Homework 09

Physics II

"Due" Friday, May 27, 2022[1]

College of the Atlantic. Spring 2022

There are two parts to this assignment.

Part 1: WeBWorK. Do Homework 09 which you will find on your WeBWorK page.

Part 2: 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. Encrypt the following message `WATCH OUT FOR THE BEES`. Use the word `BOHR` as a repeating key.
2. Decrypt the following message `ULWOWZZ EWILK HGZB`. The message was encoded using the description for course ES 3018 *Herpetology.*
3. **Optional**. The following message was encoded[2] [3]using a simple substitution scheme. I.e., each letter is encoded as some other letter. Decode the message.

```
R yldre svzex zj r grik fw kyv nyfcv, trccvu sp lj "Lezmvijv", r
grik czdzkvu ze kzdv reu jgrtv. Yv vogvizvetvj yzdjvcw, yzj
kyflxykj reu wvvczexj rj jfdvkyzex jvgrirkvu wifd kyv ivjk |
r bzeu fw fgkztrc uvcljzfe fw yzj tfejtzfljevjj. Kyzj uvcljzfe
zj r bzeu fw gizjfe wfi lj, ivjkiztkzex lj kf fli gvijferc
uvjzivj reu kf rwwvtkzfe wfi r wvn gvijfej evrivjk kf lj.
Fli krjb dljk sv kf wivv flijvcmvj wifd kyzj gizjfe sp nzuvezex
fli tzitcv fw tfdgrjjzfe kf vdsirtv rcc czmzex tivrklivj reu
kyv nyfcv fw erkliv ze zkj svrlkp. Efsfup zj rscv kf rtyzvmv
kyzj tfdgcvkvcp, slk kyv jkizmzex wfi jlty rtyzvmvdvek zj ze
zkjvcw r grik fw kyv czsvirkzfe reu r wfleurkzfe wfi zeevi
jvtlizkp.
```

[1] If you need extra time, that's totally fine.

[2] I wrote this problem eight years ago. I have no idea what the correct answer is.

[3] I am told by a student who has cracked this code that the statement is kinda weird and philosophical.

4. **Optional**. The Vigenère square—the square sorta crossword puzzle lookin thing—is actually an table for addition with letters, where the letters "wrap around". The mathematical term for this would be arithmetic modulo 26. One would refer to the letters as the set $\mathbb{Z}_{26}$, which is a set with arithmetic modulo 26.

   (a) Write out the addition and multiplication tables for $\mathbb{Z}_5$. (For example, the elements of $\mathbb{Z}_5$ are $\{0, 1, 2, 3, 4\}$, $2 + 4 = 1$, and $2 \times 4 = 3$

   (b) Write out the addition and multiplication tables for $\mathbb{Z}_6$.

   (c) Note that there is a difference between the multiplcation tables for $\mathbb{Z}_5$ and $\mathbb{Z}_6$. For $\mathbb{Z}_5$, each element appears once and only once in each row (except for the frist row), whereas this is not the case for $\mathbb{Z}_6$. Why do you think this is the case? What is different about $\mathbb{Z}_5$ and $\mathbb{Z}_6$? Make a conjecture about what must be true about n so that in the multiplication table for $\mathbb{Z}_n$ each number appears once and only once in each row except for the top row.

   (d) The next three problems lead you through a proof of the conjecture you might have formulated above. These problems are from Susan Loepp and William K. Wooters, *Protecting Information: Fomr Classical Error Correction to Quantum Cryptography*, Cambridge University Press, 2006.

      i. Let $a \in \mathbb{Z}_n$. Show that a and n are relatively prime (the only common demonimator of both a and n is 1) if and only if there exists an element $b \in \mathbb{Z}N$ such that $ab = 1$.

      ii. Let $a \in \mathbb{Z}_n$. Show that a and n are relatively prime if and only if a's row in the multiplication table of $\mathbb{Z}_n$ contains every element of $\mathbb{Z}_n$.

      iii. Show that n is a prime number if and only if in the multiplication table for $\mathbb{Z}_n$, except for the first row, all elements of $\mathbb{Z}_n$ appear in each row.

   The symbol "$\in$" is read "is in", or "is an element of". The statement $a \in \mathbb{Z}_n$ means that a is an element of or belongs to $\mathbb{Z}_n$. For example, $4 \in \mathbb{Z}_6$, but $7 \notin \mathbb{Z}_6$.