# 2014-01-22.sagews

January 22, 2014

## Contents


**1 Lecture for January 22, 2014** **1**
1.1 Computing the multiplicative order . . . . . 1
1.2 Use Eulers Phi Function $\varphi(n)$ . . . . . 1
1.3 Try out Eulers theorem . . . . . 1
1.4 Try out Wilsons theorem . . . . . 2


# 1 Lecture for January 22, 2014

```
md("## Computing the multiplicative order", hide=False)
@interact
def f(a=3, n=10):
    if gcd(a,n) != 1:
        print "We must have gcd(a,n) equal to 1."
        return
    R = Integers(n)
    abar = R(a)
    o = abar.multiplicative_order()
    print "The multiplicative order of a=%s modulo %s is %s"%(a,n,o)

    print "\nThe powers of a:\n    ",
    b = abar
    for k in range(n):
        print b,
        b *= abar
    print
```

## 1.1 Computing the multiplicative order

```
md("## Use Euler's Phi Function $\\varphi(n)$", hide=False)
@interact
def _(n=2014):
    print "euler_phi(%s) = %s"%(n, euler_phi(n))
```

## 1.2 Use Eulers Phi Function $\varphi(n)$

```
md("## Try out Euler's theorem", hide=False)
@interact
```

```
def _(n=20):
    k = euler_phi(n)
    print [Mod(x,n)^k for x in range(n) if gcd(x,n) == 1]
```

### 1.3 Try out Eulers theorem

```
md("## Try out Wilson's theorem", hide=False)
@interact
def _(n=2013):
    f = 1
    for a in [2..n-1]:
        f *= Mod(a,n)
    md("$$(p-1)! \\equiv %s \\pmod{p}$$"%f,  hide=False)
```

### 1.4 Try out Wilsons theorem