Homework 10

Physics II

Due Friday, June 3, 2022

College of the Atlantic. Spring 2022

There is one part to this assignment. There is no WeBWorK. I hope this isn't too disappointing. ☺

Part 1: Not WeBWorK. Below are some non-WeBWorK problems.

- If you want, you can do these problems in pairs and hand in one write-up.
- "Hand in" the problem on google classroom. You can take a picture of your work, or type up your work, or scan your work.

1. Evaluate the Euler totient function $\phi(N)$ for the following values of N:

    (a) $N = 15$
    (b) $N = 16$
    (c) $N = 17$

    There's no need to include a lengthy write-up, but please show your work.

2. Beowulf uses RSA with $(e = 5, n = 14)$ and sends you the encrypted message `5 8 6`. Decrypt this message, one numeral at a time, using $(d = 11, n = 14)$

3. (You will likely need to use wolframalpha to help you with these computations.) Suppose Anastajia and Beowulf are using an RSA public-key encryption to send a message from Beowulf to Ana. Suppose Ana chooses $p = 97$ and $p_2 = 89$.

    (a) What number n will Beowulf and Ana use as the modulus for their calculations?

    (b) Which of the following are possible choices that Ana could use for the public encryption exponent e?

        i. 89
        ii. 91
        iii. 100
        iv. 101

    (c) Suppose Ana chooses $e = 17$. Show that the choice of $d = 497$ satisfies the criteria for d.

    (d) Suppose that Beowulf wishes to send the message $m = 1001$ to Ana. (The message is the single number 1001, not four digits sent separately.) What would Beowulf get for the encrypted message?

    (e) How would Ana decrypt this message? Try it and see? Does she successfully recover Beowulf's original message?

4. **Optional:** Euler's theorem states that:

$$a^{\phi(N)} = 1 \mod N \; , \tag{1}$$

for any integer N for for any a that is co-prime to N. RSA encryption works because it is possible to find integers e, d, and N such that

$$(m^e)^d = m \mod N \; . \tag{2}$$

In the above equation e is the encryption exponent, d is the decryption exponent, N is the modulus, and m is the message.

Recall that the RSA recipe for finding e, d, and M is as follows:

(a) Choose two prime number p and q.

(b) The modulus N is given by $N = pq$.

(c) Calculate $\phi(N)$. Note that this is fast, since $\phi(pq) = (p-1)(q-1)$, if p and q are both prime.

(d) Choose e such that

   i. $1 < e < \phi(N)$,

   ii. e is co-prime with N and $\phi(N)$.

(e) Choose d such that $de \mod \phi(N) = 1$.

Use Euler's theorem to show that if e, d, and N are chosen as described above, then it follows that Eq. (2) is true.