Ch3

理论：

1.Equivalence relation:reflexivity,自己与自己满足关系，symmetry，a与b，那么b与a，Transivity,a与b，b与c，那么a与c

2.division theorem: 非负数a>0,b>0,q大于等于0，r在0到小于a之间，那么必然存在b=q.a+r，b是几倍的a+余数，对于给定的a,b，qr将是唯一的

3.Euclid algorithm:找gcd(a,b),大的数字放左边，b=ka+r,a=k1r+r1…..不停循环直到m=k\*r+0,那个r就是我们要的最大gcd

4.Bezout identity/extended Euclid's algorithm:基于euclid算法，如果（a,b）=d，那么d=at+bs对于某一组整数ts(唯一)。

然后我们让

大数=0a+1b

小数=1a+0b

不停重复上面一个式子尽量减下面一个式子，让大数减k小数试图得到最小值

一直求到左边这个最小值等于0

然后上面一行就是我们要求的

d=at+bs

5.如果ab互质，有整数rs让ar+bs=1

6.如果c divides a 且c divides b，那么c divides (a,b)=d

7.如果a divides bc且(a,b)=1，那么a devides c

8.如果有integer abc，c大于0，那么ax+by=c 有解当且仅当(a,b)=d divides c ，ax+by=c又叫做linear diophantine equation,但是这个问题不止单独一组解

9.让x0,y0代表ax+by=c的一组解，那么通解的形式永远是x=x0+z,y=y0+w,只要zw满足az+bw=0

10.proposition:ax+by=0的通解永远是x=bn/d,y=-an/d, ，这里的d是（a,b）

11.基于8910，ax+by=c的通解为x=x0+bk/d,y=y0-ak/d, d=(a,b)

定义：

common divisor公因数

GCD great common divisor最大公因数

common multiple 公倍数

LCM least common multiple最小公倍数

本节总结：

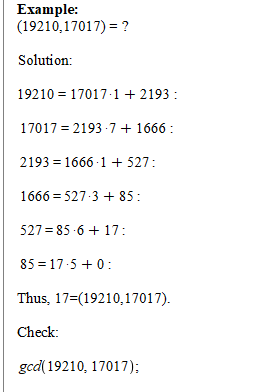
1.equivalence relation,检查是不是满足三个关系symmetry reflexivity transitivity

两个元素是equivalence relation(在一个equivalence class里)记做 a~b

2.Eulid algorithm：用来找gcd(a,b),大的数字放左边，

b=ka+r,

a=k1r+r1…..不停循环直到m=k\*r+0,那个r就是我们要的最大gcd



3.Benzout's identity & Extended Euclid's algorithm，也是求两个数最大公因数

基于性质如果（a,b）=d，那么d=at+bs对于某一组整数ts(唯一)。

先建立两个基准式子

b=0a+1b //b>a

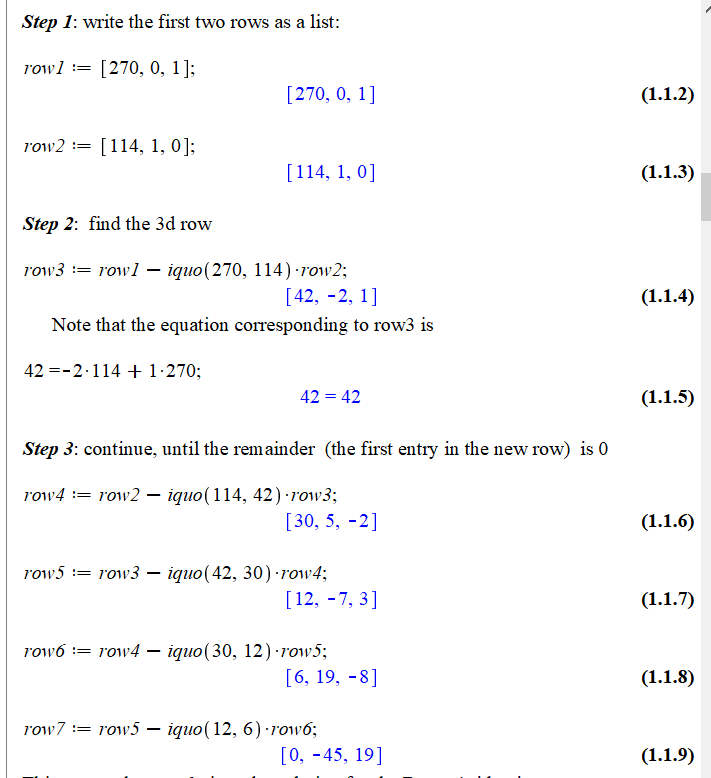
a=1a+0b

写法是[b,0,1]

[a,1,0]

然后不停的让上面的第一个数减k倍下面的第一个数，一直到第一个数为0，倒数第二行的第一个数就是最大公因数（0前面一行）

例如求270与114最大公因数



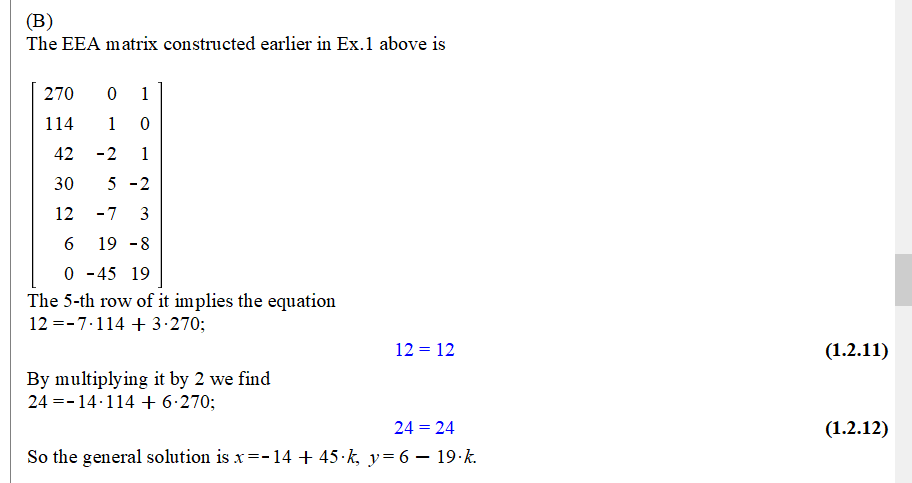
最大公因数是6

4.解决linear diophantine equation



核心是利用理论8

利用extended Euclid 找到114与270的公因数divides 24(不是最大公因数)



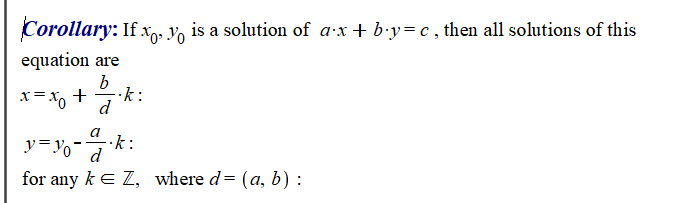
求到12的时候12是24的因数

因此12=-7\*114+3\*270

左右同时乘以2，得到xy基础解

x=-14,y=6（不是唯一解）

还要根据理论11





45=270/6

19=114/6

CH4

有无数个prime质数.

证明：

假设有限质数集P={p1,p2…pk}，我们利用它来构建一个数A=p1\*p2\*…pk,B=A+1 那么这两个数必然是互质的，因为他们的差只为1（如果ab互质，有整数rs让ar+bs=1

）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乘起来的，那么下一个数必然是质数

CH5

定义

1.congurent:：≡ 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) //换种理解，a mod m=b mod m

2.Equivalence class/congurence class: （Rm是equivalence class的总和，里面的元素是equivalence class）,可以表示所有的equivalence class,

记作

3.Least non-negative residues of a (mod m). 代表了a这个equivalence class的最小数

理论：

1.a≡b(mod m)等同于a=b+km

Congurent是equivalence relation,因为满足三个性质

Proposition 1:当m>=2, 任意整数a 与且只与Rm中的一个数是congruent modulo m

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

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

Proposition 19: 如果（a,m）=1，那么ax≡1(mod m) 有一个单独解

Proposition 4:让abcdkn都属于整数，m是一个自然数 //注意都是整数，因此乘法定律不能乘以一个分数（变相的除法定律）

(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)

Proposition 5: 如果a≡b(mod m)且d divides m,那么a≡b(mod d)

平方定律

Proposition 6: 如果a≡b(mod m)那么a^k≡b^k(mod m)

除法定律

Proposition 16:如果ra≡rb (mod rm)那么a≡b(mod m)

Proposition 17如果ra≡rb (mod m) 且(r,m)=1那么a≡b(mod m)

重点：

1.

求这类的答案的解

有解当且仅(a,m) divides b因为ax=b+(-k)m, ax+km=b，这个问题有解一定要让am最大公因数divides b

例题



第一步先check(a,m) 是不是divide b，有没有解

这里3divides 24有解

然后转换式子

9x+21y=24,

同除公因数

3x+7y=8,使用extended Euclid algorithm

[7,0,1]

[3,1,0]

[1,-2,1]

1是8的因数，停止

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

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

基础解x=-16

(9x+21y=24与3x+7y=8同解)

然后(9,21)=3,21/3=7

因此通解（看上一章最后一个重点）为-16+7k

2.

求一个数a，满足a=s1(mod m1)且a=s2(mod m2)

例题

这个问题可以被看作

a=s1+km1

a=s2+pm2

s1+km1=s2+pm2

m1k+m2p=s2-s1

这里k是x,p是y，这个问题有解当且仅当(m1,m2) divides s2-s1 //有无穷多解因为有两个未知数，你也能找到通解

例题

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

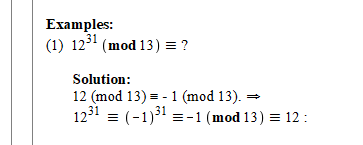
随便找一个

K=1，p=0

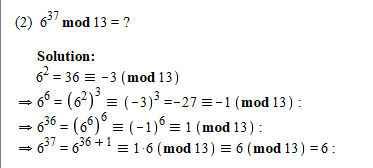
a=4

3.

解决large power，使用proposition6,a≡b(mod m)可以推出a^k≡b^k(mod m),



是利用好求的小的Power，来求出左边的a^k,不能大推小

可以一步一步推

总之点就是在找那个1或-1

6^2 mod 13= -3 mod 13

6^6 mod 13= -1 mod 13

6^36 mod 13= 1 mod 13

最后6 mod 13

CH6

定义

1.Z/mZ ，从1到m所有congurence class.的集合



2.Complete set of representatives: 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。 并不唯一，0到m-1也行，只要所有的都能对应到就行

注意两者区别，1里装的是class，2里装的是数字，

3.Unit



有inverses的congruence class [a]m 叫做units ,既[a]m\*b[m]=[1]m

4.Complete set of units: 记作在Z/mZ中所有Units的集合

5.Euler's phi function： 计算Um的元素数量的function

理论：

1:对于a与b在整数Z中，a≡b（mod m）当且仅当[a]m=b[m]

2: 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

3: 在Z/mZ中“ [a]m是一个 当且仅当am互质

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

5: 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

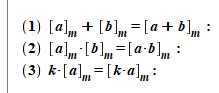
6.如果存在一个primitive root for a modulus m，那么m必然是质数

7. 如果X=X0是inhomogeneous equation aX=b(b≠0)的一个解，让N为所有homogeneous equation aX=0的解t的集合，那么 任意一个inhomo ax=b的解Z有着形式Z=X0+t

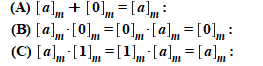
8. 让（a,m）的最大公因数d，那么[a]X=[0]的通解是X=[mk/d]，k是0,1，….d-1

9. 一个Unit有且只有一个inverse

计算规则：





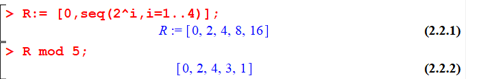


重点：

1.

这种题只要先把2转化成64，x就等于8

2.理论2，当m为质数时，找primitive roots



第一步，0，b,b^2,b^m-1 这几个数列成R，

然后再让这个list mod 5



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

查看有没有重复的

3.Unit的定义：有inverse的就叫做unit

[a]m 为Unit当且仅当a与m互质，**非常重要**

因此当我们发现[a]m是unit的时候，很容易解方程



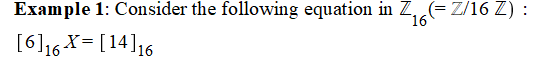
找到[3]的inverse[b]17，这里是[6]17

左右同乘[6]

[1]17 X=[66]17

X=[66]17=[15]17 解是唯一的,因为一个Unit只有一个inverse

4.解决线性方程（不是unit的时候）



显然6与16不互质因此我们不能用原来的方法

如果不是互质，即Unit，X不止一个解

（1）第一步找Homo齐次式的解集 //右边假设成0

[6]16X=[0]

6X=16Y

3X=8Y, X必然是8的倍数，满足的也就[0][8]

//这一步有更快捷的方法，直接让,d=(a,m) , 也就是16/(6,16)=8

（2）

如果X=X0是inhomogeneous的一个解 //基础解

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

上面的[0] [8]就是t

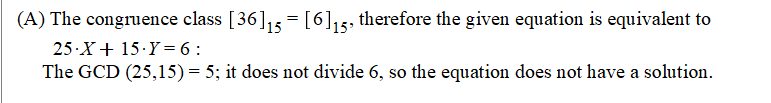
我们只要再找一个基础解就行 [5]



因此最终解为[5]+[0]=[5],[5]+[8]=[13]

(3)无解的情况





36转化为6

前者最大公因数为5，因此没有解

(系数,m) divides 右边的最简式

（6,16）=2 divides 14有解

(25,15)=5 不divides 6无解

U = {13, 14, [1], [2], [4], [7], [8], [11]}

CH7

定义:

1.Group :一个set具有以下五个axiom公理 //没有addition,只是为了接下来ring 写起来方便

**community** of addition : 交换律 3+5=5+3

**associativity** of addition: 加法结合律 (2+3)+4=2+(3+4)

additive **inverse**: 一个数a必然存在另外一个数b//-a 让a+b=0

additive **identity**/zero element //加法恒等数 ： additive identity 为0，任意a+0=a

**closure** under addition:任意a+b必然还是属于原set

2. ring：一个set R 拥有着加号+和乘号\*, 以及两个特殊element 0 与1 ，满足以下性质  可以被称作ring(with identity)

对于+号，只要满足group axiom 1到5， addictive identity是0，叫做zero element，

对于乘号，要满足以下四个性质

closure under multiplication：任意a,b属于set，a\*b仍然属于set,

associativity of multiplication :(a\*b)\*c=a\*(b\*c)

**multiplicative identity**: 1, 让1\*a=a\*1=a

distributivity of multilplication:分配率a(b+c)=ab+ac

这样就是一个标准ring

3.communtive ring， 在以上九条标准还满足community of multiplication a\*b=b\*a

4.Field: 在commutative ring的基础上额外加上两条性质

（a）在乘法中，任意一个数除了0都是invertible(任意a存在b让a\*b=1)

（b）F至少有两个元素

也等价于，如果F的unit集合包含了除零以外所有element,那么他就是field

5.在commutative ring内，一个元素被称作Unit，如果a\*b=b\*a=1  。a is a unit等价于a is invertible

6.Zero divisor: 如果有一个非零数a，在ring中存在一个非零数b，让a\*b=0, 那么这个数a叫做zero divisor ，ring a\*b不一定等于b\*a(因此b不一定是zero divisor)， 看是不是communitative  //b叫做a的codivisor

7. Order of unit a: 注意定理5，在commutative ring中，是乘法closure，任意unit的power仍然是unit，必然存在一个a^d=1, 这个d 就是order of unit a

定理：

1.一个group有且只有一个identity element e

2.在一个group内，任意element只有一个inverse

3.Z/mZ是commutative ring, [1]是multiplicative identity,[0]是additive identity

4.一个ring有且只能有一个additive identity与一个Multiplicative identity

5. 在任意commutative ring中， Unit集合 是乘法closure(任意两个数相乘仍然在集合中)

6. 在一个commutative ring R中，如果a≠0不是一个zero divisor，且a\*b=a\*c，那么b=c

7. 如果a不等于0且不是一个zero divisor在ring R中，那么无论b取什么值，a\*x=b最多一个解

8. 在一个·commutative ring R中，unit 不可能是zero divisor

9. 一个field没有zero divisor， 因为除了0以外都是Unit

10. 在Z/mZ中，任意【a】只能是以下三种情况的一种

(1)[a]是Unit当且仅当（a,m）=1

(2)[a]是zero divisor，如果1<（a,m）<m

(3)[a]=[0]如果(a,m)=m or a=0

11. Z/MZ是一个field当且仅当m是Prime的时候

12. 如果R是一个有限commutative ring，而a是R里任意非零element，那么a要么是·Unit，要么是zero divisor

重要定理：

1.Z/mZ必是commutative ring， 互质是Unit，不互质是Zero divisor , 要么[a]=[0]

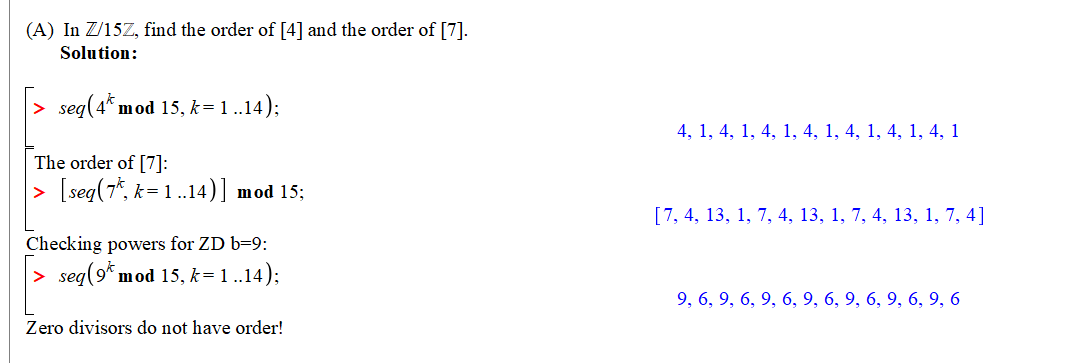
2.Z/mZ是field当m是质数

3.在commutative ring中，a要么是Unit，要么是zero divisor，因为a\*a^(-1)=1

a\*b=0

那么左右同乘a^(-1), 1\*b=0, b=0, 想做zero divisor必须乘一个不是0的数

4.Order of the unit a, 对于unit a 必然存在a^d=1, d就是order



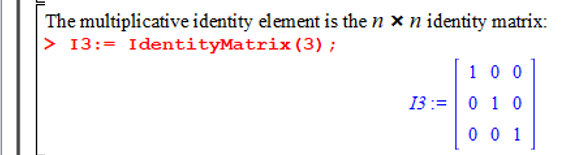
怎么找order， 就列sequence，找到k=几的时候是1

**zero divisor没有order**

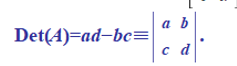
CH7.5 matrice as ring

定义：

1.Z/pZ,就是让矩阵里所有数mod p,Z/pZ天生就是一个Group，因为它完美满足五条加法定律，如果想让他进化成ring，必须让他行数列数相等，矩阵的乘法identity为identityMatrix



2.矩阵大部分情况下无法做到commutative ring， 因为A\*B!=B\*A

3.Determinants，写作Det(A),就是矩阵的值

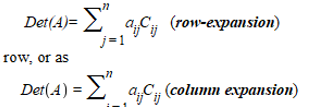
4.(ij)-th cofactor：就是切割的子矩阵，

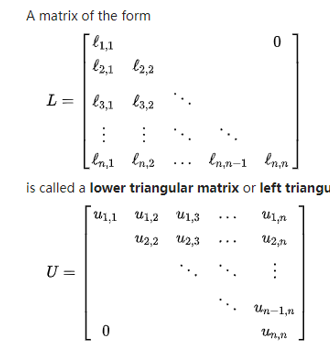
5.inverse matrix逆矩阵，逆矩阵乘原来的矩阵就是IdentityMatrix单位矩阵，maple里逆矩阵就是

6.Modular inverse of matrix, 就是原矩阵inverse以后进行mod操作，

理论：

1.cofactor expansion of the Det (A): 矩阵等于某一行或某一列子矩阵的和

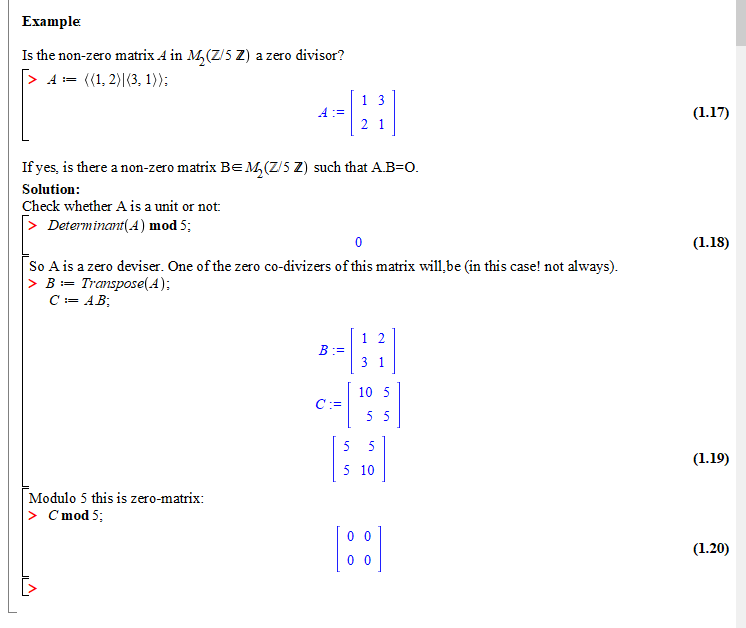


2.对于任何三角矩阵等于斜着的部分相乘

3.让一个矩阵所有的元素是[A]m (基于m的mod数)，如果Det(A) 为m的uinit，那么这个矩阵是Invertible的

重点：

1.一个矩阵是不是invertible，就看他的det 是不是mod数的unit



怎么确认一个matrix是不是zero divisor

Det(A) =5， 不是5的unit

CH8

看CH8精简版

CH9

定义：

order of A modulo m 。假设a是一个与M互质的数，那么 the order of a modulo m是**最小**的整数e，让

**Fermat's Theorem: 如果p是一个质数，且a是一个与p互质的整数，那么 //把p当做m更好记**

**Euler phi function**: //Um就是module m中unit的数量

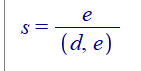
**Euler theorem**:对于Z/mZ中任意unit[a]满足

理论：

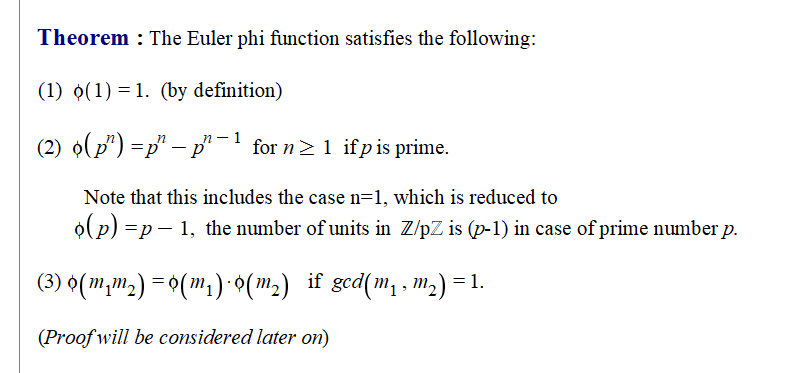
1.如果a与m互质，那么 对于1<=t<m 必然有解

2. ：如果e是order,且 ，那么e divides k

3. 如果e是a的order，那么对于a^d （另外一个基于a的整数） 的order s ,

 //根据基准数的order与基准数的power算出a^d的order

4.如果m是prime且不是a的因数，那么the order of a modulo m 是(m-1)的因数 //a与m互质且m是质数，那么order e必然是 m-1的因数

5. 

m=1那么根据定义就是1

如果p是质数，那么unit的数量为p^n-p^n-1

**注意：如果p是质数，那么phi p=p-1**

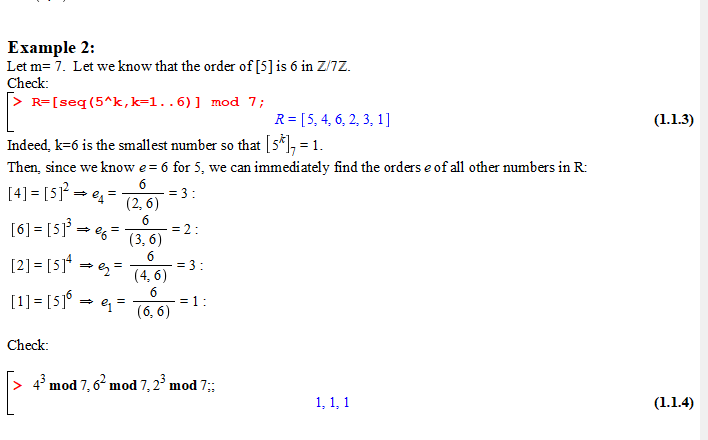
如果m1m2互质，那么他们的eulerphi可以拆解

重点：

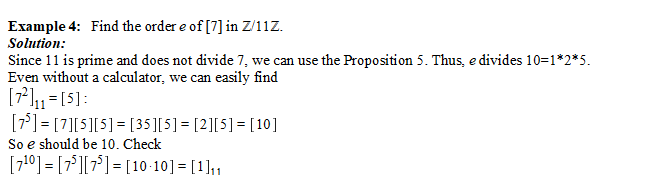
1.根据理论3，我们知道一个mod class的order，

因为5与7互质，所以其他的都是5的倍数，

然后e/(d,e)可以轻松知道其他的order



2.根据理论4，m是质数且am互质，那么order必然是m-1的因数，10的因数有125,一个一个测，求出order



**3.经典**

**证明****必然是整数**

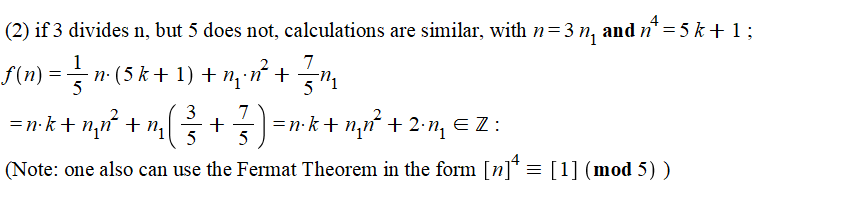
如果n是15的倍数，显然是一个整数，那么我们要考虑的就是n不是15的倍数

如果5 divides n，但是3不divide， 那么n=5m 且(n,3)=1 那么根据理论，p是质数且a与之互质，那么 必然有解，那么n^2=3k+1,

然后分解，原式子等于625^m^5 + 5m/3 \*(3k+1)+7m/3

=625^m^5+5m\*k+12m/3

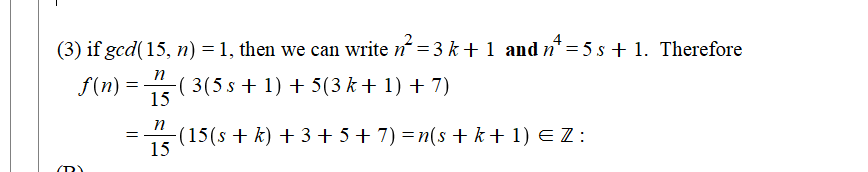
=625^m^5+5mk+4m



再假设3 divides n

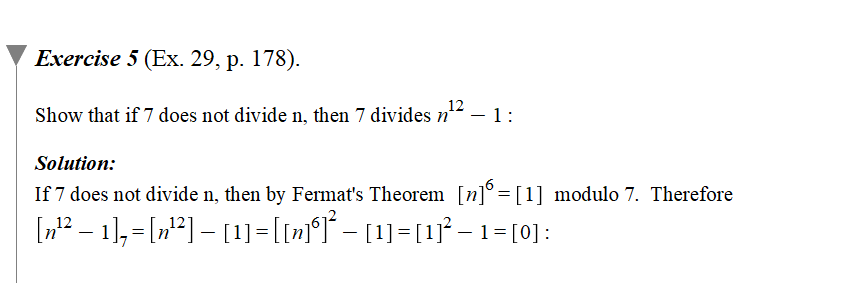
同理

最后要考虑与非15因数，



3k+1与5s+1是根据fermat theorem得到的

4.

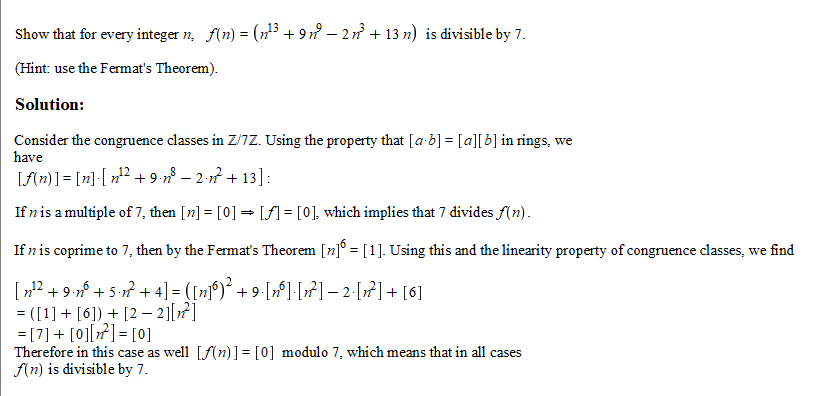


7不divide n代表n7互质

n^6≡[1] mod 7

n^12≡[1] mod 7

5.证明多项式divisible by 7



1.如果n是7的倍数，必然成功

2.如果n与7互质，

那么n^6≡1 mod 7  
原来的式子=[n][n^12+9n^8-2n^2+13]

这个式子mod7可以拆解

右边等于[1]+9[n^2][1]-2[n^2]+[13]

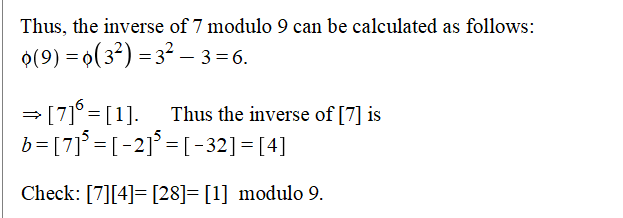
=[14]-[7n^2]

定然mod7

6.利用Euler Theorem找到 unit的inverse



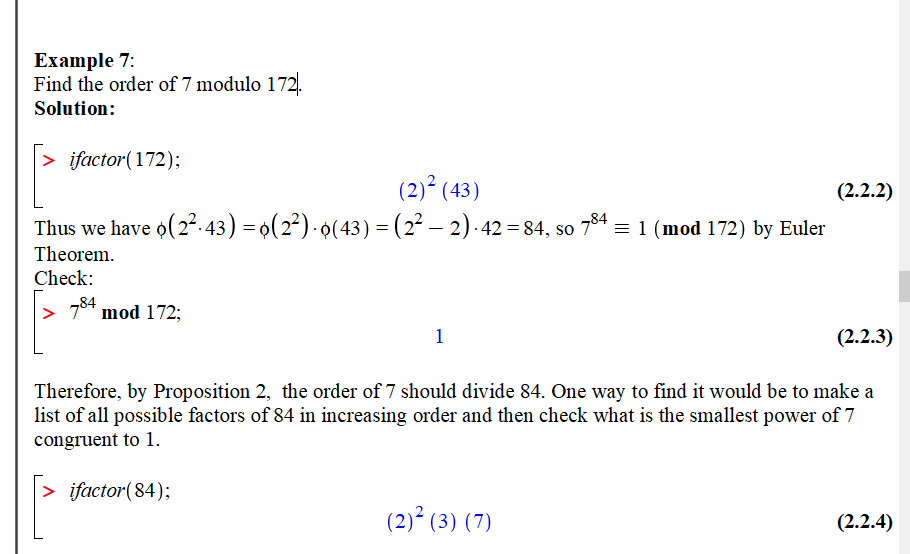
他的inverse必然是a^(φm-1)



9是3的平方，3是质数，所以phi9等于3^2-3=6

因此他的inverse就是a^5=[7]^5

7.找到大power的order



先因式分解，然后Unit数量就等于两个相乘=4-2\*42=84 , 因此7^84 全等于1(mod 172)

因为他们互质，

2^2的Phi等于2^2-2=2 \*42, 因此根据euler theorem， 7^84 mod 172=1, 然后必然是84的因数

8.计算，且n与m都特别大的时候



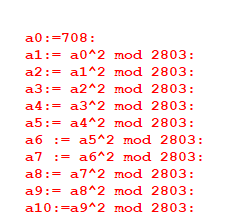
第一步把n转化成二进制



因此1463=1+2^1+2^2+2^4+2^5+2^7+2^8+2^10 //二进制要倒着看

，power加法

然后利用for loop，计算



每次在前一个的基础上平方mod 2803

最后我们pick所需的aX



CH4

Definition:

1. Factorization: 积分，把一个自然数分解成一串质数prime的乘积

2.pi(x)，代表着小于等于x的质数的数量，maple的用法是with(numtheory) :以后pi(10)=4



3.Trial Division, : 就是从最小的质数开始尝试，2357一个一个试，如果商为整数，那么下一轮从a1=a/p1,开始， 尝试的质数也是p1(上一次终结的那个)，一直重复这一过程直到约分完毕，但是我们需要知道质数列表

4.Sieve of Eratothenes, 最简单的得到质数列表的方式，先列出所有数，让这个集合乘以2，取交集，再取里面第二个数，乘，取交集，一直循环，直到 ≤根号n，

5.RSA cryptography:

首先回忆两个原则，

Fermat theorem:如果p是prime，那么a^p≡a(mod p) 对于每个整数a

如果m是一串不重复质数p1p2p3..的乘积，那么假设λ(m)=LCM(p1-1,p2-1,p3-1)



得出我们要的推论：如果m是一个squareFree integer,那么对于任何a与k

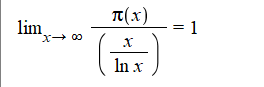
这里的phi(m)是 euler phi function里的

Theorem:

1. Fundamental Theorem of Arithmetic:任何自然数都可以分解成一系列prime的乘积，且这个factorization是唯一的//ifactor(123123)

2.Euclid's theorem,有无数prime，就是那个加一法，详见lec7，不重要

3.Hadamant &de la Vallee poussin，但x趋近于无穷大的时候， pi(x)接近x/lnx



4.对于对于任意x大于1，pi(x)<1.10555\*(x/lnx

)

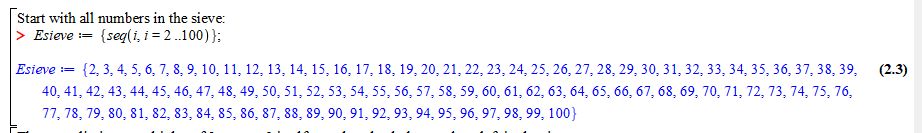
5.对于任意x大于17，pi(x)>=x/lnx



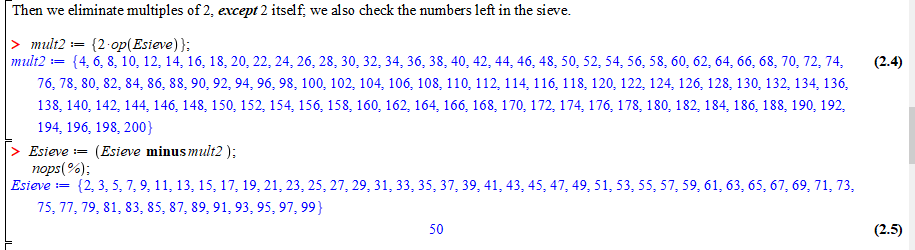
重点：

1. Sieve of Eratosthenes 求质数 //下面一长串不用看，看简化version

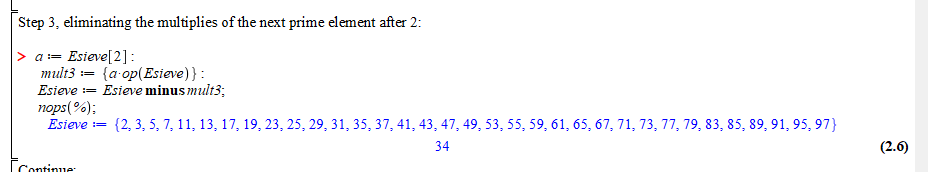
第一步：列出集合，2到n

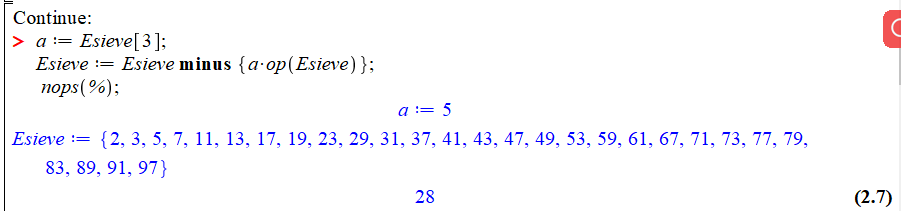


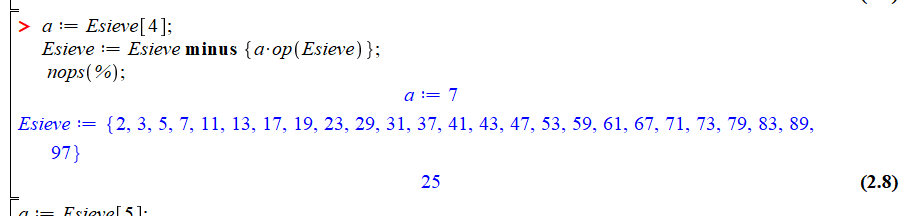
第二步，消去2的倍数，使用的是minus，

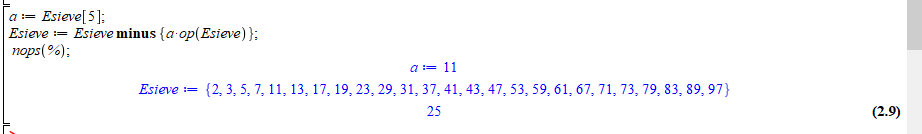


第三部开始循环，



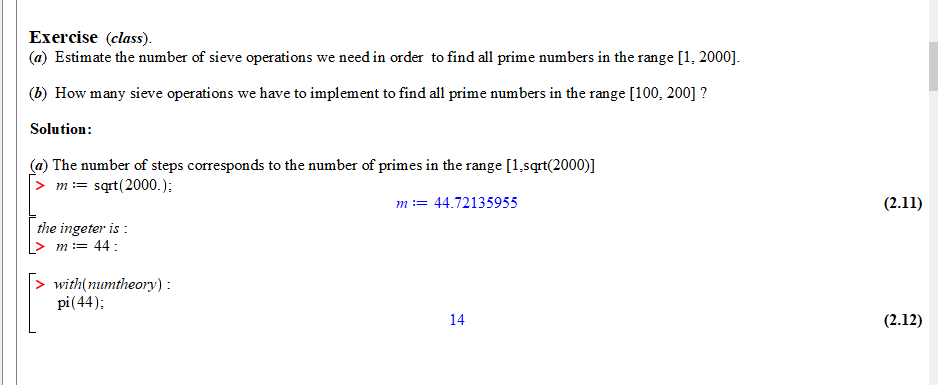






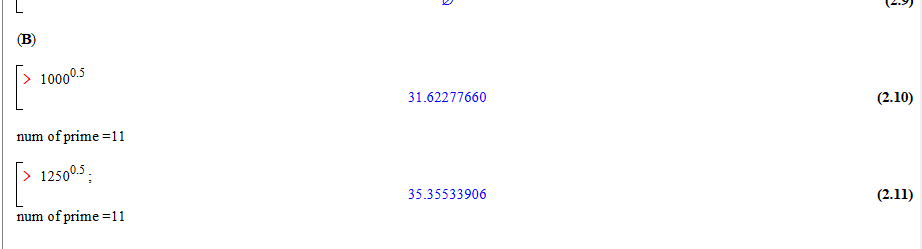
只有p小于等于根号 m就可以停下了， p就是这里的a,根号m是10，也就是说我们其实不用测11

so我们测得#step数量必定小于等于最大数根号



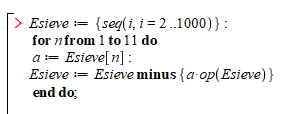
以上方法算比较麻烦的，

最好的方法是使用for loop

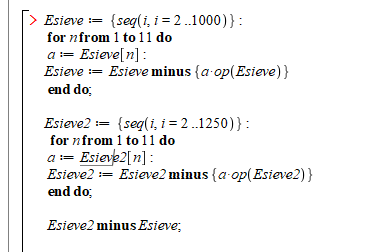


根号0.5求出最大的数也就是31，pi(31)=11

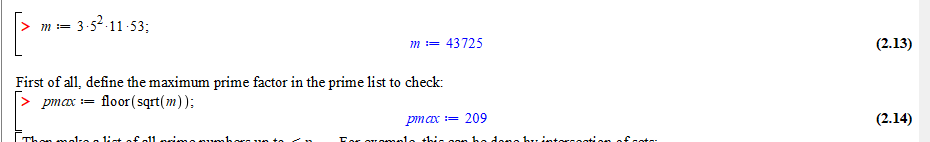
然后就可以

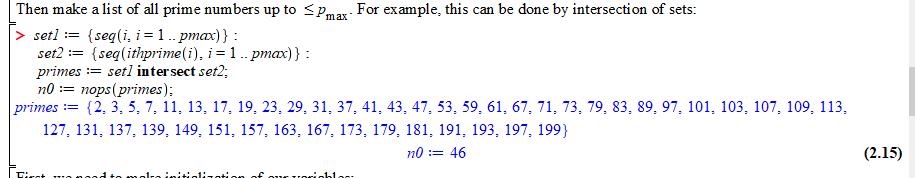
ASSIGNMENT4

问你一个区间内【1000到1250】



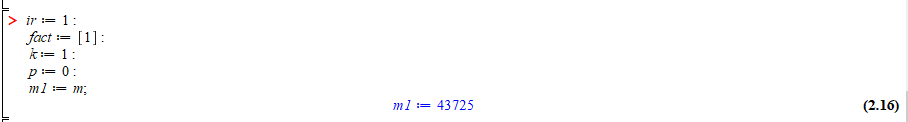
2.Trial Division





如果它让你用Ithprime，直接可以用ithprime， 如果不让，你自己esieve

然后初始化

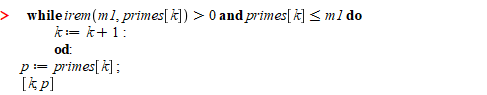


fact:factor的意思 ，所有prime因数的集合

k:第几个质数

m1：当前被除数

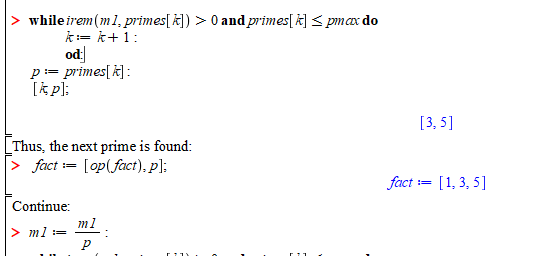
p: 质数具体值

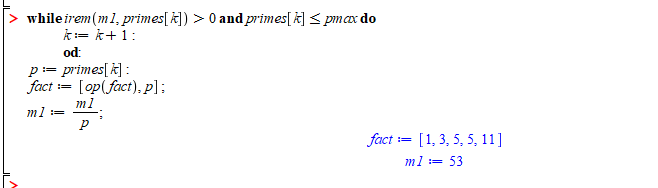




第一步要用m1

接下来的全部是



一直到m小于等于pmax=209

3.

RSA cryptography

m=p\*q//p与q是两个比较大的质数

phim=(p-1)(q-1)

e是一个与phim互质的数

发送的信息一定要小于m

例如5558686 m是556

那么就要切成555 86 86

源文件：w

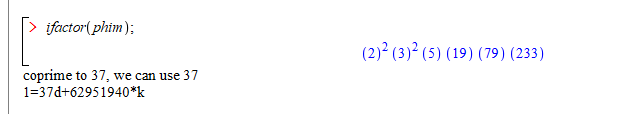
加密后，

通过求得d

解密 得到v

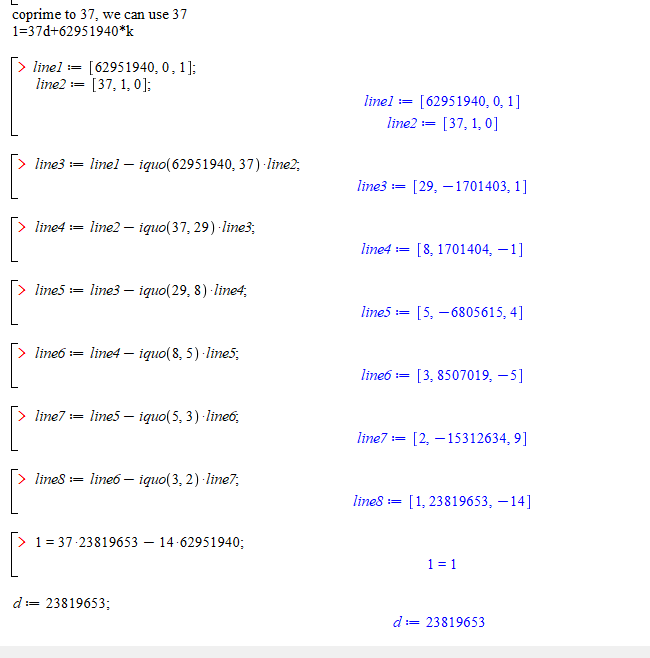
step1，求phim=(p-1)(q-1)

step2，确认e与phim互质，

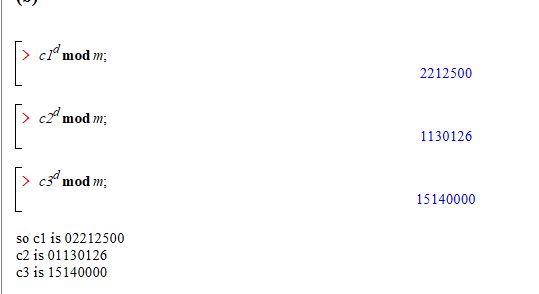


因此我们可以使用37作为e

step3求d



第四步c^d mod m



4.

计算b with超级大的anm， 利用 assignment 4 中的 SQB算法



Chinese Remainder

两个congruene



这个方程有解当且仅当(m,n) divides(b-a)



step1:联立x



step2：右边转换



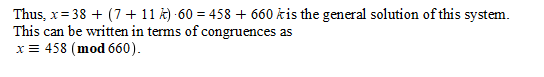
然后完全就成了mod 关系

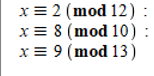


这里5与11互质

inverse数是9，



.

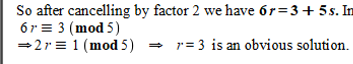


三个congurence (assignment 5 1)

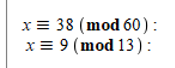
STEP1,联立上面两个

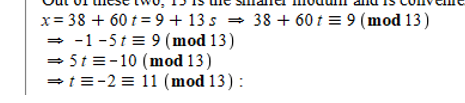


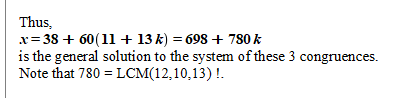
STEP2



X=38+60K





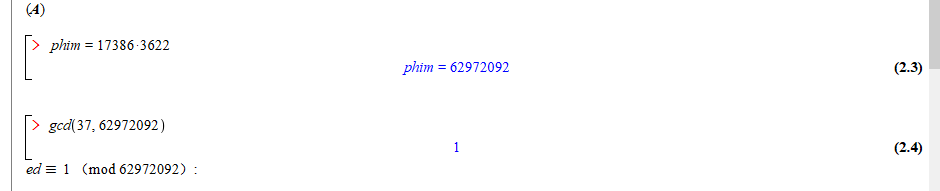


3.

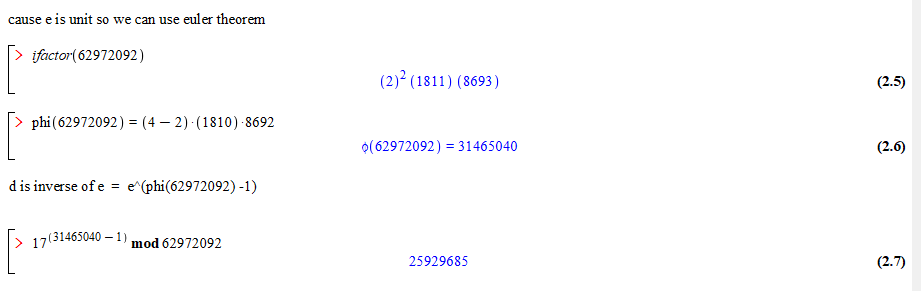
RSA with chinese theorem

p=17837,q=3623,m=62993101, e=17

第一步还是很简单，计算phim.是否与e互质，然后我们就可以计算d



第二步计算d，可以使用euler theorem



算出phim 的euler里的phim

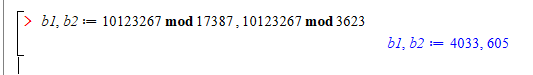
inverse就是d

STEP3

(1)让d mod p-1,q-1

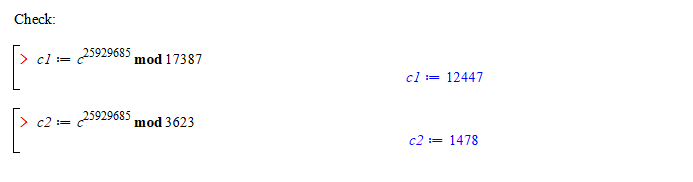


(2)让c mod p, q// c就是加密后发送的数字，得到b1b2 //



让b1^step3(1)的两个结果

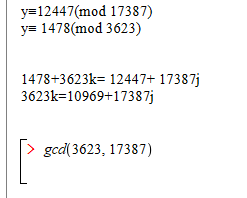
最终得到的c1c2是对原来得巧算，25929685就是c^d mod p,q



STEP4

让c1 c2 分别mod

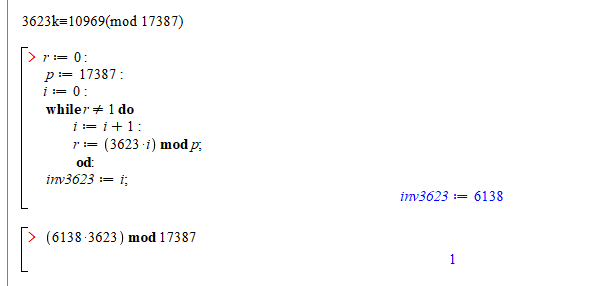
就是普通的chinese remainder



证明有解也就是3623 17387 互质

然后我们就可以找inversee

**inverse巧算：assignment5 2 里面**



因此k=5258+17387j

最后得到y

CH13

Definition:

1.degree: x^n的最大值

2.一个基于commutative ring一个基于commutative ring R的多项式可以表示成



an叫做系数coefficients,

x叫做参数argument

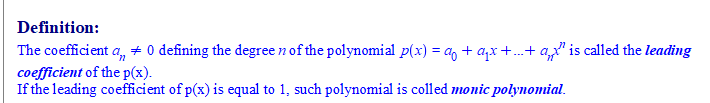
3. 两个多项式相等当且仅当他们的degree相同既n=m,且每一个系数相等

4. ，Polynomial Ring, 就是所有系数属于R的多项式组成的集合

5. Fp[x],如果m为质数p，那么Z/pZ是一个field //任何element除了[0]都是unit。

我们用这个记号notation来表示基于Fp的polynomial

6.leading coefficient, 最大项的系数an, 如果leading coefficient=1，那么这个polynomial叫做monic polynomial



7. Zero polynomial:任意系数都是0，例如p(x)=0,zero polynomial的degree

8.Divide整除， f divides g如果



9.Greatest Common Divisor: 让f与g是两个F（x）中的polynomial， 那么polynomial d 是greatest common devisor of f and g, 如果d divides f且d divides g， 且与其他同时divide fg的polynomial比，他的degree是最大的//greatest common divisor可以通过euclid's algorithm for polynomial

10.associates: 两个non-zero polynomial d 与 e被称作是associates,如果他们互相是对方的scalar倍数//scalar可以是小数, 例如X^2+2与3X^2+6

11. irreducible 不可约的，不能再消减degree的：一个polynomial p in F[x] 被称作irreducible如果p已经不再是F[x]中的unit了，如果P=f\*g，那么f与g之间必定有一个是unit//换句话说，当p=f\*g,f与g中必然有一个是非零整数，这时p叫做irreducible

//

irreducible polynomial相当于常数中的prime number的位置，已经不能再约分了（整数意义上）

12.Unit: 如果F是一个field,那么对于polynomial p来说，存在q，让pq=1,那么p就是q的unit //换句话说，只有非零整数才能算unit

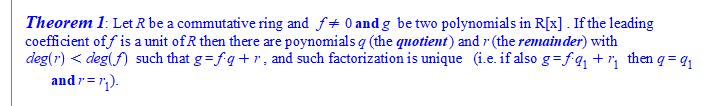
如果p是unit,那么必然存在另一个Unitq,让pq=1，那么在F【x】中，我们一直deg(p)+deg(q)=0,唯一满足的可能就是deg(p)=deg(q)=0,

13.coprime:gcd(f,g)=1

Theory

1.让R是一个commutative ring，对于每一组非0多项式p与q， 如果 p与q的leading coefficient不是R的zero divisor，那么deg(p\*q)=deg(p)+deg(q)

2.Division Theorem, 如果R是一个commutative ring，而且 f≠0,与g 是R【x】中的两个polynomial。 如果f的最大系数是R的unit，那么必然存在polynomial q (商)，以及polynomial r(余数)， deg(r)<deg(f), 让g=fq+r, 且解是唯一的



就是f是除数，除数不为0且为R的unit，那么能招到商和余数.

3. 注意如果F中有多个Unit，那么就有多个GCD, 但是，有且只有一个monic GCD divisor of f and g//通过 inverse转化而来

4.Bnzout's Identity, 对于任意F[x]内的d=gcd(f,g),inF(x),都可以写成d=Xf+Yg,对于F[x]中的某一个X,Y

5. 如果 p是irreducible且f是无法整除p的polynomial，，那么p与f之间的gcd是1

6. 任意degree>=1的polynomial在F[x]中，要么是irreducible，要么可以积分乘irreducible polynomials的乘积

7. Theorem(Unique Factorization):在F[x]中，如果f=p1p2...ps =q1q2...qt， 是monic polynomial f(最大系数为1)的两种monic irreducible polynomial积分， 那么t必然等于s，且{p1...ps}与{q1,,,qs}必然相等

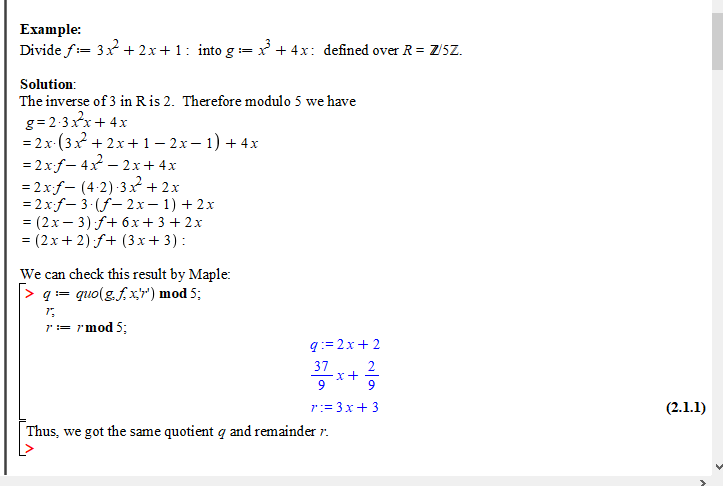
重点：

1：找到两个不同的polynomial，但是作为function相同

a^m≡a 对于Z/MZ,

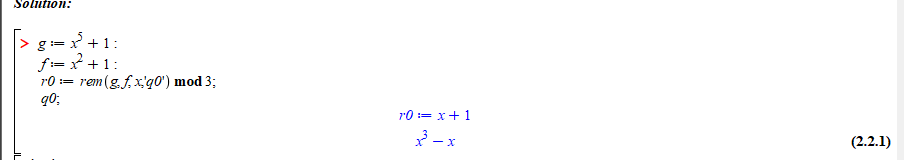
但是两个polynomial不同

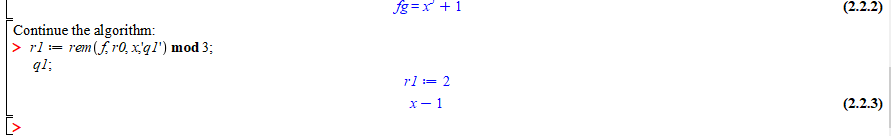
2.因式分解



最后解是唯一的

3.Euclid 找GCD

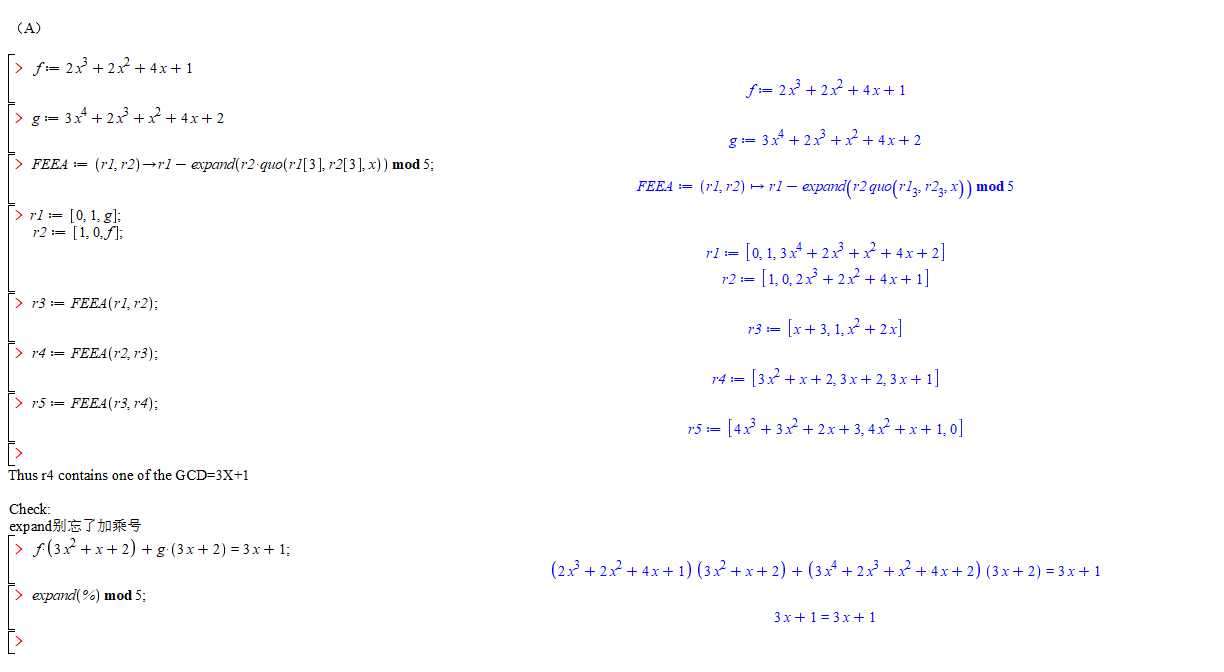




当余数是常数

4.Extended euclid algorithm

Assignment5



这是让你找的GCD

如果LINEAR CONGRUENCE要找解看lec10

5.找irreducible

任意x+a都是irreducible

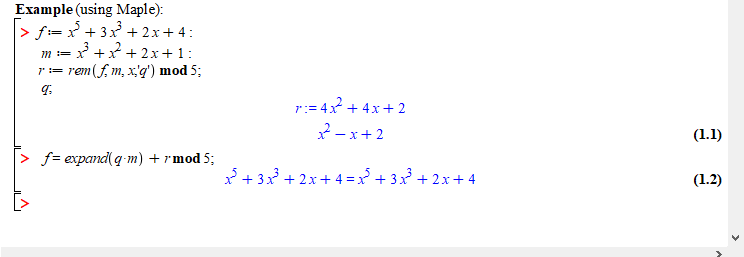
因为p=fg,那么deg(f)+deg(g)=1,那么g与f中任意一个deg必须是0

x^2+1在Z/3Z中是irreducible但是在Z/5Z中不是

CH10  
定义**Least Degree Residues**

Proposition3: residue of lease degree modulo m，让m是一个polynomial,deg(m)>=0。如果f是一个F[x]中的一个polynomial,那么，那么f将有一个独一无二的polynomial r ， congurent modulo m, 且deg(r)小于deg(m),那么这个r叫做residue of lease degree modulo m //有点像power意义上的[7]与[2] inZ/5Z

例子：

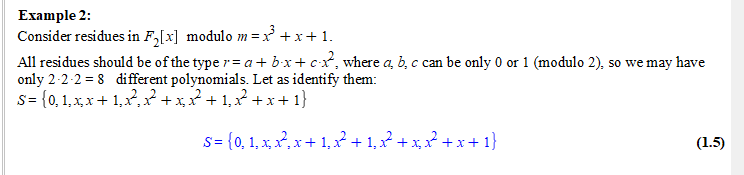


Proposition4: 两个polynomial ,f与g，是congurent modulo m关系当且仅当他们的residue of lease degree modulo m相等的时候

Proposition5: 对于任意field F,里面任意一个element a, 以及任意f(x) in F(x)， 都会有f(x)≡f(a)( mod x-a)

定义：**Complete set of representatives**

记作S，是一组set,由polynomials组成，任意Polynomial都仅与S中的一个polynomial congruent modulo m



一个complete set of representatives的数量在Fp【x】 modulo m of deg(m)=n 的数量为N=p^n

p是常数能取的值，这里01，就等于2，

n是mod的polynomial的degree，

从常数一直到n-1,一共有n位数

所以是p^n

定义Unit:

Proposition6: 让F成为一个field，且m(x)在F【x】中degree大于0，那么f(x)在F[x]中具有以下性质  
1.f(x)≡0（mod m）当且仅当m(x) divides f(x)

2.f(x) 是unit 当且仅当他们最大 greatest monic common divisor(m,f)=1

3.f(x)是一个zero-divisor当且仅当f(x)无法被m(x)所除，且（m,f）的degree>0

注意如果f是unit，那么



对于这类形式，z(x)必有解

Congurence modulo a polynomial的性质

性质1.

给你g,g1,g2,f,f1,f2,k,以及m，在F[x]中

乘法定律

1.如果f≡g(modm),那么kf≡kg(modm)

加法定律：

2.如果f1≡g1(modm)且f2≡g2(modm),那么f1+f2≡g1+g2(modm)

乘法定律

3.如果f1≡g1(modm)且f2≡g2(modm),那么f1\*f2≡g1\*g2(modm)

Power定律

4.如果f≡g(modm),那么f^n≡g^n(modm)

Proposition2:

除法定律

如果hf≡hg(mod m)且h与m为coprime，那么f≡g(mod m)

重点，直到这个polynomial是irreducible的吗

带入所有可能root，等于0，那么x-k是其中一个factor

x大于4以上可能没解但仍然irreducible

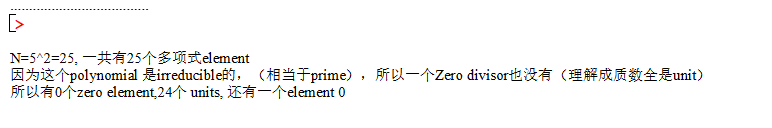
 

问你how many zero divisors

如果方程是irreducible的，

那么就除了0全是UNIT

直接



重点例题：

find all irreducible polynomial of degree n=2 in F5[x]

第一步先找出所有的irreducible monic polynomial

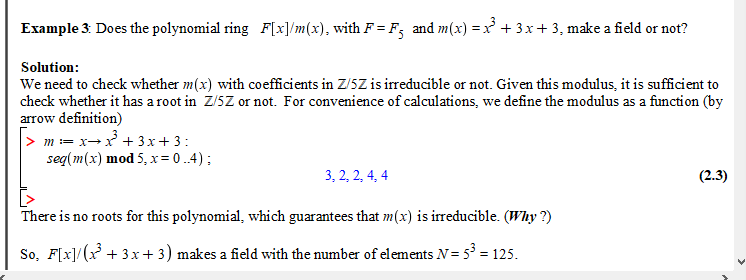
CH 11

Proposition: F(x)/m(x) 中的非零element，要么是unit,要么是zero divisor

Proposition4: F(x)/m(x) 会成为一个field 当且仅当m(x)是irreducible polynomial ，且系数全部都是Z/xZ范围，X必须是质数

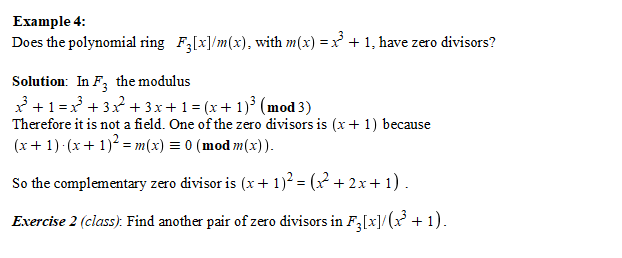
重点

1.怎么证明一个F（x）/m(x) 是field



代入m，发现没一个是0，所以是irreducible，因此是field，而5也是质数

2.



zero divisor就是polynomial的因数

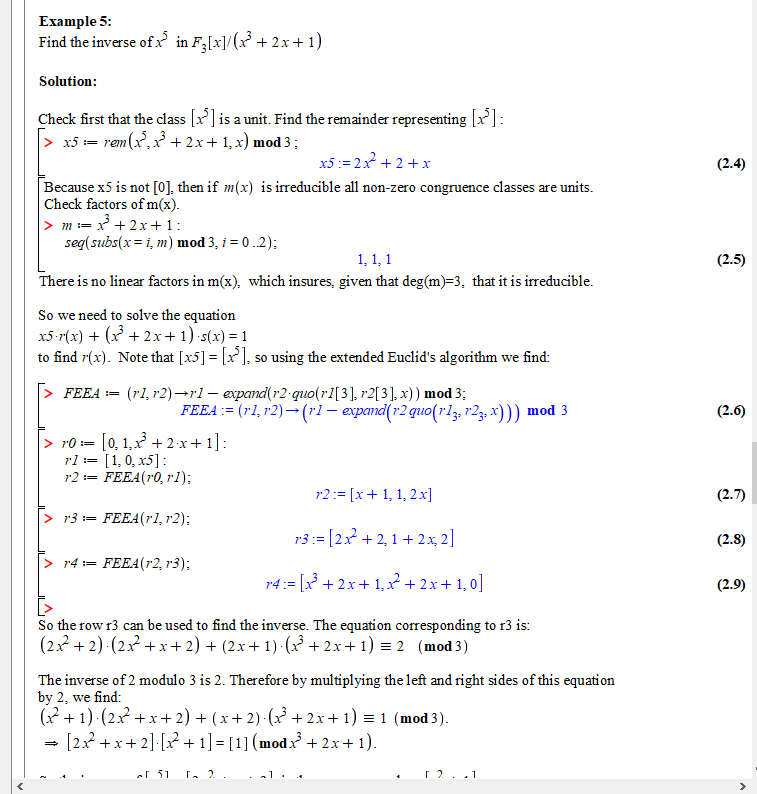
这里x&3+1可以转换成（x+1）^3 (mod 3)

因此zero divisor就是（x+1）

//这题就是在变相的问你m(x)是不是irrevelent

当x=2，原式mod 3=0，

Definition: Simple field extension of F: 一个F(x)/m(x),如果m(x)是irreducible polynomial且系数在F内，那么这个F（x）/m(x)被叫做是simple field extension of F



首先看看m是不是irreducible，因为deg=3,可以使用·check 0 法

答案是m(x)是irreducible

系数又全在3内，因此他是个field，一切都是unit,X^5 也是，因此它又inverse

先让x^5转换成Z/3Z内对应形态

也就是说我们要找

[2X^2+X+2][Y]≡[1](mod x^3+2x+1)

使用extended

相当于求

(2x^2+x+2)r(x)+（x^3+2x+1）s(x)=1的解

3

On Fermat's Theorem and Primitive Roots in F(x)/m(x)

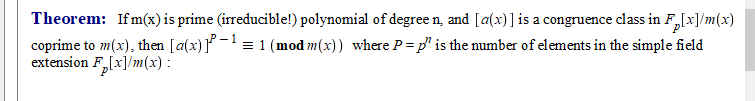
Theorem: 如果p是Prime且a是一个integer与p互质，那么a^p-1≡1（mod p）



推到polynomial中

如果m(x)是irreducible of deg n,而且a[x]与m(x)互质，那么

P=p^n, 也就是Fp[x]./m(x)的simple field extension 中element的数量



定义:order, order of a(x) modulo m 是最小整数 e，让a^e≡1(mod m), order e divides(P-1)



总结：

也就是说，当m(x)为Prime，那么unit^P-1必然≡1

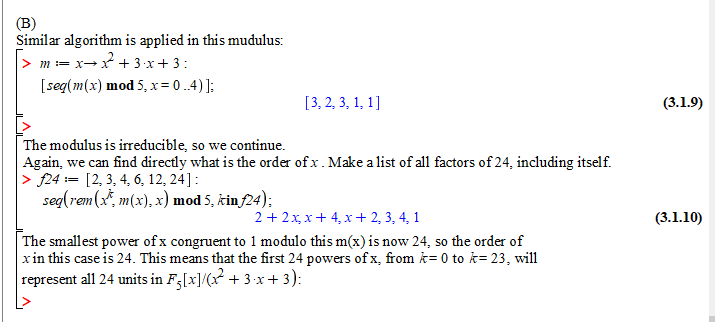
P=mod数^deg

order必然是他的factor

order找assignment 6最后一题

2.

检查primitive root



第一步是不是irreducible，irreducible继续

然后，列出所有可能order，5^2=25

25-1

然后使用这个，

我们发现order=24,

因此从k到23都是unit、primitive root

怎么使用Chinese remainder

有解当且仅当Mi 与mj互质

所以除了很明显的，第一步我们要EXTENDED