Caleb Faruki
Dr. Xiaoxu Han
CISC4080 Algorithms
November 28, 2013

Homework 4

Part A

1. $\frac{2^{100}}{\ln(2^{100})} - \frac{2^{200}}{\ln(2^{200})} = \mathbf{1.159 \cdot 10^{58}}\ \textbf{\textit{primes}}$

2.

```
Naive Primality Test:
input: Arbitrarily large integer number.
output: Boolean. True if input is prime. False if input isn't prime.

1   if input < 2 then return FALSE
2   else if input % 2 == 0 then return FALSE
3   for each integer i (i=3; i< sqrt(input); i+=2)
4      if input % i == 0 then return FALSE
5   else return TRUE
```

Part D

1.
```
p = 19
q = 31
n = 589
e = 53
Φ(n) = 540
d = 377
```

2.
$$d = e^{-1} \bmod \Phi(n)$$
$$n = 589 = 19 \cdot 31$$
$$\Phi(n) = 18 \cdot 30 = 540$$
$$d = 53^{-1} \bmod 540 = 377$$

$$\Phi(n) = (p-1)(q-1) = pq-p-q+1 = (n+1)-(p+q)$$

$$p+q = (n+1)-\Phi(n)$$

$$q = (n+1)-\Phi(n)-p$$

$$n = p \cdot q$$

$$n = p \cdot [n+1-\Phi(n)-p]$$

3.

$$n = p[n+1-\Phi(n)]-p^2$$

$$p^2-p[n+1-\Phi(n)]+n = 0$$

Apply quadratic equation...

$$a=1 \ , \ b = -[n+1-\Phi(n)] \ , \ c=n$$

$$p \vee q = \frac{-b \pm \sqrt{(|b|^2-4ac)}}{2a}$$

Substitute values of a, b, c ... voila

Moral of the story: don't publish your Φ(n).