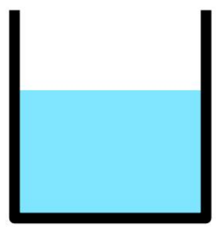
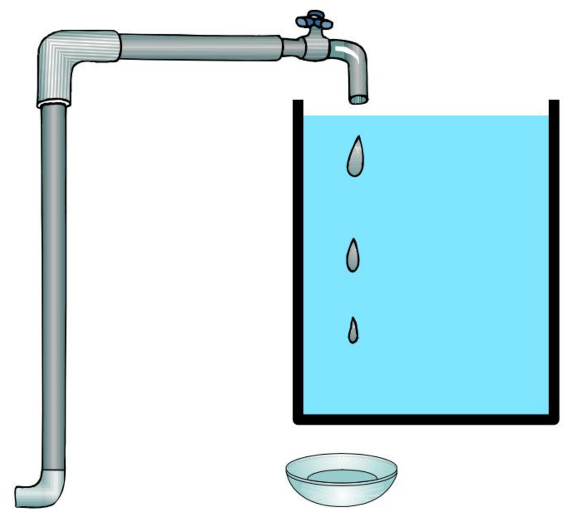
最大公约数



3加仑壶



5加仑壶

倍数和除数

b是 a 的除数,当且仅当存在整数k使得a=kb。记为b|a或b 除以 a或a除以 b

a是b的倍数,当且仅当存在一个整数k使得a=kb

b是 a 的除数当且仅当a是b的倍数

假设 a=5,b=10,然后a|b。

说 a=0,b=30,然后b|a

说a=-3,b=11,那么a不整b,记为a b。

公约数

c是a的公约数， b表示c|a和c |b。

gcd(a,b) ::= a和b的最大公约数。

假设 a=8,b=10,那么 1,2 是公约数,gcd(8,10)=2。

说a=10,b=30,那么1,2,5,10是公约数,gcd(10,30)=10。

说a=3,b=11,那么唯一的公约数是1,gcd(3,11)=1。

宣称。如果p是素数,并且p不整除a,则gcd(p,a) = 1。

商余定理

对于b > 0 和任何a,都有唯一的整数

q ::= quotient(a,b), r ::= 余数(a,b),这样

a = qb + r且 0 ⩽ r < b。

我们也说q = a div b和r = a mod b。

当 b=2 时,存在唯一的 q,使得 a=2q 或 a=2q+1。

$$q = \lfloor \frac{a}{2} \rfloor$$

当 b=3 时,存在唯一的 q,使得 a=3q 或 a=3q+1 或 a=3q+2。

$$q = \lfloor \frac{a}{3} \rfloor$$

地板函数⩽ x ⌊ ⌋ : 的最大整数

商余定理

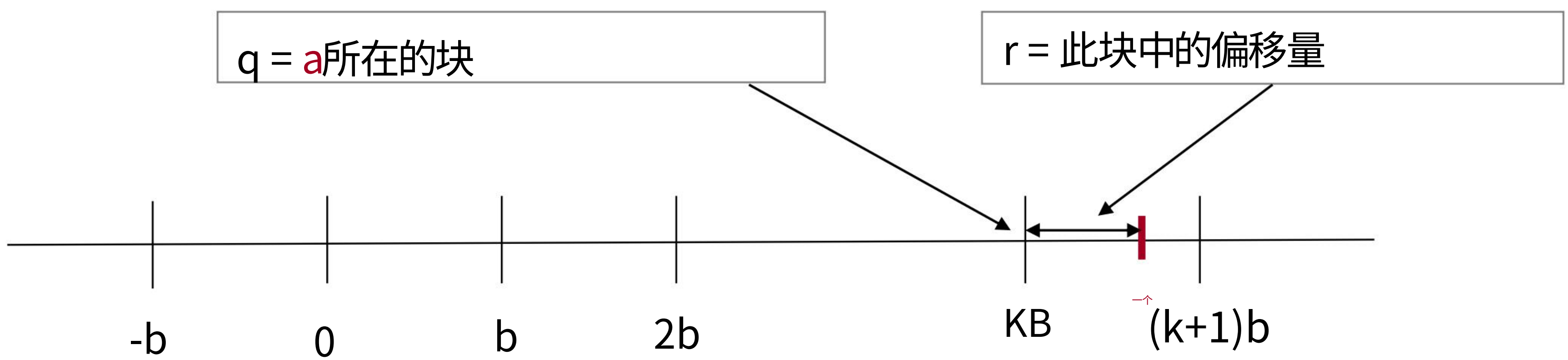
对于b > 0 和任何a,都有唯一的整数

q ::= quotient(a,b), r ::= 余数(a,b),这样

$$a = qb + r \text{且 } 0 \leqslant r < b。$$

给定任何b,我们可以将整数划分为 b 个数的块。

对于任何a,这个数字都有一个唯一的“位置”。



显然,给定a和b,数字 q 和 r 是唯一确定的。

最大公约数

给定 a 和 b,如何计算 gcd(a,b)?

也许尝试每个数字?对于大数字来说并不容易……
我们有更好的方法吗?

假设 $a \geqslant b > 0$。

1.如果a=kb,那么gcd(a,b)=b,我们就完成了。

2.否则,根据除法定理,$a = qb + r$ 其中 $r>0$。

最大公约数

假设a≥b。

1.如果a=kb,那么gcd(a,b)=b,我们就完成了。

2.否则,根据除法定理,a = qb + r 其中 r>0。

a=12, b=8 => 12 = 8 + 4 gcd(12,8) = 4 gcd(8,4) = 4

a=21, b=9 => 21 = 2x9 + 3 gcd(21,9) = 3 gcd(9,3) = 3

a=99, b=27 => 99 = 3x27 + 18 gcd(99,27) = 9 gcd(27,18) = 9

欧几里得: gcd(a,b) = gcd(b,r)!

Euclid 的 GCD 算法

a = qb + r

欧几里得： gcd(a,b) = gcd(b,r) !

假设 :a > b ⩾ 0。

gcd(a,b)

如果 b = 0 ,则答案 = a。

别的

写 a = qb + r ← $q = \lfloor \frac{a}{b} \rfloor \quad r = a - qb$

答案 = gcd(b,r)

示例 1

gcd(a,b)

如果 b = 0,则答案 = a。

别的

写 a = qb + r

答案 = gcd(b,r)

GCD(102, 70)

= GCD(70, 32)

= GCD(32, 6)

= GCD(6, 2)

= GCD(2, 0)

102 = 70 + 32

70 = 2x32 + 6

32 = 5x6 + 2

6 = 3x2 + 0

返回值： 2。

示例 2

gcd(a,b)

如果 b = 0,则答案 = a。

别的

写 a = qb + r

答案 = gcd(b,r)

GCD(252, 189)

= GCD(189, 63)

= GCD(63, 0)

252 = 1x189 + 63

189 = 3x63 + 0

返回值:63。

示例 3

gcd(a,b)
如果 b = 0,则答案 = a。
别的

写 a = qb + r

答案 = gcd(b,r)

GCD(662, 414)
= GCD(414, 248)
= GCD(248, 166)
= GCD(166, 82)
= GCD(82, 2)
= GCD(2, 0)

662 = 1x414 + 248
414 = 1x248 + 166
248 = 1x166 + 82
166 = 2x82 + 2
82 = 41x2 + 0

返回值： 2。

欧几里得 GCD 算法的正确性

$a = qb + r$

欧几里得:$gcd(a,b) = gcd(b,r)$

当 $r = 0$ 时:

那么 $a = qb$,所以 $gcd(a, b) = b$; r

$= 0$,所以 $gcd(b, r) = gcd(b, 0) = b$。

因此,$gcd(a,b) = gcd(b,r)$。

欧几里得 GCD 算法的正确性

$a = qb + r$

欧几里得 :$\gcd(a,b) = \gcd(b,r)$

当 $r > 0$ 时:

令 d 是 b 的公约数,r　b = k1d和 r =

k2d对于一些k1 , k2 。　$a = qb + r = qk1d$

$+ k2d = (qk1 + k2)d$ => d 是 a, b 的公约数

令 d 为 a, b 的公约数

$a = k3d$和 $b = k1d$对于一些k1， k3 。

$r = a - qb = k3d - qk1d = (k3 - qk1)d$ => d 是 b, r 的公约数

所以， {a, b 的公因数} = {b, r 的公因数}

$\gcd(a, b) = \gcd(b, r)$。

Euclid 的 GCD 算法快吗?

朴素算法:尝试每个数字。

假设:$a > b \geqslant 0$。

gcd(a,b)

令 d=1

1.如果d|a和d|b,则存储d。

2.令d=d+1

3.如果 $d \leqslant b$,返回1。

否则答案 = 所有存储的 “d”的最大值

所以运行时间大约是b次迭代。

Euclid 的 GCD 算法快吗?

欧几里得算法:

在两次迭代中,a､b 减半。 （为什么？）

$a = bq + r \geqslant b + r > 2r$

=> gcd(a,b) = gcd(b,r) 其中 r < a/2

类似地,如果 b = rq + r ,那么

gcd(b,r) = gcd(r,r) 其中 r < b/2

假设算法在 2k 次迭代中停止。

那么2d ⩾ 2k-1 。 （假设2d+1 ⩾ b > 2d）

所以运行时间约为 2log2b次迭代。

指数级的更快！！

线性组合与公约数

最大公约数

d 是 a 和 b 的公约数,如果 $d|a$ 和 $d|b$

gcd(a,b) = a 和 b 的最大公约数

最小正整数线性组合

如果 $d=sa+tb$ 对于整数 s,t,d是 a 和 b 的整数线性组合。

spc(a,b) = a 和 b 的最小正整数线性组合

定理。 gcd(a,b) = spc(a,b)

线性组合与公约数

定理。 $\gcd(a,b) = \mathrm{spc}(a,b)$

例如,52 和 44 的最大公约数是 4。
并且 4 是 52 和 44 的整数线性组合： $6 \cdot 52 + (-7) \cdot 44 =$
4 此外,52 和 44 的整数线性组合不等于更小的正
整数。

为了证明这个定理,我们将证明：

$\gcd(a,b) \leqslant \mathrm{spc}(a,b)$

$\gcd(a,b) \mid \mathrm{spc}(a,b)$

$\gcd(a,b) \geqslant \mathrm{spc}(a,b)$

spc(a,b) 将 a 和 b 相除

GCD⩽SPC

宣称。如果 d | a 和 d | b,然后 d | sa + tb 对于任何 s,t。

证明。

d | a => a = dk1 d |

b => b = dk2 sa + tb

= sdk1 + tdk2 = d(sk1 + tk2) => d|(sa+tb)

GCD | SPC

令 d = gcd(a,b)。根据定义,d | a 和 d |湾。

令 f = spc(a,b) = sa+tb

根据索赔,d | F。所以 gcd(a,b) ⩽ spc(a,b)。

GCD≥SPC

我们将证明 spc(a,b) 实际上是 a 和 b 的公约数。

首先,证明 spc(a,b) |一个。

1.根据除法定理（因为 a ≥ spc(a,b)），a = qx spc(a,b)

+ r spc(a,b) > r ≥ 0 2.令 spc(a,b) = sa+tb 和 待定。

3.那么 r = a – qx spc(a,b) = a – qx (sa + tb) = (1-qs)a + qtb。

4.所以 r 是 a 和 b 的整数线性组合,且 spc(a,b) > r。

5.这只有在 r = 0 时才有可能。

同样,spc(a,b) |湾。

因此,spc(a,b) 将 a 和 b 分开,遵循 spc(a,b) ≤ gcd(a,b)。

定理的应用

定理。 $\gcd(a,b) = spc(a,b)$

引理。如果 $\gcd(a,b)=1$ 且 $\gcd(a,c)=1$,则 $\gcd(a,bc)=1$。

根据定理,存在 s,t,u,v 使得

$$sa + tb = 1$$
$$ua + vc = 1$$

所以 $(sa + tb)(ua + vc) = 1$

扩展 LHS 提供

$$saua + savc + tbua + tbvc = 1$$

$$(sau + svc + tbu)a + (tv)bc = 1$$

这意味着 $spc(a,bc)=1$。根据定理,我们有 $\gcd(a,bc)=1$。

素数可分性

定理。 $\gcd(a,b) = \mathrm{spc}(a,b)$

引理。 p素数和$p|ab$意味着$p|a$或$p|b$。

证明。 Wlog,假设 p 不整除a。那么$\gcd(p,a)=1$。

所以根据定理,存在 s 和 t 使得

$$sa + tp = 1$$

$$\underbrace{(sa)b}_{p|ab} + \underbrace{(tp)b}_{p|p} = b$$

因此 $p|b$

推论。如果p是素数,并且$p|\ a_1 \cdot a_2 \cdots a_m$然后$p|a_i$对于一些i。

算术基本定理

每个整数n>1都有一个唯一的因式分解为素数：

$$p_0 \leqslant p_1 \leqslant \cdots \leqslant p_k$$

$$n = p_0\, p_1 \cdots p_k$$

例子：

$61394323221 = 3 \cdot 3 \cdot 3 \cdot 7 \cdot 11 \cdot 11 \cdot 37 \cdot 37 \cdot 37 \cdot 53$

独特的因式分解

定理。有一个独特的因式分解。

证明。假设有一个数字有两个不同的因式分解。

根据 Well Ordering 原则,我们选择最小的$n > 1$:

$$n = p_1 \cdot p_2 \cdots p_k = q_1 \cdot q_2 \cdots q_m$$

由于 n 最小,我们必须有$p_i \neq q_j$ all i,j （否则,我们可以获得更小的反例。）

矛盾!

因为$p_1 | n = q_1 \cdot q_2 \cdots q_m$,所以推论$p_1 | q_i$对于一些 i。

由于p_1和q_i都是素数,我们必须有$p_1 = q_i$ 。

扩展 GCD 算法

我们如何将 gcd(a,b) 写成整数线性组合?

这可以通过扩展欧几里得算法来完成。

示例： $a = 259$， $b=70$

$259 = 3 \cdot 70 + 49$

$49 = a - 3b$

$70 = 1 \cdot 49 + 21$

$21 = 70 - 49$

$21 = b - (a-3b) = -a+4b$

$49 = 2 \cdot 21 + 7$

$7 = 49 - 2 \cdot 21$

$7 = (a-3b) - 2(-a+4b) = \underline{3a - 11b}$

$21 = 7 \cdot 3 + 0$

完成,gcd = 7

扩展 GCD 算法

示例： a = 899， b=493

899 = 1·493 + 406 所以 406 = a - b

493 = 1·406 + 87 所以 87 = 493 – 406

= b – (ab) = -a + 2b

406 = 4·87 + 58 所以 58 = 406 - 4·87

= (ab) – 4(-a+2b) = 5a - 9b

87 = 1·58 + 29 所以 29 = 87 – 1·58

= (-a+2b) - (5a-9b) = -6a + 11b

58 = 2·29 + 0 完成,gcd = 29

死硬死硬的顽固的

西蒙说:喷泉上有两个水壶,一个是 5 加仑,另一个是

另一个是 3 加仑。用恰好 4 加仑的水填充一个,然后将其放在秤上,然后计时器将停止。你必须准确;一盎司或多或少会导致爆炸。如果你在 5 分钟内还活着,我们会说话。

死硬死硬的顽固的

布鲁斯:等等,等一下。我不明白。你明白吗?
塞缪尔:没有。

布鲁斯:拿罐子。显然,我们不能用 4 加仑的水装满 3 加仑的水壶。

塞缪尔:显然。

布鲁斯:好的。我知道,我们开始吧。我们把 3 加仑的罐子装满,对吧?

塞缪尔:嗯。

布鲁斯:好的,现在我们将这 3 加仑倒入 5 加仑的壶中,在 5 加仑的壶中正好有 3 加仑,对吧?

塞缪尔:对,然后呢?

布鲁斯:好的。我们拿起 3 加仑的罐子,把它装满三分之一……

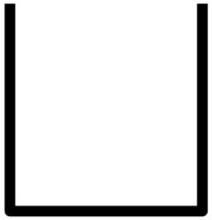
塞缪尔:不!他说:“准确一点。”正好 4 加仑。

布鲁斯:嘘 。 50英里内的每个警察都在跑他的**,我出去了在这里在公园里玩儿童游戏。

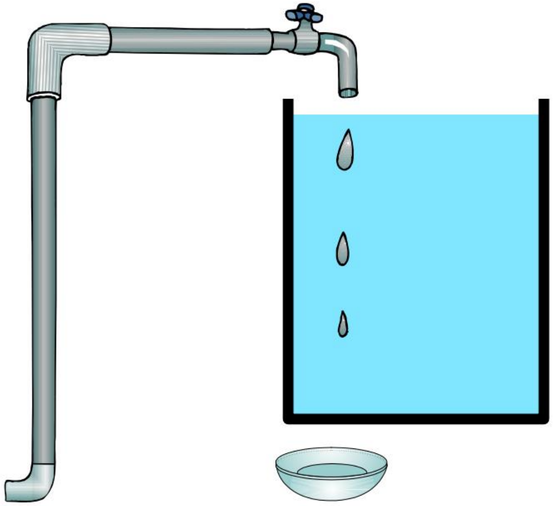
塞缪尔:嘿,你想专注于手头的问题吗?

从空罐子开始:(0,0)

装满大罐子:(0,5)

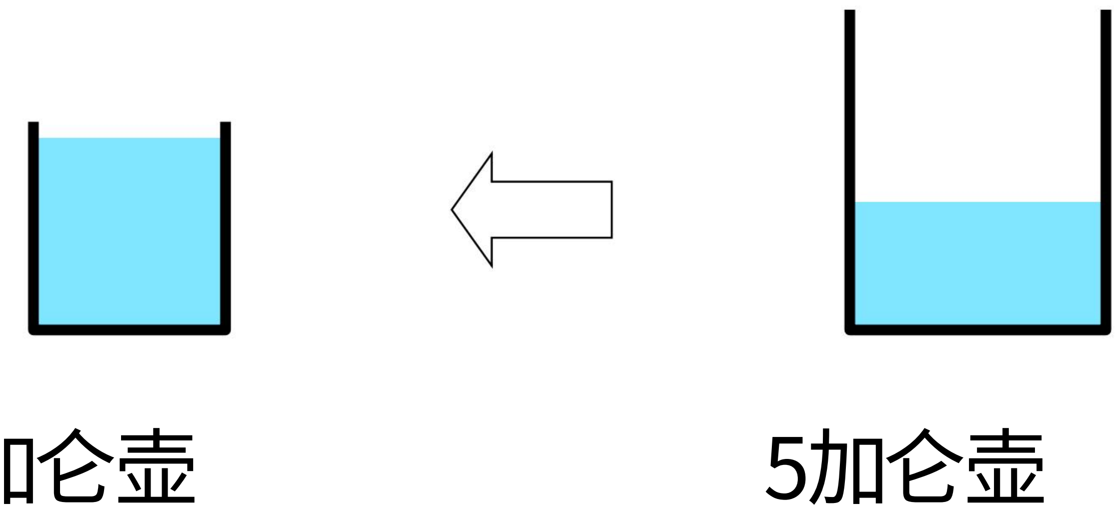


3加仑壶



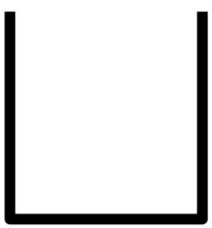
5加仑壶

从大到小倒： (3,2)

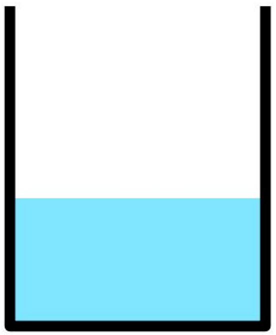


死硬死硬的顽固的

清空一点：（0,2）

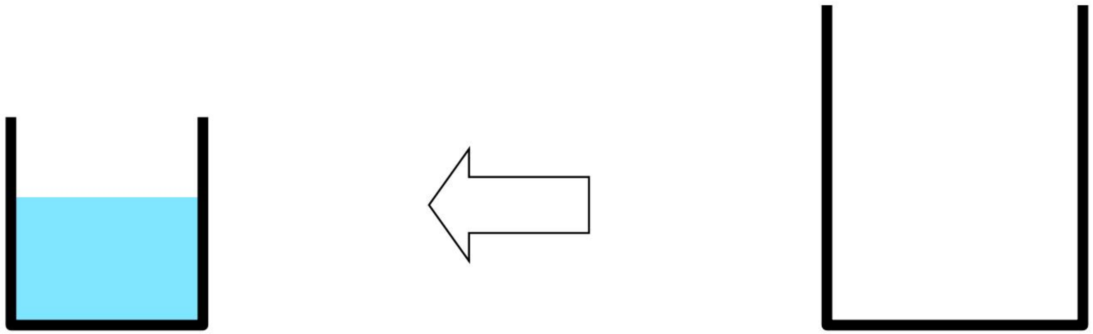


3加仑壶



5加仑壶

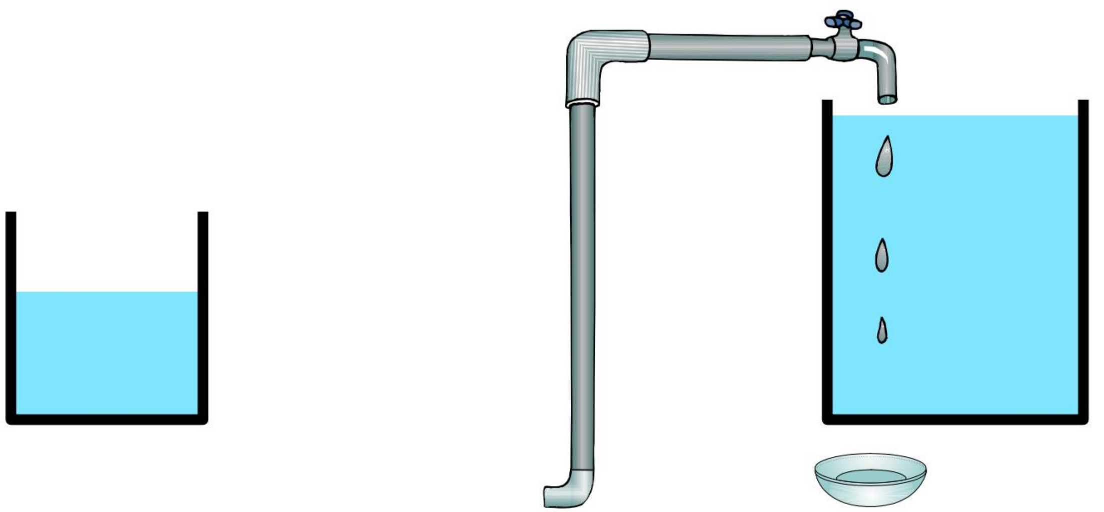
从大到小倒:(2,0)



3加仑壶

5加仑壶

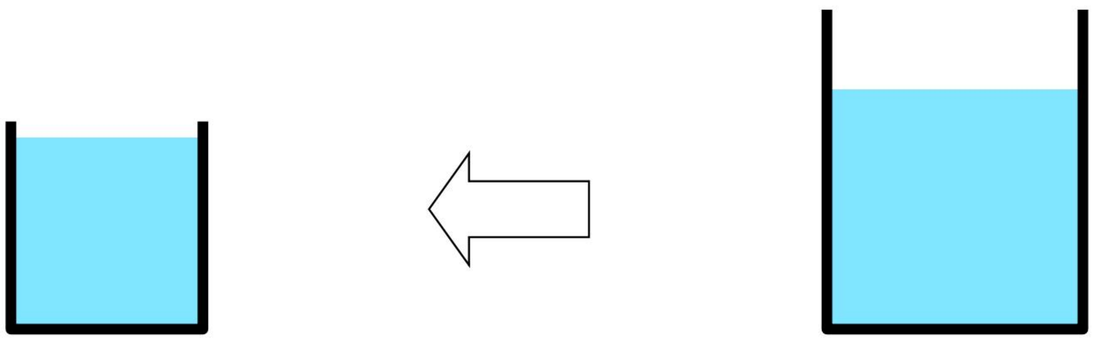
装满大罐子:(2,5)



3加仑壶

5加仑壶

从大到小倒：(3,4)



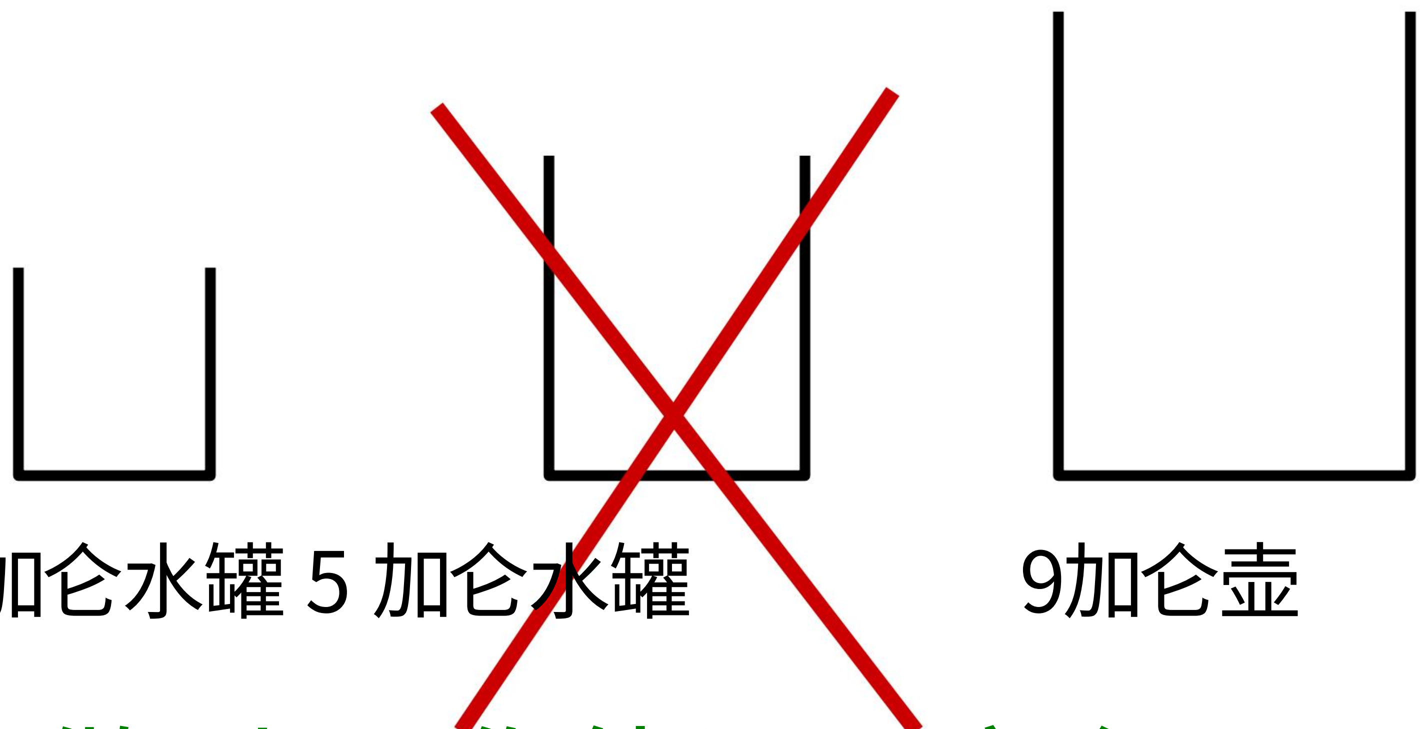
3加仑壶

5加仑水罐完

成！！

死硬死硬的顽固的

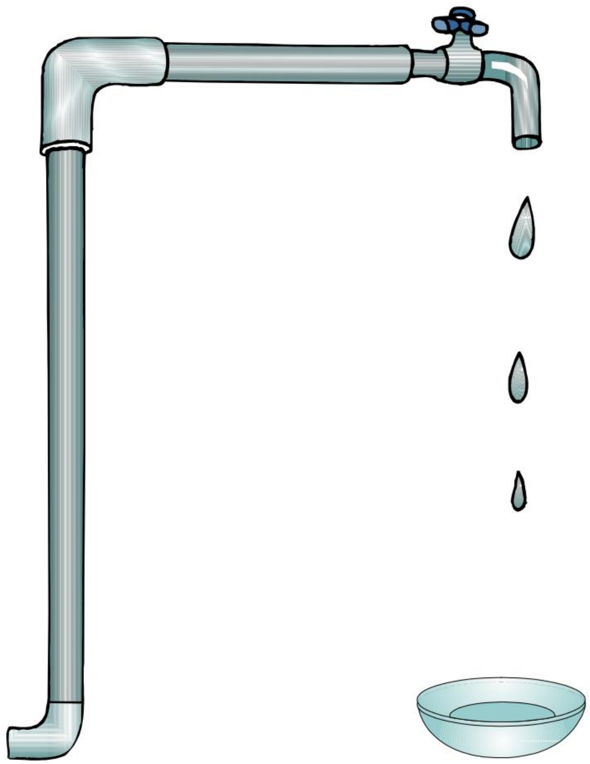
如果你有一个 9 加仑的水壶呢?



你能做到吗?你能证明这个吗?

死硬死硬的顽固的

补给品：



水

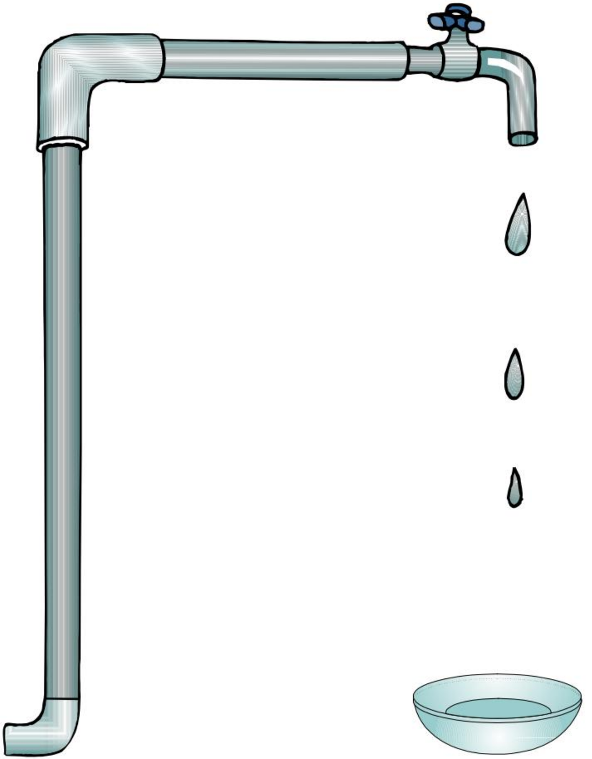
3加仑壶

9加仑壶

不变法

不变量 :每个水壶中的加仑数是 3 的倍数。即 $3|L$和 $3|B$ （3 除以L和B）

推论。一个罐子里不可能正好有 4 加仑。



布鲁斯死了！

广义的死硬

布鲁斯可以用 21 和 26 加仑的罐子形成 3 加仑吗?

如果没有数论,这个问题就不那么容易回答了。

Die Hard 的通用解决方案

顽固转换中的不变量：

假设我们有容量为 B 和 L 的水壶。

那么每个水壶里的水量总是一个整数

B 和 L 的线性组合。

引理。 gcd(a, b) 将 a 和 b 的任何整数线性组合相除。

令 $d = \gcd(a,b)$。然后

$d|a$ 和 $d|b$

所以$d|ax+by$。

推论。每个水壶中的水量是 gcd(a,b) 的倍数。

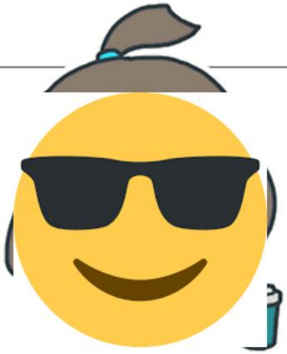
Die Hard 的通用解决方案

推论。每个水壶中的水量是 gcd(a,b) 的倍数。

给定 3 罐和 9 罐,一个罐中是否有可能正好有 4 加仑?

NO,因为 gcd(3,9)=3,而且 4 不是 3 的倍数。

给定 21 罐和 26 罐,一个罐中是否有可能正好有 3 加仑?



gcd(21,26)=1,而3是1的倍数,所以这意味着可能?？

定理。给定容量为 a 和 b 且 a ≤ b 的水壶,

当且仅当 k 是 gcd(a,b) 的倍数时,一个罐子中可能正好有 k (≤ b) 加仑。

Die Hard 的通用解决方案

定理。给定容量为 a 和 b 且 a ≤ b 的水壶，
当且仅当 k 是 gcd(a,b) 的倍数时，一个罐子中可能正好有 k
(≤ b) 加仑。

给定 21 罐和 26 罐，一个罐中是否有可能正好有 3 加仑？

$$\gcd(21,26) = 1$$
$$5\text{x}21 – 4\text{x}26 = 1$$
$$15\text{x}21 – 12\text{x}26 = 3$$

重复 15 次： 1. 装
满 21 加仑的水壶。
2. 将 21 加仑水壶中的所有水倒入 26 加仑水壶中。
每当 26 加仑的水壶装满时，将其倒空。

Die Hard 的通用解决方案

$$15 \times 21 - 12 \times 26 = 3$$

重复 15 次： 1.
装满 21 加仑的水壶。
2. 将 21 加仑水壶中的所有水倒入 26 加仑水壶中。
每当 26 加仑的水壶装满时,将其倒空。

宣称。在此过程之后必须正好剩下 3 加仑。

1.我们总共装满了 15x21 加仑。
2.我们倒出 26 加仑的 t 倍数。
3. 26加仑的水壶只能容纳0到26之间的容积。
4.所以 t 必须是 12。
5.正好剩下 3 加仑。

Die Hard 的通用解决方案

给定两个容量为 A 和容量为 B 且 A ≤ B 的水壶,目标是 C。

如果 gcd(A,B) 不整除 C,那么它是不可能的。

否则,计算 $C = sA + tB$。（我们总是可以使 $s > 0$。）

重复s次： 1. 装
满 A 加仑水罐。
2. 将 A 加仑壶中的水全部倒入 B 加仑壶中。
每当 B 加仑水罐装满时,将其倒空。

B 加仑水罐将被清空t次。

在那之后,B 加仑罐中将正好有 C 加仑。