

# 中国剩余定理

善科文库团队 2018-11-22 3916

林开亮

在最近推出的两篇文章

① 微积分之前奏 1：高阶等差数列的求和 ([http://mp.weixin.qq.com/s?\\_\\_biz=MzlyNzUxMjE1Mw==&mid=2247492896&idx=1&sn=a8823a26a8b366f4099772f0da703fbc&chksm=e862bf16df1536002ad3502024b919ff91919d51e5ea7b2468464606f212ca40a768ca3d7470&scene=21#wechat\\_redirect](http://mp.weixin.qq.com/s?__biz=MzlyNzUxMjE1Mw==&mid=2247492896&idx=1&sn=a8823a26a8b366f4099772f0da703fbc&chksm=e862bf16df1536002ad3502024b919ff91919d51e5ea7b2468464606f212ca40a768ca3d7470&scene=21#wechat_redirect))

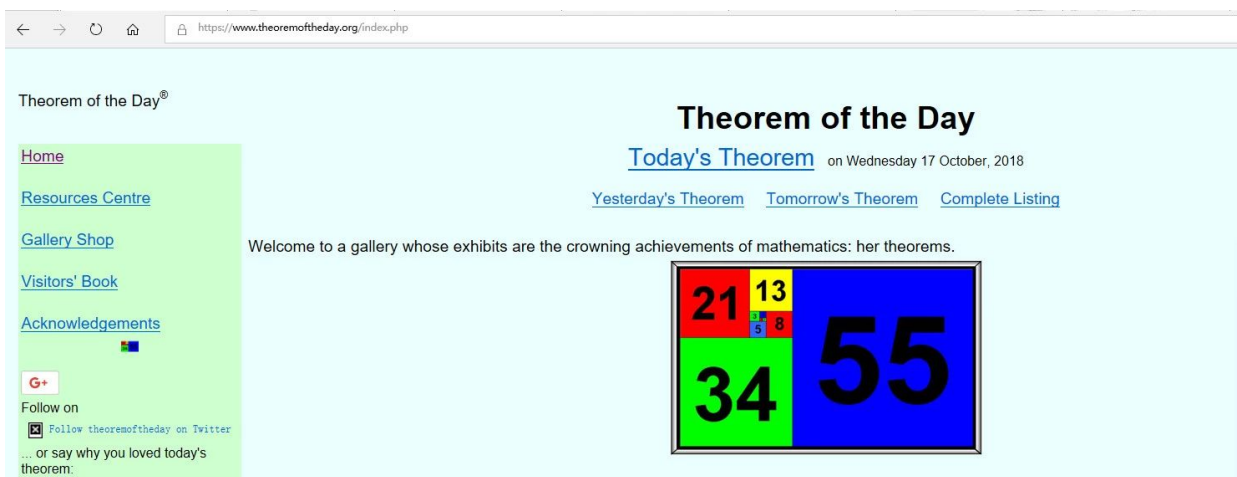
② 算命是胡扯，猜姓却不然 ([http://mp.weixin.qq.com/s?\\_\\_biz=MzlyNzUxMjE1Mw==&mid=2247492234&idx=1&sn=9f6da59f601a29330cbf2ad0c55c4806&chksm=e862b8bcd1531aa5c48c2c469e7fac4a0862a8cbd2d02f4831d2b67382fec16e138f3fda81d&scene=21#wechat\\_redirect](http://mp.weixin.qq.com/s?__biz=MzlyNzUxMjE1Mw==&mid=2247492234&idx=1&sn=9f6da59f601a29330cbf2ad0c55c4806&chksm=e862b8bcd1531aa5c48c2c469e7fac4a0862a8cbd2d02f4831d2b67382fec16e138f3fda81d&scene=21#wechat_redirect))

中，我们都提到了中国剩余定理，虽然我曾在

从射雕到九章——在天大理学院物理系的通俗报告 ([http://mp.weixin.qq.com/s?\\_\\_biz=MzU4NjAxNzg0MA==&mid=2247484388&idx=1&sn=824d2fb51f18cab9a7a81bae02f3da5e&chksm=fd80febbcaf777adf784c27e82824d581e4a9b37fe31677b3ce461fc61205b6198fbb46672dd&scene=21#wechat\\_redirect](http://mp.weixin.qq.com/s?__biz=MzU4NjAxNzg0MA==&mid=2247484388&idx=1&sn=824d2fb51f18cab9a7a81bae02f3da5e&chksm=fd80febbcaf777adf784c27e82824d581e4a9b37fe31677b3ce461fc61205b6198fbb46672dd&scene=21#wechat_redirect))

介绍过，但有点浮光掠影，我们想在此详细介绍一下。

我们期待，本文作为好玩的数学开创的头一个专栏——一周一定理——的开篇，能够打响第一炮。本专栏的开创，学习和借鉴了下述网页（感谢上海交通大学数学系吴耀琨教授向我们推荐）



有兴趣的读者，可以先浏览这个主页上的各个定理。欢迎各位读者为本专栏供稿，投稿邮箱在这里来，一起交流数学 ([http://mp.weixin.qq.com/s?\\_\\_biz=MzlyNzUxMjE1Mw==&mid=2247492220&idx=1&sn=6a5da13b5b02991e93506b3e61dc3333&chksm=e862b84adf15315c46975876689c3cc0e8f6dcd8a986939c88c0c545a465f4b7fb230ff28a94&scene=21#wechat\\_redirect](http://mp.weixin.qq.com/s?__biz=MzlyNzUxMjE1Mw==&mid=2247492220&idx=1&sn=6a5da13b5b02991e93506b3e61dc3333&chksm=e862b84adf15315c46975876689c3cc0e8f6dcd8a986939c88c0c545a465f4b7fb230ff28a94&scene=21#wechat_redirect))。

好了，现在我们直奔主题。

中国剩余定理：设正整数  $m_1, m_2, \dots, m_n$  两两互素，则下述同余方程组

$$\begin{cases} x_1 \equiv r_1 \pmod{m_1} \\ \dots \\ x_n \equiv r_n \pmod{m_n} \end{cases} \quad (*)$$

(其中  $r_1, r_2, \dots, r_n$  给定的整数) 的整数解恰好是模

$$m = m_1 m_2 \cdots m_n$$

的一个剩余类。事实上，方程 (\*) 的通解为

$$x = r_1 M_1 x_1 + \cdots + r_n M_n x_n + kM, k \in \mathbb{Z} \quad (\#)$$

其中  $M_i = M/m_i$ ，而  $x_i$  是同余方程

$$M_i x_i \equiv 1 \pmod{m_i} \quad (*i)$$

的一个特解，因而可以用求一术得出。

简单地说，中国剩余定理将一个同余方程组 (\*) 的求解，归结为多个一次同余方程 (\*i) 的求解，而后者可以用求一术来求解。那么，什么是求一术呢？我们表述成一个算法的形式：

## 求解方程

$$ax \equiv 1 \pmod{b} \quad (a, b \in \mathbb{Z}^+) \quad (\clubsuit)$$

的整数解的求一术：

首先写出矩阵

$$A = \begin{vmatrix} ab & \\ & 10 \end{vmatrix}$$

然后对第一行两个元素辗转相除，并将对应的操作应用于第二行，直至第一行某个元素变成0（停止信号），此时观察第一行的另一个元素：若它恰好是1（正常信号），则它下方的那个数就是（♣）的一个特解；否则，（♣）无整数解。此外，若已得到（♣）的一个特解，比方说， $x = u$ ，那么，（♣）的通解为

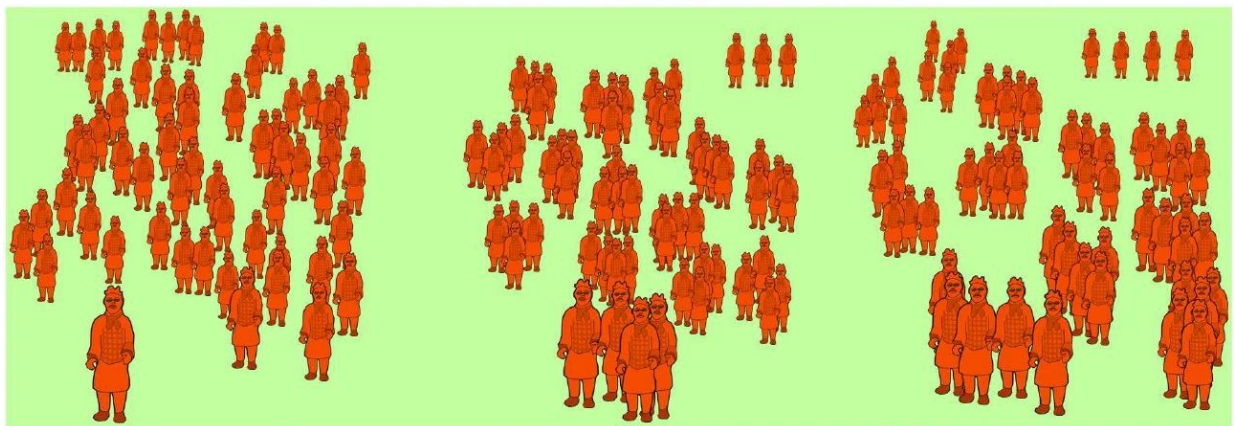
$$x = u + bk, k \in \mathbb{Z} \quad (\spadesuit)$$

注：我们不打算证明求一术，它本质上就是解线性方程组的矩阵变换方法。我们指出，在中国古代还未出现0时，通常是用辗转相减（即“更相减损术”），所以最后终止的信号是，出现的等数（即最大公因子）为1，这就是求一术名称的来由（对此，请参见许光午和李宝[4]）。另一方面，注意到方程（♣）本质上是在求逆，所以，也许一个更恰当的称谓是求逆术。由此可以理解，为什么在下述网页中，作者用了逆的记号来表述结果：



### THEOREM OF THE DAY

**The Chinese Remainder Theorem** Suppose  $n_1, n_2, \dots, n_r$  are mutually coprime positive integers (that is, no integer greater than 1 dividing one may divide any other.) Let  $y_1, y_2, \dots, y_r$  be any integers. Then there is a number  $x$  whose remainder on division by  $n_i$  is  $y_i$  for each  $i$ . That is, the system of linear congruences  $x \equiv y_i \pmod{n_i}$  has a solution. Moreover this solution is unique modulo  $N = n_1 \times n_2 \times \dots \times n_r$ .



How many people  
What is  $x$ ?

Divided into 4s: remainder 3  
 $x \equiv 3 \pmod{4}$

Divided into 5s: remainder 4  
 $x \equiv 4 \pmod{5}$

Let  $N_i = N/n_i$  for each  $i$ . Here,  $N = 4 \times 5 = 20$ , so  $N_1 = 5$  and  $N_2 = 4$ . There will be a smallest number, the *inverse* of  $N_i$ , denoted by  $N_i^{-1}$ , for which  $N_i \times N_i^{-1}$  has remainder 1 on division by  $n_i$ ; we write  $N_i N_i^{-1} \equiv 1 \pmod{n_i}$ . We find that  $N_1^{-1} = 1$ , since  $5 \times 1 = 5 = 1 \times 4 + 1$ . Similarly,  $N_2^{-1} = 4$ . Now all solutions are congruent, modulo  $N$ , to  $x = y_1 N_1 N_1^{-1} + y_2 N_2 N_2^{-1} + \dots + y_r N_r N_r^{-1}$ , which for our problem means some multiple of  $N = 20$  plus  $3 \times 5 \times 1 + 4 \times 4 \times 4 = 79$ . In fact  $-1 \times 20 + 79 = 59$  is the correct answer but 79 itself also looks like a possibility for the size of the crowd. We could narrow down the possibilities by dividing the crowd again, into 3s, since 3 is coprime to 4 and 5. Then we get  $x \equiv 359 \pmod{60}$ , giving 59 and 119 as the nearest choices: 59 must be right!

The Chinese Remainder Theorem dates back at least as early as the 3rd century, where it is used in the Mathematical Manual of Sun Zi. It may be applied when the  $n_i$  are not coprime, given suitable conditions on the  $y_i$ .

Web link: [crypto.stanford.edu/pbc/notes/numbertheory/](http://crypto.stanford.edu/pbc/notes/numbertheory/); and the history: [www.math.harvard.edu/~knill/crt/lib.html](http://www.math.harvard.edu/~knill/crt/lib.html).

Further reading: *Elementary Number Theory* by Gareth Jones and Mary Jones, Springer, Berlin, 1998.



好了，现在我们来实战吧。首先，我们解释上述网页中的例子，即我们要求解同余方程组

$$\begin{cases} x \equiv 3 \pmod{4}, \\ x \equiv 4 \pmod{5}. \end{cases} \quad (0)$$

为求解这个方程组，我们来求解两个更简单的方程组

$$\begin{cases} x \equiv 1 \pmod{4}, \\ x \equiv 0 \pmod{5}. \end{cases} \quad (1)$$

与

$$\begin{cases} x \equiv 0 \pmod{4}, \\ x \equiv 1 \pmod{5}. \end{cases} \quad (2)$$

先看（1），注意到（1）的第二个方程相当于说， $x$  是5的倍数，因此我们可以令

$$x = 5x_1, \quad (x_1 \in \mathbb{Z})$$

从而代入（1）的第一个方程，就把（1）整个转化为一次同余方程

$$5x_1 \equiv 1 \pmod{4} \quad (1^*)$$

在这个特殊情况，我们可以直接看出（1\*）的一个特解为

$$x_1 = 1$$

类似的，我们来求解方程组(2}, 注意到它的第一个方程相当于说

$$x = 4x_2, \quad (x_2 \in \mathbb{Z})$$

从而（2）可化为线性方程

$$4x_2 \equiv 1 \pmod{5} \quad (2^*)$$

容易观察到，（2\*）的一个特解为

$$x_2 = -1$$

（注：当然你也可以取  $x_1 = 4$ ，就像上述网页中那样）

因此，根据中国剩余定理，原方程组(0) 的通解为

$$\begin{aligned} x &= r_1 M_1 x_1 + r_2 M_2 x_2 + kM \\ &= 3 \cdot 5 \cdot 1 + 4 \cdot 4 \cdot (-1) + 4 \cdot 5k \\ &= 20k - 1 \quad (k \in \mathbb{Z}) \end{aligned}$$

最经典的一个例子，即金庸曾在《射雕英雄传》原著中引用的“鬼谷算题”：

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？

我们留给有兴趣的读者自行研究，其求解步骤，可以参考从射雕到九章——在天大理学院物理系的通俗报告 ([http://mp.weixin.qq.com/s?\\_\\_biz=MzU4NjAxNzg0MA==&mid=2247484388&idx=1&sn=824d2fb51f18cab9a7a81bae02f3da5e&chksm=fd80febbcaf777adf784c27e82824d581e4a9b37fe31677b3ce461fc61205b6198fbb46672dd&scene=21#wechat\\_redirect](http://mp.weixin.qq.com/s?__biz=MzU4NjAxNzg0MA==&mid=2247484388&idx=1&sn=824d2fb51f18cab9a7a81bae02f3da5e&chksm=fd80febbcaf777adf784c27e82824d581e4a9b37fe31677b3ce461fc61205b6198fbb46672dd&scene=21#wechat_redirect))。

而在94版的射雕电视剧中，这个题目被编剧稍微改了改（参见下述链接最后部分），你能算出来吗，你猜神算子瑛姑能算出来吗？

这个视频被外星人劫走，暂时看不到了~

你可以 [刷新](#) 试试

70013080.18-df1830bf86e0ac72462d9af75f4245dc



延伸阅读：



- [1]华罗庚，从孙子的“神奇妙算”谈起，数学小丛书，北京，科学出版社。
- [2]蔡聪明，谈韩信点兵问题，《科学月刊》第29卷第9期。电子版可见数学知识网页：<http://episte.math.ntu.edu.tw/> (<http://episte.math.ntu.edu.tw/>)
- [3]项武义，從韓信點兵和勾股弦說起——漫談基礎數學的古今中外，《数学传播》，电子版 [http://web.math.sinica.edu.tw/math\\_media/d211/21101.pdf](http://web.math.sinica.edu.tw/math_media/d211/21101.pdf) ([http://web.math.sinica.edu.tw/math\\_media/d211/21101.pdf](http://web.math.sinica.edu.tw/math_media/d211/21101.pdf))（建议在谷歌浏览器打开网页版，并开启翻译功能。近日我们会推出该文的简体版）
- [4]许光午，李宝，大衍求一术的算法意义与分析  
<https://arxiv.org/ftp/arxiv/papers/1610/1610.01175.pdf>  
(<https://arxiv.org/ftp/arxiv/papers/1610/1610.01175.pdf>)

作者： 林开亮，西北农林科技大学理学院讲师

## 热门文章

- 1 俄国的数学普及和英才教育 (/article/article/index/id/436.html)
- 2 数学作为一门合乎需要的语言 (/article/article/index/id/559.html)
- 3 论无穷（2） (/article/article/index/id/573.html)
- 4 数学家欧拉：所有人的老师 (/article/article/index/id/112.html)
- 5 梅森素数为何这样重要 (/article/article/index/id/113.html)

## 最新发布



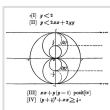
原创数学话剧《素数的故事》 2021版-直播回放视频  
(/article/article/index/id/596.html)



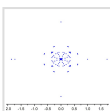
原创数学话剧《费马大定理》 直播回放视频 (/article/article/index/id/595.html)



《开讲啦》 20200222 本期演讲者：张继平 (/article/article/index/id/586.html)



椭圆函数正篇：Gauss与AGM(6-2) (/article/article/index/id/579.html)



椭圆函数正篇：Gauss与AGM(6-1) (/article/article/index/id/577.html)

---

© 2023 南方科技大学杰曼诺夫数学中心

技术支持 - 深圳市优伴教育科技有限公司 粤ICP备15097014 (<http://www.miitbeian.gov.cn>)