MATH 4410

Nate Stott A02386053

Quiz #8; Due 11:59 pm, 3/25/2024

1. Recall: the *Euler totient function* $\varphi(n)$ is defined to be the number of positive integers in the interval [1..n] that are relatively prime to n.

   Use the Principle of Inclusion/Exclusion to prove

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

   Well lets play around

   Let $n = 10$

   So the interval would be

   1 2 3 4 5 6 7 8 9 10

   Relatively prime means that they share no common factor other than 1.

   1 and 10 are relatively prime

   2 and 10 are not relatively prime as they share a factor of 2

   3 and 10 are relatively prime

   4 and 10 are not relatively prime

   5 and 10 are not relatively prime

   6 and 10 are not relatively prime

   7 and 10 are relatively prime

   8 and 10 are not relatively prime

   9 and 10 are relatively prime

   10 and 10 are not relatively prime

   So $\varphi(n)$ should be equal to 4

   Let's try it out

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

$$\varphi(10) = 10 \prod_{p|10} \left(1 - \frac{1}{p}\right)$$

$$\varphi(10) = 10(1 - \frac{1}{2})(1 - \frac{1}{5})$$

$$\varphi(10) = 10(\frac{1}{2})(\frac{4}{5})$$

$$\varphi(10) = 5(\frac{4}{5})$$

$$\varphi(10) = 4$$

   What about for an odd number?

   Let $n = 9$

   1 and 9 are relatively prime

   2 and 9 are relatively prime

   3 and 9 are not relatively prime

   4 and 9 are relatively prime

5 and 9 are relatively prime

6 and 9 are not relatively prime

7 and 9 are relatively prime

8 and 9 are relatively prime

9 and 9 are not relatively prime

So $\varphi(9)$ should be 6

$$\varphi(n) = n\prod_{p|n}\left(1-\frac{1}{p}\right)$$

$$\varphi(9) = 9\prod_{p|9}\left(1-\frac{1}{p}\right)$$

$$\varphi(9) = 9(1-\frac{1}{3})$$

$$\varphi(9) = 9(\frac{2}{3})$$

$$\varphi(9) = 6$$

Well, both those worked, so let's break what happened apart to try to understand why it worked.

If n is even

i. there will be less relatively prime numbers because you have to take out half of the numbers in the interval at least.

ii. there will be $\frac{n}{2}$ in the totient function, so $\varphi(n)$ will be at least half of n.

If n is odd

i. There are more relatively prime numbers in the interval

Looking at the equations again

$$\varphi(10) = 10(1-\frac{1}{2})(1-\frac{1}{5})$$

Foil

$$\varphi(10) = 10-\frac{10}{2}-\frac{10}{5}+\frac{1}{10}$$

$$\varphi(9) = 9(1-\frac{1}{3})$$

Foil

$$\varphi(9) = 9-\frac{9}{3}$$

n/m can be thought of the number of divisors of n relative to m.

An example, 1000/10 there are 10 divisors of 1000 that can also be divided by 10. Namely, 100, 200, 300, 400, 500, 600, 700, 800, 900, 1000.

So what we are saying in this $\varphi(9) = 9-\frac{9}{3}$ is that the number of positive integers in the interval [1..9] that are relatively prime to 9 is 9 but take away the number of divisors of 9 relative to 3 and that is 3 (3, 6, and 9).

This makes sense, as you need to take away numbers that can be divisible by another number other than 1.

$$\varphi(10) = 10-\frac{10}{2}-\frac{10}{5}+\frac{1}{10}$$

This is saying we need to take away all the numbers that are divisible by 2 and also 5. Then we need to add the numbers that are only divisible by 10 because we subtracted it off once too many times.

Generally

$$\varphi(n) = n\prod_{p|n}\left(1-\frac{1}{p}\right) = n(1-\frac{1}{p_1}-\frac{1}{p_2}-\frac{1}{p_3}-...+\frac{1}{p_1p_2p_3...})$$

So take away all the numbers that have other divisors, then 1. Then add back the numbers that got subtracted away too many times.

2. Compute 864^{-1} mod 899; that is, determine x such that $864 \cdot x \equiv 1 \bmod 899$.

$$864 = 2^5 * 3^3$$

So

$$864^{-1} = (2^5 * 3^3)^{-1} = (2^{-1})^5 * (3^{-1})^3$$

I made a program that will give me the inverse of a number

```
# mod n
n = 899

# limit l
l = 900

# array a
a = []

for i in range(0, l):
a.append([])
for j in range(0, l):
a[i].append((i * j) % n)

# get inverse
# the inverse of a number x is the number y such that (x * y) % n = 1

# search s
s = 2

# search for the inverse of s
for i in range(0, l):
if a[s][i] == 1:
print(f"Inverse of s mod n is: i", end="")
break
```

$$864^{-1} = (450)^5 * (300)^3$$

$$= 150^5 * 3^5 * 300^3 = 150^5 * 3^2 * 3^3 * 300^3 = 150^5 * 3^2 * (3 * 300)^3$$

Because we are modding by 899 we can replace $(3 * 300)^3$ with 1

$$= 150^5 * 3^2 = 150 * 150 * 150 * 150 * 3 * 150 * 3 = 150^3 * (150 * 3)^2$$

$$= 150^3 * 450^2 = (75 * 2)^3 * 450^2 = 75^3 * 2^3 * 450^2 = 75^3 * 2 * 2 * 2 * 450 * 450 = 75^3 * 2 * 900 * 900$$

We can replace those 900s with 1 because we are modding by 899

$$75^3 * 2 = 75^2 * 150 = (25 * 3)^2 * 150 = 25^2 * 3^2 * 150 = 25^2 * 1350$$

$$= 25^2 * (36^2 + 54) = 25^2 * 36^2 + 25^2 * 54 = (25 * 36)^2 + 25^2 * 54 = 900^2 + 25^2 * 54$$

We can the 900^2 with 1

$$= 1 + 25^2 * 54 = 1 + 625 * 27 * 2 = 1 + (175 + 450) * 27 * 2 = 1 + (2 * 175 + 900) * 27$$

$$= 1 + 2 * 175 * 27 + 900 * 27 = 1 + 2 * 175 * 27 + 27 = 1 + 350 * 27 + 27 = 1 + 27 * (350 + 1)$$

$$= 1 + 27 * (351) = 1 + 3 * 9 * (3 * 100 + 51) = 1 + 3 * (3 * 900 + 9 * 51) = 1 + 3 * (3 + 9 * 51)$$

$$1 + 3 * 3 + 3 * 9 * 51 = 1 + 9 + 1377 = 10 + 900 + 477 = 10 + 1 + 477 = 488$$

So $x = 488$

3. Story: I took a class on Ancient Greek Philosophy in college, and in the midst of one lecture the professor (extemporaneously) walked the class through Euclid's proof that $\mathbb{P}$ is infinite. Kudos to the prof for this, since their specialty had nothing to do with Math. But they said "... the proof also give a way to construct primes". I didn't bother to correct this, because I'm not one of those students who do that ☺

   Define the **Euclid number** e_n recursively (inspired by the proof of Theorem 13.4) as follows:

$$\begin{aligned} e_n &= e_0 e_1 e_2 \cdots e_{n-1} + 1 \qquad \text{for } n \geq 1 \\ e_0 &= 1 \end{aligned}$$

   (a) Are the Euclid numbers prime?

$$e_0 = 1$$
$$e_1 = e_0 + 1 = 1 + 1 = 2$$
$$e_2 = e_0 e_1 + 1 = 1(2) + 1 = 3$$
$$e_3 = e_0 e_1 e_2 + 1 = 1(2)(3) + 1 = 7$$
$$e_4 = e_0 e_1 e_2 e_3 + 1 = 1(2)(3)(7) + 1 = 43$$
$$e_5 = e_0 e_1 e_2 e_3 e_4 + 1 = 1(2)(3)(7)(43) + 1 = 1807$$
$$1807 = 13(139)$$

   Thus, all are not prime, but hey some of them are.

   (b) Show that $e_m \perp e_n$ for $m \neq n$.
   If $e_m \perp e_n$ then $\gcd(a, b) = 1$
   Because of, linear algebra $e_m \perp e_n$ implies $e_n x + e_m y = 1$ for some integers x and y.
   If you have $n > m$ then

$$e_n = e_0 e_1 e_2 \cdots e_{n-1} + 1$$

   e_m would have to be in the product, $e_0 e_1 e_2 \cdots e_{n-1}$ so some number of times e_m is e_n.

$$e_n = y e_m + 1$$

$$e_n - y e_m = 1$$

   Well, there is that linear algebra relationship.
   So then you can infer that $e_m \perp e_n$
   A similar argument would follow for if $n < m$