# ECE 4802 HW 5

Thomas Mackintosh

28 November 2016

## 1 Homework Problems

### 1.1 8.1

Understanding the functionality of groups, cyclic groups and subgroups is important for the use of public-key cryptosystems based on the discrete logarithm problem. That's why we are going to practice some arithmetic in such structures in this set of problems.

Let's start with an easy one. Determine the order of all elements of the multiplicative groups of:

$\mathbf{Z}_5^* = \{1, 2, 3, 4\}$

| | |
|---|---|
| Element: 1 | $ord(1) = 1$ |
| Element: 2 | $2^1 = 2, 2^2 = 4, 2^3 = 3 \bmod 5, 2^4 = 1 \bmod 5, ord(2) = 4$ |
| Element: 3 | $3^1 = 3, 3^2 = 4 \bmod 5, 3^3 = 2 \bmod 5, 3^4 = 1 \bmod 5, ord(3) = 4$ |
| Element: 4 | $4^1 = 4, 4^2 = 1 \bmod 5, ord(4) = 2$ |

$\mathbf{Z}_7^* = \{1, 2, 3, 4, 5, 6\}$

| | |
|---|---|
| Element: 1 | $ord(1) = 1$ |
| Element: 2 | $ord(2) = 3$ |
| Element: 3 | $3^2 = 2 \bmod 7, 3^3 = 6 \bmod 7, 3^4 = 4 \bmod 7,$ $3^5 = 5 \bmod 7, 3^6 = 1 \bmod 7, ord(3) = 6$ |
| Element: 4 | $4^1 = 4, 4^2 = 2 \bmod 7, 4^3 = 1 \bmod 7, ord(4) = 3$ |
| Element: 5 | $5^1 = 5, 5^2 = 4 \bmod 7, 5^3 = 6 \bmod 7, 5^4 = 2 \bmod 7,$ $5^5 = 3 \bmod 7, 5^6 = 1 \bmod 7, ord(5) = 6$ |
| Element: 6 | $6^1 = 6, 6^2 = 1 \bmod 7, ord(6) = 2$ |

$\mathbf{Z}_{13}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}$
todo

### 1.2 8.2

We consider the group $\mathbf{Z}_{53}^*$. What are the possible element orders? How many elements exist for each order?