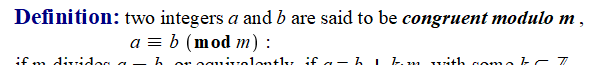
Congruence:

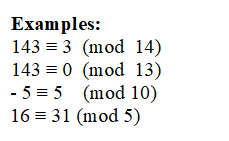


两个整数a与b被认为是全等的（congurent 三条线）当他modulo(mod)m的时候

表达方式为a=b(mod m)

当m divides a-b或者 a=b+km

也就是第一个数减第二个数是mod里的倍数



换种理解，a mod m=b mod m

所有integer都被认作是congruent如果modulo 1，所以通常来说modulus m应该是一个大于等于2的自然数

一个congerunce '≡'符号被认作是equivalence relation， 因为它满足三个性质

因此congruence modulo m把整数切割成了多个equivalence classes（这里也叫做Congruence class）,

我们用Rm来表示着所有的equivalence classes

, 每一个数字代表一组equivalence class,而且这个数通常来说是小于m大于等于0的数 （例如5 mod 7）

Proposition 1:

当m>=2, 任意整数a 与且只与Rm中的一个数是congruent modulo m

定义：在Rm set中的这个代表了a 除以m 余数的这个数，叫做least non-negative residues of a(mod m)//residues 余数

Proposition 2: a≡b (mod m)当且仅当 a mod m= b mod m//很好理解

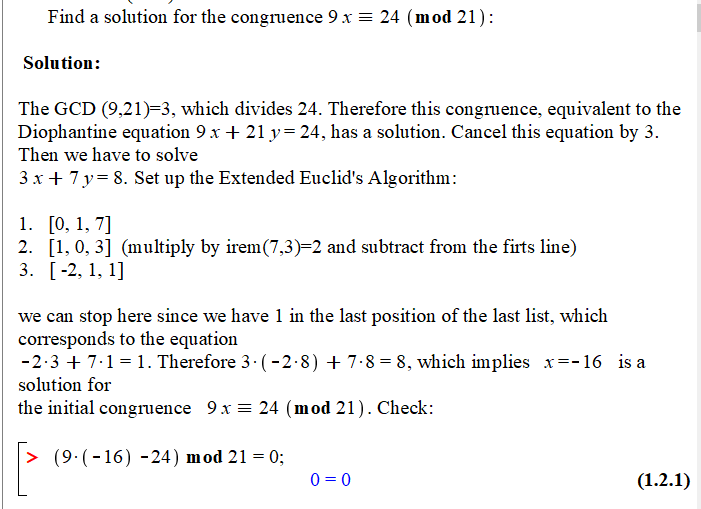
Linear Congruencies and Bezout’s identity

Proposition 18: a\*x≡b(mod m)有解当且仅当(a,m) divides b

证明：我们需要找到ax=b-ym的一组xy解，也可以写成城ax+my=b

根据proposition 10，这个diophantine equation有解当且仅当（a,m） divides b

例题：



找到这样的一个解

第一步，找amGCD，check是不是divides b,

然后转换式子9x+21y=24

同除公因数，

3x+7y=8

然后利用extended Euclid algorithm

这里3x+y7=8有点难看

8=3x+7y

[7,0,1]

[3,1,0]

[1,-2,1]

1=-2\*3+1\*7

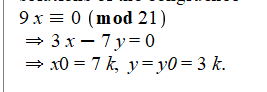
8=-16\*3+8\*7

X=-16

9(-16)-24 mod 21=0

基础解为-16

然后我们这时不看24来知道他的循环效率



(9x-0)=21y

3x-7y=0

因此x=7k，7k就是循环速率

X=-16+7k

Proposition 19

如果（a,m）=1，那么ax≡1(mod m) 有一个单独解

System of Congruences

问题：找到一个数字a，让a=s1(mod m1)且a=s2(mod m2)

这个问题可以被看作

a=s1+km1

a=s2+pm2

推出

s1+km1=s2+pm2

转换成标准形式

m1X+m2Y=s2-s1

X代表K，Y代表-p

这个方程有解consistent 当且仅当 d=(m1,m2) devides (s2-s1)

例题：找到一个number

A≡1（mod3）且a≡4(mod 6)

A=1+3k=4+6p

3k-6p=3

最大公因数3 divides 3

k-2p=1

有无穷多解

随便找一个

K=1，p=0

A=4

Basic properties of congruences //congruence的基本性质

Proposition 4:让abcdkn都属于整数，m是一个自然数

(A)乘法定律

如果a≡b(mod m)那么ka≡kb(mod m)

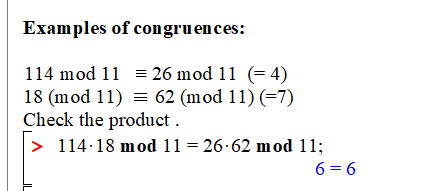
(B)加法定律

如果a≡b(mod m)而且c≡d(mod m)那么a+c≡b+d(mod m)

(C)乘法定律2

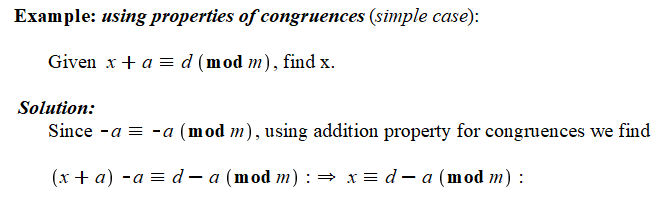
如果a≡b(mod m)且c≡d(mod m) 那么ac≡bd(mod m)

例子



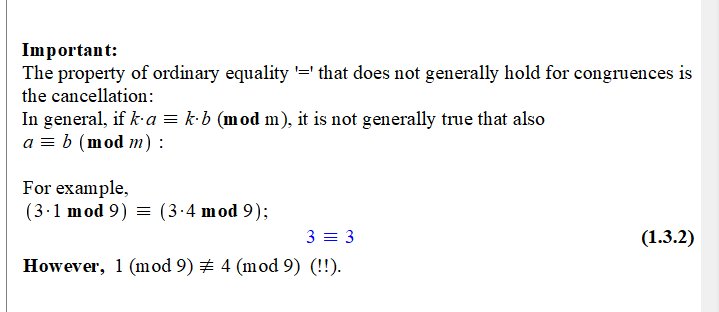
注意这里虽然mod完以后一个是4一个是7，但运用的基础在于mod的数 ，都是11

例题：



-a≡-a mod m，然后相加就行

然而不能完全把四则运算规律运用到≡上，例如除法



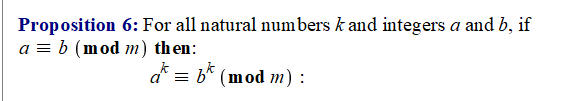
1 mod9不等于4 mod9

Proposition 5



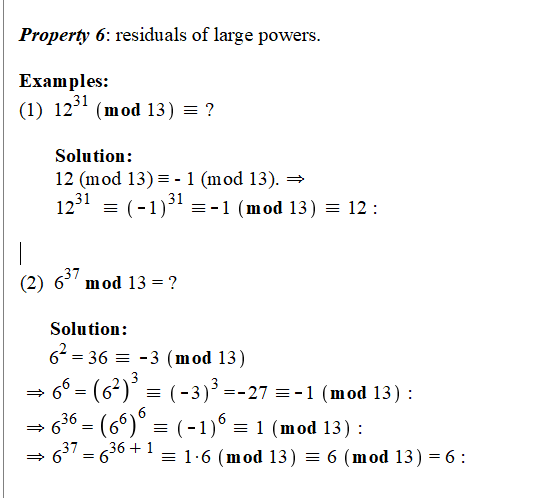
如果a≡b(mod m)且d divides m,那么a≡b(mod d)

Proposition 6:



如果a≡b(mod m)那么a^k≡b^k(mod m)

利用性质6的例题



注意只要K是自然数就好，a与b可以是负数

就是找到基本的12

然后转换到相对小的一个基本数

再利用性质6

Proposition 16:

如果ra≡rb (mod rm)那么a≡b(mod m) //≡的除法定律

Proposition 17

如果ra≡rb (mod m) 且(r,m)=1那么a≡b(mod m)

CH6 congruence Class

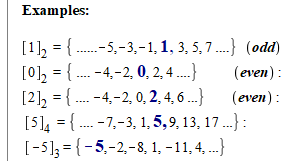


≡是一个equivalence relation关系

因此它能将整数集Z切割成多个c lass

每一个不同的class叫做congruence classes module m 记作[a]，

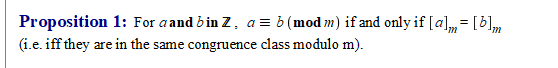
[a]m={a+km|k属于Z}



congruence class可能看起来不同，但是实际上是一样的



Proposition 1:对于a与b在整数Z中，a≡b（mod m）当且仅当[a]m=b[m]



意思是只有在一个congruence class里的才能a=b(modm)

定义



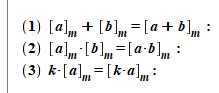
Z/mZ代表着一组set由congruence class构成

例如Z/3Z=

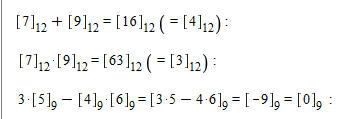


为什么-1也可以，因为实际上是2

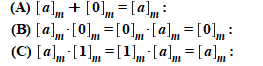
三大原则



//第三原则重要应用



注意[0]m与[1]m是特殊的



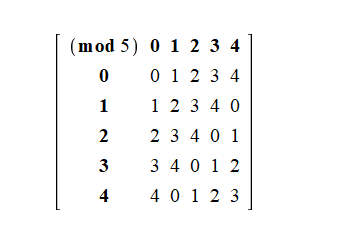
BC只是单纯的第二原则

A是第一原则应用

通过加法惩罚定律，我们可以建立

Table来表达Z/mZ也就是当限制在m个class时的四则运算定律，

例如addition table for m=5 on congruence classesZ/5Z

怎么看：横着的[0]m加上竖着的0[m]=0[m]

例子：casting out nines 去九法

我们可以利用加法的性质验一个数是否能被9整除

一个十进制的n+1位数可以表示为



例如123可以表示为1\*100+2\*10+3

然后我们用性质123得到

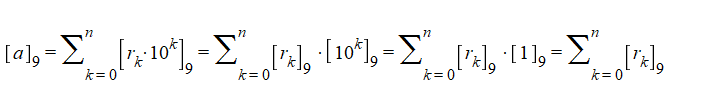


第一个等于是乘法定律

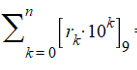
，第二个没用定律，就缩写，

第三个用了

因此



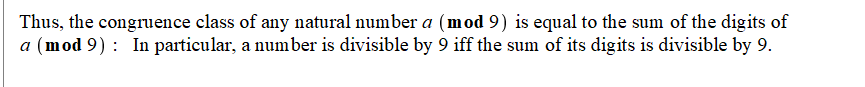
A就是一个十进制数，他可以表示成

这个用的是加法定律，即一群小数的mod相加可以等于他们的和的mod

然后乘法定律拆开

然后就照上面的换

然后你会发现a[9]等于所有位数mod9的和（字面上），实际先把所有位数相加，然后除以9





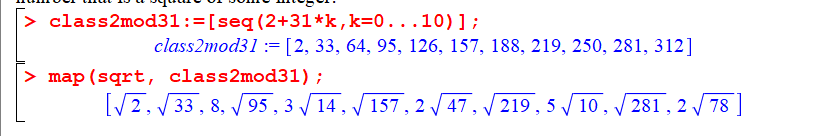
然后不停循环

虽然基本的congruence class 集合能够完整表达Z/mZ

但有时候适当的变换可以更方便的解决问题

例题，求解





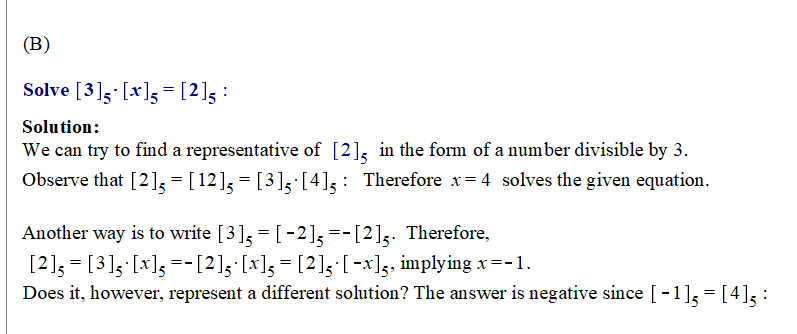
我们不可能说让x等于根号2根号33这样



可以得到一个解x=8



当然就现在为止我们的理论并不能得到一个通解，但通过适当转换我们能摸到一个解



我们可以让[2]5里的数变成3的倍数

即[12]5

然后12=3\*4

Complete sets of representatives

Definition：

如果一个set R, 让每一个整数mod m以后都能对应到有且仅有一个ri上，那么这个set就叫做complete set of representatives for Z/mZ。

注意complete sets of representatives与Z/mZ的区别



Z/mZ里的元素是class

Complete sets of representatives 是整数，代表了对应的set

换句话说如果我们已知了set R是complete set of representatives, 那么我们就能推导出对应的Z/MZ

complete set of representatives并不唯一两个都可以

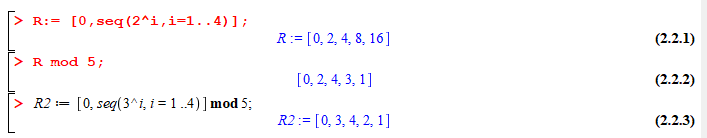
理论3：

如果m是一个质数，那么必然存在一个整数b(可能大于一个)，叫做primitive root modulo m, 让成为complete set of representatives for Z/mZ

例如



m=5,那么就能有2与3作为primitive roots

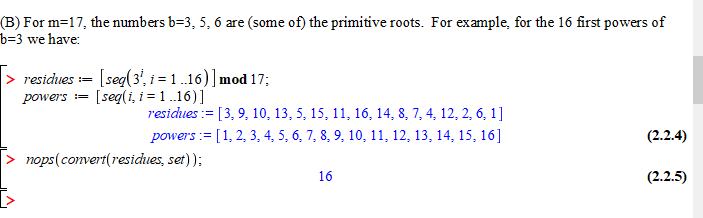


seq就是建立sequence ， 这里就是R={0, (构建seq，公式2^i,i的范围)}

第一步是给R赋值

R MOD5我们发现就是 标准的comlete set of representatives

因为R的构建过程就是0,b,b^2,b^3...



对于m=17,可以使3，5，6

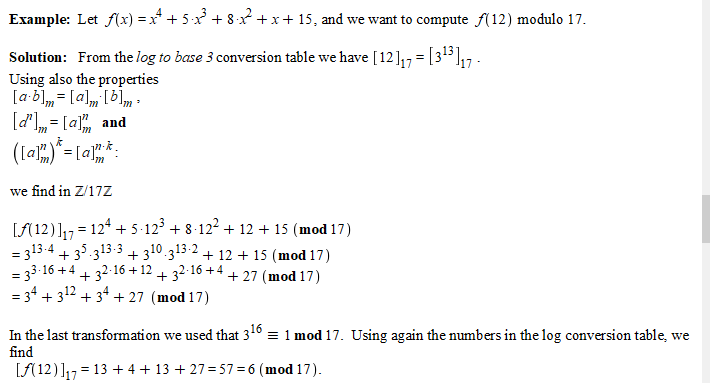
例如以3为例，我们构建seq mod 17

nops计算一个list、set里元素的数量

convert(a,set) 把a转换成一个集合

convert(a,list)把a转换成一个List

例题：



Units

对于任意除零以外有理数a我们都能找到了另一个有理数b，让a\*b=1

A与b被称作 inverse of each other， 倒数

然而对于整数来说，只有两个数字能找到另外一个整数让a\*b=1,这两个数就是1,-1, 1\*1=1

-1\*-1=1

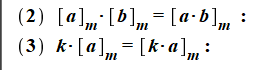
其他整数的inverse都是分数

那么对于mod计算又怎么说呢，我们试图找到a\*b=1(mod m)的解

Unit定义



有inverses的congruence class [a]m 叫做units

首先要注意的第一点：multiplicative identity，乘法性质

[1]m是和整数里的1最像，

其他任意congruence class都不能扮演这个角色，即乘另外一个congruence class后还是他自己

如果有一个[e]m 让[e]m\*a[m]=a[m] 那么[e]m只能是[1]m

那么在Z/mZ中，那些class有inverse哪些没有呢

这个问题要分析b\*a≡1(mod m)

这个问题的答案就相当于ba+km=1，利用benzout定律，当am已知，bk未知，那么根据benzout定律，(a,m)=1是有解的充分必要条件

因此Theorem5：

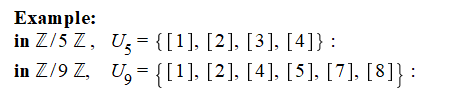


在Z/mZ中“ [a]m是一个unit当且仅当am互质

推论6,

Z/mZ中unit的数量等于最小正余数与m互质的数量（就[9]4的最小余数就是1）1,与4互质，成立

定义： 就是在Z/mZ中所有Units的集合



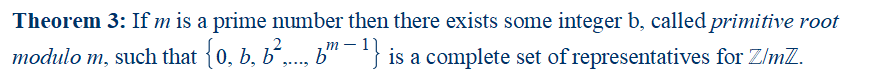
定义，Um中元素数量是一个function，叫做euler’s phi function

注意如果[a]与[b]都是Z/mZ中的unit,那么[ab]必然是一个Unit,因为没有公因数，反过来看也是一样的，如果[ab]是unit，那么a与b都是unit

理论

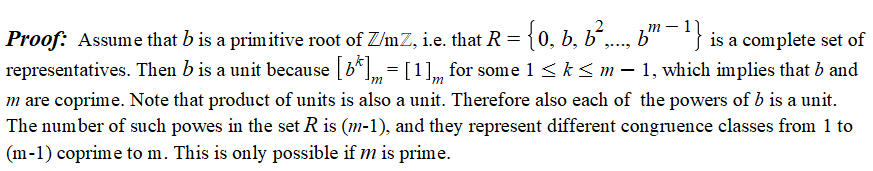


与这条理论结合看！



如果有primitive root,那么m必然是个质数

证明



如果b是prime root，那么对于某一个k，必然有[b]m对应的是[1]m，换句话说b^k与m互质，因此b与m必然互质，所以每一个b^k都是unit，而b一直到b^m-1

代表着123456789,…m-1，一个数与所有小于他的正整数互质，也就代表着这个数必然是Prime

利用unit我们很快就能找到



这样的解

我们注意到3与17互质，因此3是unit,我们找到他的inverse b这样就可以

[3][b][x]=[11][b]

这样3b会变成1

[1][x]=[11b]

X=11b

利用的是[1]\*任意x都是他自己的性质

[3]17的inverse是[6]17：怎么算的,[18]17=[1]17

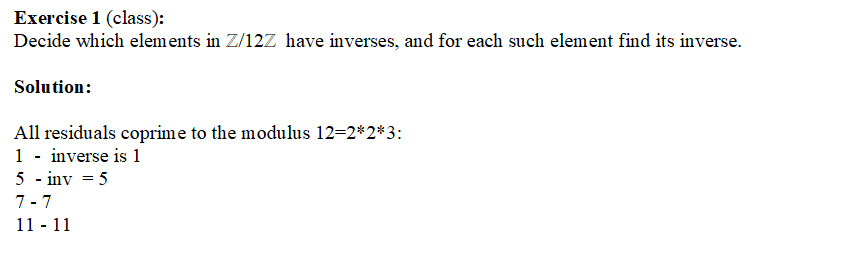
因此X=66=[15]17

解是唯一的

因为任意unit的inverse是唯一的，因此我们求得的b是唯一的，x=11b,因此x是唯一的

重要推论：

任意一个Zm内的Unit有且只有一个inverse



例题：找到Z/12中Unit与对应的inverse

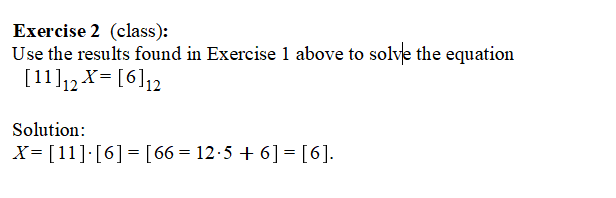
1, inverse是1

5. inverse是5

7, inverse 是7

11, inverse 是11

//怎么算的，unit找互质，inverse找乘以一个数然后除以12余1，通常从自己开始乘，

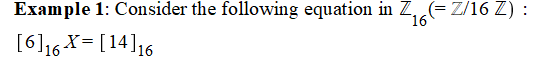


11找inverse就是11

[11][11]X=[66]

X=66=[6]

解决线性方程



显然6与16不互质因此我们不能用原来的方法

但是我们还是能找到解，通过观测

[14]16=[30]16

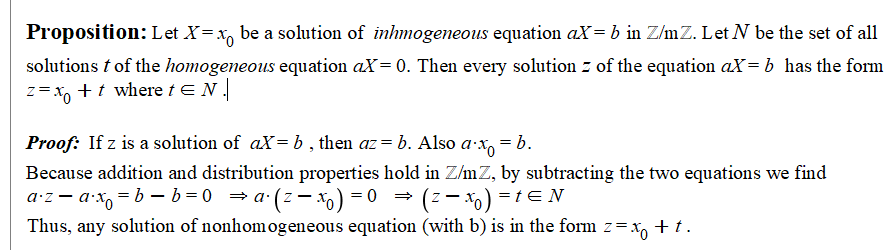
因此第一个解是[5]30

然而还有另外一个解，[14]16=[-18]16

因[-3]16也是一个解

如果不是互质，即Unit，X不止一个解

推论



Inhomogeneous equation aX=b, b不等于0

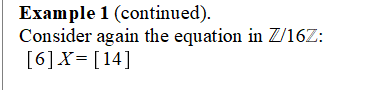
Homogeneous equation aX=0

如果X=X0是inhomogeneous的一个解，

让N为所有homogeneous equation 的解t的集合，那么 任意一个inhomo的解Z有着形式Z=X0+t

证明：如果z是一个解，那么az=b,那么ax0也等于b，因为根据性质,ax0-az=0

Z-x0=0



再解一次

我们能轻而易举找到第一个解

[5]

然后我们要找homo解集

[6]X=[0]

6X=16y

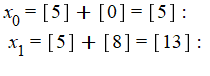
3x=8y

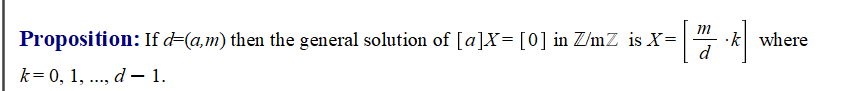
因为38互质，所以必然x是8的倍数，y是3的倍数

[X]16变成了[8k]16，在所有Z/MZ中，满足条件的情况是[0] [8]

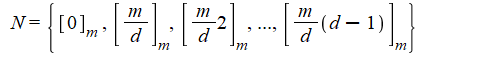
就是在[0-15]内所有的8k

因此



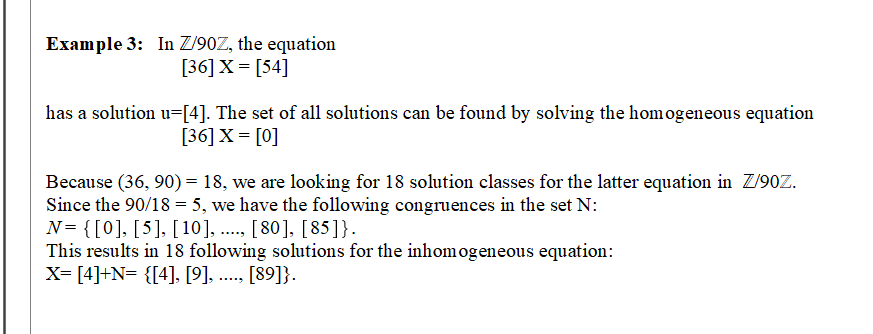


让（a,m）的最大公因数d，那么[a]X=[0]的通解是X=[mk/d]，k是0,1，….d-1



上题中m=16,a=6, d=2

通解就是8k



不互质，求Homo

D=18

通解为(90/18\*k)

=5K

在求个基础解，

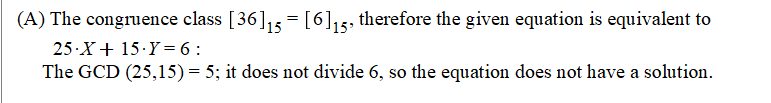
[54]90=[144]90

X=4

[4+5k]

例题





36转化为6

前者最大公因数为5，因此没有解