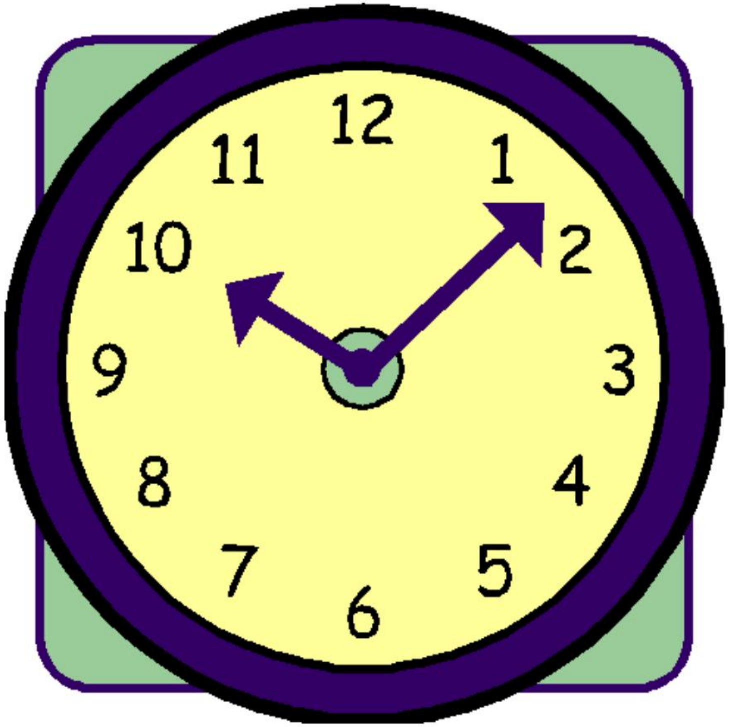
模块化算术，中国剩余定理



计划

在这篇笔记中,我们将学习一些更基本的数论。

这些数论基础是计算机科学中非常强大的工具。

- 模运算
  - 模加法,乘法
  - 应用
  - 乘法逆
  - 费马小定理,威尔逊定理
- 中国剩余定理

12 小时制

但这也可能是早上 6 点,我们应该吃早餐。

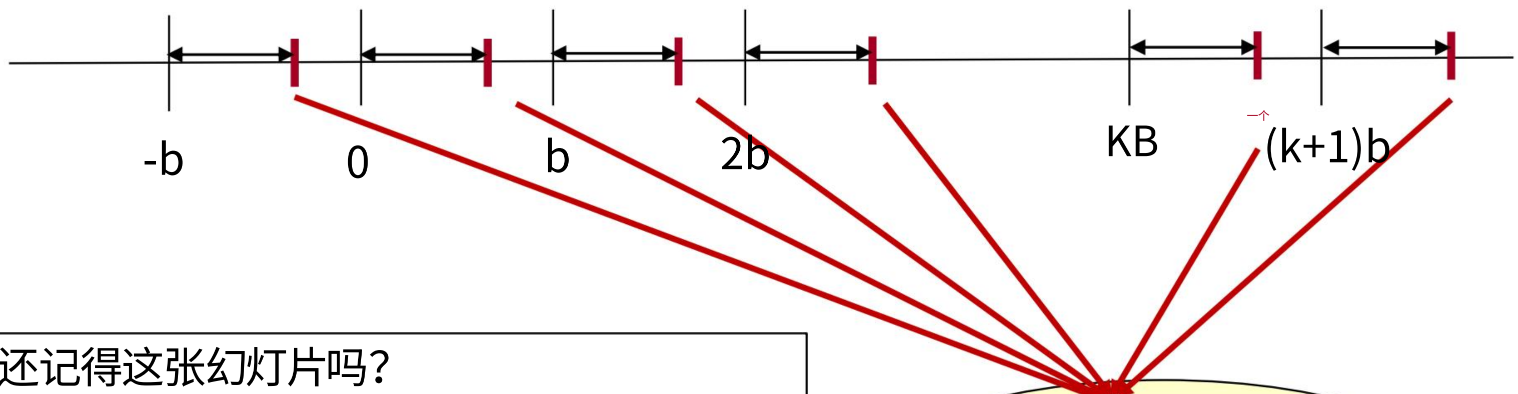
在这种情况下,我们实际上将两个 6 点钟视为一个时钟中的值。

这就是模运算的思想!

整数的划分

给定任何 b>0,我们可以将整数划分为 b 个数字的块。

对于任何 a,这个数字都有一个唯一的“位置”。



还记得这张幻灯片吗?

将位于每个 b 块的相同“位置”的整数分组形成整数分区。

a 模 b 的同余类:

[a]b = {a+kb | k∈ }

例如 = [0]3 U [1]3 U [2]3。

表示为 3 = {[0]3 , [1]3 , [2]3 }

模数运算

定义$a \equiv b \pmod{n}$当且仅当$n | (a - b)$。

例如

$12 \equiv 2 \pmod{10}$

$107 \equiv 207 \pmod{10}$

$7 \equiv 1$（模 2）

$1 \equiv -1$（模 2）

$13 \equiv -1 \pmod{7}$

$-15 \equiv 0 \pmod{5}$

模块化加法

引理。如果$a \equiv c \pmod{n}$,并且$b \equiv d \pmod{n}$那么

$$a+b \equiv c+d \pmod{n}。$$

示例 1

$12 \equiv 2 \pmod{10}$, $25 \equiv 5 \pmod{10}$

$\Rightarrow 12 + 25 \pmod{10}$

$\equiv 2 + 5 \pmod{10} \equiv 7 \pmod{10}$

示例 2

$87 \equiv 2 \pmod{17}$, $222 \equiv 1 \pmod{17}$

$\Rightarrow 87 + 222 \pmod{17}$

$\equiv 2 + 1 \pmod{17}$

$\equiv 3 \pmod{17}$

示例 3

$101 \equiv 2 \pmod{11}$, $141 \equiv -2 \pmod{11}$

$\Rightarrow 101 + 141 \pmod{11} \equiv 0 \pmod{11}$

模块化加法

引理:如果a ≡ c (mod n),并且b ≡ d (mod n)那么

a+b ≡ c+d (mod n)。

证明

a ≡ c (mod n) => a = c + nx 对于某个整数 x

b ≡ d (mod n) => b = d + ny 对于某个整数 y

要显示 a+b ≡ c+d (mod n),它等价于显示 n | (a+bcd)。

考虑 a+bcd。

a+bcd = (c+nx) + (d+ny) – c –d = nx + ny。

很明显,n | nx + ny。

因此,n | a+bcd。

我们得出结论 a+b ≡ c+d (mod n)。

模乘法

引理。如果$a \equiv c \pmod{n}$,并且$b \equiv d \pmod{n}$那么

$$ab \equiv cd \pmod{n}。$$

示例 1

$9876 \equiv 6 \pmod{10}$, $17642 \equiv 2 \pmod{10}$

$\Rightarrow 9876 * 17642 \pmod{10}$

$\equiv 6 * 2$ (模式 10)

$\equiv 2 \pmod{10}$

示例 2

$10987 \equiv 1$（模 2）、$28663 \equiv 1$（模 2）

$\Rightarrow 10987 * 28663 \pmod{2} \equiv 1 \pmod{2}$

示例 3

$999 \equiv 5 \pmod{7}$, $674 \equiv 2 \pmod{7}$

$\Rightarrow 999 * 674 \pmod{7} \equiv 5 * 2 \pmod{7} \equiv 3 \pmod{7}$

模乘法

引理:如果$a \equiv c \pmod{n}$,并且$b \equiv d \pmod{n}$那么

$ab \equiv cd \pmod{n}$。

证明

$a \equiv c \pmod{n} \Rightarrow a = c + nx$ 对于某个整数 x

$b \equiv d \pmod{n} \Rightarrow b = d + ny$ 对于某个整数 y

显示 $ab \equiv cd \pmod{n}$,相当于显示 n | （A B C D）。

考虑 ab-cd。

$ab-cd = (c+nx)(d+ny) – cd =$

$cd + dnx + cny + n2xy – cd = n(dx + cy + nxy)$。

很明显,n | n(dx + cy + nxy)。因此,n | A B C D。

我们得出结论 $ab \equiv cd \pmod{n}$。

锻炼

1444 （型号 713）

= 144 * 144 * 144 * 144（型号 713）

= 20736 * 144 * 144（型号 713）

= 59 * 144 * 144（型号 713）

= 8496 * 144（型号 713）

= 653 * 144（型号 713）

= 94032 (mod 713)

= 629 (mod 713)

20736 * 20736（型号 713）

= 59 * 59（型号 713）

= 3481 (mod 713)

= 629 (mod 713)

巧妙地使用模运算将显着降低复杂性！

计划

- 模运算
  - 模加法,乘法
  - 应用
  - 乘法逆
  - 费马小定理,威尔逊定理
- 中国剩余定理

应用

一个数能被 9 整除当且仅当它的数字之和能被 9 整除?

示例 1. 9333234513171 可以被 9 整除。

9+3+3+3+2+3+4+5+1+3+1+7+1 = 45能被9整除。

示例 2. 128573649683 不能被 9 整除。

1+2+8+5+7+3+6+4+9+6+8+3 = 62不能被9整除。

巧合?

不

这可以很容易地使用模运算来证明。

应用

宣称。一个数能被 9 整除当且仅当它的数字之和能被 9 整除。

提示:$10 \equiv 1 \pmod 9$。

设 n 的十进制表示为dkdk-1dk-2⋯d1d0。

这意味着 n = dk 10k + dk-1 10k-1 + ⋯ + d1 10 + d0

注意di 10i mod 9 ≡ (di

mod 9) (10i mod 9) mod 9 ≡ (di

mod 9) $\underbrace{(10 \bmod 9)\ (10 \bmod 9) \cdots (10 \bmod 9)}_{\text{我条款}}$ mod 9

≡ (di mod 9) (1 mod 9) (1 mod 9) ⋯ (1 mod 9) mod 9 ≡ di

mod 9

应用

宣称。一个数能被 9 整除当且仅当它的数字之和能被 9 整除。

提示:10 ≡ 1 (mod 9)。

设 n 的十进制表示为dkdk-1dk-2···d1d0。

这意味着 n = dk 10k + dk-1 10k-1 + ··· + d1 10 + d0

注意di 10i mod 9 ≡ di mod 9。

因此 n mod 9 ≡ (dk 10k + dk-1 10k-1 + ··· + d1 10 + d0) mod 9

≡ (dk 10k mod 9 + dk-1 10k-1 mod 9 ··· + d1 10 mod 9 + d0 mod 9) mod 9

+ ≡ (dk mod 9 + dk-1 mod 9 + ≡ + (dk1模式 9 + d0模式 9) 模式 9

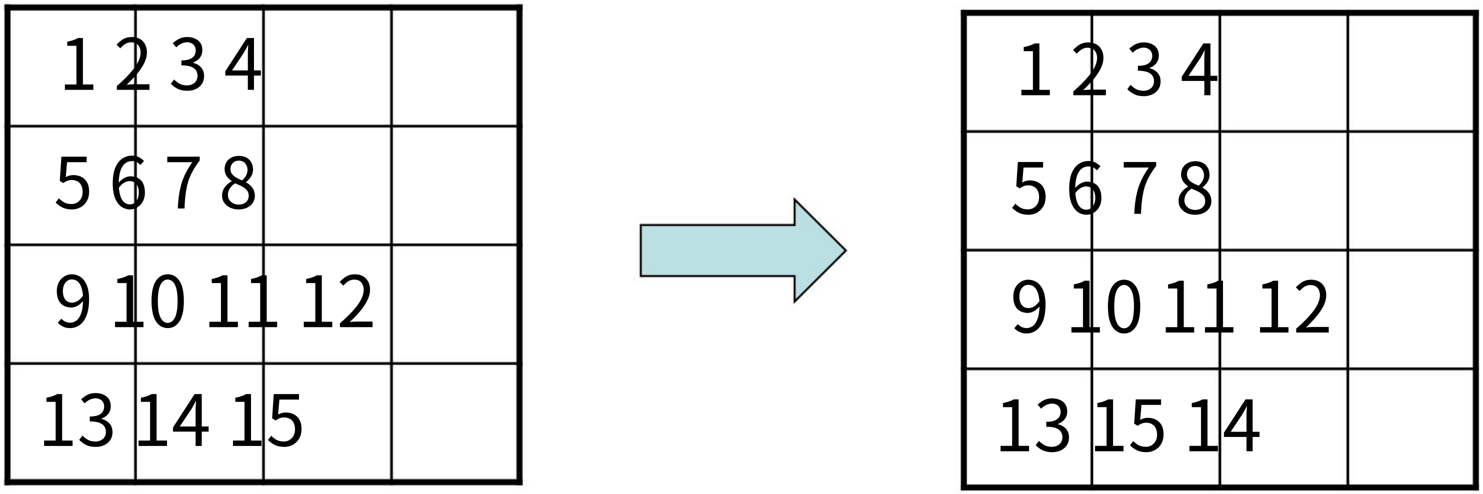
+ dk-1 + ··· + d1 + d0) 模 9

十五拼图

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

规则 :可以将一个编号的方格移动到相邻的空方格。

十五拼图



初始配置

目标配置

是否有一系列移动可以让您将初始配置更改为目标配置？

不变法

1.寻找在整个过程中都满足的性质（不变量） 。

2.表明目标不满足性质。

3.得出目标无法实现的结论。

这游戏的不变量是什么？？

这通常是证明中最难的部分。

暗示

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

初始配置

$((1,2,3,\cdots,14,15),(4,4))$

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

目标配置

$((1,2,3,\cdots,15,14),(4,4))$

提示 :这两个状态具有不同的奇偶性。

平价

给定一个序列,如果第一个元素较大,则一对是“无序的” 。

更正式地说,给定一个序列 $(a1, a2, \cdots, an)$,如果 $i<j$ 但 $ai > aj$,则一对 (i,j) 是无序的。

例如,序列 (1,2,4,5,3) 有两个无序对,(4,3) 和 (5,3)。

给定状态 $S = ((a1, a2, \ldots, a15),(i,j))$

S 的奇偶性 = (无序对数 + i) mod 2

空方格的行号

暗示

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

初始配置

$((1,2,3,\cdots,14,15),(4,4))$

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

目标配置

$((1,2,3,\cdots,15,14),(4,4))$

S 的奇偶性 = (无序对数 + i) mod 2

显然,这两个州有不同的平价。

不变法

奇偶性是偶数

1.寻找在整个过程中都满足的性质（不变量） 。

2.表明目标不满足性质。

3.得出目标无法实现的结论。

奇偶校验

不变量= 状态奇偶性

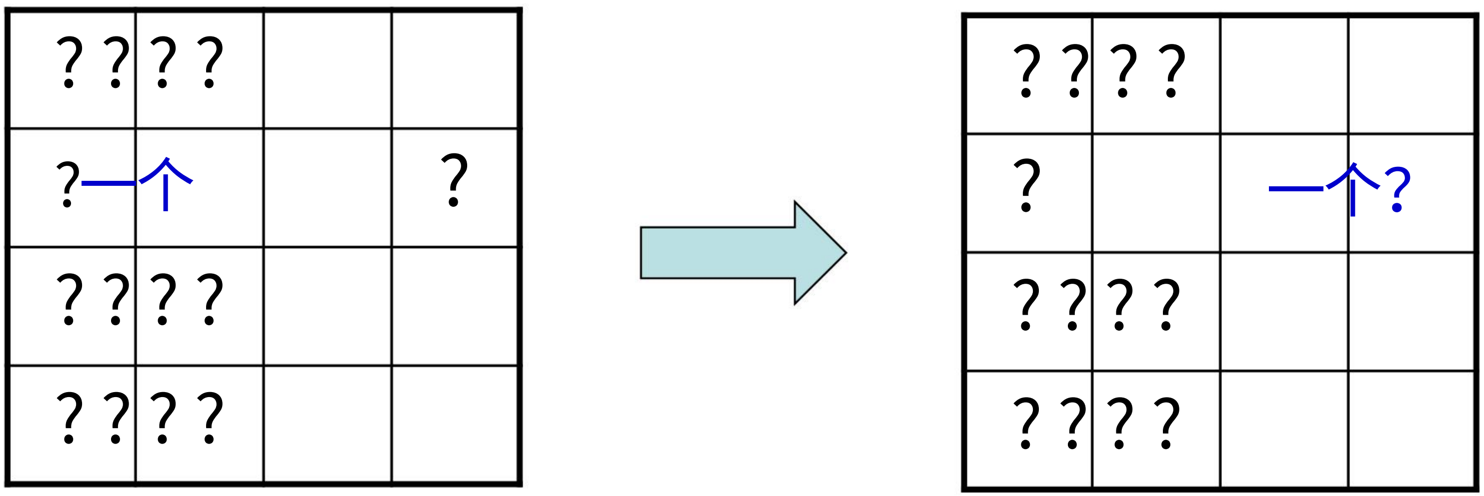
宣称。任何举动都将保持国家平等。

证明索赔将完成不可行性证明。

证明不变量

S 的奇偶性 = (无序对数 + i) mod 2

宣称。任何举动都将保持国家平等。

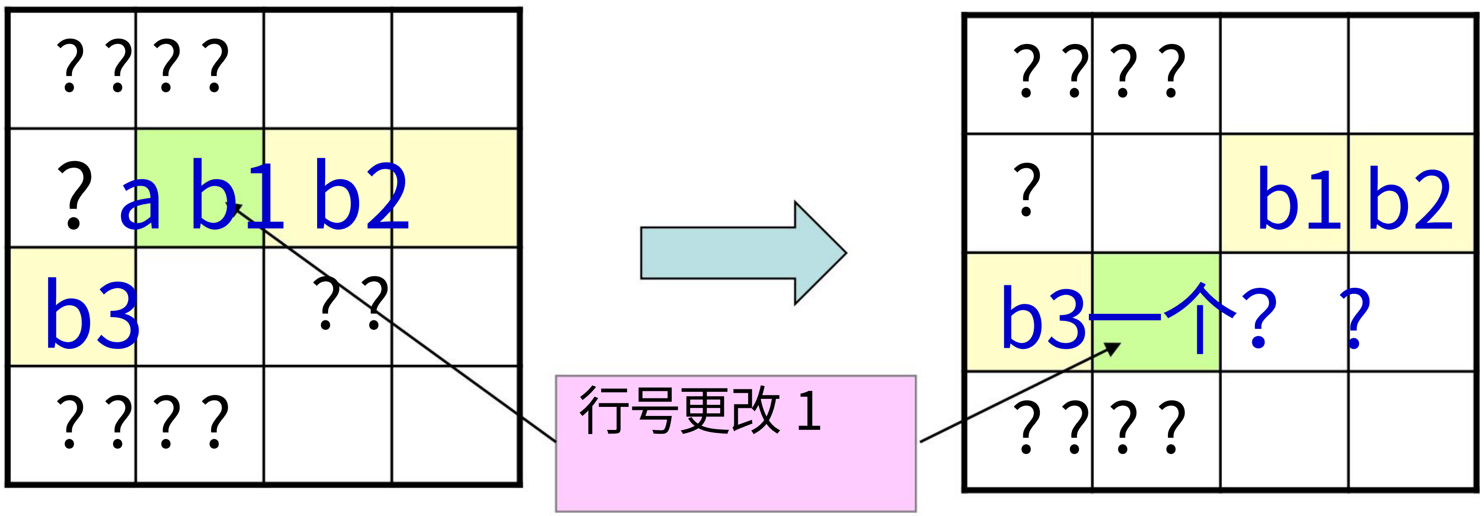


水平移动不会改变任何东西……

证明不变量

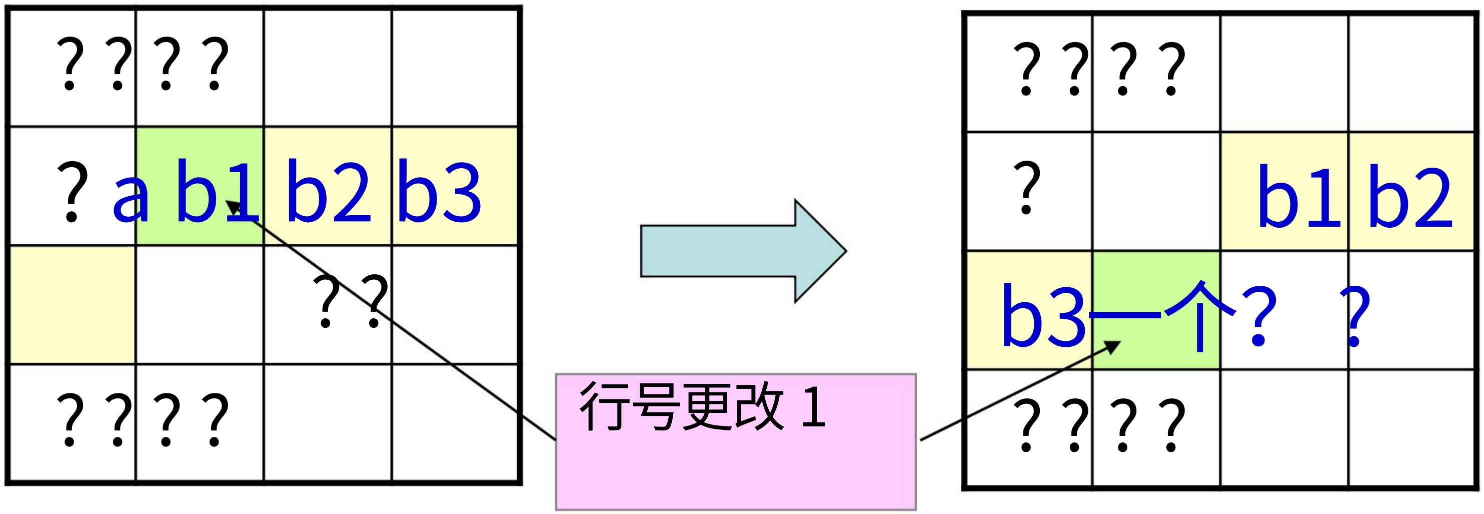
S 的奇偶性 = (无序对数 + i) mod 2

宣称。任何举动都将保持国家平等。



要计算#disorder 对的变化,我们需要讨论 4 种情况,这取决于a在 {a,b1 ,b2 ,b3 } 中的相对顺序。

证明不变量



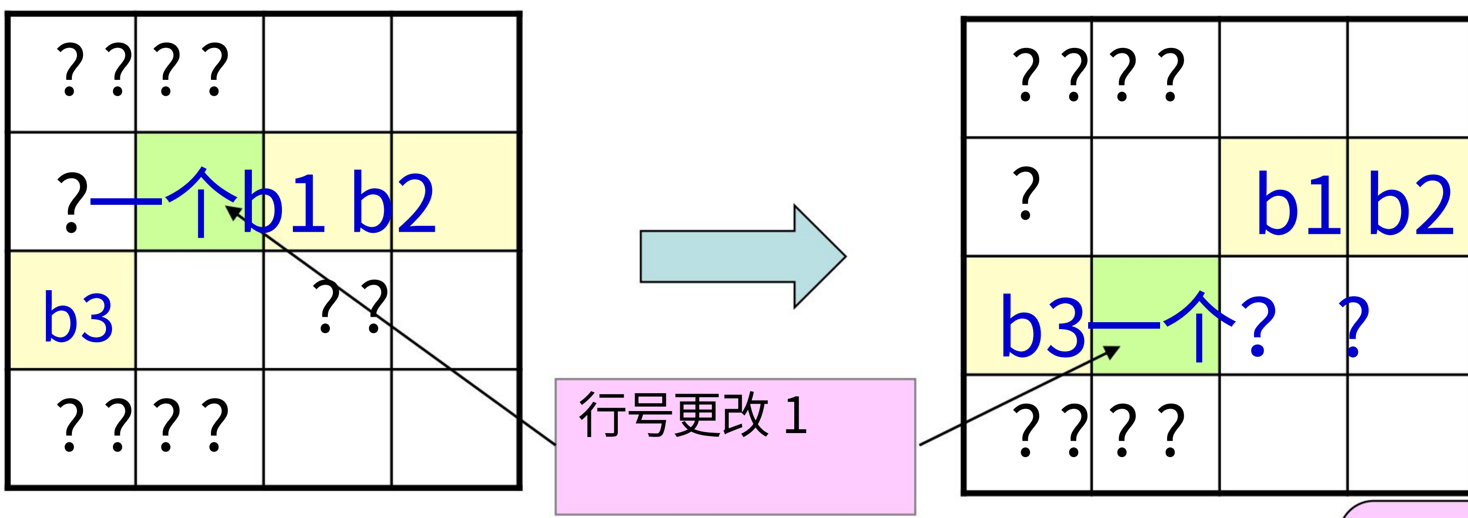
①如果a最大,那么#disorder对将减少3。 ②如果a是第二大的,那么#disorder对将减少1。 ③如果a是第二小的,那么#disorder 对将增加 1。 ④如果a最小,那么#disorder 对将增加 3。

总之， #disorder 对的变化是 1 或 3。

证明不变量

S 的奇偶性 = (无序对数 + i) mod 2

宣称。任何举动都将保持国家平等。



如果当前状态有 3/2/1/0 个无序对,则下一个状态将有 0/1/2/3 个无序对。

区别

是 1 或 3。

所以平价保持不变 !我们已经证明了这一说法。

十五拼图

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

初始配置

1	2	3	4
5	6	7	8
9	10	11	12
13	15	14	

目标配置

是否有一系列移动可以让您将初始配置更改为目标配置?

十五拼图

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

初始配置

15	14	13	12
11	10	9	8
7	6	5	4
3	2	1	

目标配置

#无序对 = 0

空方排 = 4

奇偶性是偶数。

不可能的！

#无序对 = 14 +
13 + 12 + + 1 = …
(14+1) 14/2 = 105

空方排 = 4

奇偶校验是奇数。

十五拼图

如果两种配置具有相同的奇偶性,我们是否总是可以从一种配置转移到另一种配置?

是的!

解决方案然而需要相当复杂的数学。

计划

- 模运算
  - 模加法,乘法
  - 应用
  - 乘法逆
  - 费马小定理,威尔逊定理
- 中国剩余定理

乘法逆

$a \not\equiv 0 \pmod{n}$的乘法逆元是另一个整数 a 使得：

$$a \quad a \equiv 1 \pmod{n}$$

在模算术中，一个特殊的性质是整数存在乘法逆元。

例如，

2 * 5 = 1（模 3），

所以 5 是 2 模 3 的乘法逆（反之亦然）。

每个整数在模算术中都有乘法逆吗？

乘法逆

每个整数在模算术中都有乘法逆吗?

Z_5	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

→

a	1	2	3	4
a'	1	3	2	4

Z_6	1	2	3	4	5
1	1	2	3	4	5
2	2	4	0	2	4
3	3	0	3	0	3
4	4	2	0	4	2
5	5	4	3	2	1

→

a	1	2	3	4	5
a'	1	X	X	X	5

X denotes
no inverse

乘法逆

Z_5:

a	1	2	3	4
a'	1	3	2	4

Z_6:

a	1	2	3	4	5
a'	1	X	X	X	5

Z_7:

a	1	2	3	4	5	6
a'	1	4	5	2	3	6

Z_8:

a	1	2	3	4	5	6	7
a'	1	X	3	X	5	X	7

Z_9:

a	1	2	3	4	5	6	7	8
a'	1	5	X	7	2	X	4	8

模式是什么？

乘法逆

为什么 2 在模 6 下没有乘法逆元?

假设它有一个乘法逆 y。 $2y \equiv 1 \pmod 6$

=> $2y = 1 + 6x$ 对于某个整数 x => $2y$

$- 6x = 1$

这是一个矛盾,因为 LHS 是偶数,而 RHS 是奇数。

宣称。如果整数 k,n 不是互质数（即 $\gcd(k,n) \geqslant 2$）,则 k 不具有乘法逆模 n。

证明。和上面一样。作为练习离开。

乘法逆

如果 gcd(k,n)=1 会怎样?

k 在模 n 下总是有一个乘法逆吗?

定理。如果gcd(k,n)=1 ,则有k 使得

$$k \cdot k \quad \equiv 1 \pmod{n},$$

其中k 是k (mod n)的倒数。

gcd(k,n)=spc(k,n)

证明:由于 gcd(k,n)=1 ,存在 s 和 t 使得sk + tn = 1。

所以tn = 1 - sk

这意味着n | 1 - SK。

这意味着1 – sk ≡ 0 (mod n)。

这意味着1 ≡ sk (mod n)。

所以k = s是k (mod n) 的乘法逆。

消除

请注意，$\equiv \pmod{n}$的行为类似于=。

如果$a \equiv b \pmod{n}$，则$a+c \equiv b+c \pmod{n}$。

如果$a \equiv b \pmod{n}$，则$ac \equiv bc \pmod{n}$

但是，如果$ac \equiv bc \pmod{n}$和$c \not\equiv 0 \pmod{n}$，则$a \equiv b \pmod{n}$不一定为真。

例如， $4 \cdot 2 \equiv 1 \cdot 2 \pmod{6}$，但$4 \equiv 1 \pmod{6}$

模算术中没有一般的取消。

消除

当$a \neq b$ 时,是什么使$a \cdot k \equiv b \cdot k \pmod{n}$成为可能?

不失一般性,假设$0 \leqslant a, b, k < n$。这是因为如果$a \cdot k \equiv b \cdot k \pmod{n}$,那么$(a \bmod n) \cdot (k \bmod n) \equiv (b \bmod n) \cdot (k \bmod n) \pmod{n}$。

小于 n。

这意味着$(ab)k = ak - bk \equiv 0 \pmod{n}$。

所以$(ab)k$可以被n 整除。

由于$0 \leqslant a$、$b < n$和$a \neq b$,这意味着$0 < |ab| <$名词。

这只有在n和k共享一个公约数时才有可能,即$\gcd(n,k) \geqslant 2$!

好的,那么,当$\gcd(n,k)=1$时我们可以说点什么吗?

消除

宣称。如果$i \cdot k \equiv j \cdot k \pmod{n}$且$\gcd(k,n) = 1$,则$i$

$$\equiv j \pmod{n}。$$

例如,如果 n 是素数,则乘法逆总是存在的!

证明。由于$\gcd(k,n) = 1$,因此存在k 使得kk $\equiv 1 \pmod{n}$。

$$i \cdot k \equiv j \cdot k \pmod{n}$$

$$\Rightarrow i \cdot k \cdot k \equiv j \cdot k \cdot k \pmod{n}$$

$$\Rightarrow i \equiv j \pmod{n}$$

这使得算术模素数成为一个域,一个“表现得像”实数的结构。

算术模素数在编码理论中非常强大。

计划

- 模运算
  - 模加法,乘法
  - 应用
  - 乘法逆
  - 费马小定理,威尔逊定理
- 中国剩余定理

费马小定理

如果p是素数并且gcd(k,p) = 1,那么我们可以取消k。所以

$$k \pmod p,\ 2k \pmod p,\ \ldots,\ (p-1)k \pmod p$$

都是不同的。

这产生了k (mod

p), 2k (mod p), ..., (p-1)k (mod p)

必须是一个排列

1、2、· · ·、(p-1)

（每个数字只出现一次。）

Z_5	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

费马小定理

定理。设p为素数且gcd(k,p) = 1。然后

$$k\ p-1 \equiv 1 \pmod{p}。$$

证明。

一个排列

$$1\cdot 2\cdots(p-1) \equiv (k \bmod p)\cdot(2k \bmod p)\cdots\cdots((p-1)k \bmod p) \pmod{p} \equiv$$
$$(k\cdot 2k\cdots\cdots(p-1)k) \pmod{p} \equiv (kp-1)\cdot 1\cdot 2\cdots\cdots(p-1) \pmod{p}$$

由于1, 2,· · ·, (p-1)与 p 互质,所以两边都可以抵消,我们有

$$1 \equiv k\ p-1 \pmod{p}$$

威尔逊定理

定理。 p是素数当且仅当

$$(p-1)! \equiv -1 \pmod p。$$

我们首先考虑“如果”的一面。

Wlog,假设p不是素数且$p \geqslant 6$。 （为什么？）

那么$p=qr$对于一些$2 \leqslant q, r < p$。

如果$q \neq r$,则q和r都出现在$(p-1)!$中,因此$(p-1)! \equiv$
$0 \pmod p$。

如果$q = r$,则$p = q2 > 2q$ （因为$p \geqslant 6$） 。那
么q和$2q$都在$(p-1)!$中,同样如此$(p-1)!$
$\equiv 0 \pmod p$。

威尔逊定理

定理。 p是素数当且仅当

$$(p-1)! \equiv -1 \pmod p。$$

为了证明“仅当”方向,我们需要一个引理。

引理。设 p 为素数。然后

$x^2 \equiv 1 \pmod p$当且仅当$x \equiv 1 \pmod p$或$x \equiv -1 \pmod p$。

证明。 $x^2 \equiv 1 \pmod p$

$p \mid x^2 - 1 = (x-1)(x+1)$

$p \mid (x-1)$或$p \mid (x+1)$

回想一下p prime 和p|ab意味着p|a或p|b。

$x \equiv 1 \pmod p$或$x \equiv -1 \pmod p$

威尔逊定理

定理。 p是素数当且仅当

$$(p-1)! \equiv -1 \pmod{p}。$$

让我们通过一个具体的例子来得到证明的想法。

$10!$

$\equiv 1\cdot 2\cdot 3\cdot 4\cdot 5\cdot 6\cdot 7\cdot 8\cdot 9\cdot 10 \pmod{11}$

$\equiv 1\cdot 10\cdot (2\cdot 6)\cdot (3\cdot 4)\cdot (5\cdot 9)\cdot (7\cdot 8) \pmod{11}$

$\equiv 1\cdot (-1)\cdot (1)\cdot (1)\cdot (1)\cdot (1) \pmod{11}$

$\equiv -1 \pmod{11}$

除了 1 和 10,其余的都配对成乘法逆元!

威尔逊定理

定理。 p是素数当且仅当

$$(p-1)! \equiv -1 \pmod{p}。$$

证明。考虑一个奇数素数p。从1到p-1的每个k都有一个乘法逆元。

特别是， 2和p-2之间的每个k都有一个逆k $\neq$ k的引理。

由于p是奇数,从2到p-2的数字可以分组为对$\{a_1, b_1\}, \{a_2, b_2\}, \ldots, \{a_{(p-3)/2}, b_{(p-3)/2}\}$使得$a_i b_i \equiv 1 \pmod{p}$。

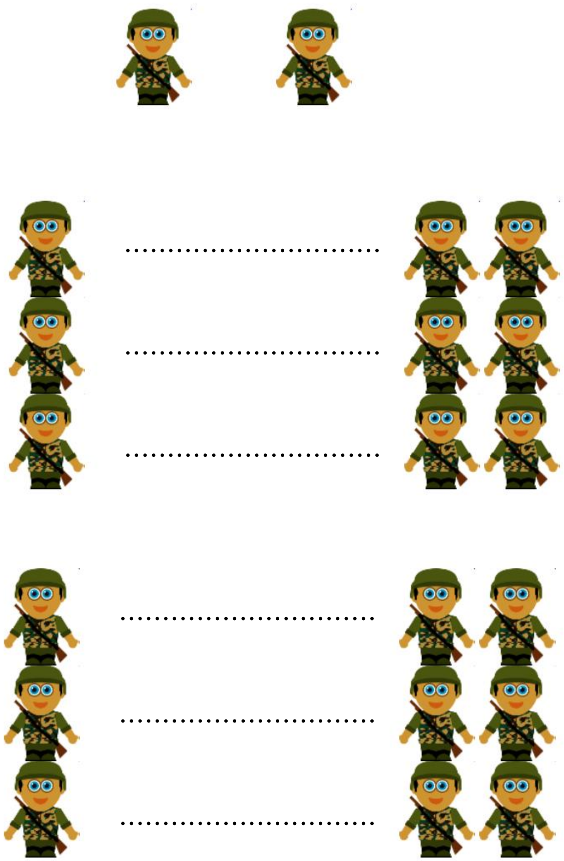
因此， $(p-1)! \equiv 1 \cdot (p-1) \cdot 2 \cdot 3 \cdot \cdots \cdot (p-3) \cdot (p-2) \pmod{p} \equiv$

$1 \cdot (p-1) \cdot (a_1 b_1) \cdot (a_2 b_2) \cdot \cdots \cdot (a_{(p-3)/2} b_{(p-3)/2}) \pmod{p} \equiv 1 \cdot (-1) \cdot (1) \cdot (1) \cdot \cdots \cdot (1) \pmod{p} \equiv -1 \pmod{p}$。

计划

- 模运算
  - 模加法,乘法
  - 应用
  - 乘法逆
  - 费马小定理,威尔逊定理
- 中国剩余定理

中国剩余定理



图片来自http://
img5.epochtimes.com/i6/801180520191974.jpg

一个方程

如何解下列方程?

$$\boxed{ax \equiv b \pmod{n}}$$

$2x \equiv 3 \pmod{7}$	$x = 5 + 7v$对于任何整数v
$5x \equiv 6 \pmod{9}$	$x = 3 + 9v$对于任何整数v
$4x \equiv -1 \pmod{5}$	$x = 1 + 5v$对于任何整数v
$4x \equiv 2 \pmod{6}$	$x = 2 + 3v$对于任何整数v
$10x \equiv 2 \pmod{7}$	$x = 3 + 7v$对于任何整数v
$3x \equiv 1 \pmod{6}$	没有解决方案

一个方程

$ax \equiv b \pmod{n}$

案例 1： $\gcd(a,n) = 1$。

注意a可以用mod n 代替,所以我们可以假设$0 < a < n$。

例如$103x \equiv 6 \pmod{9}$　　$4x \equiv 6 \pmod{9}$。

由于$\gcd(a,n) = 1$,存在 a 的乘法逆a　　。
因此我们可以在等式两边乘以a　　得到

$x \equiv a \quad b \pmod{n}$

因此,当a和n互质时,总是存在解。

一个方程

$$\boxed{ax \equiv b \pmod{n}}$$

情况 2： gcd(a,n) = c > 1。

案例 2a： c整除b。

$ax \equiv b \pmod{n}$

$ax = b + nk$对于某个整数k

a1cx = b1c + n1ck

a1x = b1 + n1k

a1x ≡ b1 (mod n1)

因此,我们可以简化为案例1。

一个方程

$$\boxed{ax \equiv b \pmod{n}}$$

情况 2： $\gcd(a,n) = c > 1$。

情况 2b： c不整除b。

$ax \equiv b \pmod{n}$

$ax = b + nk$对于某个整数k

$a1cx = b + n1ck$

$b = (a1x - n1k)c$

这是一个矛盾,因为 RHS 可以被c整除,而 LHS 不能。

所以在这种情况下没有解决方案。

一个方程

$$\boxed{ax \equiv b \pmod n}$$

定理。给定整数a, b, n,上式有解当且
仅当gcd(a,n) |湾。
此外,解都是y (mod n/gcd(a,n)) 的形式。

证明。首先,将b除以gcd(a,n)。

如果不可整除,则案例 (2b) 无解。

如果可整除,那么我们可以将方程简化为情况(2a)。

然后我们作为案例 1来计算解决方案。

数论的古代应用

中国古代有个将军叫韩信，

率领1500名士兵参加战斗。估计400-

500名士兵在战斗中丧生。当士兵站着 3

连续剩下2名士兵。当他们排成一排5人时，还剩下4名士兵。

当他们排成一排7人时，还剩下6名士兵。韩信立即道："有1049

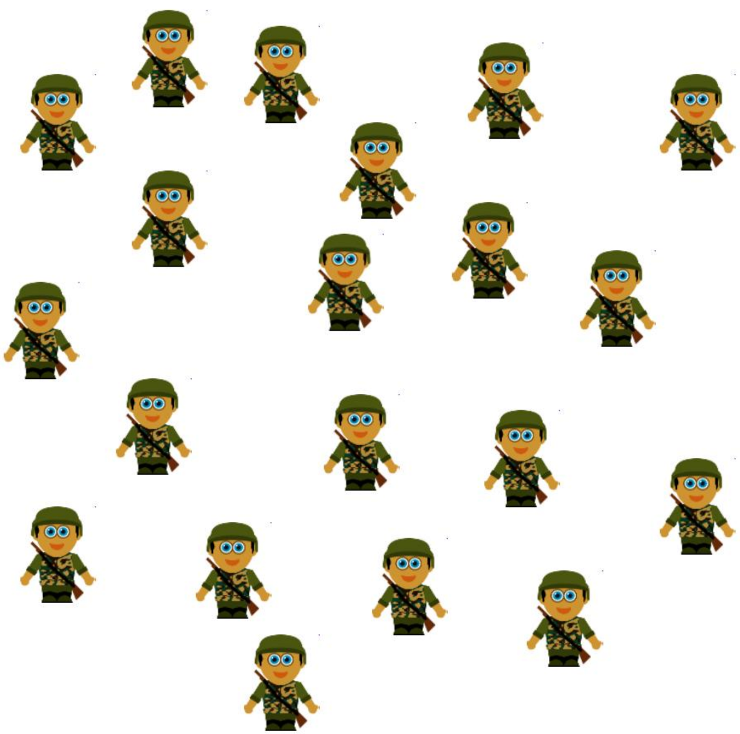
士兵。"

（来自https://chinesetuition88.com/2015/04/25/chinese剩余-theorem-history-韩信点兵/）

数论的古代应用

从1500名士兵开始，大约有400-500名士兵死于一场战斗。

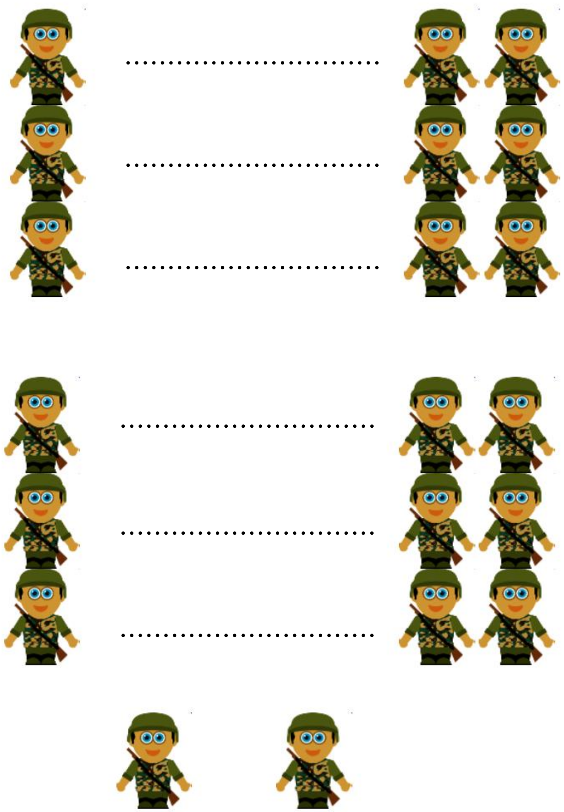
现在我们想知道还剩下多少士兵。



3名士兵组成小组

韩信

数论的古代应用

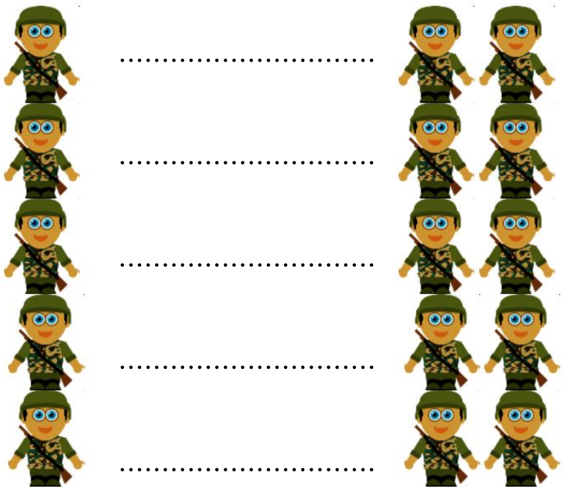


5名士兵组成一组

韩信

剩下2个士兵。

数论的古代应用

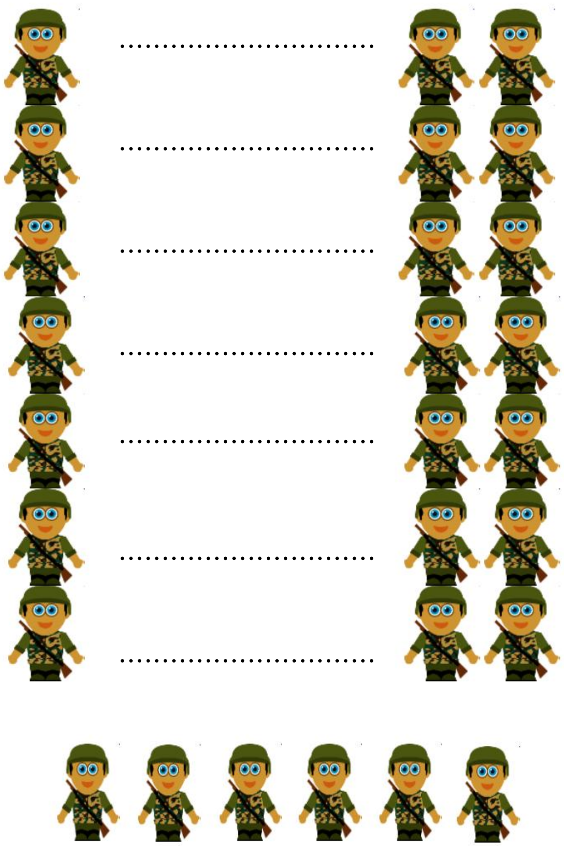


剩下4个士兵。

7名士兵组成小组

韩信

数论的古代应用



剩下6名士兵。

我们有1049名士兵。

韩信

他是怎么想出来的？！

问题

$$x \equiv 2 \pmod 3$$
$$x \equiv 4 \pmod 5$$
$$x \equiv 6 \pmod 7$$

+

$$1000 \leqslant x \leqslant 1100$$

$$x = 1049$$

如何求解这个模方程组?

两个方程

找到同时满足两个方程的解。

$$\boxed{\begin{aligned} c1\,x &\equiv d1 \pmod{m1} \\ c2\,x &\equiv d2 \pmod{m2} \end{aligned}}$$

首先,如果可能,我们可以将每个方程简化为其简单形式。

$$\boxed{\begin{aligned} x &\equiv a1 \pmod{n1} \\ x &\equiv a2 \pmod{n2} \end{aligned}}$$

当然,有时可能没有解决办法。

例如,考虑$x \equiv 1 \pmod 3$和$x \equiv 2 \pmod 3$。

$x \equiv 1 \pmod 6$和$x \equiv 2 \pmod 4$。

两个方程

情况 1： n1和n2互质。

$$x \equiv 2 \pmod 3$$
$$x \equiv 4 \pmod 7$$

那么$x = 2+3u$和$x = 4+7v$对于一些整数u, v. $2+3u = 4+7v$
=> $3u = 2+7v$

=> $3u \equiv 2 \pmod 7$

请注意， 5是3模7 的乘法逆元。

我们两边乘以5得到： $u \equiv 5 \cdot 2 \equiv 3$

$\pmod 7$

=> $u = 3 + 7w$

因此， $x = 2+3u = 2+3(3+7w) = 11+21w$。

所以任何$x \equiv 11 \pmod{21}$都是一个解。

我们在哪里使用了n1和n2互质的假设?

两个方程

情况 1： n1和n2互质。

$$x \equiv 2 \pmod{3}$$
$$x \equiv 4 \pmod{7}$$

事实上,我们可以直接构造这样一个x 。

设置$x = 3 \cdot a + 7 \cdot b$

当x除以3 时,余数由第二项确定。
当x除以7 时,余数由第一项确定。

我们如何选择a以使3a除以 7 时余数为4 ?

这只是要求$3a \equiv 4 \pmod{7} \Rightarrow a \equiv 5 \quad 4 \equiv 6 \pmod{7}$。

同样,我们有$7b \equiv 2 \pmod{3} \Rightarrow b \equiv 2 \pmod{3}$。

所以答案是$x = 3a+7b \equiv 3 \quad 6 + 7 \quad 2 \pmod{21} \equiv 32 \pmod{21} \equiv 11 \pmod{21}$。

三个方程

$$\boxed{\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 4 \pmod 5 \\ x &\equiv 6 \pmod 7 \end{aligned}}$$

设置$x = 5 \cdot 7 \cdot a + 3 \cdot 7 \cdot b + 3 \cdot 5 \cdot c$

然后第一个（第二个,第三个)项由第一个（第二个,第三个)方程确定。

现在我们只需要分别求解以下方程。

$35a \equiv 2 \pmod 3,\ 21b \equiv 4 \pmod 5,\ 15c \equiv 6 \pmod 7$。

=> $2a \equiv 2 \pmod 3,\ b \equiv 4 \pmod 5,\quad c \equiv 6 \pmod 7$。

=> $a \equiv 1 \pmod 3,\ b \equiv 4 \pmod 5,\quad c \equiv 6 \pmod 7$。

那么$x = 35a + 21b + 15c \equiv 35 \quad 1 + 21 \quad 4 + 15 \quad 6 \pmod{3 \quad 5 \quad 7} \equiv 209 \pmod{105}$。

由于韩信知道$1000 \leqslant x \leqslant 1100$,所以得出$x=1049$。

等等,但他怎么知道没有其他解决方案?

中国剩余定理

定理。令$n_1, n_2, \cdots, n_k$互质。然后

$$x \equiv a_1 \pmod{n_1}$$
$$x \equiv a_2 \pmod{n_2}$$

$$x \equiv a_k \pmod{n_k}$$

有一个模 n 的唯一解,其中$n = n_1 n_2 \cdots n_k$。

我们将在 k=3 时给出一个证明,但它可以很容易地扩展到任何 k。

中国剩余定理的证明

让 $N_1 = n_2 n_3 \quad N_2 = n_1 n_3 \quad N_3 = n_1 n_2$

由于 N_i 和 n_i 互质,所以存在 x_1, x_2, x_3 使得

$$N_1 x_1 \equiv 1 \pmod{n_1} \qquad N_2 x_2 \equiv 1 \pmod{n_2} \quad N_3 x_3 \equiv 1 \pmod{n_3}$$

$$\Rightarrow N_1 x_1 a_1 \equiv a_1 \pmod{n_1},\ N_2 x_2 a_2 \equiv a_2 \pmod{n_2},\ N_3 x_3 a_3 \equiv a_3 \pmod{n_3}$$

$$\boxed{\text{令 } x = N_1 (x_1 a_1) + N_2 (x_2 a_2) + N_3 (x_3 a_3)}$$

请注意， n_1 除以 N_2 和 N_3， 所以

$$x \equiv N_1 (x_1 a_1) \equiv a_1 \pmod{n_1}$$

类似地， $x \equiv \boxed{a_2 \pmod{n_2}}$ $\quad \boxed{x \equiv a_3 \pmod{n_3}}$

独特性

$$x \equiv a1 \ (\text{mod } n1\ )$$
$$x \equiv a2 \ (\text{mod } n2\ )$$

$$x \equiv ak \ (\text{mod } nk\ )$$

- 令x, y为上述系统的解。
- 然后对于每个i， $x - y \equiv 0 \ (\text{mod } ni\ )$ 。
- 因此$ni \mid x - y$对于每个i。
- 由于$n1, n2, \cdots, nk$互质，
- 随之而来的是$n1n2\cdots nk \mid x - y$。 （为什么？ ）
- 因此， $x \equiv y \ (\text{mod } n1n2\cdots nk\ )$。

通用系统

如果$n_1, n_2, \ldots, n_k$不互质怎么办?

$x \equiv 3 \pmod{10}$

- $\cancel{x \equiv 3 \pmod{2} \equiv 1 \pmod{2}}$ (一个)
- $x \equiv 3 \pmod{5}$ (二)

$x \equiv 8 \pmod{15}$

- $x \equiv 8 \pmod{3} \equiv 2 \pmod{3}$ (C)
- $\cancel{x \equiv 8 \pmod{5} \equiv 3 \pmod{5}}$ (d)

$x \equiv 5 \pmod{84}$

- $x \equiv 5 \pmod{4} \equiv 1 \pmod{4}$ (e)
- $\cancel{x \equiv 5 \pmod{3} \equiv 2 \pmod{3}}$ (F)
- $x \equiv 5 \pmod{7}$ (G)

所以我们将问题简化为互质的情况。

答案是$173 \pmod{420}$。

(e) 比 (a) 强。 (b) 和 (d) 相同。 (c) 和 (f) 相同。

更快的方法

有另一种方法可以求解模方程组。 $x \equiv 3 \pmod{10}$ $x \equiv 8 \pmod{15}$ $x \equiv 5 \pmod{84}$

从第三个方程我们有$x = 5+84u$。

将其代入第二个方程得到$5+84u \equiv 8 \pmod{15} \Rightarrow 9u \equiv 3 \pmod{15}$。

解决这个问题得到$u \equiv 2 \pmod{5} \Rightarrow u = 2 + 5v$。

因此， $x = 5+84u = 5+84(2+5v) = 173 + 420v$。

将其插入第一个给出$173+420v \equiv 3 \pmod{10} \Rightarrow 420v = -170 \pmod{10}$。

这个等式总是正确的。

因此我们得出结论$x = 173+420v$,或等效地$x \equiv 173 \pmod{420}$。

这种方法也可以用来证明中国剩余定理。

它要快得多（无需找到因式分解） ,只求解 k-1 个模方程。