Math 440/540 Homework 4

1. (by hand) Let $n = 55$. Determine the set of allowable e such that (n, e) can be used as the public key in an RSA cryptosystem.

   Answer: First we need to find $\phi(55)$ which we can do by saying

   $$\phi(55) = \phi(5) * \phi(11) = (5-1)(11-1) = 40$$

   Now we need to find all numbers who fulfill $gcd(40, n) = 1$ where $2 \leq n < 40$ This gives us

   $$[3, 7, 9, 11, 13, 17, 19, 21, 23, 27, 29, 31, 33, 37, 39]$$

2. (using SageMath) Nikita underestimated you as an adversary, and decided to use small numbers for her RSA cryptosystem out of laziness... In particular, she published the following public key:

   $$(4460543, 1407259).$$

   (a) Determine Nikita's secret decryption key d.

   (b) You intercept the following encoded message to Nikita,

   $$(507330, 766099, 704785, 3564829).$$

   Decode the secret message!

```
n = 4460543
e = 1407259

factored = factor(n)
p,q = [f[0]for f in factored]
print(p,q)

phi = (p-1) * (q-1)

print(phi)

d = inverse_mod(e, phi)

print(d)

cmessage = [507330, 766099, 704785, 3564829]

decode = [pow(c, d, n) for c in cmessage]
print(decode)
```

```
alphabet = " ABCDEFGHIJKLMNOPQRSTUVWXYZ"

text = []
for t in decode:
    word = []
    while t > 0:
        t, r = divmod(t, 27)
        word.append(alphabet[r])
    if len(word)<4:
        word.append(' ')
    text.append(word)
decoded = ''
for w in text:
    for c in w:
        decoded += c
print(decoded)



--------

2111 2113
4456320
19
[171900, 14094, 3881, 407648]
RUSH IS THE BEST
```

3. (#4.1 in Stein) (by hand) Calculate the following Legendre symbols:

$$\left(\frac{3}{97}\right), \left(\frac{3}{389}\right), \left(\frac{22}{11}\right), \left(\frac{5!}{7}\right).$$

Answer With quadratic reciprocity we can determine that for an odd prime p

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}}$$

Using that we can determine the solutions

$$\left(\frac{3}{97}\right) = \left(\frac{97}{3}\right)$$

Since we have an odd prime

$$\left(\frac{97}{3}\right) => 97(mod3) \equiv 1(mod3)$$

And since $1^2(mod3) \equiv 1(mod3)$

$$\left(\frac{3}{97}\right) = 1$$

4. (*) (#4.3 in Stein) (by hand) Use Gauss's Quadratic Reciprocity Law (Thm. 4.1.7 in book) to prove that for $p \geq 5$ prime,

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{if } p \equiv 1, 11 \pmod{12} \\ -1 & \text{if } p \equiv 5, 7 \pmod{12}. \end{cases}$$

Answer First we have quadratic reciprocity which says for odd primes p,

$$\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)(-1)^{\frac{3-1}{2} * \frac{p-1}{2}} = \left(\frac{p}{3}\right)(-1)^{\frac{p-1}{2}}$$

And we know that $\left(\frac{p}{3}\right) = 1$ if $p \equiv 1(mod3)$ and -1 if $p \equiv 2(mod3)$ Then we can look at $(-1)^{\frac{p-1}{2}}$ and determine that it equals 1 if $p \equiv 1(mod4)$ and equals -1 if $p \equiv 3(mod4)$. From there we can use CRT we can combine. For the cases that equal 1 when $p \equiv 1(mod3)$ and $p \equiv 1(mod4)$ we get $p \equiv 1(mod12)$ then we have $p \equiv 2(mod3)$ and $p \equiv 3(mod4)$ which gives us $p \equiv 11(mod12)$. Then for the cases that equal -1 we have $p \equiv 1(mod3)$ and $p \equiv 3(mod4)$ which gives us $p \equiv 5(mod12)$ and $p \equiv 2(mod3)$ and $p \equiv 1(mod4)$ which gives us $p \equiv 7(mod12)$. Therefor we have proved the above statement is true.

5. (*) (#4.7 in Stein) (by hand with calculator) Use Gauss's Quadratic Reciprocity Law (Thm. 4.1.7 in book) to determine the number of positive integers $x < 2^{13}$ that satisfy the equation

$$x^2 \equiv 5 \pmod{2^{13} - 1}.$$

Note: you can use the fact that the number $2^{13} - 1$ is prime.

Answer We can start with the fact that $2^{13} - 1 = 8191$ which is prime. Then we can use quadratic reciprocity to get from $\left(\frac{5}{8191}\right)$ to $\left(\frac{8191}{5}\right)$. From there we can get to $8191 \equiv 1(mod5)$ and due to the properties of the Legendre symbol we know that that means we have exactly 2 distinct solutions.