

原方程解为 $x\equiv 385-231+2\times 165\times 2-2\times 105\times 2=394(\bmod 3\times 5\times 7\times 11)$.

习题 3—4

解：$S(0)=0$，$S(1)=0$，$S(2)=1$，$S(3)=9$，$S(4)=36$，n 表示项数.

由插值公式，

$$S(n)=\frac{n(n-1)(n-3)(n-4)}{2(2-1)(2-3)(2-4)}+9\frac{n(n-1)(n-2)(n-4)}{3(3-1)(3-2)(3-4)}+36\frac{n(n-1)(n-2)(n-3)}{4(4-1)(4-2)(4-3)}$$

$$=\frac{n(n-1)}{4}[(n-3)(n-4)-6(n-2)(n-4)+6(n-2)(n-3)]$$

$$=\frac{n(n-1)}{4}(n^2-7n+12+6n-12)=\frac{n^2(n-1)^2}{4}.$$

习题 3—5

略.

习题第三章巩固与提高

1. 解：用 $x=1$，2，3 代入知 $x\equiv 1$，2，3$(\bmod 31)$是解. 因 31 是素数，方程的解的个数不超过 3. 因此方程全部解为 $x\equiv 1$，2，3$(\bmod 31)$.

2. 解：问题化为求解同余方程组

$$x\equiv 2(\bmod 7),$$
$$x\equiv 3(\bmod 8),$$
$$x\equiv 1(\bmod 9).$$

先解辅助方程

$$72x\equiv 1(\bmod 7),\ \Rightarrow x\equiv\frac{1}{72}\equiv\frac{1}{2}\equiv\frac{1+7}{2}\equiv 4(\bmod 7),$$

$$63x\equiv 1(\bmod 8),\ \Rightarrow x\equiv\frac{1}{63}\equiv\frac{1}{-1}\equiv -1(\bmod 8),$$

$$56x\equiv 1(\bmod 9),\ \Rightarrow x\equiv\frac{1}{56}\equiv\frac{1}{2}\equiv\frac{1+9}{2}\equiv 5(\bmod 9).$$

原方程组解

$$x\equiv 2\times 72\times 4-3\times 63+56\times 5\equiv 163(\bmod 7\times 8\times 9).$$

3. 证明：必要性：若有解 x_0，则 $x_0=km_1+b_1$，$x_0=lm_2+b_2$，$\Rightarrow km_1-lm_2+b_1-b_2=0$，$\Rightarrow b_1-b_2\equiv 0(\bmod d)$.

充分性：由 $d\mid b_1-b_2\Rightarrow b_1=kd+b_2$，存在 p，q 使 $d=pm_1+qm_2$.

$\Rightarrow b_1=k(pm_1+qm_2)+b_2$. 令 x_0 是 $x\equiv b_1(\bmod m_1)$的唯一解，则

$$x_0\equiv b_1\equiv k(pm_1+qm_2)+b_2\equiv kqm_2+b_2(\bmod m_1).$$

$\Rightarrow x_0\equiv b_2(\bmod m_2)$. 可见方程组有解.

4. 证明：由(1，m)=1，题中同余方程 $x\equiv a(\bmod m)$有唯一解 $x\equiv a(\bmod m)$. 根据孙子定理，题中方程组有唯一解 $x\equiv a(\bmod m)$，所以二者有相同的解.

5. 证明：由 $\alpha\geqslant\beta$，(p^α，p^β)=p^β. 由题 1 可知 $p^\beta\mid a_1-a_2$，$\Rightarrow a_1=lp^\beta+a_2$. 第一个方程的解可表为

$$x\equiv a_1+kp^\alpha\equiv lp^\beta+a_2+kp^\alpha\equiv a_2(\bmod p^\beta),$$

可见 $x\equiv a_1(\bmod p^\alpha)$是方程组的解.

6. 由题 4，$x=2(\bmod 35)$可化为$\begin{cases}x\equiv 2(\bmod 5)\\ x\equiv 2(\bmod 7)\end{cases}$

$x=9(\bmod 14)$可化为$\begin{cases}x\equiv 9(\bmod 2)\\ x\equiv 9(\bmod 7)\end{cases}\Rightarrow\begin{cases}x\equiv 1(\bmod 2)\\ x\equiv 2(\bmod 7)\end{cases}$

$x=7(\bmod 20)$可化为$\begin{cases}x\equiv 7(\bmod 4)\\ x\equiv 7(\bmod 5)\end{cases}\Rightarrow\begin{cases}x\equiv 3(\bmod 4)\\ x\equiv 2(\bmod 5)\end{cases}$

原方程组可化为

$$\begin{cases}x\equiv 2(\bmod 5)\\ x\equiv 2(\bmod 7)\\ x\equiv 3(\bmod 4)\end{cases}$$（上面 6 个方程有两对相同，而 $x\equiv 3(\bmod 4)$包含 $x\equiv 1(\bmod 2)$）

解辅助方程组

$$28x\equiv 1(\bmod 5)\Rightarrow x\equiv 2(\bmod 5),$$
$$20x\equiv 1(\bmod 7)\Rightarrow x\equiv -1(\bmod 7),$$
$$35x\equiv 1(\bmod 4)\Rightarrow x\equiv -1(\bmod 4).$$

原方程组的解为

$$x\equiv 2\times 28\times 2-2\times 20-3\times 35\equiv -33\equiv 107(\bmod 140).$$

习题第三章自测与评估

1. 解：$x\equiv\frac{13}{5}\equiv\frac{13+4\times 43}{5}\equiv\frac{185}{5}\equiv 37$

2. 解：问题化为求解同余方程

$$n\equiv 1(\bmod 3),$$
$$n\equiv 2(\bmod 5),$$
$$n\equiv 3(\bmod 7).$$

先解辅助方程

$$\begin{array}{lcl}35n\equiv 1(\bmod 3) & & n\equiv 2(\bmod 3)\\ 21n\equiv 1(\bmod 5) & \Rightarrow & n\equiv 1(\bmod 5)\\ 15n\equiv 1(\bmod 7) & & n\equiv 1(\bmod 7)\end{array}$$

原方程组的解

$$n\equiv 2\times 35+2\times 21+3\times 15\equiv 52(\bmod 105).$$

3. 解：

$$\begin{cases}3x\equiv 2(\bmod 5)\\ 7x\equiv 3(\bmod 8)\\ 4x\equiv 7(\bmod 11)\end{cases}\Rightarrow\begin{cases}-2x\equiv 2(\bmod 5) & (-2,\ 5)=1\\ -x\equiv 3(\bmod 8) & \text{因为}(-1,\ 8)=1\\ -7x\equiv 7(\bmod 11) & (-7,\ 11)=1\end{cases}$$

所以方程可化为$\begin{cases}x\equiv -1(\bmod 5)\\ x\equiv -3(\bmod 8)\\ x\equiv -1(\bmod 11)\end{cases}$

先解辅助方程

$$88x\equiv 1(\bmod 5)\qquad x\equiv\frac{1}{88}\equiv\frac{1}{3}\equiv\frac{1+5}{3}\equiv 2(\bmod 5)$$

$$55x\equiv 1(\bmod 8)\quad\Rightarrow\quad x\equiv\frac{1}{55}\equiv\frac{1}{-1}\equiv -1(\bmod 8)$$

$$40x\equiv 1(\bmod 11)\qquad x\equiv\frac{1}{40}\equiv\frac{1}{7}\equiv\frac{1\times 3}{7\times 3}\equiv\frac{3}{-1}\equiv -3(\bmod 11)$$

原方程的解为

$$x\equiv(-1)\times 88\times 2+(-3)\times 55\times(-1)+(-1)\times 40\times(-3)\equiv 109(\bmod 5\times 8\times 11)$$

4. 解：由 7 是素数，$6!+1\equiv 0(\bmod 7)$，即 721 满足题设条件. $[2,\ 3,\ 4,\ 5,\ 6,\ 7]=420$.
所求数 $n=721+420k$，k 为整数. 适合条件最小的正整数 $n=301$.
或将问题化为求解同余方程组

$$\begin{cases}x\equiv 0(\bmod 7)\\ x\equiv 1(\bmod 5)\\ x\equiv 1(\bmod 12)\end{cases}$$

先解辅助方程

$$84x\equiv 1,\ (\bmod 5)\Rightarrow x\equiv\frac{1}{84}\equiv\frac{1}{-1}\equiv -1,$$

$$35x\equiv 1,\ (\bmod 12)\Rightarrow x\equiv\frac{1}{35}\equiv\frac{1}{-1}\equiv -1.$$

$x=-84-35\equiv -119\equiv 301(\bmod 420)$.

5. 证明：取 n 个不同的素数 p_1，p_2，…，p_n. 命题转化为下列同余方程组有解：

$$\begin{cases}x\equiv -1(\bmod p_1^2)\\ x\equiv -2(\bmod p_2^2)\\ x\equiv -3(\bmod p_3^2)\\ \quad\vdots\\ x\equiv -n(\bmod p_n^2)\end{cases}$$

由孙子定理，此方程组有解.
例如，$n=4$，取素数 2，3，5，7. 解同余方程组

$$x\equiv -1(\bmod 4),$$
$$x\equiv -2(\bmod 9),$$
$$x\equiv -3(\bmod 25),$$

$$x\equiv 0(\bmod 49).$$

解辅助方程

$$9\times 25\times 49x\equiv 1(\bmod 4),\ \Rightarrow x\equiv\frac{1}{9\times 25\times 49}\equiv\frac{1}{1\times 1\times 1}=1(\bmod 4),$$

$$4\times 25\times 49x\equiv 1(\bmod 9),\ x\equiv\frac{1}{4\times 25\times 49}\equiv\frac{1}{1\times 4}\equiv\frac{2}{8}\equiv\frac{2}{-1}=-2(\bmod 9),$$

$$4\times 9\times 49x\equiv 1(\bmod 25),\ x\equiv\frac{1}{4\times 9\times 49}\equiv\frac{1}{11\times(-1)}=\frac{1\times 2}{-11\times 2}\equiv\frac{2}{3}=\frac{2+25}{3}\equiv 9(\bmod 25),$$

$$\begin{aligned}x&\equiv -1\times 9\times 25\times 49+(-2)\times 4\times 25\times 49\times(-2)+(-3)\times 4\times 9\times 49\times 9\\&=-39\ 053\ (\bmod 4\times 9\times 25\times 49)\\&\equiv 5\ 047\ (\bmod 4\times 9\times 25\times 49),\end{aligned}$$

$\Rightarrow$5 047，5 048，5 049，5 050 这四个连续的整数都含素因子的平方.