欧几里得算法证明：

gcd(a,b)=gcd(b,a mod b)

证明：a可以表示成a = kb + r，则r = a mod b

假设d是a,b的一个[公约数](http://baike.baidu.com/view/58629.htm" \t "_blank)，则有

d|a, d|b，而r = a - kb，因此d|r

因此d是(b,a mod b)的公约数

假设d 是(b,a mod b)的公约数，则

d | b , d |r ，但是a = kb +r

因此d也是(a,b)的公约数

因此(a,b)和(b,a mod b)的公约数是一样的，其最大公约数也必然相等，得证

扩展欧几里德算法

基本算法：对于不完全为 0 的非负整数 a，b，gcd（a，b）表示 a，b 的最大公约数，必然存在整数对 x，y ，使得 gcd（a，b）=ax+by。

证明：设 a>b。

　　1，显然当 b=0，gcd（a，b）=a。此时 x=1，y=0；

　　2，ab!=0 时

　　设 ax1+by1=gcd(a,b);

　　bx2+(a mod b)y2=gcd(b,a mod b);

　　根据朴素的欧几里德原理有 gcd(a,b)=gcd(b,a mod b);

　　则:ax1+by1=bx2+(a mod b)y2;

　　即:ax1+by1=bx2+(a-(a/b)\*b)y2=ay2+bx2-(a/b)\*by2;

　　根据恒等定理得：x1=y2; y1=x2-(a/b)\*y2;

这样我们就得到了求解 x1,y1 的方法：x1，y1 的值基于 x2，y2.

　 上面的思想是以递归定义的，因为 gcd 不断的递归求解一定会有个时候 b=0，所以递归可以结束。

扩展欧几里德算法应用

1.求解不定方程

对于不定整数方程ax+by=c，求解满足其方程的整数解。

对于不定整数方程ax+by=c，若 c mod gcd(a, b)=0,则该方程存在整数解，否则不存在 x , y 整数解。（很明显，因为a mod gcd(a, b)=0 && b mod gcd(a, b)=0）

x 的答案 ，应为下面代码函数中返回值 x 再乘上 c / gcd(a, b);

同样 y 的答案 ， 应为下面代码函数中返回值 y 再 乘上c / gcd(a, b);

根据算法，所得到的 x , y 是其中一个解，而其他整数解则满足：

x(i) = x + b/Gcd(a, b) \* t

y(i) = y - a/Gcd(a, b) \* t (其中t为任意整数)

乘法逆元

定义：

满足a\*k≡1 (mod p)的k值就是a关于p的乘法逆元。要求a和p互质，想下为什么！

为什么要有乘法逆元呢？

当我们要求（a/b） mod p的值，且a很大，无法直接求得a/b的值时，我们就要用到乘法逆元。

我们可以通过求b关于p的乘法逆元k，将a乘上k再模p，即(a\*k) mod p。其结果与(a/b) mod p等价。

证：（其实很简单。。。）

根据b\*k≡1 (mod p)有b\*k=p\*x+1。

k=(p\*x+1)/b。

把k代入(a\*k) mod p，得：

(a\*(p\*x+1)/b) mod p

=((a\*p\*x)/b+a/b) mod p

=[((a\*p\*x)/b) mod p +(a/b)] mod p

=[(p\*(a\*x)/b) mod p +(a/b)] mod p

//p\*[(a\*x)/b] mod p=0

所以原式等于：(a/b) mod p

Ax + by = 1

X为a关于b的乘法逆元