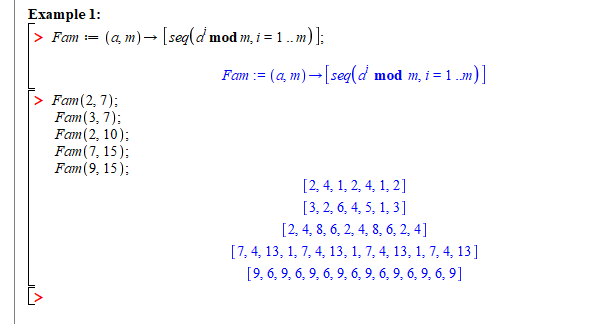
Fermat's theorem

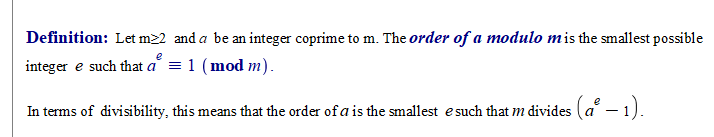
a的power mod m



你会发现在一定r<m不停循环

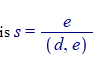
性质1：如果a与m互质，那么a^t≡1 mod m 对于1<=t<m

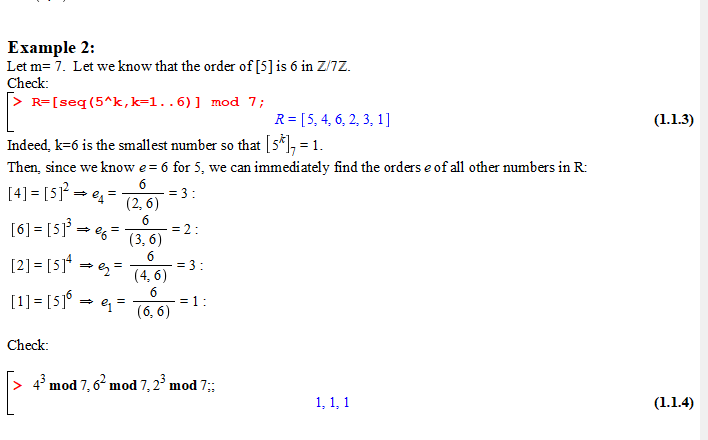
定义：order of A modulo m 。假设a是一个与M互质的数，那么 the order of a modulo m是**最小**的整数e，让a^e≡1(mod m)



换句话说，m divides a^e-1

性质2：如果e是order,且a^k ≡1(mod m) ，那么e divides k

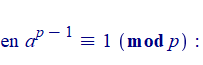
性质3： 如果e是a的order，那么对于a^d 的order s , 



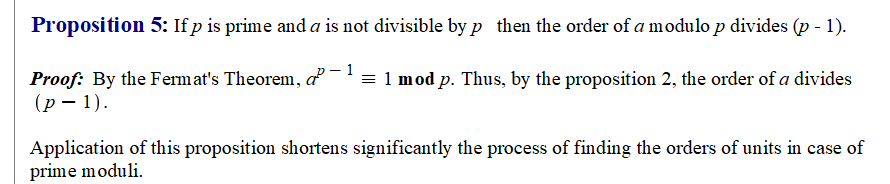
例题，我们知道了[5]的order

那么我们可以知道5^q的所有Order

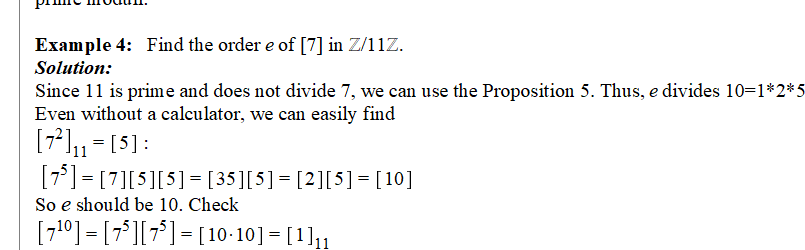
Fermat Theorem

如果p是一个质数，且a是一个与p互质的整数，那么

性质5：如果P是prime且不是a的因数，那么the order of a modulo p 是(p-1)的因数



例子：



11是质数且与7互质，那么e 是 应该是mod数p-1的因数，就是10的因数

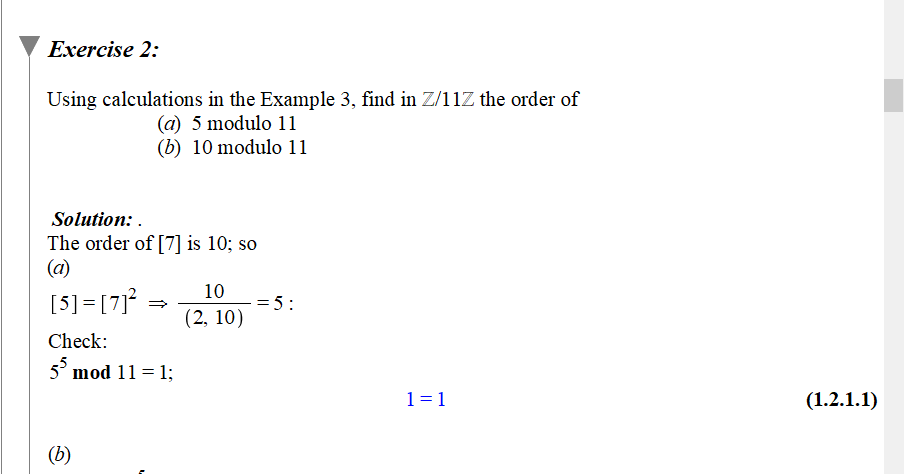
要么是2要么是5，要么是10

7^2=5不合格

7^5=10不合格 //合格不合格看结果是不是[1]

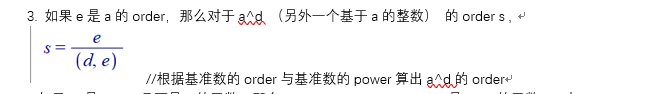
因此e就是 10

例子2：



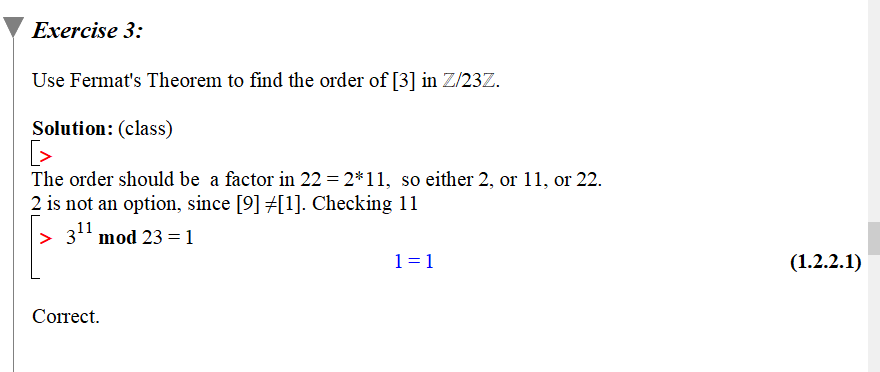
我们已经知道7 mod 11 的order

可以以【7】为基准数，运用Position 3



10/2=5

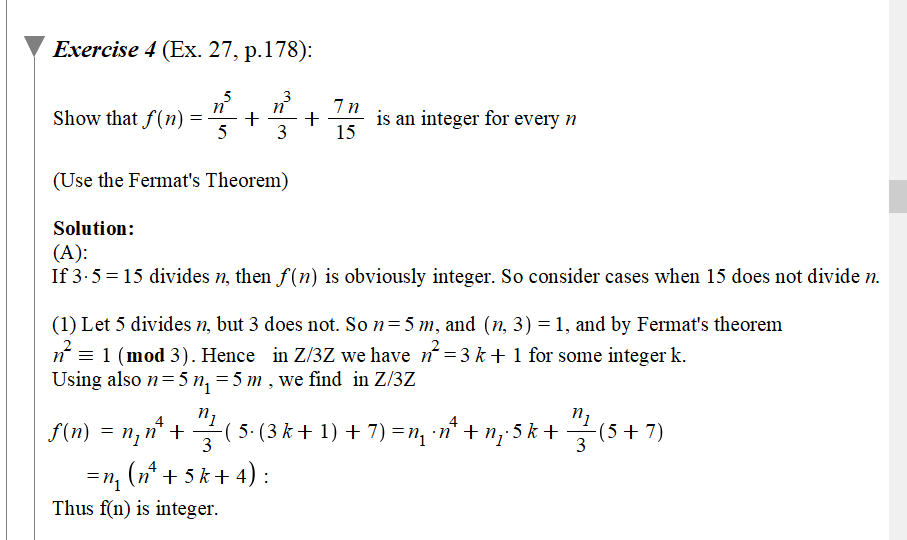
…



a与m互质且m是质数，那么e必然是22的因数

2,11,22

一个一个测试



**经典例题：**

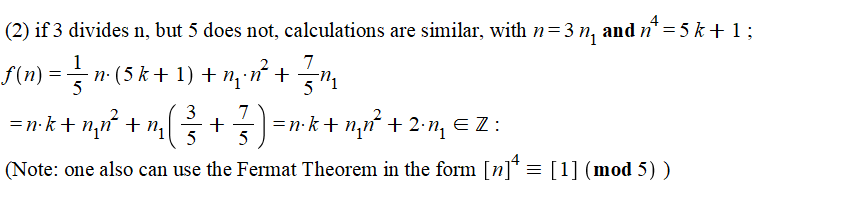
如果n是15的倍数，显然是一个整数，那么我们要考虑的就是n不是15的倍数

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

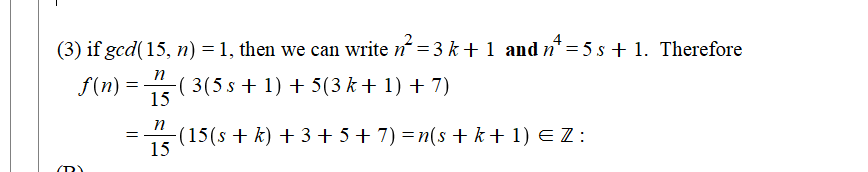
=625^m^5+5mk+4m



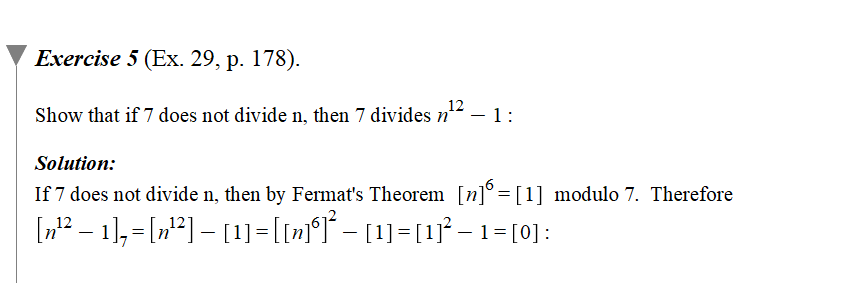
再假设3 divides n

同理

最后要考虑与非15因数，



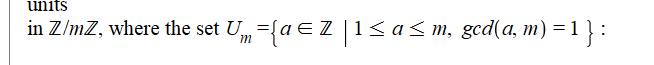
3k+1与5s+1是根据fermat theorem得到的



Euler's theorem

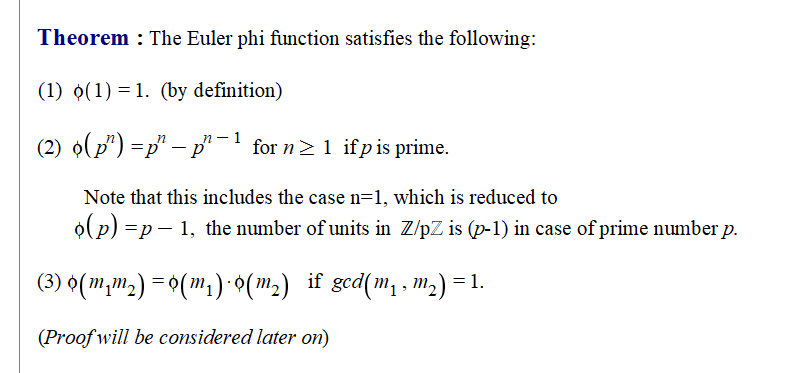
Definition:对于正整数m>1，Euler phi function 

Um就是unit的数量



在Z/mZ中，gcd为1的数就是unit

注意在这个定义中m是可以等于1的

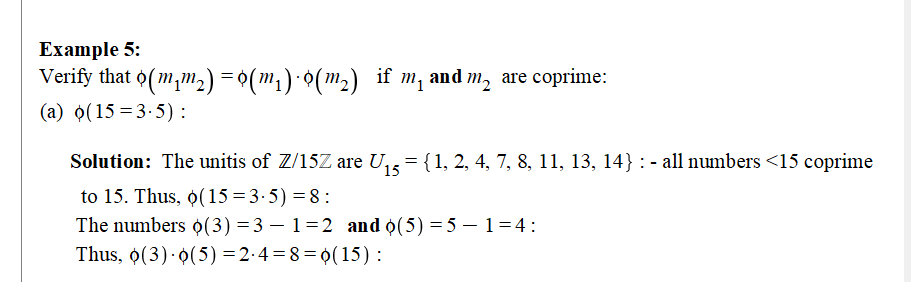


m=1那么根据定义就是1

如果p是质数，那么unit的数量为p^n-p^n-1

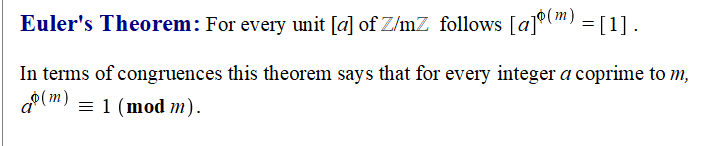
**注意：如果p是质数，那么phi p=p-1**

如果m1m2互质，那么他们的eulerphi可以拆解



例子，验证  
15所有互质Unit，

Euler theorem:

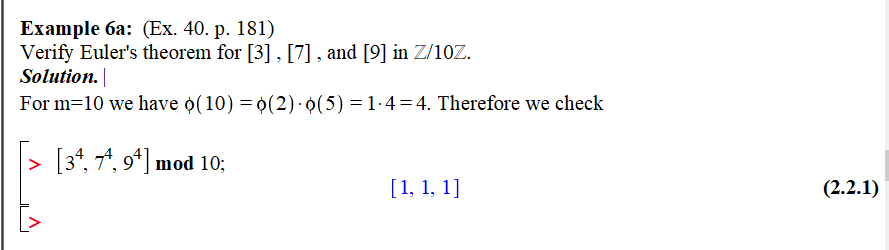


[a]一定要是unit

φm 是Z/mZ Unit的数量

这两个power一下一定是[1]的convergence class

换句话说=mk+1



10的unit为1,3,7,9

3^4 mod 10guo ran =1

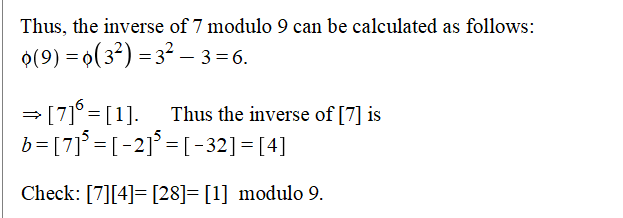
运用EULER 理论来计算mod

Euler理论用来寻找order或者找到unit a的Inverse是很有效的

因为

inverse:我们可以直接找到a^phim-1,必然就是他的inverse

order: 我们已经知道了phi m是Power，那么order必然是Phi m的因数

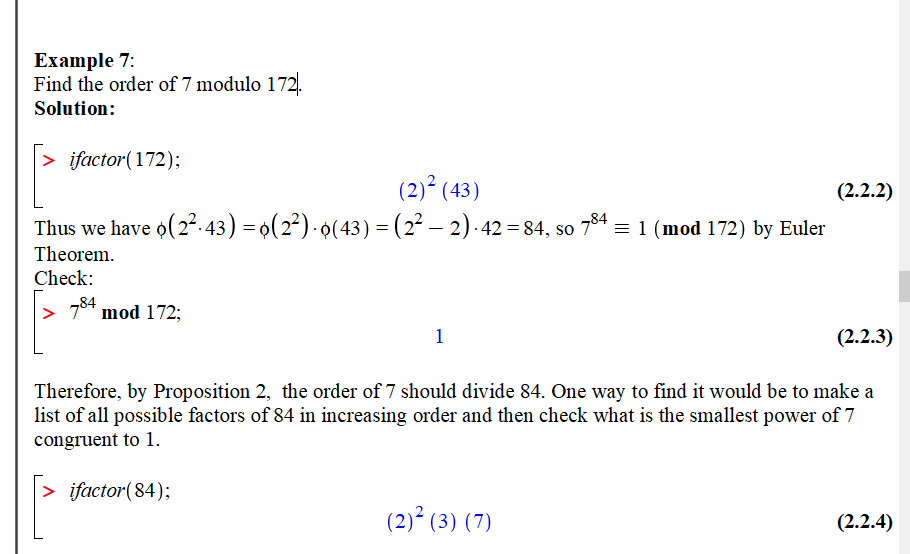


例如7 mod 9 的inverse

7是9的Unit ，9的unit有124578 6 个

那么inverse就是

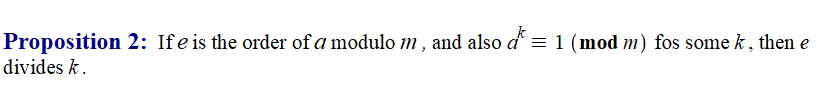
[7]^5=[4]



找到7 mod 172的order

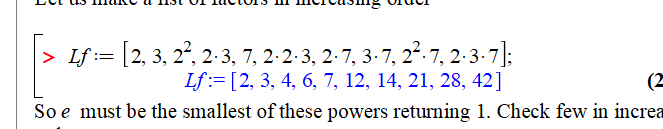
第一步因式分解

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)



然后根据 proposition2,

k已经找到84了，那么我们想找order只需要找到84的因数



为2346712 14 21 28 42之一

分别7^k mod 172代入，找到 order

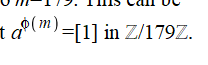
CH9F

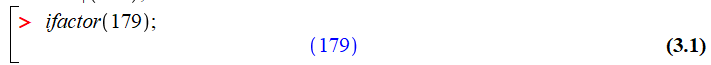
计算

且n与m都特别大的时候

可以先利用Euler theorem

假设a=87, m=179





因此Phi179 =178

所以Inverse就是



而177可以拆解成1+16+32+128

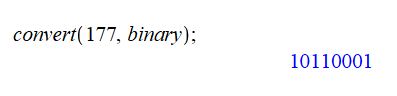
因此

1是2^**0**, 16是2^**4,** 32是2^**5,**128是2^**7**

你会发现都是2的倍数

巧算技巧一：

我们要把177这个数转化成二进制的数

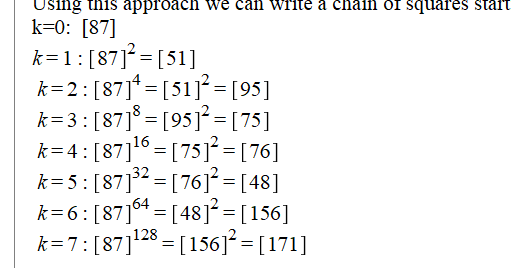


然后你会发现 所有出现的二的倍数恰好等于出现1的位置（倒着看，index 0 开始）

因此有1的index为，0 ，4,5,7

因此[87^177]=[87]^128\*[87]^32,,,

后面的这些比较好转，就是在原来的基础上平方就行



因此我们得到inverse[87]^177=[171][48][76][87]=[107]

检查inverse

