Tyler Nevell

101039497

Problem Set Week 9

P1

Part A:

- Our prime numbers are as follows: 2, 3, 7, 11, 13, 17, 19...
- (starting with 1) So our first 6 Euclidian numbers are:

$$(1x2) + 1 = 3$$
$$(1x2x3) + 1 = 7$$
$$(1x2x3x5) + 1 = 31$$
$$(1x2x3x5x7) + 1 = 211$$
$$(1x2x3x5x7x11) + 1 = 2311$$
$$(1x2x3x5x7x11x13) + 1 = 30031$$

The 6th Euclidian number is not a prime, as it's factors are 59 and 509.

Part B:

- As you can clearly see, the claim that E_n will be a prime number is false when $n = 6$. In our proof, we used the case that there are a finite number of primes, but this was shown to be false and infinite number of primes was proven. Since, E_n is always prime when there are a finite number of primes, and we've shown by example E_n is not always prime, there are not a finite number of primes.

P2

Let a,b be two positive natural numbers. Show that there exists $k \in N$ such that $a + kb$ is composite.

1. The definition of a composite number is a number that is divisible by 2 numbers that are not 1 and itself.

Proof 1: $a \geq 2$

- We set k to a and the equations becomes:

$$a + ab$$
$$a(1 + b)$$

- We set $(1 + b)$ to equal an arbitrarily named variable x.

Therefore: we now have the equation $a * x$ which is the definition of a composite number and therefore, to ensure the equation $a + kb$ will be a composite, we can set $k = a$ so long as $a \geq 2$.

QED

Proof 2: $a = 1$

- We can't apply the same rule from Case 1. So we set k to $(b + 2)$.

$$a = 1, 1 + (b + 2)b$$
$$1 + (b + 2)b = b^2 + 2b + 1$$
$$b^2 + 2b + 1 = (b + 1)^2$$

- Perfect squares such as $(b + 1)^2$ are composites by definition.

Therefore: in order for the equation $a + kb$ to be composite when $a = 1$, we can make $k = (b + 2)$.

QED

P3

Show that if someone knows a secret n and its encrypted form e, then she can compute the password s.

$e : n \oplus s$

- We use a simple example to show what the encrypted message looks like. According to XOR, for every message bit and it's corresponding key bit, if it is the same bit value, the encrypted bit equals 0. If the corresponding bits are of different value, then the encrypted bit equals 1. This was also highlighted through *logical* use of XOR that shows an XOR of 2 truth values is never $TRUE$ if both truth values are the same value. The XOR is only true when both truth values are of opposite values.

$$n = 11010010$$
$$s = 01110101$$

Using the previously stated rule, the encrypted message e is:

$$e = 10100111$$

$n : e \oplus s$

- These rules hold for decryption as well.

$$e = 10100111$$
$$s = 01110101$$

- We then get our original message n:

$$n = 11010010$$

So, if we want to crack the key s using plaintext attack, we can use $s : n \oplus e$.

$$n = 11010010$$
$$e = 10100111$$

- Which then gives us our Key s.

$$s = 01110101$$

Regardless of the number of bits used, this principle can be applied across the board. This is too vulnerable to attack if you have two elements of the problem. Hacker “0xc1ue1e55” is not l33t enough and needs to go back to school to learn proper cryptography.

P4

(A)

$\varphi(9)$ is rel. prime to $1, 2, 4, 5, 7, 8$.

$\varphi(9) = 6$

$\varphi(6)$ is rel. prime to $1, 5$.

$\varphi(6) = 2$

$\varphi(10)$ is rel. prime to $1, 3, 7, 9$.

$\varphi(10) = 4$

(B)

Write down all numbers that are not relatively prime to the number $77 = 7 \times 11$. Using this, compute $\varphi(77)$.

- 7, 11, 14, 21, 22, 28, 33, 35, 42, 44, 49, 55, 56, 63, 66, 70.

Every other number leading up to 77 is rel. prime. Therefore, we can take the number of numbers not rel. prime and subtract it from the number we're analyzing - 1, since we are only analyzing every number *up to* our n: 76. $76 - 16 = 60$. We get 60 numbers. $\varphi(77) = 61$

(C)

Proof 1: $n \geq 2$, If n is prime, then $\varphi(n) = n - 1$

By definition, prime numbers are only divisible by themselves and 1.

Any numbers that share a gcd of 1 are relatively prime. Since according to the def. of prime numbers, every number $1 \leq j < n$ is relatively prime to n, the list of rel. prime numbers to n are:

$\{n-1, n-2, \ldots, 2, 1.\}$

The count of numbers in the list above is $n - 1$. Since all numbers between 1 and n are relatively prime to n, we have $n - 1$ numbers that are relatively prime.

Therefore: $n \geq 2$, If n is prime, then $\varphi(n) = n - 1$.

Proof 2: $n \geq 2$, If $\varphi(n) = n - 1$, then n is prime

According to Euler Totient Function, the symbol phi φ is used on a number n to designate how many numbers between 1 and up to n are rel. prime to that number n.

$\varphi(n) = n - 1$ tells us there are $n - 1$ numbers in $\varphi(n)$ which are rel. prime to n. Definition of rel. prime numbers states that two numbers are relatively prime if their $gcd = 1$. Since every number up to n shares no common denominator besides itself and 1, n is not divisible by any number between 1 and up to n and is only divisible by itself and 1. By definition, n is prime.

Therefore: $n \geq 2$, If $\varphi(n) = n - 1$, then n is prime

QED

(D)

Show that $\varphi(n) = (p-1)(q-1)$ if n can be written as the product of two primes p, q.

Theorem: If $n = p * q$, then $\varphi(n) = (p-1)(q-1)$ where p and q are prime numbers.

Proof: Let p and q be primes and $n = p * q$.

$n = p * q$

Because $p * q$ is n and we can only analyze up to $n-1$, the largest multiple of p up to $n-1$ is $p * (q-1)$ or $(p * q - p)$. Same goes for multiples of q: $q * (p-1)$ or $q * p - q$.

Since n is divisible by p, and p is prime, n has a gcd of p with multiples of p. The count of those numbers is $q-1$ since p goes into $n-1$ a max of $q-1$ times.

Since n is divisible by q, and q is prime, n has a gcd of q with multiples of q. The count of those numbers is $p-1$ since q goes into $n-1$ a max of $p-1$ times.

- The count of numbers available to analyze is $n-1$. Since $n = p * q$, we can substitue in $p * q$ for n.

$$n - 1 = p * q - 1$$

The totient of n is the count of numbers that are relatively prime to n. $p * q - 1$ is our total count of numbers up to n. To find what numbers are rel. prime to n, we subtract from $p * q - 1$ the count of numbers that are not rel. prime to n which are multiples of p that appear $(q-1)$ times and multiples of q that appear $(p-1)$ times.

$$\varphi(n) = (p * q - 1) - (q - 1) - (p - 1)$$
$$\varphi(n) = p * q - 1 - q + 1 - p + 1$$
$$\varphi(n) = p * q - q - p + 1$$

- Factorize

$$\varphi(n) = (p-1)(q-1)$$

Therefore: If $n = p * q$, and p, q are prime numbers, then $\varphi(n) = (p-1)(q-1)$.

QED