欧几里得算法

记住两个整数 A 与 B 的最大公约数是 **最大的可以被 A 和 B 整除的整数。**

扩展欧几里德算法 是一个很快地计算两个整数的 **最大公约数** 的方法。

算法

计算 GCD(A,B) （A 和 B 的最大公约数）的扩展欧几里德算法如下：

- 如果 A = 0， GCD(A,B)=B，因为 GCD(0,B)=B，我们就到此为止。
- 如果 B = 0，GCD(A,B)=A，因为 GCD(A,0)=A，我们就到此为止。
- 用商和余数的表达方式 (A = B·Q + R) 写出 A
- 用扩展欧几里德算法计算 GCD(B,R)，因为 GCD(A,B) = GCD(B,R)

例子：

计算 270 与 192 的最大公约数

- A=270, B=192
- A ≠0
- B ≠0
- 用长除法算出 270/192 = 1， 余数是 78。我们可以把这个写为： 270 = 192 * 1 +78
- 计算 GCD(192,78)， 因为 GCD(270,192)=GCD(192,78)

A=192, B=78

- A ≠0
- B ≠0
- 用长除法算出 192/78 = 2，余数是 36。我们可以把这个写为：
- 192 = 78 * 2 + 36
- 计算 GCD(78,36)，因为 GCD(192,78)=GCD(78,36)

A=78, B=36

- A ≠0
- B ≠0
- 用长除法算出 78/36 = 2 ，余数是 6我们可以把这个写为：
- 78 = 36 * 2 + 6
- 计算 GCD(36,6)，因为 GCD(78,36)=GCD(36,6)

A=36, B=6

- A ≠0
- B ≠0
- 用长除法算出 36/6 = 6，余数是 0我们可以把这个写为：
- 36 = 6 * 6 + 0
- 计算 GCD(6,0)，因为 GCD(36,6)=GCD(6,0)

A=6, B=0

- A ≠0
- B =0, GCD(6,0)=6

因此我们已经证明：

GCD(270,192) = GCD(192,78) = GCD(78,36) = GCD(36,6) = GCD(6,0) = 6

GCD(270,192) = 6

理解扩展欧几里德算法

如果我们观察扩展欧几里德算法，可以看到它使用了以下的属性：

- GCD(A,0) = A
- GCD(0,B) = B
- **如果 A = B·Q + R 和 B≠0 那么 GCD(A,B) = GCD(B,R)**，在此 Q 是整数，R 是 0 与 B-1 之间的整数。

前面两个属性让我们在一个数字是 0 的时候计算最大公约数。第三个属性让我们面对一个更大，更难解决的问题，并将问题 **简化成更小，更容易解决的问题。**

扩展欧几里德算法用这些属性来很快地将问题简化成越来越容易的问题，用第三个属性，直到很容易用前面两个属性来解决。

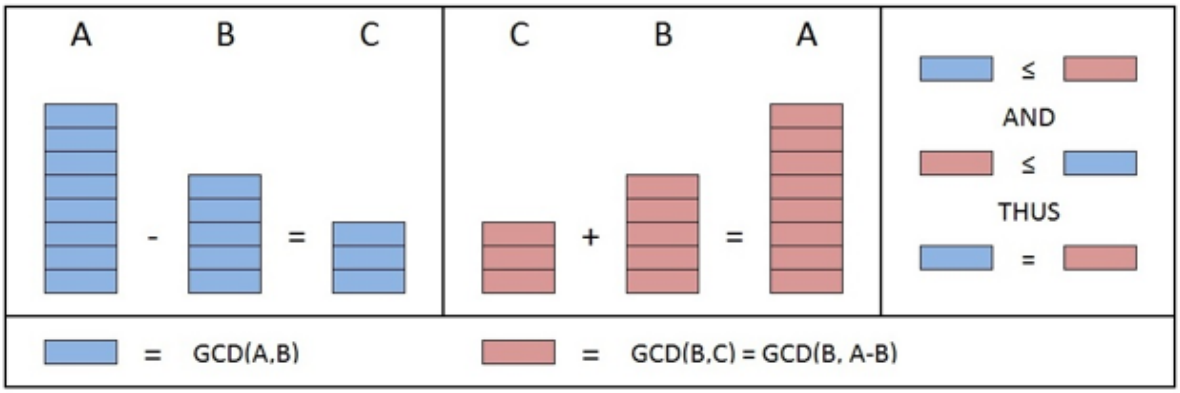
我们可以通过证明这些属性来理解它们。

我们可以如下证明 GCD(A,0)=A

- 最大的可以被 A 整除的整数是 A。
- 0 能被所有整数整除，因为对于任何整数 C。我们可以说 C · 0 = 0因此可以总结 0 一定能被 A 整除。
- 最大的能够整除 A 和 0 的数字是 A。

GCD(0,B)=B 的证明是类似的。(同一个证明，但是我们用 B 来代替 A）。

要证明 **GCD(A,B)=GCD(B,R)**，我们首先必须证明 **GCD(A,B)=GCD(B,A-B)**.



假如我们有三个整数 **A,B** 与 **C**，在此 **A-B=C**。

GCD(A,B) 能整除 C 的证明

GCD(A,B)，据其定义，可以整除 A。因此，A 必须是 GCD(A,B) 的某一个倍数. i.e. X·GCD(A,B)=A，在此 X 是某一个整数

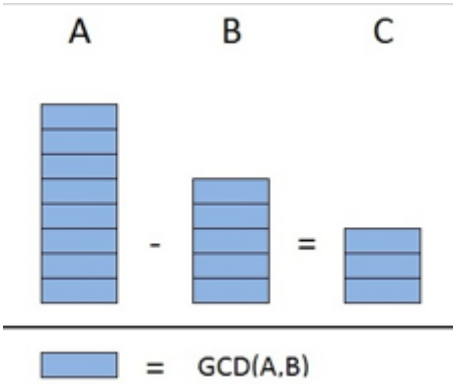
GCD(A,B)，据其定义，可以整除 B。因此，B 必须是 GCD(A,B) 的某一个倍数. i.e. Y·GCD(A,B)=B，在此 Y 是某一个整数

A-B=C 给了我们：

- X·GCD(A,B) - Y·GCD(A,B) = C
- (X - Y)·GCD(A,B) = C

因此我们看到 GCD(A,B) 可以整除 C。

这个证明的图示如左下图所示：



证明 GCD(B,C) 可整除 A

GCD(B,C)，据其定义，可以整除 B。因此，B 必须是 GCD(B,C) 的某一个倍数. i.e. M·GCD(B,C)=B，在此 M 是某一个整数

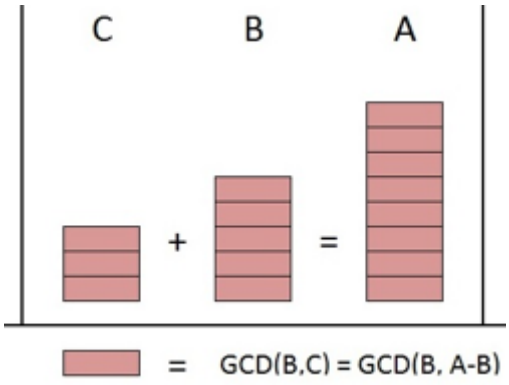
GCD(B,C)，据其定义，可以整除 C。因此，C 必须是 GCD(B,C) 的某一个倍数. i.e. N·GCD(B,C)=C，在此 N 是某一个整数

A-B=C 给了我们：

- B+C=A
- M·GCD(B,C) + N·GCD(B,C) = A
- (M + N)·GCD(B,C) = A

因此我们看到 GCD(B,C) 可整除 A。

这个证明的图示如下图所示：



GCD(A,B)=GCD(A,A-B) 的证明

- GCD(A,B)，据其定义，可整除 B。
- 我们证明了 GCD(A,B) 可整除 C.
- 因为 GCD(A,B) 可整除 B 和 C 它就是 B 和 C 的公约数。

GCD(A,B) 一定小于等于，GCD(B,C)，因为 GCD(B,C) 是 B 和 C 的 “最大” 公约数

- GCD(B,C)，据其定义，可整除 B。
- 我们证明了 GCD(B,C) 可整除 A.
- 因为 GCD(B,C) 可整除 A 和 B 它就是 A 和 B 的公约数。

GCD(B,C) 一定小于等于 GCD(A,B)，因为 GCD(A,B) 是 A 和 B 的 “最大” 公约数

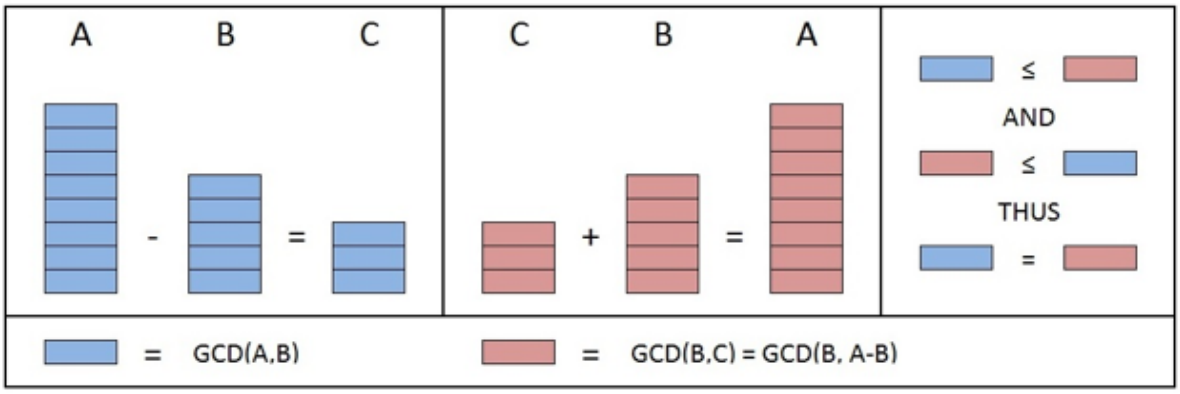
已知 GCD(A,B)≤GCD(B,C) 和 GCD(B,C)≤GCD(A,B)，我们可以总结为：

GCD(A,B)=GCD(B,C)

这相当于：

GCD(A,B)=GCD(B,A-B)

这个证明的图示如右下图所示：



GCD(A,B) = GCD(B,R) 的证明

我们已经证明 GCD(A,B)=GCD(B,A-B)

这些项顺序不重要，因此我们可以说 GCD(A,B)=GCD(A-B,B)

我们可以重复应用 GCD(A,B)=GCD(A-B,B) 来得到：

GCD(A,B)=GCD(A-B,B)=GCD(A-2B,B)=GCD(A-3B,B)=...=GCD(A-Q·B,B)

但是 A= B·Q + R ，因此 A-Q·B=R

因此 **GCD(A,B)=GCD(R,B)**

这些项的顺序不重要，因此：

GCD(A,B)=GCD(B,R)