中国剩余定理

又名「孙子定理」或称「鬼谷算」、「隔墙算」、「剪管术」、「秦王暗点兵」或「韩信点兵」，但当今数学界则称之为「**中国剩余定理**」（***Chinese Remainder Theorem***）。

「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？」（摘自《孙子算经》卷下，第26题），意思是：现在一个未知数，除3时，余数是2；除5时，余数是3；除7时，余数是2，问这个未知数的最小值？

中国著名数学家华罗庚教授，对这道题目有以下的说法：「求一个数，3除余2，5除余3，7除余 2。这个问题太容易回答了，因为3除余2，5除余3，7除余2，则21除余2。而23是3、7余2最小的数，刚好又是5除余3的数。所以心算快的人都算出！」（摘自《华罗庚科普著作选集》第84页）

正如华罗庚教授所说，重点并不是计算出23这个结果，数学便是不仅于此。数学的研究便是希望找到这道题的特质，作出普遍化的解法。你又可知道这道名题的普遍解吗？

很多中国的名事迹或名题，在民间都有歌谣，有的唱出一个故事，有的唱出这些名题的解法。而这「鬼谷算」也不例外，而且还有几个不同版本，以下是其中之一： **三人同行七十稀，  五树梅花廿一枝， 七子团圆正月半， 除百零五便得知。** 摘自《算法统宗》卷四

这些解的意思是说，用70乘3除所得的余数，用21乘5除所得的余数，用15乘7除所得的余数，然后再加起来。如果其和大于105，则减去105，直至小于 105为止，最后这个数便是答案。以「鬼谷算」中的余数为例： 2×70+3×21+2×15－105－105 =23

那么，（一）如何推出这个结果？（二）如果除数改变了，或有更多的余数时又如何？简而言之，可以把这个方法推广吗？

讨论中国剩余定理，**同余**（*congruence*）的概念是必须的理论基础。

给定一个正整数*n*，我们说两个数*a*、*b*是对模*n*同余，如果*a*－*b*是*n*的倍数。用符号*a*≡*b*(*mod* *n*)来代表。一般来说，*a*≡*b*(*mod* *n*)等同于*a*＝*b*+*kn*，而*a*，*b*，*k*，*n*都是整数，所以，13≡1(*mod* 6)、19≡1(*mod* 6)。

但同余并不只是一个代号，而是有很很多有趣的特性：

（一）整数加法跟普通加法相似，if *a*≡*b*(*mod* *n*) then *a*+*c*≡(*b*+*c*)(*mod* *n*)；

（二）整数乘法跟普通乘法相似，if *a*≡*b*(*mod* *n*) then *ac*≡*bc*(*mod* *n*)，而*a*，*b*，*c*，*n*都是整数。但如果*ac*≡*bc*(*mod* *n*)，则不一定能得到*a*≡*b*(*mod* *n*)。

以「鬼谷算」为例，假设*x*是那个未知数，而除3，5，7后的余数分别为*r*1，*r*2，*r*3。因此有

*x*≡*r*1(*mod* 3)  ， *x*≡*r*2(*mod* 5)  ， *x*≡*r*3(*mod* 7)

而另一方面

70＝(5×7)×2≡1(*mod* 3)、70≡0(*mod* 5)及70≡0(*mod* 7)

21＝(3×7)×1≡1(*mod* 5)、21≡0(*mod* 3)及21≡0(*mod* 7)

15＝(3×5)×1≡1(*mod* 7)、15≡0(*mod* 3)及15≡0(*mod* 5)

由同余的特性，我们有

70*r*1≡*r*1(*mod* 3)、70*r*1≡0(*mod* 5)及70*r*1≡0(*mod* 7)

21*r*2≡*r*2(*mod* 5)、21*r*2≡0(*mod* 3)及21*r*2≡0(*mod* 7)

15*r*3≡*r*3(*mod* 7)、15*r*3≡0(*mod* 3)及15*r*3≡0(*mod* 5)

因此亦有

70*r*1+21*r*2+15*r*3≡*r*1(*mod* 3)

70*r*1+21*r*2+15*r*3≡*r*2(*mod* 5)

70*r*1+21*r*2+15*r*3≡*r*3(*mod* 7)

最后得到这个精彩的结果，*x*≡(70*r*1+21*r*2+15*r*3)(*mod* 105)，而105正便是3，5，7的最小公倍数。所以其实在很多数字可以满足这几个余数条件的，要找到最小值才要减105。

由以上的推导方法，我们可以知道，无论余数是多少，也可运用这个方法；而且无论除数有多少个，也可用同一个推导的方法找到一公式来计算出符合条件的未知数。而这种一般的解法便是「中国剩余定理」。

**一、基本解法——层层推进法**

以“物不知其数”为例：物品的个数满足除以3余2，除以5余3，除以7余2，则有物品多少个？

解析：满足除以3余2的最小数为2；在2的基础上每次加3，直到满足除以5余3，这个最小的数为8；在8的基础上每次加3、5的最小公倍数15，直到满足除以7余2，这个最小的数为23。所以满足条件的最小自然数为23，而3、5、7的最小公倍数为105，故满足条件的数可表示为105*n*+23（*n*=0，1，2，…，下同）。

**二、余同取余，和同加和，差同减差，最小公倍数做周期**

（1）余同取余，最小公倍数做周期

如果一个数除以几个不同的数，余数相同，则这个数可以表示成这几个除数的最小公倍数的倍数与余数相加的形式。

例1：一个数除以3余1，除以4余1，除以10余1。则这个数可表示为[3,4,1]*n*+1=60*n*+1（60为3、4、10的最小公倍数，*n*=0，1，2，…，下同）。

（2）和同加和，最小公倍数做周期

如果一个数除以几个不同的数，除数与余数之和相同，则这个数可以表示成这几个除数的最小公倍数的倍数与该和（除数与余数之和）相加的形式。

例2：一个数除以5余4，除以6余3，除以8余1。则这个数可表示为[5,6,8]*n*+(5+4)=120*n*+9。

（3）差同减差，最小公倍数做周期

如果一个数除以几个不同的数，除数与余数之差相同，则这个数可以表示成这几个除数的最小公倍数的倍数与该差（除数与余数之差）相减的形式。

例3：一个数除以3余1，除以4余2，除以10余8。则这个数可表示为[3,4,10]*n*-(3-1)=60*n*－2（*n*=1，2，…）。

**三、巧妙应用——余同、和同、差同的构造思想**

有些题目是上面第二条所述的三种特殊情况之一，就可以直接利用其口诀做题，而有些题目不属于这三种特殊情况的任何一种，是不是就必须用最基本的层层推进法解了呢？

不是。我们可以利用余数的规律，将其转化成这三种特殊情况之一，进而快速解题，节约宝贵时间。

例4：某出版社工作人员将一批书打包，每包装11本则多出5本，每包装13本则多出6本，每包装15本则多出7本，问这批书至少有多少本？

A．1072 B．2144 C．2145 D．3217

【分析】观察发现，余不同、差不同、和不同，但是我们可以将书的数量乘2，如此构造出差同的情况。

解析：将书的数量*a*乘以2，则根据余数的性质可知2*a*除以11余10，除以13余12，除以15余14，此时三者的差均为1，根据“差同减差，最小公倍数做周期”可知，2*a*可表示为2145*n*－1（2145为11、13和15的最小公倍数），2*a*最小为2144，故这批书至少有2144÷2=1072本，选A。

**四、用中国剩余定理解决实际问题**

例5：有些数既能表示成3个连续自然数的和，又能表示成4个连续自然数的和，还能表示5个连续自然数的和，如30就满足上述要求，因为30=9+10+11，30=6+7+8+9，30=4+5+6+7+8，在700至1000之间满足要求的数有：

A．5个 B．7个 C．8个 D．10个

解析：设分别将该数分解为3、4、5个连续自然数的和时，加数中最小的自然数分别为*x*、*y*、*z*，则有

*x*+(*x*+1)+(*x*+2)=3*x*+3=3（*x*+1）， 或者 设为 (*x*-1)+ *x*+ (*x*+1) =3*x* ；

*y*+(*y*+1)+(*y*+2)+(*y*+3)=4（*y*+1）+2， 或者 (*y*-1) +*y*+(*y*+1)+(*y*+2) =4*y*+2 ；

*z*+(*z*+1)+(*z*+2)+(*z*+3)+(*z*+4)=5（*z*+2） 或者 (*z*-2)+ (*z*-1)+ *z*+ (*z*+1)+(*z*+2) =5*z* 。

即该数能同时被3、5整除，并且被4除余数为2，求得满足条件的最小自然数为30。

而3、4、5的最小公倍数为60，则所有这样的数可表示为60*n*+30，

且700≤60*n*+30≤1000，故满足题意的数有12、13、14、15、16，共5个。

**中国剩余定理练习题**

1．一个数被3除余1，被4除余2，被5除余4，这个数最小是几？

1. N=a+b+c， a=40，b=30，c=24， [3,4,5]=60, N=(40+30+24) mod 60=94 mod 60=34

另解 N=1×m+2×n+4×k，m=40，n=45，k=36，N=（40+90+144）mod 60=34

2．一个数被3除余2，被7除余4，被8除余5，这个数最小是几？

2. [7,8]-(7-4)=56-3=53, 53 mod 3=2,

N=2m+4n+5k， m=112, n=120, c=105, N=(224+480+525) mod 168=53

3．一个数除以5余4，除以8余3，除以11余2，求满足条件的最小的自然数。

3. N=a+b+c, a=264, b=275,c=200, [5,8,11]=440, N=(a+b+c) mod 440=739 mod 440=299

Or N=4m+3n+2k, m=176,n=385,k=100, N=(176×4+385×3+200) mod 440=299

4．有一个年级的同学，每9人一排多5人，每7人一排多1人，每5人一排多2人，问这个年级至少有多少人？

4. N=a+b+c, a=140, b=225, c=252, (a+b+c) mod [9,7,5]=617 mod 315=302

Or N=5m+n+2k, m=280, n=225, k=126, N=(1400+225+252) mod 315=302

5．有一个年级的同学，每9人一排多6人，每7人一排多2人，每5人一排多3人，问这个年级至少有多少人？

5. N=a+b+c, a=105,b=135,c=63, (a+b+c) mod [9,7,5]=303 mod 315=303

Or 第4题，余数加1， 为302+1=303

6．一个数被3除余2，被7除余4，被8除余5，这个数最小是几？在1000内符合这样条件的数有几个？

6. 按照第2题的解法，得到最小为53，故通解为 53+[3,7,8]n=53+168n,其中 n为自然数；要求

53+168n≤1000, n≤(947÷168), n≤5, 即n可取0,1,2,3,4,5这六个数，有六个满足条件的数。