Advances in Education 教育进展, 2024, 14(8), 1115-1123
Published Online August 2024 in Hans. https://www.hanspub.org/journal/ae
https://doi.org/10.12677/ae.2024.1481529

Hans汉斯

《初等数论》教学中的启示及应用

姚晨蕊

黑龙江大学数学科学学院，黑龙江 哈尔滨

收稿日期：2024年7月16日；录用日期：2024年8月19日；发布日期：2024年8月26日

摘　要

初等数论是一门研究“数”的学科，是针对数学专业的本科生开设的一门课程。本文主要阐述了在初等数论的教学过程中得到的一些启示和应用，分别为以下三方面内容：一是利用同余的性质得到了任意整数b能被给定正整数a整除的等价条件；二是给出了求解任意同余式的方法；三是给出了指数的两种证明方法。

关键词

数论，同余，整除，同余式，指数

Enlightenment and Applications in the Teaching of Elementary Number Theory

Chenrui Yao

School of Mathematical Sciences, Heilongjiang University, Harbin Heilongjiang

Received: Jul. 16th, 2024; accepted: Aug. 19th, 2024; published: Aug. 26th, 2024

Abstract

Elementary Number Theory is a subject that studies “number” and is a course for undergraduates majoring in mathematics. This paper mainly expounds enlightenment and applications obtained in the teaching process of elementary number theory, which are as follows: First, the equivalent condition that any integer b can be evenly divided by a given positive integer a is obtained by using the property of congruence. Second, the method of solving any congruence formula is given. Third, two methods of proving the index are given.

Keywords

Number Theory, Congruence, Divide Exactly, Congruence, Exponent

文章引用: 姚晨蕊. 《初等数论》教学中的启示及应用[J]. 教育进展, 2024, 14(8): 1115-1123.
DOI: 10.12677/ae.2024.1481529

1. 引言

初等数论是一门古老的学科，有着相当悠久的历史。它的主要研究内容是整数的性质及其应用。但是随着计算机和科学技术的发展，信息安全这一重大问题被提出。在这一背景下，数论为解决信息安全问题提供了一种核心技术——公开密钥，为信息技术的发展做出了巨大的贡献。此外，数论在密码学、算子理论、代数编码、最优设计、计算方法、组合代数及信息科学等诸多领域都有着极其重要的应用[1]-[4]。

在高等学校的教学中，这门课程的教学对象一般是数学专业的二、三年级的本科生，因此教材多数选用的都是闵嗣鹤、严士健主编的《初等数论》。这本教材的内容比较基础、通俗易懂，主要的教学内容包括整数的性质、不定方程的求解、同余的性质以及同余式的求解、原根及指标的性质及其应用、连分数的性质、代数数与超越数以及数论函数。作者所在高校也开设了初等数论这门课程，是针对数学与应用数学专业一年级的本科生开设的专业选修课，教材选用的也是闵嗣鹤、严士健主编的《初等数论》。作者已经连续两年承担初等数论这门课程的教学。在教学过程中，获得了一些有关初等数论教学的启示及应用。本文将详细阐述这些启示和应用。本文的结构如下：

在第二部分，首先列举同余的一些性质，然后在此基础上得到同余的一个应用，即给出任意整数能被给定正整数 a 整除的判定条件；

在第三部分，首先列举孙子定理、平方剩余及平方非剩余、原根和指标的性质，然后在此基础上给出求解一般同余式的方法；

在第四部分，首先给出指数的定义，然后给出指数的两种证明方法；

在第五部分，对本文进行总结。

2. 同余的应用

定义 1 [5]给定正整数 m。对任意的整数 a，b，如果 m 去除 a 和 b 所得的余数相同，则称 a 和 b 对模 m 同余，记作 $a\equiv b\pmod m$。如果所得的余数不同，则称 a 和 b 对模 m 不同余，记作 $a\neq b\pmod m$。

定理 1 [5]给定整数 m。如果整数 a 和 b 都是 m 的倍数，则 $a+b$ 和 $a-b$ 也是 m 的倍数。

定理 2 [5]给定正整数 m。则对任意整数 a,b 来说，a 和 b 对模 m 同余的充分必要条件是 m 能整除 $a-b$。

定理 3 [5]设 $A_{\alpha_1\alpha_2\cdots\alpha_k}\equiv B_{\alpha_1\alpha_2\cdots\alpha_k}\pmod m$，$x_i\equiv y_i\pmod m$，$i=1,2,\cdots,k$。则

$$\sum_{\alpha_1,\alpha_2,\cdots,\alpha_k}A_{\alpha_1\alpha_2\cdots\alpha_k}x_1^{\alpha_1}x_2^{\alpha_2}\cdots x_k^{\alpha_k}\equiv\sum_{\alpha_1,\alpha_2,\cdots,\alpha_k}B_{\alpha_1\alpha_2\cdots\alpha_k}y_1^{\alpha_1}y_2^{\alpha_2}\cdots y_k^{\alpha_k}\pmod m。$$

特别地，如果 $a_i\equiv b_i\pmod m$，$i=0,1,2,\cdots,n$，则

$$a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0\equiv b_nx^n+b_{n-1}x^{n-1}+\cdots+b_0\pmod m。$$

应用定理 1，定理 2 和定理 3，我们能给出任意整数被给定正整数 a 整除的判定条件。

定理 4 给定正整数 a。如果存在正整数 i 使得 $10^i\equiv1\pmod a$，那么对任意整数 b，b 能被 a 整除的充分必要条件是 $a\mid\sum_{j=0}^{n}b_j$，其中 $b=b_n\left(10^i\right)^n+b_{n-1}\left(10^i\right)^{n-1}+\cdots+b_0$，$0\le b_j<10^i$。

如果存在正整数 i 使得 $10^i\equiv-1\pmod a$，那么对任意整数 b，b 能被 a 整除的充分必要条件是

$a\left|\sum_{j=0}^{n}(-1)^{j}b_j\right.$，其中 $b=b_n\left(10^i\right)^n+b_{n-1}\left(10^i\right)^{n-1}+\cdots+b_0$，$0\le b_j<10^i$。

证明：如果存在正整数 i 使得 $10^i\equiv 1(\bmod a)$，则由定理 3 知

$$b=b_n\left(10^i\right)^n+b_{n-1}\left(10^i\right)^{n-1}+\cdots+b_0\equiv b_n1^n+b_{n-1}1^{n-1}+\cdots+b_0=\sum_{j=0}^{n}b_j\,(\bmod a),$$

即 $b\equiv\sum_{j=0}^{n}b_j\,(\bmod a)$。由定理 2 可 a 知能整除 $b-\sum_{j=0}^{n}b_j$。

若 a 能整除 b，则由定理 1 知 a 就能整除 $b-\left(b-\sum_{j=0}^{n}b_j\right)$，即 a 能整除 $\sum_{j=0}^{n}b_j$。

反之，若 a 能整除 $\sum_{j=0}^{n}b_j$，则由定理 1 知 a 就能整除 $\left(b-\sum_{j=0}^{n}b_j\right)+\sum_{j=0}^{n}b_j$，即 a 能整除 b。

因此，b 能被 a 整除的充分必要条件是 $a\left|\sum_{j=0}^{n}b_j\right.$。

如果存在正整数 i 使得 $10^i\equiv -1(\bmod a)$，则由定理 3 知

$$b=b_n\left(10^i\right)^n+b_{n-1}\left(10^i\right)^{n-1}+\cdots+b_0\equiv b_n(-1)^n+b_{n-1}(-1)^{n-1}+\cdots+b_0=\sum_{j=0}^{n}(-1)^j\,b_j\,(\bmod a),$$

即 $b\equiv\sum_{j=0}^{n}(-1)^j\,b_j\,(\bmod a)$。由定理 2 可知 a 能整除 $b-\sum_{j=0}^{n}(-1)^j\,b_j$。

若 a 能整除 b，则由定理 1 知 a 就能整除 $b-\left(b-\sum_{j=0}^{n}(-1)^j\,b_j\right)$，即 a 能整除 $\sum_{j=0}^{n}(-1)^j\,b_j$。

反之，若 a 能整除 $\sum_{j=0}^{n}(-1)^jb_j$，则由定理 1 知 a 就能整除 $\left(b-\sum_{j=0}^{n}(-1)^j\,b_j\right)+\sum_{j=0}^{n}(-1)^j\,b_j$，即 a 能整除 b。

因此，b 能被 a 整除的充分必要条件是 $a\left|\sum_{j=0}^{n}(-1)^j\,b_j\right.$。

下面，我们将列举一些例题来阐述上述定理得应用。

例 1 任意整数 a 能被 11 整除的充分必要条件是 $11\left|\sum_{i=0}^{n}(-1)^i\,a_i\right.$，其中 $a=a_n10^n+a_{n-1}10^{n-1}+\cdots+a_0$，$0\le a_i<10$。

解：因为 $10\equiv -1(\bmod 11)$，所以由定理 4 知 a 能被 11 整除的充分必要条件是 $11\left|\sum_{i=0}^{n}(-1)^i\,a_i\right.$，其中 $a=a_n10^n+a_{n-1}10^{n-1}+\cdots+a_0$，$0\le a_i<10$。

若 $a=54897635$，则 $a=5\times10^7+4\times10^6+8\times10^5+9\times10^4+7\times10^3+6\times10^2+3\times10+5$，所以 $\sum_{i=0}^{7}(-1)^i\,a_i=(-1)^7\times5+(-1)^6\times4+(-1)^5\times8+(-1)^4\times9+(-1)^3\times7+(-1)^2\times6+(-1)\times3+5=1$ 而 11 不能整除 1，所以 11 不能整除 54,897,635。

例 2 任意整数 a 能被 37 整除的充分必要条件是 $37\left|\sum_{i=0}^{n}a_i\right.$，其中 $a=a_n1000^n+a_{n-1}1000^{n-1}+\cdots+a_0$，$0\le a_i<1000$。

解：因为 $1000\equiv 1(\bmod 37)$，所以由定理 4 知 a 能被 37 整除的充分必要条件是 $37\left|\sum_{i=0}^{n}a_i\right.$，其中 $a=a_n1000^n+a_{n-1}1000^{n-1}+\cdots+a_0$，$0\le a_i<1000$。

若 $a=54897635$，则 $a=54\times1000^2+897\times1000+635$，所以 $\sum_{i=0}^{2}a_i=54+897+635=1586$，而 37 不能整除 1586，所以 37 不能整除 54,897,635。

例 3 任意整数 a 能被 101 整除的充分必要条件是 $101|\sum_{i=0}^{n}(-1)^i a_i$，其中 $a=a_n100^n+a_{n-1}100^{n-1}+\cdots+a_0$，$0\le a_i<100$。

解：因为 $100\equiv-1(\mathrm{mod}101)$，所以由定理 4 知 a 能被 101 整除的充分必要条件是 $101|\sum_{i=0}^{n}(-1)^i a_i$，其中 $a=a_n100^n+a_{n-1}100^{n-1}+\cdots+a_0$，$0\le a_i<100$。

若 $a=54897635$，则 $a=54\times100^3+89\times100^2+76\times100+35$，所以 $\sum_{i=0}^{3}(-1)^i a_i=(-1)^3\times54+(-1)^2\times89+(-1)\times76+35=-6$，而 101 不能整除−6，所以 101 不能整除 54,897,635。

由上述几个例题可以看出，同余有着很重要的应用。事实上，同余在整个初等数论的教学过程中都具有非常重要的位置和作用。所以，在实际教学过程中，当讲解同余时，可以在讲解同余的概念和性质时适当穿插一些相关的应用，如上面列举的得到任意整数被给定正整数整除的条件，或者是利用同余的性质验算两个比较大的整数做乘法结果是否正确等。这样不仅能让学生了解同余的广泛应用，增加对知识的兴趣，也能缓解学生在长时间的理论学习中所带来的注意力不集中、分散的现象。

3. 一般同余式的求解

定义 2 [5]设 $f(x)=a_nx^n+a_{n-1}x^{n-1}+\cdots+a_0$，其中 a_i 是整数。给定正整数 m。则 $f(x)\equiv0(\mathrm{mod}\,m)$ 叫做模 m 的同余式。如果 $a_n\not\equiv0(\mathrm{mod}\,m)$，则该同余式的次数为 n。

若 a 是使 $f(a)\equiv0(\mathrm{mod}\,m)$ 成立的一个整数，则 $x\equiv a(\mathrm{mod}\,m)$ 叫做该同余式的一解。

定理 5 [5]一次同余式

$$ax\equiv b(\mathrm{mod}\,m),\quad a\not\equiv0(\mathrm{mod}\,m)$$

有解的充分必要条件是 a 和 m 的最大公约数 (a,m) 能整除 b。

由定理 5 可以看出，求解一次同余式 $ax\equiv b(\mathrm{mod}\,m)$，也就相当于求解二元一次方程 $ax-my=b$，找到满足条件的 x，并将所有满足条件的 x 在模 m 的意义下分类。

定理 6 [5] **(孙子定理)**设 $m_1,m_2,\cdots,m_k$ 是 k 个两两互素的正整数，$m=m_1m_2\cdots m_k$，$M_i=\frac{m}{m_i}$，$i=1,2,\cdots,k$，则同余式组

$$x\equiv b_1(\mathrm{mod}\,m_1),x\equiv b_2(\mathrm{mod}\,m_2),\cdots,x\equiv b_k(\mathrm{mod}\,m_k)$$

的解为

$$x\equiv M_1'M_1b_1+M_2'M_2b_2+\cdots+M_k'M_kb_k(\mathrm{mod}\,m),$$

其中 M_i' 满足 $M_i'M_i\equiv1(\mathrm{mod}\,m_i)$，$i=1,2,\cdots,k$。

定理 7 [5]设 $m_1,m_2,\cdots,m_k$ 是 k 个两两互素的正整数，$m=m_1m_2\cdots m_k$。则同余式

$$f(x)\equiv0(\mathrm{mod}\,m)$$

与同余式组

$$f(x)\equiv0(\mathrm{mod}\,m_1),f(x)\equiv0(\mathrm{mod}\,m_2),\cdots,f(x)\equiv0(\mathrm{mod}\,m_k)$$

等价。

由定理 6 和定理 7 可知，对于一般的同余式 $f(x)\equiv 0(\bmod m)$，可以先将 m 进行标准分解，求出 m 的标准分解式 $m=2^{\alpha}p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_k^{\alpha_k}$，其中 $p_i(i=1,2,\cdots,k)$ 是奇素数，然后再分别求出同余式 $f(x)\equiv 0(\bmod 2^{\alpha})$ 的解 $x\equiv b_{0t_0}(\bmod 2^{\alpha})$，其中 $t_0=1,2,\cdots,T_0$ 以及同余式 $f(x)\equiv 0(\bmod p_i^{\alpha_i}),(i=1,2,\cdots,k)$ 的解 $x\equiv b_{it_i}(\bmod p_i^{\alpha_i})$，其中 $t_i=1,2,\cdots,T_i$。最后再求解同余式组

$$x\equiv b_{0t_0}(\bmod 2^{\alpha}),x\equiv b_{1t_1}(\bmod p_1^{\alpha_1}),x\equiv b_{2t_2}(\bmod p_2^{\alpha_2}),\cdots,x\equiv b_{kt_k}(\bmod p_k^{\alpha_k})。$$

对于同余式 $f(x)\equiv 0(\bmod p^{\alpha})$，其中 p 是素数，有如下的定理：

定理 8 [5]如果 $x\equiv x_1(\bmod p)$ 是同余式 $f(x)\equiv 0(\bmod p)$ 的解并且满足 p 不能整除 $f'(x_1)$，则由 x_1 可以诱导出 $f(x)\equiv 0(\bmod p^{\alpha})$ 的一解，即存在整数 x_{α} 使得 $x\equiv x_{\alpha}(\bmod p^{\alpha})$ 是 $f(x)\equiv 0(\bmod p^{\alpha})$ 的一解，其中 $x_{\alpha}\equiv x_1(\bmod p)$。

由定理 8 可知，要求解同余式 $f(x)\equiv 0(\bmod p^{\alpha})$，可以先求解出同余式 $f(x)\equiv 0(\bmod p)$ 的全部的解 $x\equiv x_1(\bmod p)$，$x\equiv x_2(\bmod p)$，…，$x\equiv x_k(\bmod p)$。如果 x_i 满足 p 不能整除 $f'(x_i)$，则将 $x=x_i+pt_1$ 代入到同余式 $f(x)\equiv 0(\bmod p^2)$ 中，并在点 x_i 处进行泰勒展开，于是有

$$f(x_i)+pt_1f'(x_i)\equiv 0(\bmod p^2),$$

即

$$f'(x_i)t_1\equiv -\frac{f(x_i)}{p}(\bmod p)。$$

又因为 p 不能整除 $f'(x_i)$，所以 $(p,f'(x_i))=1$，所以同余式 $f'(x_i)t_1\equiv -\frac{f(x_i)}{p}(\bmod p)$ 有一解 $t_1\equiv t_1'(\bmod p)$，即 $t_1=t_1'+pt_2$。代入到 $x=x_i+pt_1$ 有 $x=x_i+p(t_1'+pt_2)=x_2^i+p^2t_2$，其中 $x_2^i=x_i+pt_1'\equiv x_i(\bmod p)$ 且满足 $f(x_2^i)\equiv 0(\bmod p^2)$。所以 $x\equiv x_2^i(\bmod p^2)$ 是同余式 $f(x)\equiv 0(\bmod p^2)$ 的解。如此迭代下去，最终可以求出同余式 $f(x)\equiv 0(\bmod p^{\alpha})$ 的解 $x\equiv x_{\alpha}^i(\bmod p^{\alpha})$ 且 $x_{\alpha}^i\equiv x_i(\bmod p)$。

对于同余式 $f(x)\equiv 0(\bmod p)$，当 $f(x)$ 是一般的多项式时，只能通过试根的方法求出它的全部解，即依次将 $0,1,2,\cdots,p-1$ 代入到 $f(x)\equiv 0(\bmod p)$ 中判断哪些是解。

当 $f(x)$ 是如下几种特殊的多项式时，可以通过更便捷的方法求出 $f(x)\equiv 0(\bmod p)$ 的解。

当 $f(x)=x^2$ 且 $p=2$ 时，对于同余式 $x^2\equiv a(\bmod p^{\alpha})$，$(a,p)=1$ 有如下的定理。

定理 9 [5]设 $\alpha>1$。则同余式 $x^2\equiv a(\bmod 2^{\alpha})$，$(a,2)=1$ 有解的充分必要条件是当 $\alpha=2$ 时，$a\equiv 1(\bmod 4)$；当 $\alpha\geq 3$ 时，$a\equiv 1(\bmod 8)$。在有解的情况下，当 $\alpha=2$ 时，解数是 2；当 $\alpha\geq 3$ 时，解数是 4。

由定理 9 可以看出，对于同余式 $x^2\equiv a(\bmod 2^{\alpha})$，$(a,2)=1$，

当 $\alpha=1$ 时，显然同余式 $x^2\equiv a(\bmod 2)$ 的解只有 $x\equiv 1(\bmod 2)$；

当 $\alpha=2$ 且 $a\equiv 1(\bmod 4)$ 时，显然同余式 $x^2\equiv a(\bmod 2^2)$ 有两解 $x\equiv 1(\bmod 4)$，$x\equiv 3(\bmod 4)$；

当 $\alpha=3$ 且 $a\equiv 1(\bmod 8)$ 时，显然同余式 $x^2\equiv a(\bmod 2^3)$ 有四解 $x\equiv 1(\bmod 8)$，$x\equiv 3(\bmod 8)$，$x\equiv 5(\bmod 8)$，$x\equiv 7(\bmod 8)$；

当 $\alpha>3$ 且 $a\equiv 1(\bmod 8)$ 时，由定理 8 可知，求解同余式 $x^2\equiv a(\bmod 2^{\alpha})$，需要通过一次次迭代求解。而 $x^2\equiv a(\bmod 2^3)$ 的解已经求出，是全部的奇数，而全部奇数又可以表示成 $\pm(1+4t)$，$t=0,\pm 1,\pm 2,\cdots$。所以可以将 $\pm(1+4t_3)$ 代入到 $x^2\equiv a(\bmod 2^4)$ 中，即 $(1+4t_3)^2\equiv a(\bmod 16)$，解得 $t_3\equiv\frac{a-1}{8}(\bmod 2)$，即 $t_3=\frac{a-1}{8}+2t_4$，令 $t_3'=\frac{a-1}{8}$，则 $t_3=t_3'+2t_4$。所以 $x=\pm(1+4t_3'+8t_4)$，令 $x_4=1+4t_3'$，则 $x=\pm(x_4+8t_4)$，

$t_4=0,\pm1,\pm2,\cdots$ 是同余式 $x^2\equiv a\left(\mathrm{mod}\,2^4\right)$ 的解。如此迭代下去，最终可以求出同余式 $x^2\equiv a\left(\mathrm{mod}\,2^\alpha\right)$ 的解。

当 $f\left(x\right)=x^n$，$m=2$ 或 4 或 p^α 或 $2p^\alpha$ 且 $\left(a,m\right)=1$ 时，对于同余式 $x^n\equiv a\left(\mathrm{mod}\,m\right)$ 有如下的求解方法。为此，我们先回顾一些基本概念。

定义 3 [2]设 $m>1$ 且 $\left(a,m\right)=1$。则使得同余式

$$a^\gamma\equiv1\left(\mathrm{mod}\,m\right)$$

成立的最小正整数 γ 叫做 a 对模 m 的指数。

若 a 对模 m 的指数是 $\varphi\left(m\right)$，则 a 叫做模 m 的一个原根。

定理 10 [5]模 m 的原根存在当且仅当 $m=2$ 或 4 或 p^α 或 $2p^\alpha$。

定义 4 [5]设 g 是模 m 的一个原根。对任意的整数 a 来说，若存在正整数 γ 使得

$$a\equiv g^\gamma\left(\mathrm{mod}\,m\right)$$

则称 γ 是以 g 为底的 a 对模 m 的一个指标。

定理 11 [5]设 g 是模 m 的一个原根，a 是一整数且 $\left(a,m\right)=1$，$c=\varphi\left(m\right)$，则存在 $0\le\gamma'<c$ 使得 γ' 是以 g 为底的 a 对模 m 的一个指标；且以 g 为底的 a 对模 m 的指标是满足 $\gamma\equiv\gamma'\left(\mathrm{mod}\,c\right)$ 的一切正整数 γ。记以 g 为底的 a 对模 m 的所有指标模 c 的最小非负剩余为 $ind_g a$ 或 $ind\ a$。

定理 12 [5]设 g 是模 m 的一个原根，$c=\varphi\left(m\right)$，a 是一整数且 $\left(a,m\right)=1$，n 是正整数。记 $d=\left(n,c\right)$。则同余式

$$x^n\equiv a\left(\mathrm{mod}\,m\right)$$

有解当且仅当 $d\mid ind_g a$；并且在有解的情况下解数是 d。

基于以上的准备知识，我们可以得到同余式 $x^n\equiv a\left(\mathrm{mod}\,m\right)$ 的求解过程。

首先，找到模 m 的一个原根 g；然后，构造出以 g 为底的模 m 的指标表。由定理 12 可知同余式 $x^n\equiv a\left(\mathrm{mod}\,m\right)$ 与同余式 $n\,ind_g x\equiv ind_g a\left(\mathrm{mod}\,c\right)$ 等价。所以当 $d\mid ind_g a$ 时，可以先求解同余式 $n\,ind_g x\equiv ind_g a\left(\mathrm{mod}\,c\right)$，求出它的解 $ind_g x\equiv t_1\left(\mathrm{mod}\,c\right)$，$ind_g x\equiv t_2\left(\mathrm{mod}\,c\right)$，$ind_g x\equiv t_3\left(\mathrm{mod}\,c\right)$，……，$ind_g x\equiv t_s\left(\mathrm{mod}\,c\right)$，然后再由指标表查出对应的 x 的值，即为同余式 $x^n\equiv a\left(\mathrm{mod}\,m\right)$ 的解。

下面，我们将列举一些例题来看一下同余式的具体求解。

例 4 解同余式 $31x^4+57x^3+96x+191\equiv0\left(\mathrm{mod}\,225\right)$。

解：因为 $225=3^2\times5^2$，所以同余式 $31x^4+57x^3+96x+191\equiv0\left(\mathrm{mod}\,225\right)$ 与同余式组

$$31x^4+57x^3+96x+191\equiv0\left(\mathrm{mod}\,9\right),\ 31x^4+57x^3+96x+191\equiv0\left(\mathrm{mod}\,25\right)$$

等价。

记 $f\left(x\right)=31x^4+57x^3+96x+191$，则 $f'\left(x\right)=124x^3+171x^2+96$。

先求解同余式 $31x^4+57x^3+96x+191\equiv0\left(\mathrm{mod}\,9\right)$。经试根发现同余式 $31x^4+57x^3+96x+191\equiv0\left(\mathrm{mod}\,3\right)$ 的解为 $x_1\equiv1\left(\mathrm{mod}\,3\right)$，$x_2\equiv2\left(\mathrm{mod}\,3\right)$。经计算知 $f'\left(x_1\right)=391$，$f'\left(x_2\right)=1772$，3 不能整除 $f'\left(x_1\right)$ 和 $f'\left(x_2\right)$。

将 $x=1+3t_1$ 代入到 $31x^4+57x^3+96x+191\equiv0\left(\mathrm{mod}\,9\right)$ 中并在 $x=1$ 处泰勒展开有

$$3t_1\times391+375\equiv0\left(\mathrm{mod}\,9\right),$$

即 $391t_1+125\equiv0\left(\mathrm{mod}\,3\right)$。又 $391\equiv1\left(\mathrm{mod}\,3\right)$，$125\equiv2\left(\mathrm{mod}\,3\right)$，所以 $t_1+2\equiv0\left(\mathrm{mod}\,3\right)$，即 $t_1\equiv1\left(\mathrm{mod}\,3\right)$。所以 $t_1=1+3t_2$，$t_2=0,\pm1,\pm2,\cdots$。所以 $x=4+9t_2$，即 $x\equiv4\left(\mathrm{mod}\,9\right)$。

将 $x=2+3t_1$ 代入到 $31x^4+57x^3+96x+191\equiv0\left(\mathrm{mod}\,9\right)$ 中并在 $x=1$ 处泰勒展开有

$$3t_1\times1772+1335\equiv0\left(\mathrm{mod}\,9\right),$$

即$1772t_1+445\equiv 0\pmod 3$。又$1772\equiv 2\pmod 3$，$445\equiv 1\pmod 3$，所以$2t_1+1\equiv 0\pmod 3$，即$t_1\equiv 1\pmod 3$。所以$t_1=1+3t_2$，$t_2=0,\pm 1,\pm 2,\cdots$。所以$x=5+9t_2$，即$x\equiv 5\pmod 9$。

因此，$31x^4+57x^3+96x+191\equiv 0\pmod 9$的解为$x\equiv 4\pmod 9$，$x\equiv 5\pmod 9$。

再求解同余式$31x^4+57x^3+96x+191\equiv 0\pmod{25}$。经试根发现同余式$31x^4+57x^3+96x+191\equiv 0\pmod 5$的解为$x_1\equiv 1\pmod 5$，$x_2\equiv 2\pmod 5$。经计算知$f'(x_1)=391$，$f'(x_2)=1772$，5不能整除$f'(x_1)$和$f'(x_2)$。

将$x=1+5t_1$代入到$31x^4+57x^3+96x+191\equiv 0\pmod{25}$中并在$x=1$处泰勒展开有

$$5t_1\times 391+375\equiv 0\pmod{25},$$

即$391t_1+75\equiv 0\pmod 5$。又$391\equiv 1\pmod 5$，$75\equiv 0\pmod 5$，所以$t_1\equiv 0\pmod 5$。所以$t_1=5t_2$，$t_2=0,\pm 1,\pm 2,\cdots$。所以$x=1+25t_2$，即$x\equiv 1\pmod{25}$。

将$x=2+5t_1$代入到$31x^4+57x^3+96x+191\equiv 0\pmod 9$中并在$x=1$处泰勒展开有

$$5t_1\times 1772+1335\equiv 0\pmod{25},$$

即$1772t_1+267\equiv 0\pmod 5$。又$1772\equiv 2\pmod 5$，$267\equiv 2\pmod 5$，所以$2t_1+2\equiv 0\pmod 5$，即$t_1\equiv 4\pmod 5$。所以$t_1=4+5t_2$，$t_2=0,\pm 1,\pm 2,\cdots$。所以$x=22+25t_2$，即$x\equiv 22\pmod{25}$。

因此，$31x^4+57x^3+96x+191\equiv 0\pmod{25}$的解为$x\equiv 1\pmod{25}$，$x\equiv 22\pmod{25}$。

最后，求解同余式组

$$x\equiv b_1\pmod 9,\quad x\equiv b_2\pmod{25},\quad b_1=4,5,\quad b_2=1,22。$$

可知$m_1=9$，$m_2=25$，$m=m_1m_2=225$，$M_1=\dfrac{m}{m_1}=25$，$M_2=\dfrac{m}{m_2}=9$。

求解一次同余式$M_1M_1'\equiv 1\pmod 9$，即$25M_1'\equiv 1\pmod 9$，解得$M_1'\equiv 4\pmod 9$，所以取$M_1'=4$。

求解一次同余式$M_2M_2'\equiv 1\pmod{25}$，即$9M_2'\equiv 1\pmod{25}$，解得$M_2'\equiv -11\pmod{25}$，所以取$M_2'=14$。

由孙子定理知该同余式组的解为$x\equiv M_1M_1'b_1+M_2M_2'b_2\equiv 100b_1+126b_2\pmod{225}$。分别代入$b_1$和$b_2$的取值可知同余式$31x^4+57x^3+96x+191\equiv 0\pmod{225}$的解为$x\equiv 22\pmod{225}$，$x\equiv 76\pmod{225}$，$x\equiv 122\pmod{225}$，$x\equiv 176\pmod{225}$。

例 5 解同余式$x^2\equiv 41\pmod{64}$。

解：因为$41\equiv 1\pmod 8$，所以该同余式有解。

将$x=\pm(1+4t_3)$代入到$x^2\equiv 41\pmod{16}$中有$(1+4t_3)^2\equiv 41\pmod{16}$，即$8t_3\equiv 40\pmod{16}$，所以$t_3\equiv 5\equiv 1\pmod 2$，即$t_3=1+2t_4$，$t_4=0,\pm 1,\pm 2,\cdots$。所以$x=\pm(5+8t_4)$。

将$x=\pm(5+8t_4)$代入到$x^2\equiv 41\pmod{32}$中有$(5+8t_4)^2\equiv 41\pmod{32}$，即$80t_4\equiv 16\pmod{32}$，所以$5t_4\equiv 1\pmod 2$，即$t_4\equiv 1\pmod 2$，所以$t_4=1+2t_5$，$t_5=0,\pm 1,\pm 2,\cdots$。所以$x=\pm(13+16t_5)$。

将$x=\pm(13+16t_5)$代入到$x^2\equiv 41\pmod{64}$中有$(13+16t_5)^2\equiv 41\pmod{64}$，即$416t_5\equiv -128\pmod{64}$，所以$13t_5\equiv -4\pmod 2$，即$t_5\equiv 0\pmod 2$，所以$t_5=2t_6$，$t_6=0,\pm 1,\pm 2,\cdots$。所以$x=\pm(13+32t_6)$。

因此，$x^2\equiv 41\pmod{64}$的解为$x\equiv 13\pmod{64}$，$x\equiv 19\pmod{64}$，$x\equiv 45\pmod{64}$，$x\equiv 51\pmod{64}$。

例 6 解同余式$x^{15}\equiv 14\pmod{41}$。

解：已知6是模41的一个原根，且有如下的指标表：

	0	1	2	3	4	5	6	7	8	9
0		0	26	15	12	22	1	39	38	30
1	8	3	27	31	25	37	24	33	16	9

续表

2	34	14	29	36	13	4	17	5	11	7
3	23	28	10	18	19	21	2	32	35	6
4	20									

	0	1	2	3	4	5	6	7	8	9
0	1	6	36	11	25	27	39	29	10	19
1	32	28	4	24	21	3	18	26	33	34
2	40	35	5	30	16	14	2	12	31	22
3	9	13	37	17	20	38	23	15	8	7

因为 $d=(n,c)=(15,40)=5$，而 $ind_6 14=25$，$5\mid 25$，所以该同余式有解。同余式 $x^{15}\equiv 14(\mathrm{mod}\,41)$ 与同余式 $15ind_6 x\equiv ind_6 14(\mathrm{mod}\,40)$ 等价，即 $15ind_6 x\equiv 25(\mathrm{mod}\,40)$，所以 $3ind_6 x\equiv 5(\mathrm{mod}\,8)$。解得 $ind_6 x=15+8t$，$t=0,\pm 1,\pm 2,\cdots$。所以 $ind_6 x\equiv 7,15,23,31,39(\mathrm{mod}\,40)$，查表可知 $x\equiv 3,7,13,29,30(\mathrm{mod}\,41)$。所以同余式 $x^{15}\equiv 14(\mathrm{mod}\,41)$ 的解为 $x\equiv 3,7,13,29,30(\mathrm{mod}\,41)$。

同余式的求解一直是初等数论教学中的一个重点内容，在整本教材中有三章的内容都在讲解同余式的求解。所以学生在学习起来也会比较吃力。在实际的教学过程中，首先就是要打好基础，这个基础指的就是“一次同余式”，这是同余式的开端。所以在这一部分教学中，应该加强学生对“一次同余式”的理解，可以类比着“一元方程”，来让学生理解一次同余式，同时也应强调它区别于一元方程的地方，也就是一次同余式的解有很多数，只不过在同余的关系下将它们看成一个剩余类。其次，在讲解高次同余式的求解时，因为涉及到的相关定理如上面定理 7 和定理 8，它们的证明有一定的难度。在实际教学过程中，在讲这些证明时，学生接受的效果也不是太好，所以在这一部分教学时，可以适当略去一些证明，多增加一些练习，让学生掌握解题的思路和方法，这样学生接受的效果也能更好一些。然后就是指数和指标这两个定义，学生在学习过程中总容易弄混淆，所以在教学时可多强调几遍，多列举一些例子帮助学生辨析这两个概念。最后，在讲解完全部的同余式求解的知识后，应该对一般同余式的求解的方法加以总结，不然这部分知识有些分散，学生理解的也不是很透彻，很容易学完就忘，对同余式也没有系统化的理解和认知。在加以总结后，学生就能系统地掌握同余式的求解方法和步骤了。

4. 指数的两种证明方法

在第 2 章，已经给出了指数的定义。在这一章，我们将给出指数的两种证明方法。

给定正整数 m。要想证明 a 对模 m 的指数是 γ，也即证明 γ 是使得同余式 $a^{\gamma}\equiv 1(\mathrm{mod}\,m)$ 成立的最小正整数。所以有如下两种方法：

第一种，先证明 $(a,m)=1$ 以确保 a 对模 m 的指数存在；然后证明 $a^{\gamma}\equiv 1(\mathrm{mod}\,m)$；最后假设正整数 δ 满足 $a^{\delta}\equiv 1(\mathrm{mod}\,m)$，证明 $\gamma\le\delta$；

第二种，先证明 $(a,m)=1$ 以确保 a 对模 m 的指数存在；然后设 a 对模 m 的指数是 δ，证明 $\delta=\gamma$。

下面，我们将举例来看一下这两种方法的具体应用。

例 7 已知 a 对模 m 的指数是 δ。证明 a^{λ} 对模 m 的指数是 $\dfrac{\delta}{(\lambda,\delta)}$。

证明：因为 a 对模 m 的指数存在，所以 $(a,m)=1$，从而 $(a^{\lambda},m)=1$。因此，a^{λ} 对模 m 的指数存在。

方法 1. 设 $\lambda = k_1(\lambda,\delta)$，$\delta = k_2(\lambda,\delta)$。则

$$\left(a^{\lambda}\right)^{\frac{\delta}{(\lambda,\delta)}} = a^{\frac{\lambda}{(\lambda,\delta)}\delta} = a^{k_1\delta} = \left(a^{\delta}\right)^{k_1} \equiv 1(\bmod m)。$$

设正整数 η 满足 $\left(a^{\lambda}\right)^{\eta} \equiv 1(\bmod m)$。则 $a^{\lambda\eta} \equiv 1(\bmod m)$。又 a 对模 m 的指数是 δ，所以 $\delta \mid \lambda\eta$，即 $k_2(\lambda,\delta) \mid k_1(\lambda,\delta)\eta$，即 $k_2 \mid k_1\eta$。又因为 $(k_1,k_2) = \left(\frac{\lambda}{(\lambda,\delta)},\frac{\delta}{(\lambda,\delta)}\right) = 1$，所以 $k_2 \mid \eta$，所以 $k_2 \le \eta$，即 $\frac{\delta}{(\lambda,\delta)} \le \eta$。

因此，a^{λ} 对模 m 的指数是 $\frac{\delta}{(\lambda,\delta)}$。

方法 2. 设 $\lambda = k_1(\lambda,\delta)$，$\delta = k_2(\lambda,\delta)$。设 a^{λ} 对模 m 的指数是 η。则 $a^{\lambda\eta} \equiv 1(\bmod m)$。又 a 对模 m 的指数是 δ，所以 $\delta \mid \lambda\eta$，即 $k_2(\lambda,\delta) \mid k_1(\lambda,\delta)\eta$，即 $k_2 \mid k_1\eta$。又因为 $(k_1,k_2) = \left(\frac{\lambda}{(\lambda,\delta)},\frac{\delta}{(\lambda,\delta)}\right) = 1$，所以 $k_2 \mid \eta$，所以 $k_2 \le \eta$，即 $\frac{\delta}{(\lambda,\delta)} \le \eta$。

反之，又

$$\left(a^{\lambda}\right)^{\frac{\delta}{(\lambda,\delta)}} = a^{\frac{\lambda}{(\lambda,\delta)}\delta} = a^{k_1\delta} = \left(a^{\delta}\right)^{k_1} \equiv 1(\bmod m)，$$

所以 $\eta \mid \frac{\delta}{(\lambda,\delta)}$，所以 $\eta \le \frac{\delta}{(\lambda,\delta)}$，从而 $\eta = \frac{\delta}{(\lambda,\delta)}$。

因此，a^{λ} 对模 m 的指数是 $\frac{\delta}{(\lambda,\delta)}$。

在这一小节，我们给出了指数的两种证明方法，这样不仅可以帮助学生从不同角度理解指数的定义，也可以拓宽学生的数学思维。在实际教学过程中，不仅仅是“指数”这一知识点，其它内容都可以去积极探索有没有不同于书上的证明方法，这样便可以为学生提供多种解题思路，拓宽学生的思维，不使学生的思维固化，让其更加发散。

5. 小结

在这篇文章中，我们主要列出了初等数论的一些应用，一是得到了任意整数能被给定正整数整除的等价条件；二是给出了一般同余式的求解方法及过程；三是给出了指数的两种证明方法。这些不仅丰富了初等数论的教学内容，也能给学生提供系统化的方法，使得学生对初等数论的理解更加深刻，从而增加学生的学习兴趣。

参考文献

[1] 程庆丰, 汪定, 张卫明. 初等数论教学及其在密码学中的应用探讨[J]. 计算机教育, 2022(3): 94-97.

[2] 王婧哲. 《初等数论》课程教学改革研究[J]. 内蒙古财经大学学报, 2019, 17(2): 115-117.

[3] 晏燕雄, 徐海静. 我国初等数论课程教学改革的必要性及途径[J]. 西南师范大学学报(自然科学版), 2012, 37(4): 217-220.

[4] 袁兰党, 高印芝. 初等数论教学中的辩证法——关于素性检验和正整数的素因数分解的一次课程设计[J]. 高等数学研究, 2023, 26(1): 92-94.

[5] 闵嗣鹤, 严士健. 初等数论[M]. 第四版. 北京: 高等教育出版社, 2020.