南秀全初等数学系列

同余理论

南秀全 刘汉文 编著

- 同余式生质的应用
- 剩全剩余系
- 欧费马小定理
- 中理及其应用
- 平
- 佩

HITP
哈尔滨工业大学出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS

南秀全初等数学系列

同余理论

南秀全　刘汉文　编著

◎同余式性质
◎剩余类和完
◎欧拉定理与
◎中国剩余定
◎平方和问题
◎佩尔方程

理
用

HITP
哈爾濱工業大學出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS

内容简介

本书介绍了同余的概念及其基本性质,以及解同余式的理论和方法,展示了同余理论在数学竞赛中的重要应用。本书不仅介绍了同余的基本概念及简单性质,还指出了一些值得深入探讨的研究性问题。主要内容包括欧拉定理、费马定理、中国剩余定理、佩尔方程和费马大定理。

本书适合大、中学生及数学爱好者阅读。

图书在版编目(CIP)数据

同余理论/南秀全,刘汉文编著. —哈尔滨:
哈尔滨工业大学出版社,2012.5
ISBN 978-7-5603-3519-3

Ⅰ.①同… Ⅱ.①南… ②刘… Ⅲ.①同余式-理论
Ⅳ.①O156.1

中国版本图书馆 CIP 数据核字(2012)第 042760 号

策划编辑 刘培杰 张永芹
责任编辑 王勇钢 刘家琳
封面设计 孙茵艾
出版发行 哈尔滨工业大学出版社
社 址 哈尔滨市南岗区复华四道街 10 号 邮编 150006
传 真 0451-86414749
网 址 http://hitpress.hit.edu.cn
印 刷 哈尔滨市石桥印务有限公司
开 本 787mm×960mm 1/16 印张 15.75 字数 200 千字
版 次 2012 年 5 月第 1 版 2012 年 5 月第 1 次印刷
书 号 ISBN 978-7-5603-3519-3
定 价 38.00 元

前　言

◎前言

同余是数论中的一个基本概念，它是整除概念的拓展与发展. 同余的引入大大简化了数论中许多问题的解决，它的应用十分广泛. 在日常生活中也经常遇到，例如，1996年元旦是星期一，由于1996年共有366天，而366 = 7 × 52 + 2，所以，1997年元旦应是星期三，这里我们只关心余数.

有关同余的理论是在公元1800年前后由德国数学家高斯（C. F. Gauss，1777—1855）首先创立的，它是数论的重要工具. 我国早在公元前后的《孙子算经》里就提出了“物不知其数”的问题：“今有物不知其数，三三数之剩二，五五数之剩三，七七数之剩二，问物几何？答曰二十三”. 这是世界上最早提出解同余式组

$$x\equiv 2(\mathrm{mod}\ 3)$$

$$x\equiv 3(\mathrm{mod}\ 5)$$

$$x\equiv 2(\mathrm{mod}\ 7)$$

的问题.关于解上述同余式组的定理,在初等数论书中称为孙子定理,有的外文书中称为中国剩余定理.

掌握同余的概念及同余式的性质,并利用它们来处理数学问题,特别是数学竞赛中的某些数论题,已成为当前每一位数学竞赛参加者必须掌握的重要方法.因此,在这本小册子里,我们将较系统地介绍同余的概念及其基本性质,解同余式的理论和方法.在每章里配备了从国内外数学竞赛中精选出来的试题作为例题或习题,对习题大都给出了较为详尽的解答或提示,附于书后.在本书的编写过程中,我们参阅了大量的有关书刊,在此表示诚挚的谢意.

限于作者水平,本书的缺点与疏漏在所难免,敬请广大读者批评指正.

作　者

2012 年 3 月

◎目录

同余的概念及其基本性质

第1章

在整数的理论以及日常应用中，我们有时不必去关心一个数是多少，而只关心一个数被某一确定的整数去除后的余数是多少，对于余数相同的数，都可以用同一种方法去处理，这就需要引进同余的概念.

定义 设 a,b 是两个整数，如果 a 和 b 用正整数 m 除所得的余数相同，则称 a 与 b 对于模 m 同余，记作 $a\equiv b(\bmod m)$，读作 a 同余 b 模 m.

如果余数不相同，就称 a 与 b 关于模 m 不同余，记作 $a\not\equiv b(\bmod m)$.

例如，9 除以 7 余 2，23 除以 7 也余 2，就是说 9 与 23 对于模 7 是同余的，记作 $9\equiv 23(\bmod 7)$，$8\not\equiv 1(\bmod 3)$，$-2\equiv 9(\bmod 11)$.

显然，同余的概念也可用下面两种方式之一来定义：

(1)若 $m\mid a-b$，则 a 与 b 对模 m 同余；

(2)若 $a=b+mt$（t 为任意整数），则称 a 与 b 对模 m 同余.

以上三种定义彼此是等价的，以后我们将不加区别地任意选用，掌握并熟练地运用它们，对讨论同余的一些基本性质是很有用的.

由定义,可以得到同余的基本性质:

性质1 $a\equiv a(\bmod m)$(反身性).

性质2 若 $a\equiv b(\bmod m)$,则 $b\equiv a(\bmod m)$(对称性).

性质3 若 $a\equiv b, b\equiv c(\bmod m)$,则 $a\equiv c(\bmod m)$(传递性).

性质4 若 $a_1\equiv b_1(\bmod m), a_2\equiv b_2(\bmod m)$,则:

(1) $a_1+a_2\equiv b_1+b_2(\bmod m)$;

(2) $a_1-a_2\equiv b_1-b_2(\bmod m)$;

(3) $a_1a_2\equiv b_1b_2(\bmod m)$.

证明 因为 $a_1\equiv b_1(\bmod m), a_2\equiv b_2(\bmod m)$

所以 $a_1=b_1+mt_1, a_2=b_2+mt_2$ (t_1,t_2 为整数)

所以 $a_1a_2=b_1b_2+m(b_1t_2+b_2t_1+mt_1t_2)$

所以 $a_1a_2\equiv b_1b_2(\bmod m)$

推论1 若 $a_i\equiv b_i(\bmod m), k=1,2,\cdots,n$,则:

(1) $a_1+a_2+\cdots+a_n\equiv b_1+b_2+\cdots+b_n(\bmod m)$;

(2) $a_1a_2\cdots a_n\equiv b_1b_2\cdots b_n(\bmod m)$.

特别地,有:

推论2 若 $a\equiv b(\bmod m)$,则 $a^n\equiv b^n(\bmod m)$.

性质5 若 $a_1a_2\equiv b_1b_2(\bmod m), a_2\equiv b_2(\bmod m)$且$(a_2,m)=1$,则 $a_1\equiv b_1(\bmod m)$.

证明 因为 $a_1a_2\equiv b_1b_2(\bmod m), a_2\equiv b_2(\bmod m)$,所以 $b_1b_2=a_1a_2+mt_1, b_2=a_2+mt_2$ (t_1,t_2 为整数),所以 $b_1(a_2+mt_2)=a_1a_2+mt_1$,即

$$(a_1-b_1)a_2=m(b_1t_2-t_1)$$

因为$(a_2,m)=1$,所以 $m\mid a_1-b_1$,所以 $a_1\equiv b_1(\bmod m)$.

特别地,若 $ac\equiv bc(\bmod m)$,且$(c,m)=1$,则 $a\equiv b(\bmod m)$.

性质6 若 $ac\equiv bc(\bmod m)$,且$(c,m)=d>1$,则 $a\equiv b(\bmod \frac{m}{d})$.

证明 设 $c=dc_1, m=dm_1$. 因$(c,m)=d$,故$(c_1,m_1)=1$,由 $m\mid c(a-b)$得 $m_1\mid c_1(a-b)$. 从而 $m\mid a-b$,又 $m_1=\frac{m}{d}$,所以 $a\equiv$

$b(\mathrm{mod}\ \frac{m}{d})$.

性质 7　若 $a\equiv b(\mathrm{mod}\ m)$，且 $k>0$，则 $ak\equiv bk(\mathrm{mod}\ km)$.

性质 8　若 $m_1>0, m_1\mid m$，且 $a\equiv b(\mathrm{mod}\ m)$，则 $a\equiv b(\mathrm{mod}\ m_1)$.

性质 9　若 $a\equiv b(\mathrm{mod}\ m)$，且 d 是 a,b,m 的正的公因数，则 $\frac{a}{d}\equiv\frac{b}{d}(\mathrm{mod}\ \frac{m}{d})$.

证明　$a\equiv b(\mathrm{mod}\ m)$，即 $m\mid a-b$. 因 d 是 a,b,m 的公共正约数，且 $\frac{m}{d}$ 为正整数，有

$$\frac{m}{d}\mid\frac{a-b}{d},\frac{a-b}{d}=\frac{a}{d}-\frac{b}{d}$$

即
$$\frac{a}{d}\equiv\frac{b}{d}(\mathrm{mod}\ \frac{m}{d})$$

性质 10　若 $a\equiv b(\mathrm{mod}\ m_i)(i=1,2,\cdots,n)$，则

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

证明　由 $a\equiv b(\mathrm{mod}\ m_i)(i=1,2,\cdots,n)$，即 $m_i\mid(a-b)$，这就是说，$a-b$ 是 $m_1,m_2,\cdots,m_n$ 的公倍数，所以

$$[m_1,m_2,\cdots,m_n]\mid(a-b)$$

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

特别地，当 $(m_i,m_j)=1(i\neq j)$ 时，即 $m_1,m_2,\cdots,m_n$ 之间两两互质时，由 $a\equiv b(\mathrm{mod}\ m_i)(i=1,2,\cdots,n)$，可得

$$m_1\cdot m_2\cdot\cdots\cdot m_n\mid(a-b)$$

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

性质 11　若 $a_i\equiv b_i(\mathrm{mod}\ m)(i=0,1,2,\cdots,n)$，$x\equiv y(\mathrm{mod}\ m)$，则

$$a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\equiv$$
$$b_ny^n+b_{n-1}y^{n-1}+\cdots+b_1y+b_0(\mathrm{mod}\ m)$$

证明　因为 $x\equiv y(\mathrm{mod}\ m)$，所以 $x^i\equiv y^i(\mathrm{mod}\ m)(i=1,2,\cdots,n)$，所以 $a_ix^i\equiv b_iy^i(\mathrm{mod}\ m)$，又 $a_0\equiv b_0(\mathrm{mod}\ m)$，即有

$$a_nx^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0\equiv$$
$$b_ny^n+b_{n-1}y^{n-1}+\cdots+b_1y+b_0(\mathrm{mod}\ m)$$

同余式性质的应用

第2章

利用同余式解某些整除问题,可以做到条理清晰,叙述简单,特别是在解某些数学竞赛题时,可以十分简明,十分优雅,下面就几个主要方面的应用,叙述如下.

1. 用于解决某些整除的问题

例1 求证:任一自然数被9除的余数与其数字和被9除的余数相同.

分析 为证本题只需证明任一自然数与其各数位上数字之和在模9下同余.

证明 设自然数为

$$a_n \times 10^n + a_{n-1} \times 10^{n-1} + \cdots + a_1 \times 10^1 + a_0$$

则各数位上数字和为

$$a_n + a_{n-1} + \cdots + a_1 + a_0$$

因为

$$1 \equiv 1 \pmod 9, 10 \equiv 1 \pmod 9$$

$$\vdots$$

$$10^{n-1} \equiv 1 \pmod 9, 10^n \equiv 1 \pmod 9$$

所以

$$a_0 \equiv a_0 \pmod 9, a_1 \times 10 \equiv a_1 \pmod 9$$

$$\vdots$$

$$a_{n-1} \times 10^{n-1} \equiv a_{n-1} \pmod 9, a_n \times 10^n \equiv a_n \pmod 9$$

所以

$$a_n \times 10^n + a_{n-1} \times 10^{n-1} + \cdots + a_1 \times 10 + a_0 \equiv (a_n + a_{n-1} + \cdots + a_1 + a_0) \pmod 9$$

即任一自然数与其各数位上数字之和被9除的余数必相同.

例2　任一自然数被11除所得的余数与这个自然数偶数位数字和与奇数位数字和的差被11除所得的余数相同.

证明　设自然数为 $a_n \times 10^n + a_{n-1} \times 10^{n-1} + \cdots + a_1 \times 10 + a_0$,则偶数位上数字和为 $a_0 + a_2 + a_4 + \cdots$,奇数位上数字和为 $a_1 + a_3 + a_5 + \cdots$. 因为

$$1 \equiv 1 \pmod{11}, 10 \equiv -1 \pmod{11}, 10^2 \equiv 1 \pmod{11}$$

$$10^3 \equiv -1 \pmod{11}, \cdots, 10^{n-1} \equiv (-1)^{n-1} \pmod{11}$$

$$10^n \equiv (-1)^n \pmod{11}$$

所以

$$a_0 \equiv a_0 \pmod{11}, a_1 \times 10 \equiv -a_1 \pmod{11}$$

$$a_2 \times 10^2 \equiv a_2 \pmod{11}, a_3 \times 10^3 \equiv -a_3 \pmod{11}$$

$$\vdots$$

$$a_{n-1} \times 10^{n-1} \equiv (-1)^{n-1} a_{n-1} \pmod{11}$$

$$a_n \times 10^n \equiv (-1)^n a_n \pmod{11}$$

所以

$$a_n \times 10^n + a_{n-1} \times 10^{n-1} + \cdots + a_2 \times 10^2 + a_1 \times 10 + a_0 \equiv$$

$$[(a_0 + a_2 + a_4 + \cdots) - (a_1 + a_3 + a_5 + \cdots)] \pmod{11}$$

即任一自然数被11除所得的余数与其偶数位数字和与奇数位数字和之差被11除所得的余数相同.

类似地,读者可用上面例题的方法探寻自然数被7整除的简便检验法.

例3　(1956年上海市高三数学竞赛复试试题)设 n 是正整数,证明:$13^{2n} - 1$ 是168的倍数.

证明　因为　$13^2 = 169 \equiv 1 \pmod{168}$

所以 $13^{2n} \equiv 1^n \pmod{168}$,所以 $13^{2n} - 1 \equiv 0 \pmod{168}$,即 $13^{2n} - 1$ 是168的倍数.

例4　(1899年匈牙利数学竞赛题)证明:对任意自然数 n,表达式 $A = 2\,903^n - 803^n - 464^n + 261^n$ 能被1 897整除.

证明　$1\,897 = 7 \times 271$,7与271均为质数.

$2\ 903\equiv 5(\mathrm{mod}\ 7)$,$803\equiv 5(\mathrm{mod}\ 7)$,$464\equiv 2(\mathrm{mod}\ 7)$,$261\equiv 2(\mathrm{mod}\ 7)$.

所以

$$A=2\ 903^n-803^n-464^n+261^n\equiv$$
$$5^n-5^n-2^n+2^n\equiv 0(\mathrm{mod}\ 7)$$

又因为

$$2\ 903\equiv 193(\mathrm{mod}\ 271),803\equiv 261(\mathrm{mod}\ 271)$$
$$464\equiv 193(\mathrm{mod}\ 271)$$

所以

$$A=2\ 903^n-803^n-464^n+261^n\equiv$$
$$193^n-261^n-193^n+261^n\equiv 0(\mathrm{mod}\ 271)$$

所以 $$A\equiv 0(\mathrm{mod}\ 7\times 271)$$

例 5 证明:$641\mid 2^{25}+1$.

证明 因为

$$2^{25}+1=2^5(2^9)^3+1=$$
$$32\times(512)^3+1\equiv$$
$$32\times(-129)^3+1\equiv$$
$$32\times(-2\ 146\ 689)+1\equiv$$
$$32\times 20+1\equiv 0(\mathrm{mod}\ 641)$$

所以 $$641\mid 2^{25}+1$$

说明 形如 $F_n=2^{2^n}+1$ 的数称为费马(Fermat)数. 费马数的前几个是 $F_0=3$,$F_1=5$,$F_2=17$,$F_3=257$,$F_4=65\ 537$,它们都是素数,费马便猜测,对所有自然数 n,F_n 都是素数. 显然这一猜测是错误的. 首先推翻这一猜测的是大数学家欧拉(Euler),他证明了下一个费马数

$$F_5=4\ 294\ 967\ 297=641\times 6\ 700\ 417$$

不是素数. 上面我们利用同余,也证明了 F_5 是合数.

例 6 (1961 年第 6 届 IMO 试题)(1)确定所有的正整数 n,使得 2^n-1 能被 7 整除;

(2)证明:对于所有的正整数 n,2^n+1 不能被 7 整除.

解法 1 (1)因为 $2^3\equiv 1(\mathrm{mod}\ 7)$,故有

$$2^{3m}\equiv 1^m(\bmod 7),2^{3m}\equiv 1(\bmod 7)$$
$$2^{3m}\times 2\equiv 1\times 2(\bmod 7),2^{3m+1}\equiv 2(\bmod 7)$$
$$2^{3m}\times 2^2\equiv 1\times 2^2(\bmod 7),2^{3m+2}\equiv 4(\bmod 7)$$

于是

$$2^{3m}-1\equiv 0(\bmod 7),2^{3m+1}-1\equiv 1(\bmod 7),2^{3m+2}-1\equiv 3(\bmod 7)$$

而任何一个正整数 n,都可以表示为 $3m,3m+1$ 或 $3m+2$ 的形式之一,因此,当且仅当 $n=3m$,即 n 为3的倍数时,2^n-1 能被7整除.

(2)由(1)有

$$2^{3m}\equiv 1(\bmod 7),2^{3m+1}\equiv 2(\bmod 7),2^{3m+2}\equiv 4(\bmod 7)$$

所以

$$2^{3m}+1\equiv 2(\bmod 7),2^{3m+1}\equiv 3(\bmod 7),2^{3m+2}+1\equiv 5(\bmod 7)$$

因此,对于所有的正整数 n,2^n+1 都不能被7整除.

解法2　(1)若 m 是正整数或0,则

$$2^{3m}=(2^3)^m=(7+1)^m=7M_0+1\quad(M_0\text{ 是非负整数})$$

因此

$$2^{3m+1}=2\times 2^{3m}=2(7M_0+1)=7M_1+2\quad(M_1\text{ 是非负整数})$$
$$2^{3m+2}=4\times 2^{3m}=4(7M_0+1)=7M_2+4\quad(M_2\text{ 是非负整数})$$

所以

$$2^n-1=\begin{cases}7M_0 & \text{当 } n=3m \text{ 时}\\ 7M_1+1 & \text{当 } n=3m+1 \text{ 时}\\ 7M_2+3 & \text{当 } n=3m+2 \text{ 时}\end{cases}$$

故当且仅当 n 是3的倍数时,2^n-1 能被7整除.

(2)因为

$$2^n+1=\begin{cases}7M_0+2 & \text{当 } n=3m \text{ 时}\\ 7M_1+3 & \text{当 } n=3m+1 \text{ 时}\\ 7M_2+5 & \text{当 } n=3m+2 \text{ 时}\end{cases}$$

所以对于所有的正整数 n,2^n+1 都不能被7整除.

说明　一般的,请读者研究 2^n+k(k 为某整数)被7除时的情况:当 n 为何数时,2^n+k 能被7整除.

例 7 一个整数 a 的 100 次方被 125 除，其余数是什么？即 $a^{100}\equiv b(\mathrm{mod}\ 125)$，试求 b 可能值有哪些？

解 分以下几种情形讨论：

若 $a=5k$，那么易见 $a^{100}\equiv 0(\mathrm{mod}\ 125)$；

若 $a=5k\pm 1$，由于

$$a^{100}=(5k\pm 1)^{100}=(5k)^{100}\pm 100(5k)^{99}+\cdots+500k+1$$

所以 $$a^{100}\equiv 1(\mathrm{mod}\ 125)$$

若 $a=5k\pm 2$，由于

$$634\mid(5^{8k+4}+3^{4k+2})$$

现当 $n=k+1$ 时，有

$$5^{8(k+1)+4}+3^{4(k+1)+2}=$$
$$(5^4)^2\times 5^{8k+4}+3^4\times 3^{4k+2}=$$
$$(625)^2\times 5^{8k+4}+9^2\times 3^{4k+2}\equiv$$
$$(-9)^2\times 5^{8k+4}+9^2\times 3^{4k+2}(\mathrm{mod}\ 634)\equiv$$
$$0(\mathrm{mod}\ 634)$$

这样就证明了，此题目稍强的结论，对任意非负整数 n，可得

$$3\ 804\mid(n^3-n)(5^{8n+4}+3^{4n+2})$$

例 8 （1990 年第一届墨西哥数学奥林匹克试题）证明：对任意的正整数 n，数 $(n^3-n)\cdot(5^{8n+4}+3^{4n+2})$ 能被 3 804 整除.

证明 $3\ 804=6\times 634$，对任意的整数 n，不难证明 $6\mid(n^3-n)$. 下面证明，对任意的非负整数 n，$634\mid(5^{8n+4}+3^{4n+2})$.

(1) 当 $n=0$ 时，$5^4+3^2=625+9=634$，结论显然成立.

(2) 设 $n=k$ 时结论成立，即

$$a^{100}=(5k\pm 2)^{100}=(5k)^{100}\pm 100(5k)^{99}+\cdots\pm 500k\times 2^{99}+2^{100}$$

所以 $$a^{100}\equiv 2^{100}(\mathrm{mod}\ 125)$$

又由于

$$2^{100}=4^{50}=(5-1)^{50}=50^2-50\times 5^{49}+\cdots-250+1$$

所以 $2^{100}\equiv 1(\mathrm{mod}\ 125)$，由此即得 $a^{100}\equiv 1(\mathrm{mod}\ 125)$.

这样，便得 b 的可能值是 0（当 $5\mid a$）和 1（当 $5\nmid a$）.

例 9 （第 16 届 IMO 试题）证明：不存在自然数可使数

$\sum_{i=0}^{n}\binom{2n+1}{2k+1}2^{3k}$被5整除.

分析　令所求的和数为x,要证$x\equiv 0(\bmod 5)$不能成立. 因为x是一个二项式的一部分,故可设法凑成二项式来研究.

证明　将和数x变成二项式的项,令

$$x=\sum_{k=0}^{n}\binom{2n+1}{2k+1}2^{3k}=$$

$$\frac{1}{\sqrt{8}}\sum_{k=0}^{n}\binom{2n+1}{2k+1}(\sqrt{8})^{2k+1} \qquad ①$$

再补齐二项式所缺的偶次项,令

$$y=\sum_{k=0}^{n}\binom{2n+1}{2k}(\sqrt{8})^{2k}=\sum_{k=0}^{n}\binom{2n+1}{2k}2^{3k} \qquad ②$$

由式②+①得

$$\sqrt{8}x+y=\sum_{k=0}^{n}\binom{2n+1}{2k+1}(\sqrt{8})^{2k+1}+\sum_{k=0}^{n}\binom{2n+1}{2k}(\sqrt{8})^{2k}=$$

$$\sum_{k=0}^{2n+1}\binom{2n+1}{k}(\sqrt{8})^{k}=(\sqrt{8}+1)^{2n+1} \qquad ③$$

由式①-②得

$$\sqrt{8}x-y=\sum_{k=0}^{n}\binom{2n+1}{2k+1}(\sqrt{8})^{2k+1}(-1)^{(2n+1)-(2k+1)}+$$

$$\sum_{k=0}^{n}\binom{2n+1}{2k}(-1)^{(2n+1)-2k}=(\sqrt{8}-1)^{2n+1} \qquad ④$$

式③·④,得

$$y^2-8x^2=7^{2n+1}$$

因为

$$7^2\equiv -1(\bmod 5),7^{2n+1}\equiv 2(-1)^n(\bmod 5)$$

$$y^2\equiv 0,1,4(\bmod 5)$$

故

$$y_2\not\equiv \pm 2(\bmod 5)$$

所以 $$3x^2 \equiv y^2 - 7^{2n+1} \not\equiv 0 \pmod 5$$

因此不存在自然数 n,使 $5 \mid x$.

例 10 (第 31 届 IMO 备选题)设 m 是一个奇自然数,不能被 3 整除. 证明:$4^m - (2+\sqrt{2})^m$ 的整数部分可被 112 整除.

证明 由二项式定理可知

$$(2+\sqrt{2})^m + (2-\sqrt{2})^m$$

是整数,从而

$$4^m - (2+\sqrt{2})^m = \text{整数} + (2-\sqrt{2})^m$$

因为 $0 < 2-\sqrt{2} < 1$,所以 $4^m - (2+\sqrt{2})^m$ 的整数部分是

$$I = 4^m - \{(2+\sqrt{2})^m + (2-\sqrt{2})^m\}$$

先证 $16 \mid I$.

当 $m=1$ 时,可得

$$I = 4^m - \{(2+\sqrt{2})^m - (2-\sqrt{2})^m\} = 0 \equiv 0 \pmod{16}$$

当 m 为大于 3 的奇数时,可得

$$I = 4^m - \{(2+\sqrt{2})^m - (2-\sqrt{2})^m\} \equiv$$
$$-2 \times 2 \times (\sqrt{2})^{m-1} \equiv 0 \pmod{16}$$

再证 $7 \mid I$.

因为 m 是一个不被 3 整除的奇自然数,所以 $m = 6k+1$ 或 $6k+5$.

(1) $m = 6k+1$. 因为 $4^6 \equiv 1 \pmod 7$,可得

$$(2+\sqrt{2})^6 = 2^6 + 2^3(15 \times 2^2 + 15 \times 2 + 1) + 2^3 \times \sqrt{2}(6 \times 2^2 +$$
$$20 \times 2 + 6) = 1 + 7(a + b\sqrt{2}) \quad (a, b \in \mathbf{Z})$$
$$(2-\sqrt{2})^6 = 1 + 7(a - b\sqrt{2})$$

所以

$$I = 4^{6k+1} - \{(2+\sqrt{2})(2+\sqrt{6})^{6k} + (2-\sqrt{2})(2-\sqrt{2})^{6k}\} \equiv$$
$$4 - \{(2+\sqrt{2})(1+7(c+d\sqrt{2})\} +$$
$$(2-\sqrt{2})(1+7(c-d\sqrt{2})) \equiv$$
$$4 - 4 \equiv 0 \pmod 7 \quad (c, d \in \mathbf{Z})$$

(2) $m = 6k+5$,可得

$$I\equiv 4^5-\{(2+\sqrt{2})^{-1}(1+7(c+d\sqrt{2}))+$$
$$(2-\sqrt{2})^{-1}(1+7(c-d\sqrt{2}))\}\equiv$$
$$2-\left\{\frac{2-\sqrt{2}}{2}+\frac{2+\sqrt{2}}{2}\right\}\equiv 0(\mathrm{mod}\ 7)$$

所以 $4^m-(2+\sqrt{2})^m$ 的整数部分可被 112 整除.

例 11　(1993 年第 11 届美国数学邀请赛试题)能同时表示成连续 9 个整数之和,连续 10 个整数之和,及连续 11 个整数之和的最小正整数是哪一个?

解　设 $a=l+(l+1)+\cdots+(l+8)=m+(m+1)+\cdots+(m+9)=n+(n+1)+\cdots+(n+10)$,其中 $l,m,n\in\mathbf{N}$,则

$$l=n+2+\frac{2n+1}{9},m=\frac{n}{10}+n+1$$

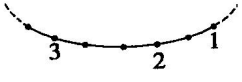
所以

$$2n+1\equiv 0(\mathrm{mod}\ 9),n\equiv 0(\mathrm{mod}\ 10)\qquad ⑤$$

易知满足上式的最小 n 为 40.

故　　$a_{\min}=40+41+\cdots+50=495$

例 12　(1993 年第 11 届美国数学邀请赛试题)在一圆周上给定 2 000 个点,取其中一点标记上数 1,从这点开始按顺时针方向数到第二个点标记上数 2. 从标记上 2 的点开始按顺时针方向数到第三个点标记上数 3(见下图)继续这个过程直到 1,2,3,…,1 993 都被标记到点上. 圆周上这些点中有一些会标记上不止一个数,也有一些点未被标记上任何数,标上 1 993 的那一点上标记的最小整数是什么?



解　将 2 000 个点按顺时针方向依次记为 1,2,…,2 000(图 1),依题意的标数为 $a_1,a_2,\cdots,a_{1\,993}$. 于是

$$a_1=1,a_2=3,a_3=6,\cdots,a_n=1+2+\cdots+n=\frac{1}{2}n(n+1)$$

所以　　$a_{1\,993}\equiv\frac{1}{2}\times 1\,993\times 1\,994\equiv 1\,021(\mathrm{mod}\ 2\,000)$

故 $a_{1\,993}$ 位于第 1 021 号位置.