**Recitation 5**

**RSA: Let’s try it out!**

p=7

p=13

n=pq=91

e=11 , such that gcd(e, (p-1)(q-1))=1

Public key: (e, n)=(11,91)

d could be computed using the Pulverizer. This would require using Euclid’s gcd algorithm on n and k while keeping track of the linear combinations used to express the remainders up to the point where you have a linear combination for the remainder 1. This coefficient of k will be d, however it may be negative, in which case n should be added to reach a congruent positive.

But we will use Euler’s theorem this time.

Secret key:

Pretend the secret message is “6”, which corresponds to something on a message key everyone has.

Encryption:

Decryption:

Had to enter these in Wolfram Alpha to compute the massive numbers. JavaScript wouldn’t do it.

The method for encrypting by hand with **repeated squaring**:

So: