Jeremy Barthélemy  
ECE 746  
Hw. 1

1.  
(*Z*13*, \**)  
a. In order to be a valid group, this must satisfy the following three conditions:  
-The group operation is associative (which it is): 3\*(4\*2) = (3\*4)\*2  
-It has an identity element (which it does, element 1 for all a): a\*1 = 1\*a = a  
-Every element has an inverse element:  
1\*1 mod 13 = 1  
2\*7 mod 13 = 1  
3\*9 mod 13 = 1  
4\*10 mod 13 = 1  
5\*8 mod 13 = 1  
6\*11 mod 13 = 1  
12\*12 mod 13 = 1  
Thus, (*Z*13*, \**) is a valid group.  
b. To be an Abelian group, it must be commutative, which it is. (*Z*13*, \**) is an Abelian group.  
c. The group is finite.  
d. The order of this group is 13 (elements 0 – 12).   
e. All we need to do to determine whether or not this is a cyclic group is to find a generator.  
We find that indeed it is cyclic if we test 2i mod 13 with increasing values of i, we find the following values: {2, 4, 8, 3, 6, 12, 11, 9, 5, 10, 7, 1}. Since 2 is a generator for this group, we know that it must be a cyclic group as well.  
(*Z*26*,* +)  
a. It is associative and it has an identity element a + 0 = 0 + a = a.  
Each entity does have an inverse element as well, for example: 0 + 1 mod 26 = 1, 25 + 2 mod 26 = 1, 2 + 25 mod 26 = 1, etc., for all elements a. It is a valid group.  
b. 5+3 mod 26 = 3+5 mod 26, thus it is commutative, and it is an Abelian group.  
c. This is a finite group.  
d. The order of this group is 26 (elements 0 – 25).  
e. There are no generators, and so this is not a cyclic group.  
(*Z\**17*, \**)a. It is associative, there is an identity element (1), and there is an inverse for every element:  
1\*1 mod 17 = 1  
2\*9 mod 17 = 1  
3\*6 mod 17 = 1  
4\*13 mod 17 = 1  
5\*7 mod 17 = 1  
8\*15 mod 17 = 1  
10\*12 mod 17 = 1  
11\*14 mod 17 = 1  
16\*16 mod 17 = 1  
Thus it is a valid group.  
b. This is also an Abelian group, since it is commutative.c. This is a finite group.  
d. The order of this group is 16 (elements 1 – 16).e. We find that 3 is a generator as it generates the entire set of numbers: {3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6, 1}. Since there is a generator, it is a cyclic group.  
(*Z\**26*, \**)  
a.  
It is associative and there lies an identity element (1), but is there an inverse for each element?  
No, for example, there is no x such that 2\*x = 1. This is not a valid group.b. It would be an Abelian group if it were indeed a valid group as it is commutative.  
c. This group is finite.  
d. The order of this group is 25 (elements 1 – 25).  
e. This is not a valid group, and so it is not a cyclic group either.(*Z*+*,* +)  
a. The identity is not present (0), and so this cannot be a group.  
b. It is not a valid group, so it cannot be an Abelian group.  
c. Not finite  
d. Infinity  
e. It cannot be a cyclic group, as it is not a valid group at all.(*Z,* +)  
a. It is associative (5+2)+7 = 5+(2+7), it has an identity element: 0+a = a+0 = a, and there is an inverse element for each element. It is a valid group.  
b. It is an Abelian group as it is commutative. 5+2 = 2+5 = 7.   
c. This group is not finite.  
d. The order of this group is infinity.  
e. This is not a cyclic group as there is no generator for all possible values.  
  
2.a. What orders are possible for subgroups of this group?  
Since the order of this group is 16 (elements 1-16), it is possible to have subgroups of the following orders: 1, 2, 4, 8, and 16, as these values divide 16.b. Determine the order of each element of this group.   
There will be φ(15) = (3-1)\*(5-1) = 2\*4 = 8 generators in this group. This means that 8 of these elements from the 16 will have a full order of 16.  
We determine the order of each element below:  
For 1, the order is simply 1, 12 mod 17 = 1, and no matter how many more times we do this, we just get 1, so the order is 1.  
For 2, we perform the calculations for 2i mod 17 and get: {2, 4, 8, 16, 15, 13, 9, 1}.  
We can see that there are 8 elements in this subgroup, which divides 16.  
For 3, 31 mod 17 = 3, 3\*3 mod 17 = 9, 9\*3 mod 17 = 10, 10\*3 mod 17 = 13, 13\*3 mod 17 = 5, 5\*3 mod 17 = 15, 15 \* 3 mod 17 = 11, 11\*3 mod 17 = 16, 16 \* 3 mod 17 = 14, 14\*3 mod 17 = 8, 8\*3 mod 17 = 7, 7\*3 mod 17 = 4, 4\*3 mod 17 = 12, 12\*3 mod 17 = 2, 2 \*3 mod 17 = 6, 6\*3 mod 17 = 1. Thus we have the subgroup: {3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6, 1}, which contains all 16 elements! So we have 16 elements in our subgroup, which obviously divides 16, and so 3 is a generator.  
 Going through with 4i mod 17, we come up with {4, 16, 13, and 1} a subgroup of 4 elements, which, again, divides 16, as expected.  
Performing the same operations, we find that 5 is a generator, as the subgroup is this: { 5, 8, 6, 13, 14, 2, 10, 16, 12, 9, 11, 4, 3, 15, 7, 1}.  
Again, we have a generator in 6: {6, 2, 12, 4, 7, 8, 14, 16, 11, 15, 5, 13, 10, 9, 3, 1}.  
7 is also a generator: {7, 15, 3, 4, 11, 9, 12, 16, 10, 2, 14, 13, 6, 8, 5, 1}.  
8 produces only these elements: {1, 13, 2, 16, 9, 4, 15, 1}.  
9 produces only these elements: {9, 13, 15, 16, 8, 4, 2, 1}.  
10 is also a generator : {10, 15, 14, 4, 6, 9, 5, 16, 7, 2, 3, 13, 11, 8, 12, 1}  
11 is also a generator: {11, 2, 5, 4, 10, 8, 3, 16, 6, 15, 12, 13, 7, 9, 14, 1}  
12 is also a generator: {12, 8, 11, 13, 3, 2, 7, 16, 5, 9, 6, 4, 14, 15, 10, 1}  
13 only produces these four elements: {13, 16, 4, 1}  
14 is also a generator: {14, 9, 7, 13, 12, 15, 6, 16, 3, 8, 10, 4, 5, 2, 11, 1}  
15 only produces these eight elements: {15, 4, 9, 16, 2, 13, 8, 1}  
Finally, continuing with 16i mod 17, 16 produces only two elements: {16, 1}!  
So we see, it is true that we have only subgroups of orders that divide 16: 1, 2, 4, 8, and 16.  
Below is a full list of the elements and their respective orders:

|  |  |
| --- | --- |
| Element | Order |
| 1 | 1 |
| 2 | 8 |
| 3 | 16 |
| 4 | 4 |
| 5 | 16 |
| 6 | 16 |
| 7 | 16 |
| 8 | 8 |
| 9 | 8 |
| 10 | 16 |
| 11 | 16 |
| 12 | 16 |
| 13 | 4 |
| 14 | 16 |
| 15 | 8 |
| 16 | 2 |

c. Construct the multiplication table for the subgroup *<* 2 *>*.  
The subgroup <2> is as follows: {1, 2, 4, 8, 9, 13, 15, 16}. Taking these values in a table with a modulus of 17: We take integers A and B and multiply them, then perform the modulus operation with respect to 17, as seen in the table below.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| x | 1 | 2 | 4 | 8 | 9 | 13 | 15 | 16 |
| 1 | 1 | 2 | 4 | 8 | 9 | 13 | 15 | 16 |
| 2 | 2 | 4 | 8 | 16 | 1 | 9 | 13 | 15 |
| 4 | 4 | 8 | 16 | 15 | 2 | 1 | 9 | 13 |
| 8 | 8 | 16 | 15 | 13 | 4 | 2 | 1 | 9 |
| 9 | 9 | 1 | 2 | 4 | 13 | 15 | 16 | 8 |
| 13 | 13 | 9 | 1 | 2 | 15 | 16 | 8 | 4 |
| 15 | 15 | 13 | 9 | 1 | 16 | 8 | 4 | 2 |
| 16 | 16 | 15 | 13 | 9 | 8 | 4 | 2 | 1 |

3.  
3 is a generator and I use it to produce the following: {3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6, 1} for i from 1 to 16 in 3i mod 17.

|  |  |
| --- | --- |
| k | alog(k) |
| 1 | 3 |
| 2 | 9 |
| 3 | 10 |
| 4 | 13 |
| 5 | 5 |
| 6 | 15 |
| 7 | 11 |
| 8 | 16 |
| 9 | 14 |
| 10 | 8 |
| 11 | 7 |
| 12 | 4 |
| 13 | 12 |
| 14 | 2 |
| 15 | 6 |
| 16 | 1 |

|  |  |
| --- | --- |
| K | log(k) |
| 1 | 16 |
| 2 | 14 |
| 3 | 1 |
| 4 | 12 |
| 5 | 5 |
| 6 | 15 |
| 7 | 11 |
| 8 | 10 |
| 9 | 2 |
| 10 | 3 |
| 11 | 7 |
| 12 | 13 |
| 13 | 4 |
| 14 | 9 |
| 15 | 6 |
| 16 | 8 |

a. 15\*9 mod 17 = 16 upon calculation. We verify using the tables.  
15\*9 mod 17 = alog[(log[15] + log[9]) mod 16] = alog[(6+2) mod 16] = alog[8] = 16, which is the correct value

b. 13\*12 mod 17 = alog[(log[13] + log[12]) mod 16] = alog[(4+13) mod 16] = alog[1] = 3  
c. 6\*8 mod 17 = alog[(log[6] + log[8]) mod 16] = alog[(15+10) mod 16] = alog[9] = 14  
4.  
a.  
i qi ri xi

-2 - 34 0

-1 6 5 1

0 1 4 -6

1 4 1 7

The final result is in the bottom corner: the multiplicative inverse of 5 in this case is 7.   
b.

|  |  |
| --- | --- |
|  | i qi ri xi  -2 - 283 0  -1 8 34 1  0 3 11 -8  1 11 1 25 |

For this case, the multiplicative inverse of 34 is 25.  
Below is the code I built for this:  
/\*Please note that “i” is used to index the current value such as qi, ri, and xi. Ri is the current remainder, qi is the current quotient. Last\_ri, Last\_qi, and Last\_xi refer to the previous entries of ri, qi, and xi in the table, for calculation purposes. At the end, there is a “divide by zero” error, but this does not matter as this only occurs after the proper multiplicative inverse is calculated (the final value for xi).\*/  
  
a = 5; m = 34; last\_ri = m; last\_xi = 0; ri = 0; xi = 0; qi = 0;

print "i qi ri xi"; print "-2", " -", " ", m," ", 0;

q\_1 = last\_ri//a; ri = a;xi = 1;

print "-1 ", q\_1, " ", a," ", 1;

last\_qi = q\_1;i = 0;

for 0 in range(0,m-1):

new\_ri = last\_ri % ri;

qi = ri//new\_ri;

temp\_xi = last\_xi; last\_xi = xi;

xi = temp\_xi-last\_qi\*xi;

temp\_ri = ri; ri = new\_ri; last\_ri = temp\_ri;

print i," ", qi," ", ri," ", xi;

last\_qi = qi; i = i + 1;  
5.   
a. (x2 + 1) \* (x3 + x2 + 1) mod x4 + x + 1  
= x5 + x4 + x2 + x3 + x2 + 1 mod x4 + x + 1  
= x5 + x4 + x3 + 1 mod x4 + x + 1  
 11   
10011| 111001  
 10011  
 011111  
 10011  
 01100  
Result: x3 + x2  
  
b. (x2 + 1) \* (x + 1) mod x4 + x + 1  
= x3 + x2 + x + 1 mod x4 + x + 1  
Result: x3 + x2 + x + 1  
6.   
a. (x2 + 2) \* (x + 1) mod x3+ 2x2 + 1  
= x3 + x2 + 2x + 2 mod x3 + 2x2 + 1  
1122  
1201  
0221  
Result: 2x2 + 2x + 1  
  
b. (2x2 + x) \* 2x mod x3 + 2x2 + 1  
= x3 + 2x2 mod x3 + 2x2 + 1  
4200  
1201  
3003  
Result: 3x3 + 3  
  
7. The multiplication table for GF(23) will be 8x8, for bits ranging from 0-7.  
We perform the multiplication between the matching row and column, then perform the modular arithmetic for P(x) to get the result.  
Here is the multiplication for 4x5:  
0100 \* 0101 mod 1011  
 0100 (4)  
 0101 (5)  
 0100  
 00000  
010000  
010100 (20)  
  
 000010  
1011 | 010100  
 1011  
 00010  
Result: 0010  
  
The result for this calculation is highlighted in the table.   
Another example is 5 \* 5:  
101 \* 101 🡪 10001 mod 1011 🡪 0111 = 7

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **\*** | **0** | **1** | **2** | **3** | **4** | **5** | **6** | **7** |
| **0** | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| **1** | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |
| **2** | 0 | 2 | 4 | 6 | 3 | 1 | 7 | 5 |
| **3** | 0 | 3 | 6 | 5 | 7 | 4 | 1 | 2 |
| **4** | 0 | 4 | 3 | 7 | 6 | **2** | 5 | 1 |
| **5** | 0 | 5 | 1 | 4 | **2** | 7 | 3 | 6 |
| **6** | 0 | 6 | 7 | 1 | 5 | 3 | 2 | 4 |
| **7** | 0 | 7 | 5 | 2 | 1 | 6 | 4 | 3 |

8.  
a. We can represent P(x) as 10011. We have an order of 15 elements.   
b. The possible orders of the field elements are 1, 3, 5, and 15.  
c. To determine the order of both elements, we need to multiply these two elements by themselves repetitively until we find if they are able to generate all elements in the group.  
Generated in the same fashion as previously, below is a multiplication table for P(x) = 10011.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| × | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |
| 2 | 2 | 4 | 6 | 8 | 10 | 12 | 14 | 3 | 1 | 7 | 5 | 11 | 9 | 15 | 13 |
| 3 | 3 | 6 | 5 | 12 | 15 | 10 | 9 | 11 | 8 | 13 | 14 | 7 | 4 | 1 | 2 |
| 4 | 4 | 8 | 12 | 3 | 7 | 11 | 15 | 6 | 2 | 14 | 10 | 5 | 1 | 13 | 9 |
| 5 | 5 | 10 | 15 | 7 | 2 | 13 | 8 | 14 | 11 | 4 | 1 | 9 | 12 | 3 | 6 |
| 6 | 6 | 12 | 10 | 11 | 13 | 7 | 1 | 5 | 3 | 9 | 15 | 14 | 8 | 2 | 4 |
| 7 | 7 | 14 | 9 | 15 | 8 | 1 | 6 | 13 | 10 | 3 | 4 | 2 | 5 | 12 | 11 |
| 8 | 8 | 3 | 11 | 6 | 14 | 5 | 13 | 12 | 4 | 15 | 7 | 10 | 2 | 9 | 1 |
| 9 | 9 | 1 | 8 | 2 | 11 | 3 | 10 | 4 | 13 | 5 | 12 | 6 | 15 | 7 | 14 |
| 10 | 10 | 7 | 13 | 14 | 4 | 9 | 3 | 15 | 5 | 8 | 2 | 1 | 11 | 6 | 12 |
| 11 | 11 | 5 | 14 | 10 | 1 | 15 | 4 | 7 | 12 | 2 | 9 | 13 | 6 | 8 | 3 |
| 12 | 12 | 11 | 7 | 5 | 9 | 14 | 2 | 10 | 6 | 1 | 13 | 15 | 3 | 4 | 8 |
| 13 | 13 | 9 | 4 | 1 | 12 | 8 | 5 | 2 | 15 | 11 | 6 | 3 | 14 | 10 | 7 |
| 14 | 14 | 15 | 1 | 13 | 3 | 2 | 12 | 9 | 7 | 6 | 8 | 4 | 10 | 11 | 5 |
| 15 | 15 | 13 | 2 | 9 | 6 | 4 | 11 | 1 | 14 | 12 | 3 | 8 | 7 | 5 | 10 |

Using the multiplication table, we find:  
A(x) is 00110 in binary, which we can represent in decimal as the number 6. If we continue to square 6 and perform the modulus operation upon it, we find that A(x) will produce the following numbers: {6, 7, 1}. We have only three elements in this set, so A(x) is not a generator in this case. Note that there are three elements generated by A(x) here, which divides 15. Its order is 3.   
We can represent B(x) as 00010 in binary or as 2 in decimal form. If we continue to square 2 and perform the modulus operation by P(x) (or by using the multiplication table above for verification), we find that B(x) generates the following elements: {2, 4, 8, 3, 6, 12, 11, 5, 10, 7, 14, 15, 13, 9, 1}. We find that B(x) has an order of 15, and so it is a generator.   
d. A primitive entity is also known as a generator. A(x) is not a primitive entity as it is not a generator. B(x), on the other hand, is in this case a primitive entity, as, it is a generator.