Math 440/540 Homework 2

1. (# 1.7 in Stein)

   (a) (using python or SageMath) Compute $\pi(x) = \#\{p \leq x \mid p \text{ prime}\}$ and $x/\log(x)$ for $x \in \{1000, 10000, 100000\}$.

```
# Example Python (SageMath) code
print(f'pi(1000)={prime_pi(1000)}')
print(f'1000/log(1000)={1000 / log(1000).n()}')
print(f'pi(10000)={prime_pi(10000)}')
print(f'10000/log(10000)={10000 / log(10000).n()}')
print(f'pi(100000)={prime_pi(100000)}')
print(f'1000000/log(1000000)={1000000 / log(1000000).n()}')
```

   (Example output:)

```
pi(1000)=168
1000/log(1000)=144.764827301084
pi(10000)=1229
10000/log(10000)=1085.73620475813
pi(100000)=9592
1000000/log(1000000)=72382.4136505420
```

   (b) (by hand) The Prime Number Theorem states that $\pi(x)$ is asymptotic to $x/\log(x)$. What does that mean (in your own words)?

   Answer: That means that as $x \to \infty$ the ratio $\dfrac{\pi(x)}{x/\log x} \to 1$. This means that as we get to larger numbers, $\pi(x)$ can be better approximated by $x/log(x)$ This also means that as x approaches infinity, the distance between primes generally becomes greater and greater.

2. (#2.7 in Stein) (by hand) Find complete sets of residues modulo 7 satisfying each condition below.

   (a) all elements are nonnegative

   $$\{0, 1, 2, 3, 4, 5, 6\}$$

   (b) all elements are odd

   $$\{1, 3, 5, 7, 9, 11, 13\}$$

   (c) all elements are even

   $$\{2, 4, 6, 8, 10, 12, 14, \}$$

(d) all elements are prime

$$\{2, 3, 5, 11, 7, 13, 29\}$$

(e) all elements are multiples of 3

$$\{0, 3, 6, 9, 12, 15, 18\}$$

since $gcd(7, 3) = 1$

3. (by hand)

(a) Show how the Extended Euclidean Algorithm can be used to compute the inverse of 3 modulo 20.

Answer: First we can expand $gcd(20, 3)$

$$20 = 3 * 6 + 2 => 3 = 2 * 1 + 1 => 2 = 1 * 2 + 0$$

Then we have

$$1 = 3 - 2 * 1$$

and

$$2 = 20 - 3 * 6$$

so we can subsitute and get

$$1 = 3 - (20 - 3 * 6) * 1 = 21 - 1 * 20 = 7 * 3 - 1 * 20$$

thus

$$7 * 3 \equiv 1(mod 20)$$

so the inverse of 3 mod 20 is 7

(b) Use your result from part (a) to solve the linear equation $3x \equiv 4 \pmod{20}$.

Answer: We will multiply both sides by the inverse 7

$$7 * 3x \equiv 7 * 4(mod 20) => x \equiv 28 \equiv 8(mod 20)$$

which can be checked

$$3 * 8 = 24 \equiv 4(mod 20)$$

4. (*) (by hand) A troop of 17 monkeys store their bananas in 11 piles of equal size, each containing more than 1 banana, with a twelfth pile of 6 left over. When they divide the bananas into 17 piles of equal size, none remain.

(a) How can you set up this problem to use the Chinese Remainder Theorem?

Answer: To start we can set this up as $N = 11k + 6$ with N being total number of bananas and $k > 1$ being the size of piles. When divided into equal piles we have $N \equiv 0(mod 17)$. We can write the original set up as $N \equiv 6(mod 11)$ which sets us up to use the chinese remainder theorem.

(b) What is the smallest number of bananas they can have?

Answer: to start we can have $N = 17t$ for the second situation which is the total amount of bananas. From there we can set $17t \equiv 6(mod 11)$ Looking quickly we can see that $17 \equiv 6(mod 11)$ so $6t \equiv 6(mod 11)$ and we can further simplify to $t \equiv 1(mod 11)$. Therefore $t = 1 + 11m$ and $N = 17(1 + 11m) = 17 + 187m$. If we try $m = 0$ we get that k=1 which we said before isn't true, so the next lowest is $m = 1$ which gives us

$$N = 17 + 187 = 204$$

So the smallest valid number of bananas is 204

5. (using python or SageMath) Euler's Theorem states that $x^{\varphi(n)} \equiv 1 \pmod{n}$ when $\gcd(x, n) = 1$. Consider what happens when $\gcd(x, n) \neq 1$. For $n = 100$, determine all possible values of $x^{\varphi(n)}$ modulo n for x satisfying $\gcd(x, n) \neq 1$. Note any patterns you observe.

```
# Example Python (SageMath) code
n = 100
p_n = euler_phi(n)
l1 = {}
for x in range(0, n):
    if gcd(n,x) != 1:
        l1[x] = power_mod(x, p_n, n)

print(l1)
```

(Example output:)

```
{0: 0, 2: 76, 4: 76, 5: 25, 6: 76, 8: 76, 10: 0, 12: 76, 14: 76,
   15: 25, 16: 76, 18: 76, 20: 0, 22: 76, 24: 76, 25: 25, 26: 76,
   28: 76, 30: 0, 32: 76, 34: 76, 35: 25, 36: 76, 38: 76, 40: 0,
   42: 76, 44: 76, 45: 25, 46: 76, 48: 76, 50: 0, 52: 76, 54: 76,
   55: 25, 56: 76, 58: 76, 60: 0, 62: 76, 64: 76, 65: 25, 66: 76,
   68: 76, 70: 0, 72: 76, 74: 76, 75: 25, 76: 76, 78: 76, 80: 0,
   82: 76, 84: 76, 85: 25, 86: 76, 88: 76, 90: 0, 92: 76, 94: 76,
   95: 25, 96: 76, 98: 76}
```

Which we can see only has values of 0, 25, and 76. Also they seem to follow the pattern, 0, 76, 76, 25, 76, 76, 0.