AMA1D01C　Lecture Notes Set #04

中國剩餘定理

Chinese Remainder Theorem

By

李向榮博士　梁信謙博士

香港理工大學應用數學系

中國剩餘定理

- 《孫子算經》「物不知數」問題， 又稱「孫子定理」

  （《孫子算經》編纂年代估計約在公元四、五世紀，南北朝時期）
- 明代程大位《算法統宗》：「物不知總」、「韓信點兵」
- 宋代楊輝《續古摘奇算法》：「秦王暗點兵」
- 宋代周密《志雅堂雜鈔》卷下：「鬼谷算」、「隔牆算」
- 剪管術
- 南宋數學家秦九韶《 數書九章》： 大衍求一術 （1247）

- 同餘(congruence)問題，Indeterminate Analysis (i.e. solving the problem of linear congruences)。
- Chinese Remainder Theorem (CRT)

《孫子算經》
(原書卷下第26題)

- 『今有物不知其數,　　Let x be an integer
  三三數之賸二,　　$x \equiv 2 \pmod 3$
  五五數之賸三,　　$x \equiv 3 \pmod 5$
  七七數之賸二,　　$x \equiv 2 \pmod 7$
  問物幾何?』　　Find x.

- 答曰:『二十三』。

Congruence relation

$$x \equiv y \pmod{m}$$

Suppose x and y are integers, and m is a positive integer, the above relation means there exists an integer k such that

$$x = y + km$$

We say: *x is congruent to y modulo m*

E.g. $38 \equiv 2 \pmod{12}$, $-8 \equiv 7 \pmod{5}$,

$2 \equiv -3 \pmod{5}$, $-3 \equiv -8 \pmod{5}$.

Two properties of the congruence relation we will be using later:

If $x \equiv y \pmod{m}$, then

$$xz \equiv yz \pmod{m},$$

where z is a non-zero integer.

If $x \equiv y \pmod{m}$, and z is a multiple of m, then

$$x+z \equiv y \pmod{m}.$$

韓信點兵

先集合部隊但未知士兵的總數

- 要求部下三人一伍排好，看剩下幾人
- 又叫他們五人一伍排好，看剩下幾人
- 再命他們七人一伍排好，看剩下幾人

由此他就知道士兵的總數。

Some work in Europe on CRT around the18th century

- French mathematician Claude Gaspard Bache de Méziriac (1581-1638): connect CRT to the Euclidean algorithm and with Diophantine analysis in1624.
- German mathematician Christlieb von Clausberg (1689-1751) generalised and systematised methods which used the greatest common divisor procedure in 1732.
- Swiss mathematician Leonhard Euler (1707-1783) independently rediscovered similar methods in 1734.
- Joseph Louis Lagrange (1736-1813), Abraham Gotthelf Kästner (1719-1800) and Euler provided a general framework essentially equivalent to Bache's.
- Carl Friedrich Hindenburg (1741-1808): Diophantine problems in 1776,1786
- Carl Friedrich Gauss (1777-1855), published *Disquisitiones Arithmeticae* in 1801

CRT to the West

- Leonardo Pisano (Fibonacci) published his book *Liber Abaci* introducing the CRT to the west in 1202.
- A British Protestant Christian missionary Alexander Wylie (1815-1887), published an article entitled *Jottings on the Science of the Chinese : Arithmetic*中國科學箚記：數學 in a Shanghai English-language newspaper *North China Herald* **北華捷報** in 1852, in which the《孫子算經》「物不知數」problem was translated into English. (*North China Herald was* renamed as *North China Daily News* 字林西報 in 1864) .
- 在1874年，德國科學史家馬蒂生(L. Mathiesen)指出「孫子定理」的解法等同Gauss的定理，卻又遠早於Gauss得出這結果，所以從此在西方的數學史裡將這個定理稱為中國的剩餘定理Chinese Remainder Theorem.

《孫子算經》的解法

- 術曰：三三數之剩二，置一百四十；五五數之剩三，置六十三；七七之數剩二，置三十。并之得二百三十三。以二百一十減之，即得。凡三三數之剩一，則置七十；五五數之剩一，則置二十一；七七數之剩一，則置十五。一百六以上，以一百五減之，即得。

今有物不知其數三三數之賸二五五數之賸二七七數之賸二問物幾何

答曰二十三

術曰三三數之賸二置一百四十五五數之賸三置六十三七七數之賸二置三十并之得二百三十三以二百一十減之即得凡三三數之賸一則置七十五五數之賸一則置二十一七七數之賸一則置十五一百六以上以一百五減之即得

今有歌六首四足禽四首二足亦有七十六首

$$x \equiv R_1 \pmod 3 \equiv R_2 \pmod 5 \equiv R_3 \pmod 7$$

找5×7的一個倍數可被3除餘1，得70。

找3×7的一個倍數可被5除餘1，得21。

找3×5的一個倍數可被7除餘1，得15。

3、5、7的最小公倍數為105。

$$x = R_1 \times 70 + R_2 \times 21 + R_3 \times 15 - 105 \times k$$

選一個合適的k令 $0 < x \leq 105$

$$R_1 = 2，\ R_2 = 3\ ，R_3 = 2$$

$$x = 2\times70 + 3\times21 + 2\times15 - 105\times k$$

$$=140 + 63 + 30 - 105\times k$$

$$=233 - 105\times k$$

選一個合適的 k 令 $0 < x \leq 105$，得k=2。

所以，x =233 − 105 ×2 = 23。

- 此數23是最小的正整數解。

- 為了突顯 70、21、15、105 這些數目，明朝的程大位在《算法統宗》（1592年）中，把它們及解答編成歌訣：

三人同行七十稀，五樹梅花廿一枝，
七子團圓正半月，除百零五便得知。

- 在宋代已有人編成這樣的四句詩：

三歲孩兒七十稀，五留廿一事尤奇，
七度上元重相會，寒食清明便可知。

「上元」是指正月十五日，即元宵節，暗指「15」；而「寒食」是節令名，從冬至到清明，間隔105日，這段期間叫做「寒食」，故「寒食」暗指「105」。

Why does it work?

Given that

$$x \equiv R_1 \pmod{m_1}$$
$$x \equiv R_2 \pmod{m_2}$$
$$x \equiv R_3 \pmod{m_3}$$

assuming m_1 , m_2 , m_3 are pairwise co-prime.

(sometimes the problem can be solved even if this pairwise co-prime condition is not satisfied).

Find positive integers α_1 ,α_2 ,α_3 so that

$$m_2 m_3 \alpha_1 \equiv 1 \pmod{m_1}$$
$$m_1 m_3 \alpha_2 \equiv 1 \pmod{m_2}$$
$$m_1 m_2 \alpha_3 \equiv 1 \pmod{m_3}$$

If such α_1 ,α_2 ,α_3 exist, then, we have

$$m_2 m_3 \alpha_1 R_1 \equiv R_1 \pmod{m_1}$$
$$m_1 m_3 \alpha_2 R_2 \equiv R_2 \pmod{m_2}$$
$$m_1 m_2 \alpha_3 R_3 \equiv R_3 \pmod{m_3}$$

Therefore, we have

$$m_2 m_3 \alpha_1 R_1 + m_1 m_3 \alpha_2 R_2 + m_1 m_2 \alpha_3 R_3 \equiv R_1 \pmod{m_1}$$
$$m_2 m_3 \alpha_1 R_1 + m_1 m_3 \alpha_2 R_2 + m_1 m_2 \alpha_3 R_3 \equiv R_2 \pmod{m_2}$$
$$m_2 m_3 \alpha_1 R_1 + m_1 m_3 \alpha_2 R_2 + m_1 m_2 \alpha_3 R_3 \equiv R_3 \pmod{m_3}$$

That is to say,

$$x = m_2 m_3 \alpha_1 R_1 + m_1 m_3 \alpha_2 R_2 + m_1 m_2 \alpha_3 R_3 \pmod{M}$$

where M is the LCM of $\{m_1, m_2, m_3\}$,

or $M = m_1 m_2 m_3$ if m_1, m_2 and m_3 are co-primes.

Back to the 「物不知數」 problem:

$x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 2 \pmod 7$

Find integers $\alpha_1, \alpha_2, \alpha_3$ so that

$5 \times 7 \times \alpha_1 \equiv 1 \pmod 3$, thus, $\alpha_1 = 2$.

$3 \times 7 \times \alpha_2 \equiv 1 \pmod 5$, thus, $\alpha_2 = 1$.

$3 \times 5 \times \alpha_3 \equiv 1 \pmod 7$, thus, $\alpha_3 = 1$.

$\alpha_1=2, \quad m_2 m_3 \alpha_1 R_1 = 5\times7\times2\times2 = 140.$

$\alpha_2=1, \quad m_1 m_3 \alpha_2 R_2 = 3\times7\times1\times3 = 63.$

$\alpha_3=1, \quad m_1 m_2 \alpha_3 R_3 = 3\times5\times1\times2 = 30.$

$$x = 140 + 63 + 30 \pmod{105}$$

$$= 233 \pmod{105}$$

$$= 233 - 2\times105 = 23.$$

Chinese Remainder Theorem

Consider the k simultaneous linear congruences

$$x \equiv R_i \pmod{m_i} \quad \text{for} \quad i=1,2,\ldots,k.$$

assuming $m_1, m_2, \ldots, m_k$ are pairwise co-prime.

Let

$$M = m_1 m_2 \ldots m_k, \text{ and}$$

$$M_i = M / m_i \quad \text{for} \quad i=1,2,\ldots,k.$$

Find positive integers $\alpha_1, \alpha_2, \ldots, \alpha_k$ so that

$$M_i \alpha_i \equiv 1 \pmod{m_i} \quad \text{for} \quad i=1,2,\ldots,k.$$

Then,

$$x = \sum_{i=1}^{k} M_i \alpha_i R_i \pmod{M}$$

大衍求一術

南宋數學家秦九韶把解決一次同餘問題的方法推廣，並稱之為「大衍求一術」，記載在他的著作《數書九章》之中。

求整數 α使其滿足$\alpha G \equiv 1 \pmod{m}$,

其中m、G是互質自然數,

m 稱為「定母」,G 稱為「衍數」,

α稱為「乘率」。

數書九章卷第一　大衍類

魯郡　秦九韶

蓍卦發微

問易曰大衍之數五十其用四十有九又曰分而爲二以象兩掛一以象三揲之以四以象四時三變而成爻十有八變而成卦欲知所衍之術及其數各幾何

荅曰衍母一十二　衍法三

一元衍數二十四　二元衍數一十二

三元衍數八　四元衍數六

已上四位衍數計五十

一揲用數一十二　二揲用數二十四

若$m < G$，則先以m 除G, 得餘數G_1（奇數），
然後求整數α使其滿足

$$\alpha G_1 \equiv 1 \pmod{m}。$$

There exists k such that $G = mk + G_1$.

Thus,$\alpha G = \alpha mk + \alpha G_1 \equiv 1 \pmod{m}$

Therefore, $\alpha G_1 \equiv 1 \pmod{m}$.

《數書九章》求乘率α的步驟為:

『置奇右上，定居右下，立天元一於左上。先以右上除右下，所得商數與左上一相生， 入左下，然後乃以右行上下以少除多，遞互除之，所得商數隨即遞互累乘，歸左行上下，須使右上末後奇一而止。乃驗左上所得以為乘率，或奇數已見單一者便為乘率。』

試以 $20\alpha \equiv 1 \pmod{27}$ 為例：

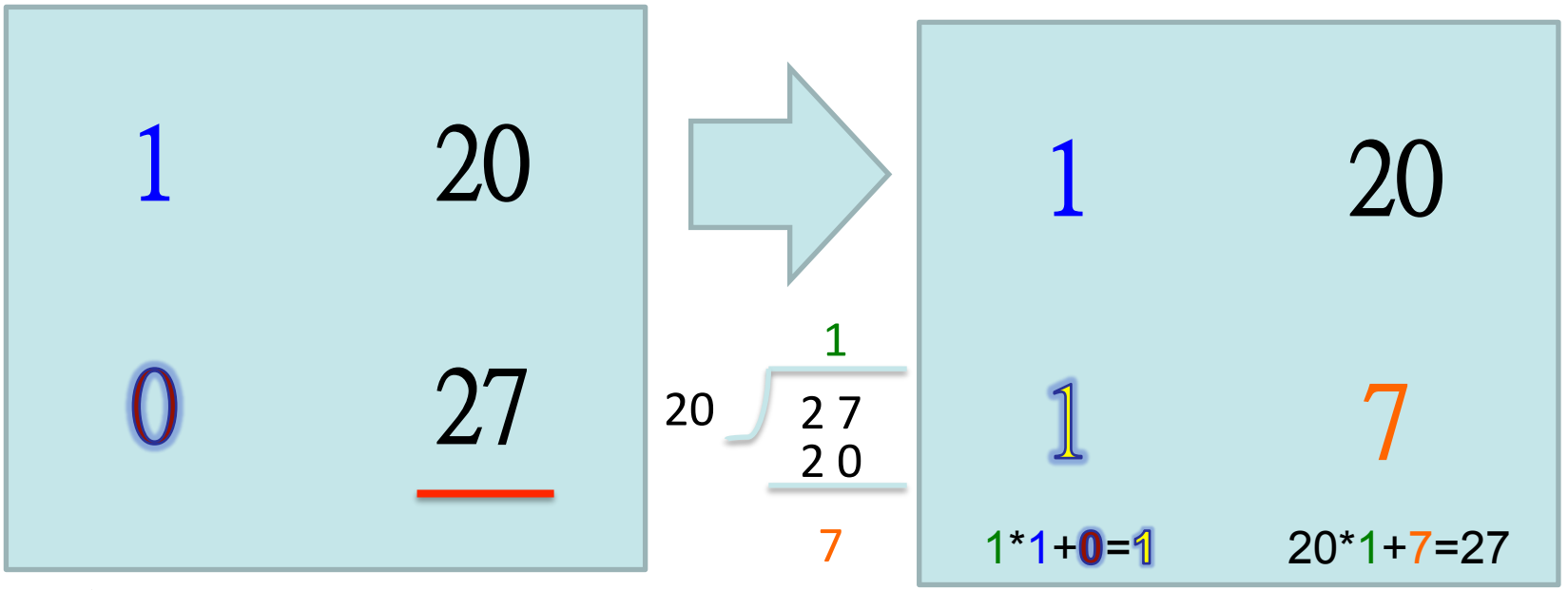
奇數(衍數)= 20

定母=27

置奇右上，定居右下，立天元一於左上。

1	20
0	27

先以右上除右下，所得商數與左上一相生，
入左下

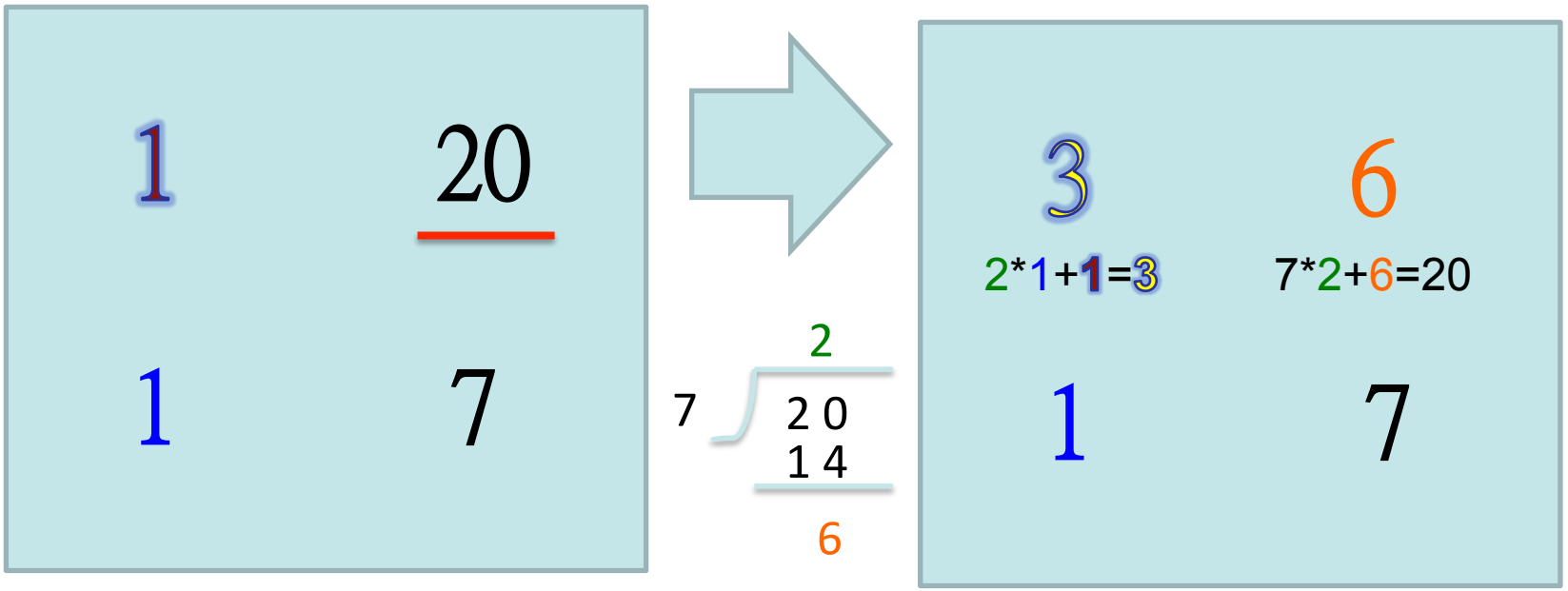


20除27：27=1×20+7

所得商數=1

與左上一相生:1×1=1，入左下:1+0=1

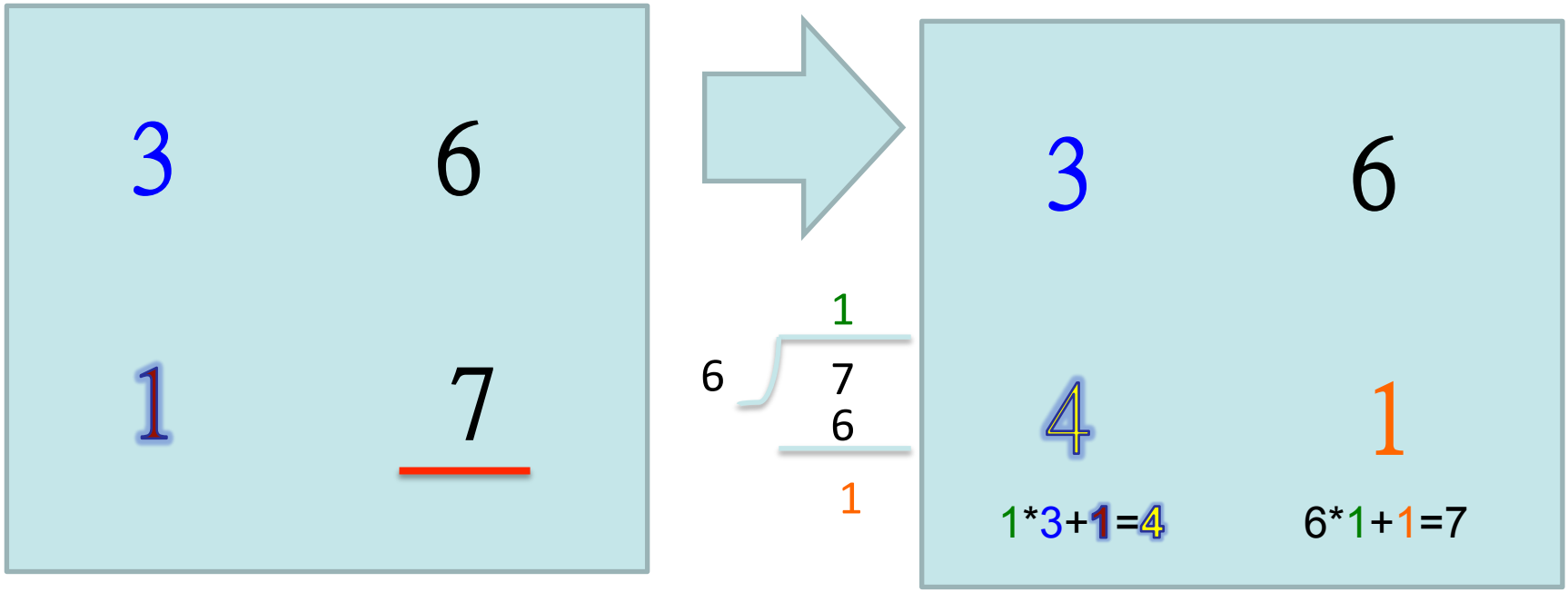
然後乃以右行上下以少除多，遞互除之，所得商數隨即遞互累乘，歸左行上下，須使右上末後奇一而止。



7除20：20=2×7+6

所得商數=2

與左下一相生:2×1=2，入左上:2+1=3

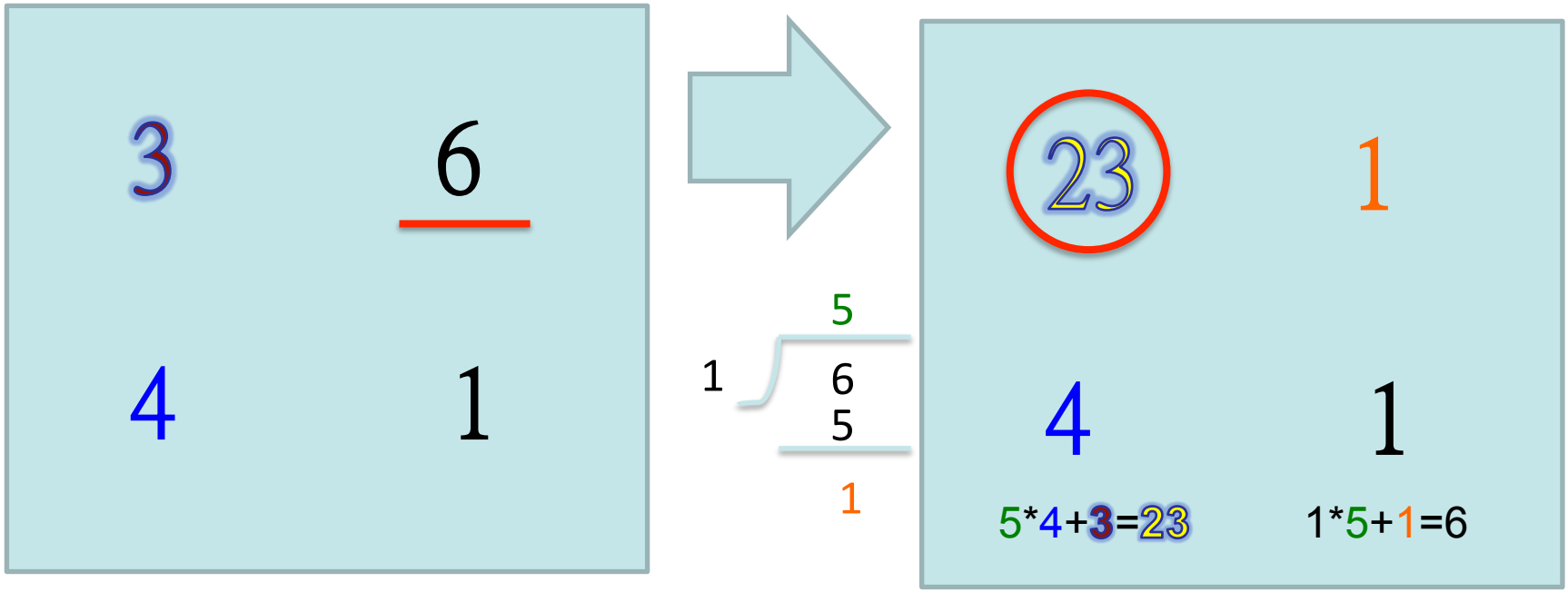


6除7：7=1×6+1

所得商數=1

與左上一相生:1×3=3，入左下:3+1=4

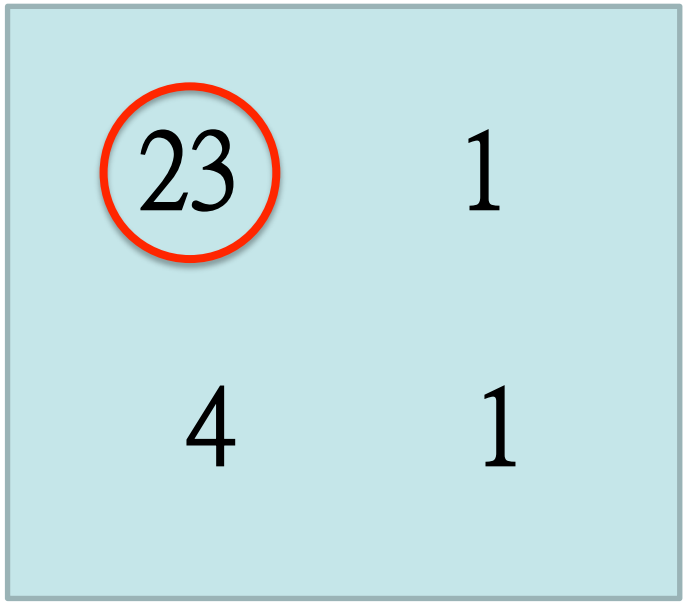
須使右上末後奇一而止



1除6：6=5×1+1　(Note: we need a remainder 1)

所得商數=5

與左下一相生:5×4=20，入左上:20+3=23



以上例子，20α ≡ 1 (mod 27)，得出乘率α =23。

Check: $20\times23=460=27\times17+1$。

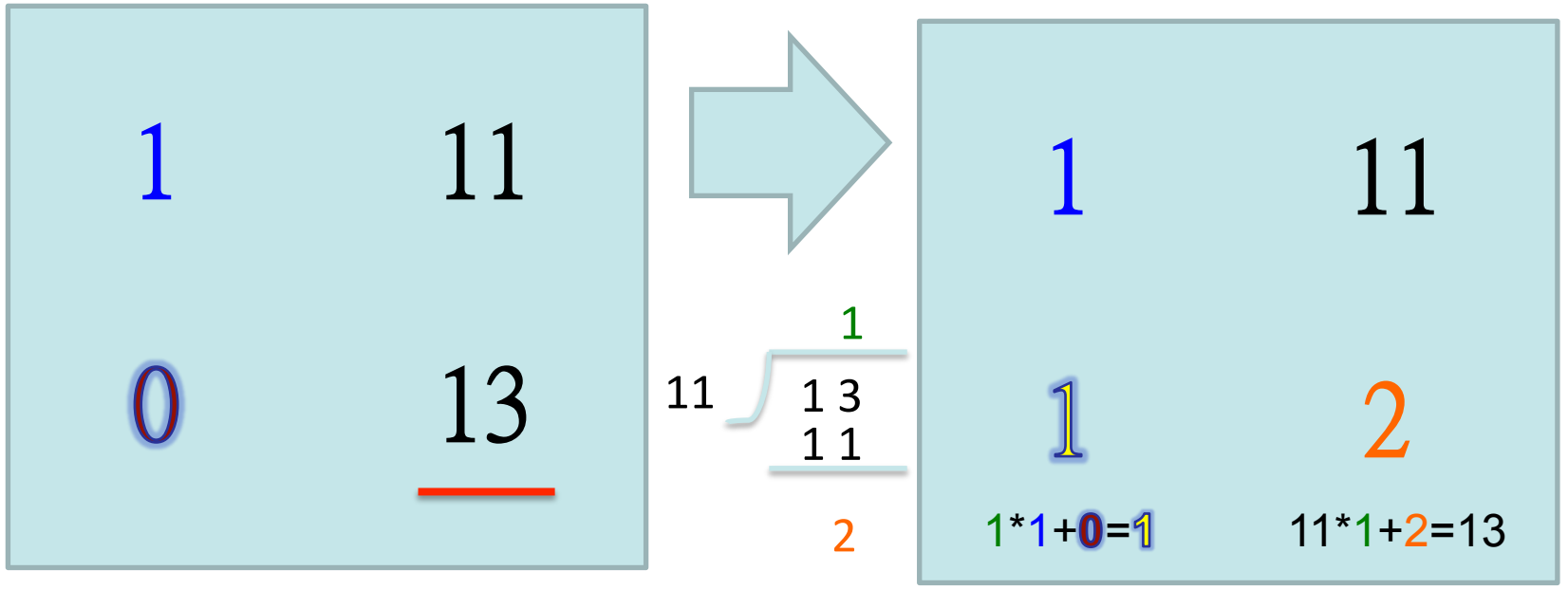
又以 $1155\alpha \equiv 1 \pmod{13}$ 為例：

13＜1155，13除1155得餘數11

奇數= 11

定母=13

1	11
0	13

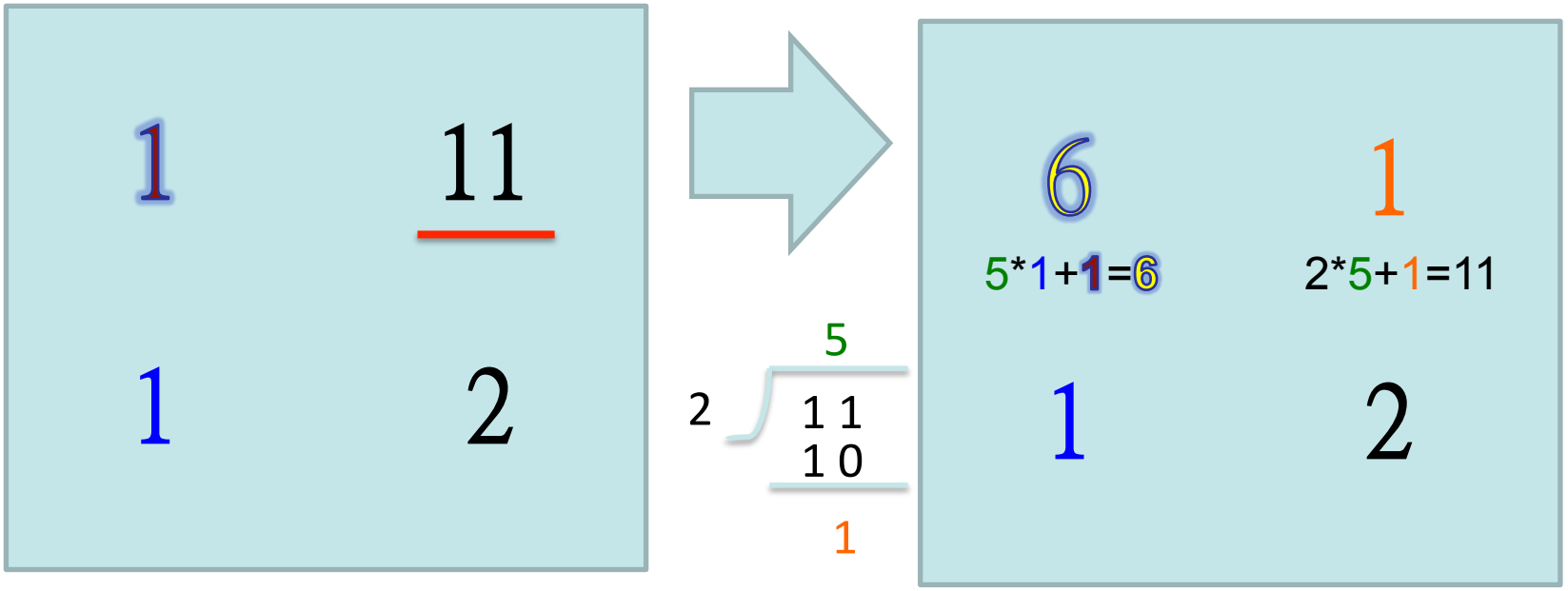


11除13：13=1×11+2

所得商數=1

與左上一相生:1×1=1，入左下:1+0=1

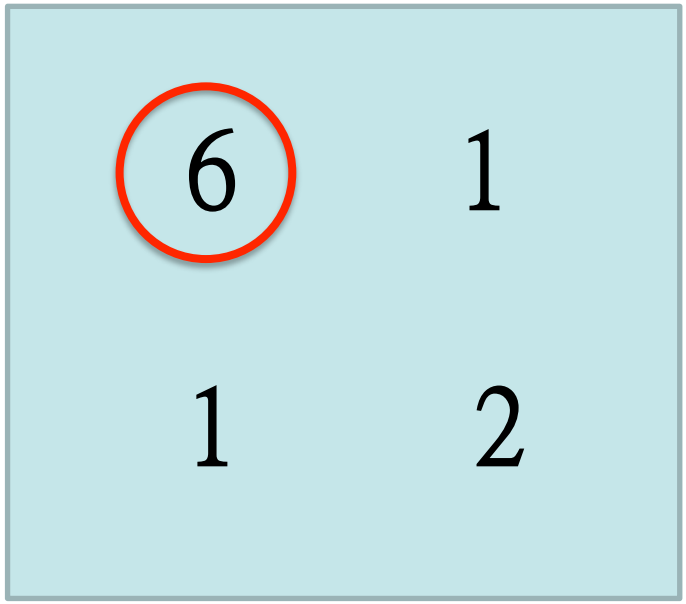
須使右上末後奇一而止



2除11：11=5×2+1

所得商數=5

與左下一相生:5×1=5，入左上:5+1=6



須使右上末後奇一而止

以上例子，1155α ≡ 1 (mod 13)，得出乘率α =6。

Check: $1155\times6=6930=533\times13+1$。

四川安岳圓覺洞塑像

- 對於秦九韶究竟是何等樣人，除了“偉大的數學家”之外，通常就諱莫如深了。用現代的眼光看，秦九韶可能是中國歷史上少見的奇人之一。關於秦九韶究竟是何等樣人，其實宋人文獻中留下了相當豐富的記載，主要可見於周密（人名）的《癸辛雜識續集》卷下和著名詞人劉克莊文集中的“繳秦九韶知臨江軍奏狀”。秦九韶18歲就統帥私人武裝，為人“豪宕不羈”，如果將他和意大利文藝復興時期的那些風雲人物相比，竟有幾分相似：他多才多藝，懂得星占、數學、音樂、建築，還擅長詩文，會騎術、劍術、踢球等等。同時又利欲熏心，驕奢淫逸，熱衷於做官，一心往上爬。秦九韶做過幾任地方官，最後死在梅州任上。他最高做到大約相當於今天局級的官職。秦九韶行為乖戾，出人意表，被他的同時代人認為是“不孝、不義、不仁、不廉”，平日橫行鄉里，惡霸一方，所以多次被褫去官職或取消任命。例如，在他擔任地方長官的父親宴客時，他帶著妓女出席。又如，他竟能將他上司的田產“以術攫取之”，在其中建造他的超豪華莊園（他親自設計那些奇特的房屋）。再如，他命令手下殺死自己的兒子，而且親自設計了毒死、用劍自裁、溺死三種方案；當得知這名手下偷偷放了他兒子時，他竟巨額懸賞，滿世界追殺兒子和這名手下。有一年夏天，秦九韶和一個他所寵愛的姬妾月夜在庭院中交歡，不意被一個汲水的僕役撞見，他認為那僕役有意窺探他的隱私，就誣告該僕役偷盜，將其送官，要求判僕役黥面流放。地方官認為該僕役罪不至此，沒有按照秦九韶的要求判決，秦九韶為此懷恨地方官，竟企圖將他毒死。當時的記載說秦九韶“多蓄毒藥，如所不喜者，必遭其毒手”。這就是被劉克莊稱為“暴如虎狼，毒如蛇蠍，非複人類”的秦九韶。毫無疑問，他是一個瘋狂的惡棍，但與此同時，他確實也是一個天才的數學家。我們甚至可以推想，如果他有時間或精力寫下音樂或建築方面的著作，也可能又有某項歷史性的貢獻。可惜他的絕大部分時間和精力，看來都耗費在放縱物慾上了。

- 《數書九章》 最初叫《數術大略》或《數學大略》(9卷)，分為9類，每類為一卷。約到元代時更名為《數學九章》，內容也由9卷改為18卷。明初抄本被收入《永樂大典》(1408)，另抄本藏於文淵閣。明代學者王應遴傳抄時定名為《數書九章》，明末學者趙琦美再抄時沿用此名。抄本形式流傳到清代，1781年由李鋭校訂後收入《四庫全書》。 1842年由宋景昌校訂後收入《宜稼堂叢書》 第一次印刷出版，結束了近600年的傳抄歷史。 1898年收入《古今算學叢書》，為第二次印刷。 1936年又分別被收入《叢書集成初編》 和《國學基本叢書》 出版，流傳甚廣。