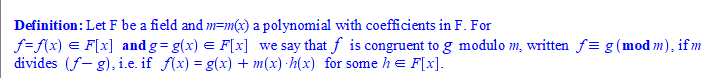
Congurence Modulo a Polynomial

polynomial的mod

定义：让m=m(x)，f=f(x).g=g(x)是F中的三个polynomial, 我们说f≡g(mod m)如果m divides(f-g)

换句话说f(x)=g(x)+m(x)h(x)，对于·F[x]中某一多项式h(x)



例如在F5【x】

中

f=2x^3+3x^2+2与g=x^2+2 是congurent modulo m=x+1

因为

f-g=2x^3+2x^2 divides x+1

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：

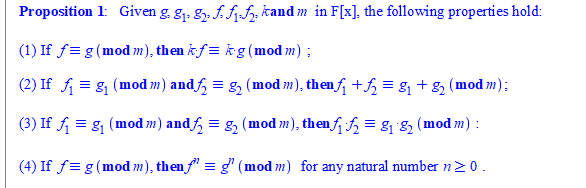
2.如果f1≡g1(modm)且f2≡g2(modm),那么f1+f2≡g1+g2(modm)

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)



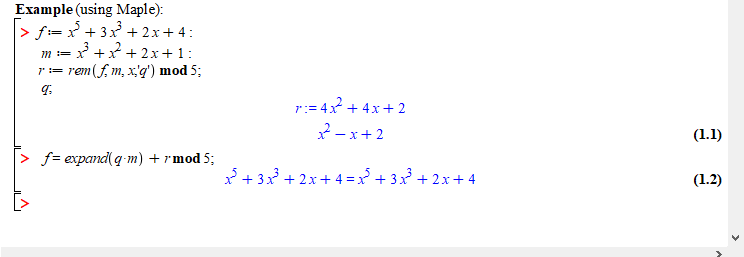
Proposition2:

除法定律

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

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将于一个独一无二的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

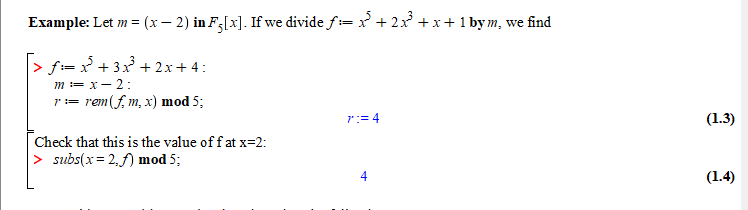
例子：

我们必然能算出一个r来

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)

例子

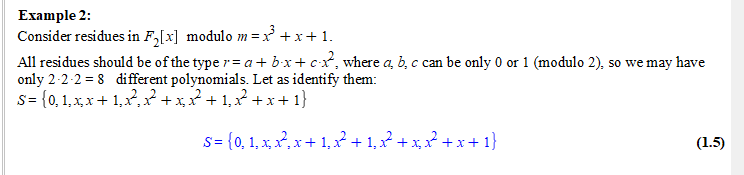


rem： 用第一个数除以第二个数，得到的余数为x， return的数为x， 再让这个数mod5也就是我们的r

subs(x=2.f) ，f(2)的值

Complete set of representatives

定义：一个complete **set** of representative modulo m in F[x] 就是一个由polynomials组成的set， 任意polynomial in F[x]都与且仅与S中的一个polynomial congruent modulo m



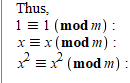
例如在F2[x]中，mod数为m=x^3+x+1

所有的residues余数都应该是type r=a+bx+cx^2,而且a与b与c只能是0或1（因为是modulo 2），

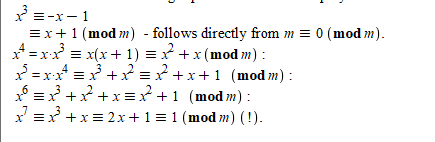
所以最多8个

//解释，超级简单， 我们只需要列出0到m之间所有的东西，因为他们就代表了所有的余数，

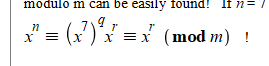
那么我们怎么找到一个大power对应的 polynomial呢



从m≡0（mod m）开始推



这样我们得到了1在x^7的时候

因此任意power可以转换成

x^7=1被减去，

通常来说，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就是有几位可以操纵的数，

从常数一直到n-1,一共有n位数

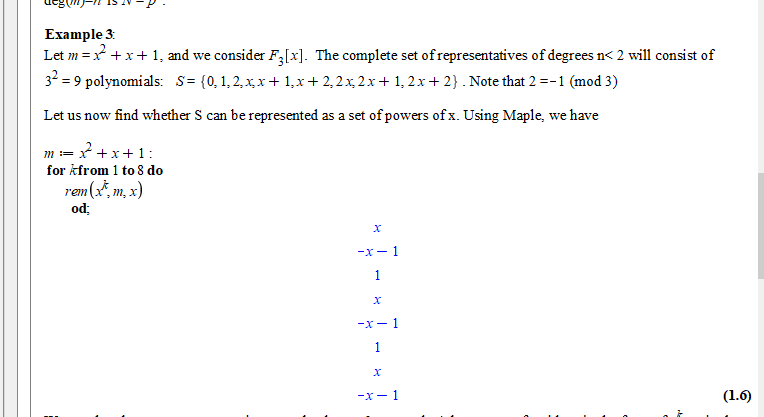
所以是p^n

例题：

让m=x^2+x+1,在F3[x]中，那么p=3, n=2， 所以一共有9个



然后我们来验证S是否能·表达所有的power



发现在deg3以后就重复了,我们并没有得到我们预想中的余数set

可以发现与example2不一样

因为

mod m=x^2+x+1是reducible的

m=x^2+x+1=x^2-2x+1=(x-1)^2

但是还是可以用的

例如



一直x^3≡1 //这个3叫做order

所以



.

Linear Congruences

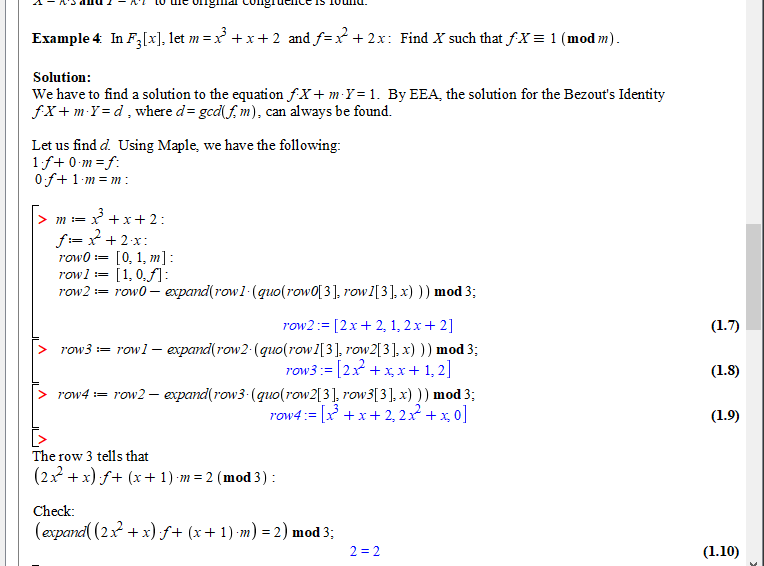
aX=b(mod m)

给你Polynomial a,b,m a(x) X(x)≡b(x)(mod m(x))

等同于aX+mY=b,

这个问题有解当且仅当gcd(a.m)=d divides b, 也就是说b=kd,

例子



我们知道m与f

fX≡1（mod m）

转换成fX+mY=1。

然后就是eea的一段

注意他这里第三个才是减的

所以row3第三个也就是2就是我们要的gcd

(2x^2+x)f+(x+1)m=2(mod 3)

左右同时乘以2，

(x^2+2x)f+(2x+2)m=1(mod 3)

所以我们就有第一组XY的解了



通解：

我们需要找到右边等于0

aX≡0(mod m)的解

fX=km

(x^2+2x)X=k(x^3+x+2) //我们check两边是不是互质，让最大公约数除以系数就是X的step

x=(x^3+x+2)k

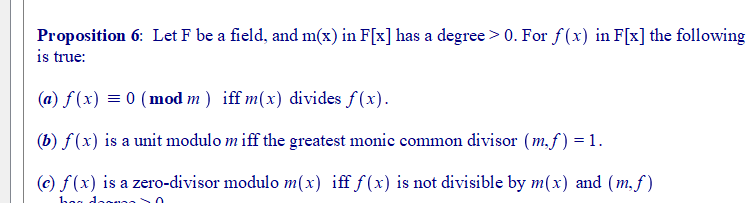
因此X=(x^2+2x)+(x^3+x+2)k

定义:unit 一个polynomial f=f(x)被称作unit在F【x】中当且仅当存在g=f-1属于F[x]，让f(x)\*g(x)=1(mop m(x))

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



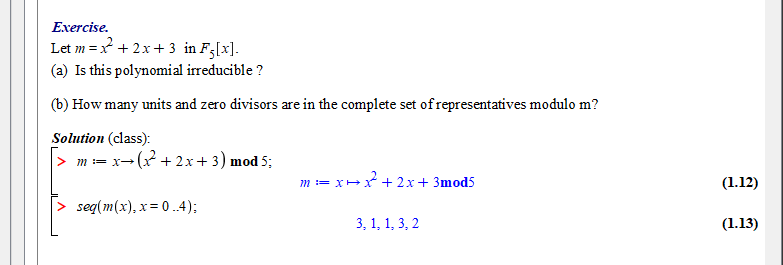
注意如果f是unit，那么



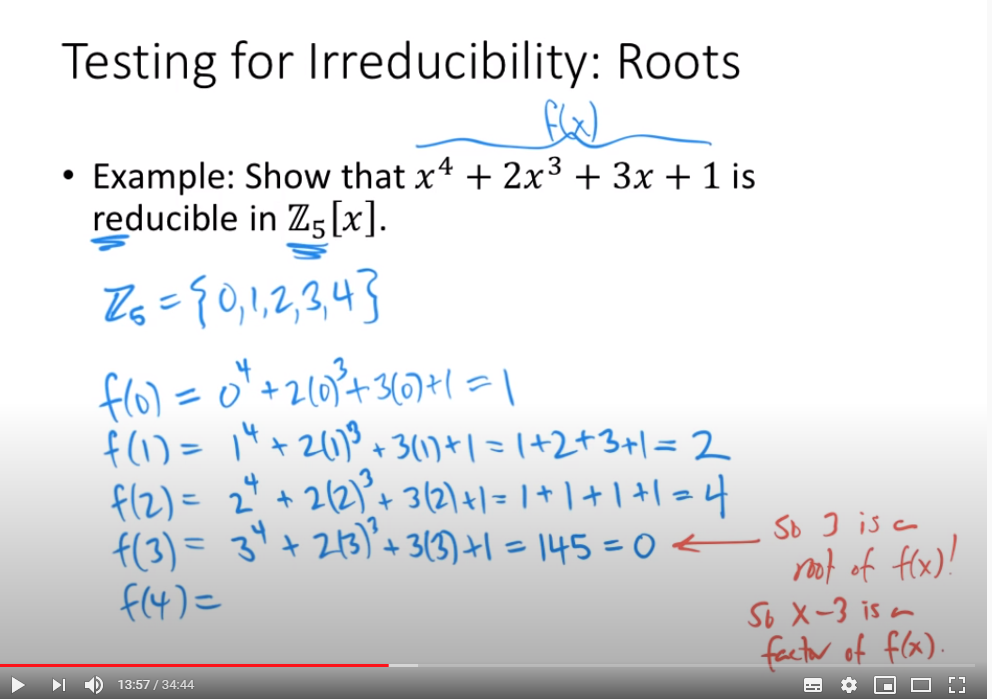
对于这类形式，z(x)必有解

Existence of irreducible polynomials

在Fp[x]中，每一个n>=1的degree都有一个irreducible polynomial



这个polynomial 是irreducible的吗



直接带入所有可能root，如果有一个=0，代表x-k是其中一个factor

