**Introduction to Cryptography (462)**
**Homework 02**
**T.J. Borrelli**
**Due: Thursday, September 21st, 2017 at 2pm**

- Be sure to put your NAME and Section number on the first page.
- If you upload your submission to the myCourses dropbox, I will only accept .pdf format and only the last thing you submit will be accepted.
- This homework is related to Chapter 1 in the Paar and Pelzl book.

1. **(2 Points)** Compute the following without a calculator (difficulty: easy):

   (a) $15 \cdot 29 \bmod 13$
   (b) $2 \cdot 29 \bmod 13$
   (c) $2 \cdot 3 \bmod 13$
   (d) $-11 \cdot 3 \bmod 13$

   The results should be given in the range from 0, 1, . . . , mod-1. Briefly describe the relationship between the different parts of the problem.

2. **(3 Points)** Compute the following without a calculator (difficulty: moderate):

   (a) $1/5 \bmod 13$
   (b) $1/5 \bmod 7$
   (c) $3 \cdot 2/5 \bmod 7$

3. **(6 Points)**

   (a) We consider the ring $\mathbb{Z}_4$. Construct a table which describes the addition of all elements in the ring with each other.

| + | 0 | 1 | 2 | 3 |
|---|---|---|---|---|
| 0 | 0 | 1 | 2 | 3 |
| 1 | 1 | 2 | . . . | |
| 2 | . . . | | | |
| 3 | | | | |

(b) Construct the multiplication table for $\mathbb{Z}_4$.

(c) Construct the addition and multiplication tables for $\mathbb{Z}_5$.

(d) Construct the addition and multiplication tables for $\mathbb{Z}_6$.

(e) There are elements in $\mathbb{Z}_4$ and $\mathbb{Z}_6$ without a multiplicative inverse. Which elements are those? Why does a multiplicative inverse exists for all nonzero elements in $\mathbb{Z}_5$.

4. **(3 Points)** What is the multiplicative inverse of 5 in $\mathbb{Z}_{11}$ , $\mathbb{Z}_{12}$, and $\mathbb{Z}_{13}$? You can do a trial-and-error search using a calculator or write a short program (you do not need to turn in the program here).

5. **(4 Points)** Compute the following without a calculator:

   (a) $3^2 \bmod 13$

   (b) $7^2 \bmod 13$

   (c) $3^{10} \bmod 13$

   (d) $7^{100} \bmod 13$

6. **(1 Point)** Discrete Log. Solve for $x$. (It's ok to use a calculator, trial-and-error or a short program):
   $7^x = 11 \bmod 13$

7. **(4 Points)** Find all integers $n$ between $0 \leq n < m$ that are relatively prime to $m$ for $m = 4, 5, 9, 26$. We denote the *number* of integers $n$ which fulfill the condition by $\phi(m)$. For example, $\phi(3) = 2$. This function is called "Euler's phi function" and we will see more about it later on. What is $\phi(m)$ for $m = 4, 5, 9, 26$ ?

8. **(3 Points)** Using an Affine Cipher with key parameters: $a = 7, b = 22$. Decrypt the text below:

   `falszztysyjzyjkywjrztyjztyynaryjkyswarztyegyyj`