Exercise 1  
先找0，再带入check



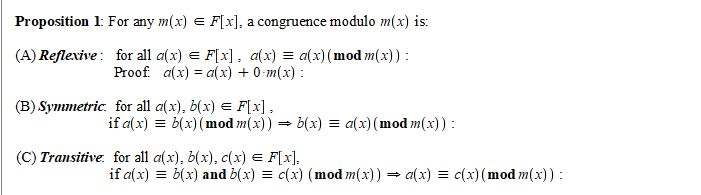




Exercise 2: 找到所有irreducible polynomials of degree n=2 in F5[x]

看note

Congruence class modulo polynomial m(x)



proposition1 ，equivalence class三个性质

因此在modulo polynomial中，我们也可以把所有polynomial切割成不同的congurence classes



写作[a(x)]m(x) ，，代表着所有与他全等的东西

同时，这些congurence classes将完美把ring F[x]切割成无重复的子集

Proposition2



a(x)m(x)与bxmx相等当且仅当a(x)≡b(x)(mod m(x)) 的时候

s

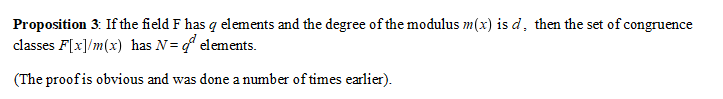
Definition:F(X)/m(x) **complete set of congurence class**总集： 由congurence classes in F(x) mod m(x)组成的总集叫做F（x）/m(x)。 任意polynomial b(x) 在a(x)m(x)中都是他对应congurence class的representative

让所有deg<m(x)的r(x)将组成 **complete set of representatives**

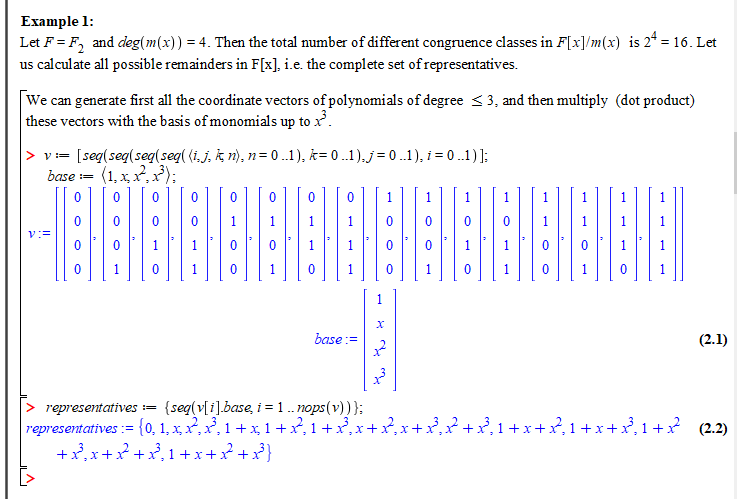
就是整数里mod5  
那么｛0，1，2，3，4｝ 就是complete set of representatives

{[0],[1],[2],[3],[4]}就是complete set of congurence class

Proposition 3: 如果一个Field F 有q个element且deg(m(x))=d, 那么set of congruence c lasses F(x)/m(x)有q^d个元素



例子

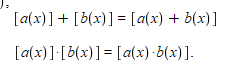


所有的r就是从0到x^3+x^2+x+1这些，, d=4, q=2

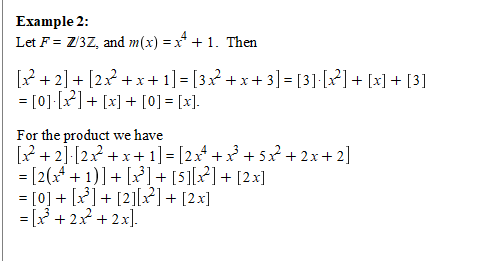
注意这里的deg包括常数项，

2^4=16

Algebraic operations in F[x]/m(x)



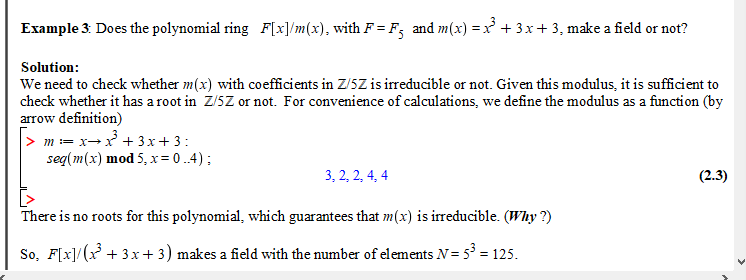




Proposition: F(x)/m(x) 中的非零element，要么是unit,要么是zero divisor

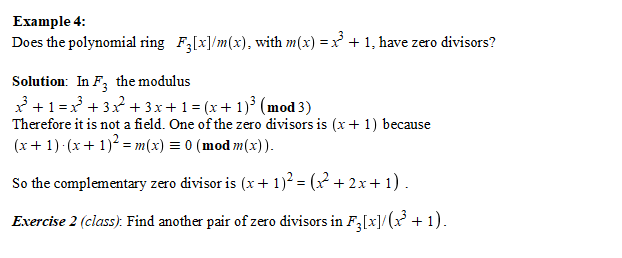
Proposition4: F(x)/m(x) 会成为一个field 当且仅当m(x)是irreducible polynomial ，且系数全部都是Z/xZ范围，X必须是质数





因为deg=3, 可以用代0法

这里X=5是质数，所以是 field



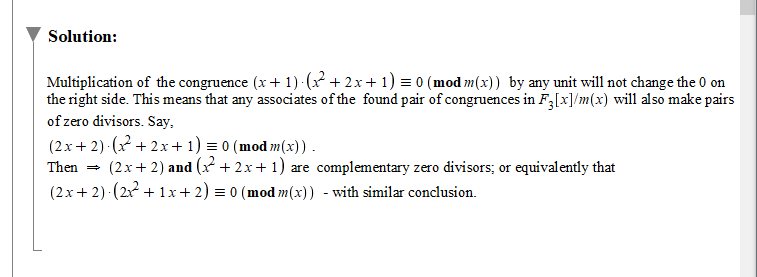
zero divisor就是polynomial的因数

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，

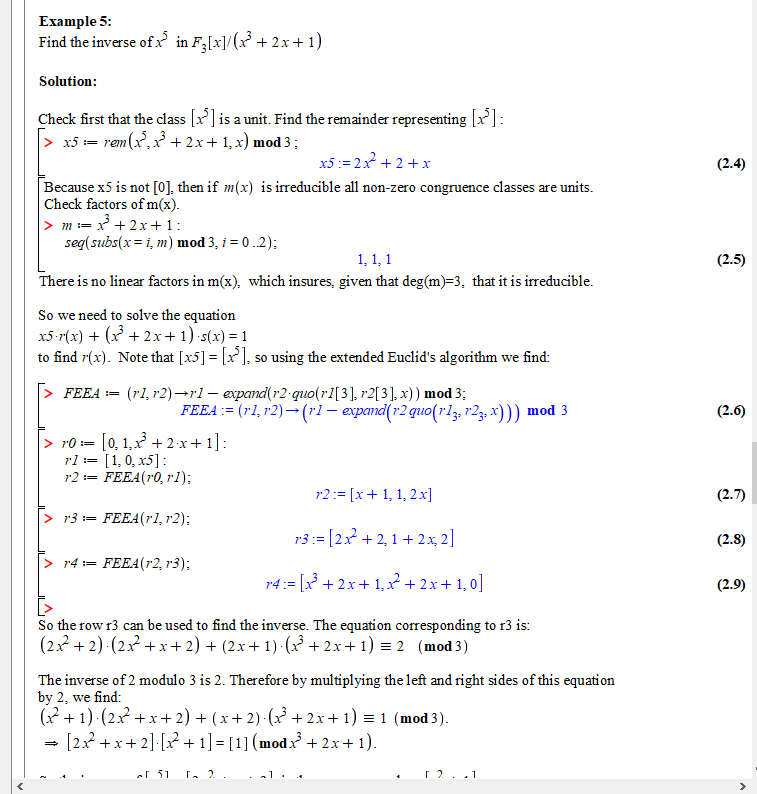


找到另一组zero divisor

因为x+1是 zero divisor，那么乘以任意unit Z/3/Z，还是zero divisor，所以就直接乘以2

(2x+2)(x^2+2x+1)还是的·

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

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

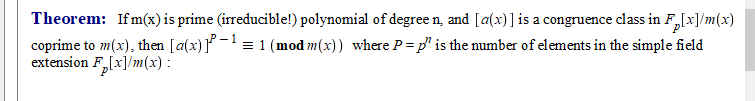
Theorem: 如果p是Prime且a是一个integer与p互质，那么a^p-1≡1（mod p）



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