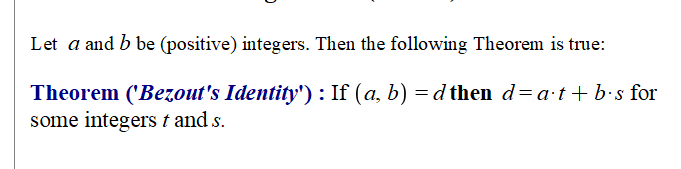
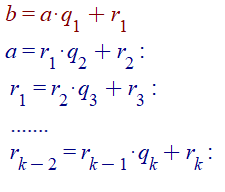
Bezout identity

如果a与b是整数，那么必然有

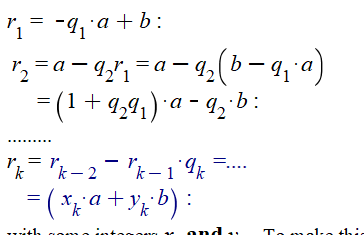


如果ab有公因数，那么d=a\*t+b\*s对某些整数ts

是由euclid算法推导出出来的



上面的是euclid 算法

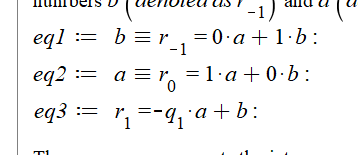


R放到左边，ab放右边，最后r总能得到一个系数的a+一个系数的b

以上是大概思路

具体解题思路

两个基本式



B=0a+1b

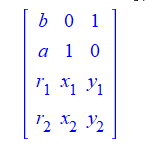
A=1a+0b

R1=-q1a+b

我们怎么求第三行第四行？

Ba找iquo//就是a\*一个最大倍数然后能接近b，然后让下面一行乘以这个系数，上面一行与之相减

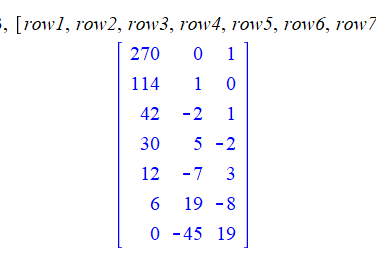




这整个matrix叫做EEA

一直求到rk=0





Rk=0的上面一行就是我们们要求的，6就是最大公因数，19就是a=系数，-8就是b系数

因此270与114最大公因数为6

6=19\*114-8\*270

推论：

两个数字ab coprime互质，当且仅当存在整数r与s让ar+bs=1



证明，让a与b互质，那么



那么根据bezout性质

是成立的

反过来：如果ar+bs=1但是ab的最大公因数d>1，那么a=da1,b=db1,推出 d(a1r+b1s)=1,这是不可能的因为ar1b1s不是0.几的数

，因此d必然等于1

推论：



如果c 是a的因数，c是b的因数，那么c也是ab最大公约数d的因数

证明：

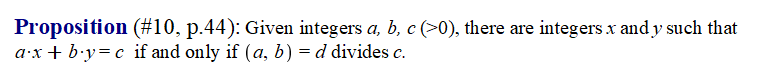
推论

如果a是bc的因数，且ab互质，那么a是c的因数



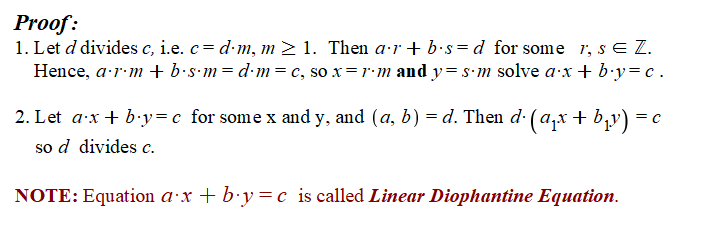
Diophantine equations

基于benzout’s identity theorem,我们可以证明一个重要命题proposition



有整数abc>0,必然存在ax+by=c如果ab最大公约数d是c的因数

证明



反证：如果d divide c,那么c=dm, 然后又因为ax+by=d//benzout,整合一下就行

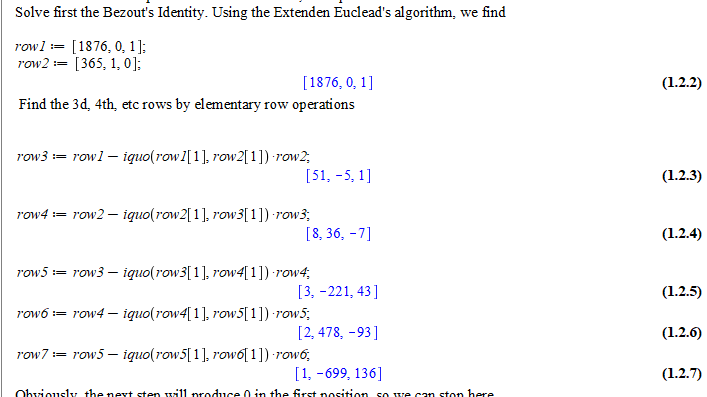
顺正。如果ax+by=c，且ab有最大公因数d，那么d(a1x+b1y)=c, d divides c

例题：找到365，1876的最大公因数

解法1

找到row1, [1876 0,1]

row2 [365,1,0]



猛减，下一步显然是0没必要了，我们就知道了

1=-699\*365+136\*1876

问题是



乘24就好

第二种解法：



其实我们求到第四行就好

因为这时余数8已经是24的因数了

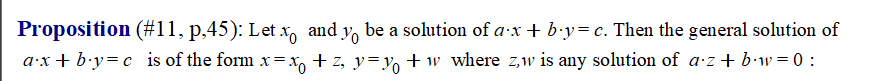
但这样我们求到的解就是



那么问题来了：一共有多少解，通解是什么

理论11

如果让x0与Y0代表ax+by=c的其中一组解，那么通解关于ax+by=c的形式永远是x=x0+z,y=y0+w, 只要zw满足关系az+bw=0



证明：

让xy与x0y0代表两组解



两式相减

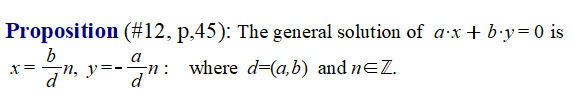


因此z=x-x0,w=y-y0

完美满足az+bw=0

理论12

Ax+by=0的通解



D是ab最大公因数，

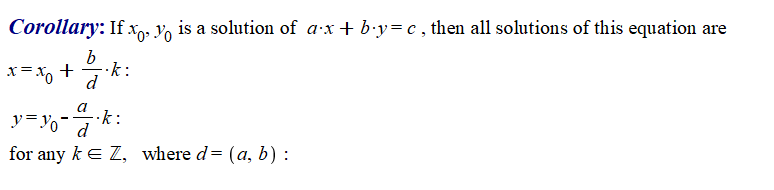
证明：

A=a1d,b=b1d

因此a1x+b1y=0

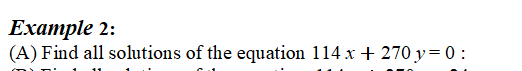
因为a1与b1必然互质所以a1/b1所以x必然等于nb1=nb/d，y是-na1,

推论，（基于理论1112）如果x0y0是ax+by=c的一组解



K是任意整数

例题：



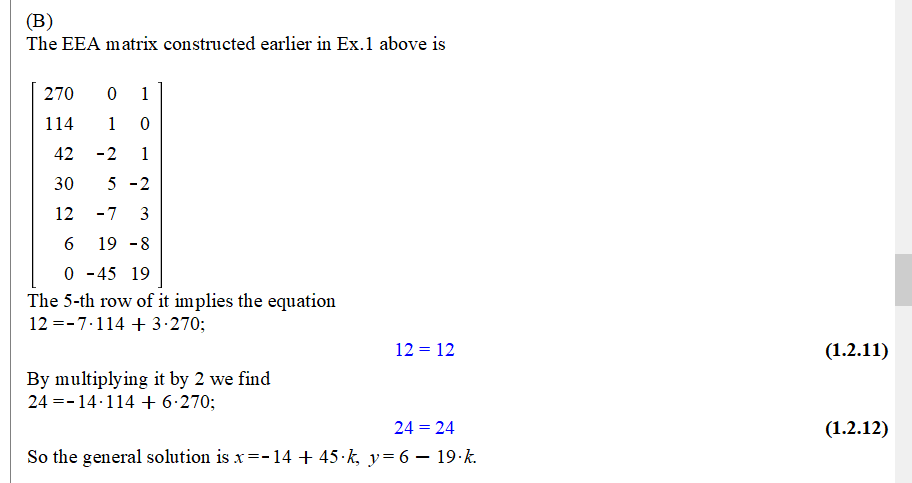
理论12

114与270最大公因数=6,

19x+45y=0

X0=45k,y0=-19k





找到第五航，得到24

然后利用11+12推论就能得到通解

第四章：

Induction theorem

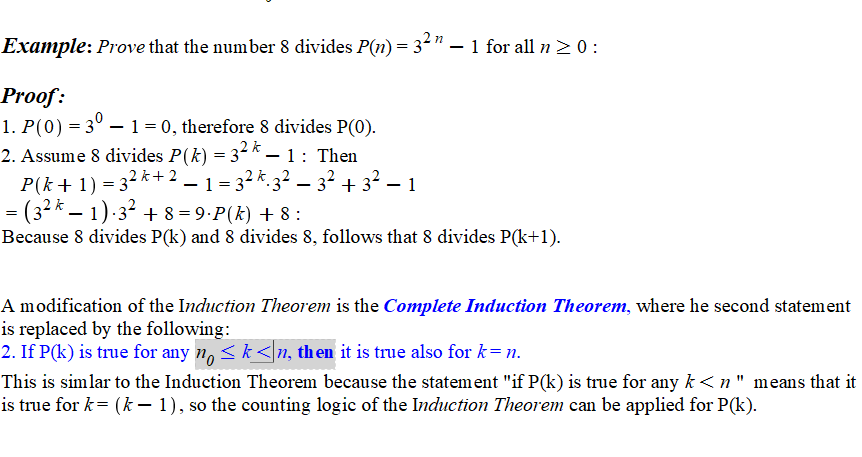
让P（n）是一个对于任意大于n0的整数n都成立的命题

那么P(n)成立挡一下两个命题成立：

P（n0）是true

如果P（n）true对于某些对于n0的n，那么P（n+1）也是true

证明

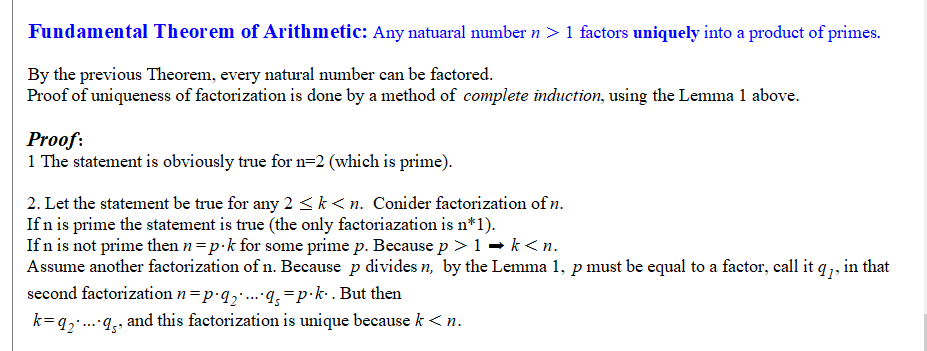


这里的格式注意使用了P（0）

1.P(0)成立

2.assume for all k<=n, P（k） is true, then p(k+1)

经典证明。任意大于等于2的自然数都能被唯一分解成一组质数相乘



基本当N=2，当然成立

格式：让statement be true for any 2<=k<n

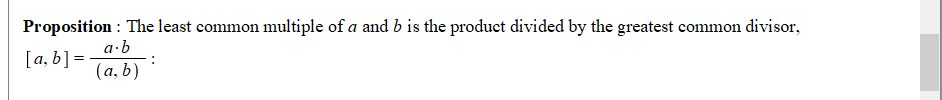
假设n是prime，那么这个推论是正确的

如果n不是prime。必然能分解成p.k,且p是某一质数，

Least common multiple

Common multiple：公倍数，如果a devide c, b devide c

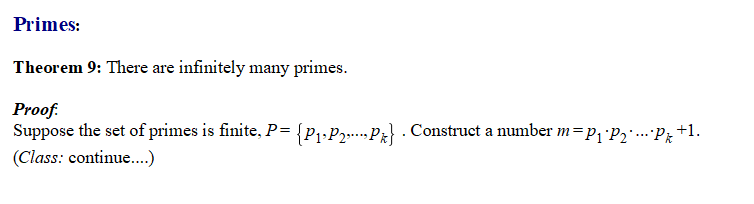
最小公倍数求法：

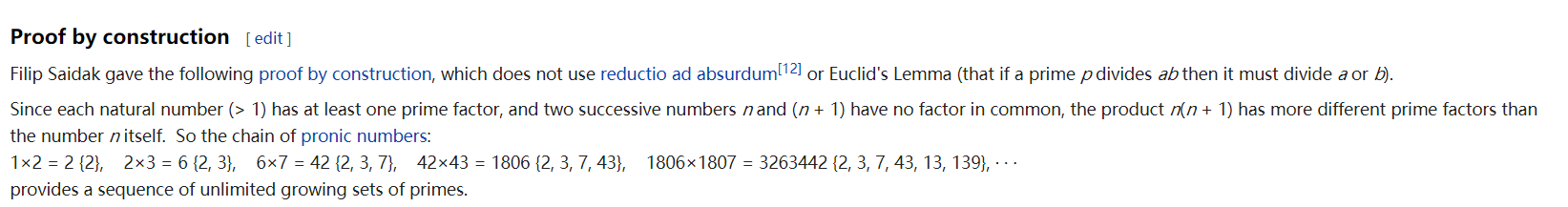


乘积除最大公因数

理论：

有无数个prime，





证明：假设是有限的，那么下一个number就是有限所有集合相乘+1, 那么这两个数必然是互质的，因此两个数没有一个公因数，而前一个连乘数是由多个质数撑起来的，那么下一个数必然是质数