CS346 - Asg 4 - David Ko - dpk326

Problem 1

I am a super senior after spending the first 3 years of my college career miserable as an electrical engineer and now I am finally going to graduate this May. Originally I took AP comp sci in high school and learned basic html and thought it was pretty easy so after I left EE, thought I would give CS a try but it was not the same, but it was at least enjoyable. No, I am not a Turing Scholar sadly and I am in social organizations like VSA.

Problem 2

a. This is a group because it is closed under closure; has the associative property; it has an identity element which would be the zero matrix since a matrix + a matrix full of zeros would equal itself; and it has an inverse.

b. This is not a group. It fulfills closure, associativity, and identity element, but it does not the inverse the 2x2 matrix wit only the real number '2' does not have an inverse since the determinant is 1/0.

c. This is not a group. For a matrix to have an inverse, all entries in the matrix must be *all* non-zero.

Problem 3

a. GCD(2015,5797)
-want to find the GCD of 2015 and 5797
-swap the numbers to make $a > b$ so it becomes GCD(5797,2015)
5797 mod 2015 = 1767
2015 mod 1767 = 248
1767 mod 248 = 31
So the GCD is 31.

b. $15^{-1} \pmod{346}$

Here we set it up like the Euclidean algorithm, but for inverse:

$346 = 15 * (x) + 1$

Calcuating for x,

$346 = 15 * (23) + 1$

Now, working backwards we get:

$346 - 345 = 1$

Now subbing for 346:

$(15 * 23 + 1) - 345 = 1$

Now subbing for 345 we get:

$(15 * 23 + 1) + 15 * (-23) = 1 \pmod{346}$

So we take 346 - 23 = 323 and we sub it back in for -23:

$(15 * 23 + 1) + 15 * (323) = 1 \pmod{346}$

As we can see, the first part $(15 * 23 + 1) \bmod 346$ goes to 0, so we can remove it,

So we are left with $15 * (323) = 1 \pmod{346}$,

And now we know that the answer to $15^{-1} \pmod{346}$ is 323.

Problem 4

a. Subgroups: The group itself and {1} are the trivial groups so they are subgroups, {1,2,3}, {1,2,4}, {1,2,5}, {1,2}, {1,3}, {1,4}, {1,5}, {1,6}, {1,7}, {1,8}, {1,9}, {1,10}.

b. Order of the group is $\Phi(p) = p - 1 = 11 - 1 = 10$.

c. The generators of this group are 2, 6 and 8.

The way I calculated this was I was through each number in the group and figured out if it hit all members: For example for 8: **8** $\rightarrow$ 64 mod 11 = **9**$\rightarrow$72 mod 11 = **6**$\rightarrow$48 mod 11 = **4**$\rightarrow$32 mod 11 = **10**$\rightarrow$80 mod 11 = **3**$\rightarrow$24 mod 11 = **2**$\rightarrow$16 mod 11 = **5**$\rightarrow$40 mod 11 = **7**$\rightarrow$56 mod 11 = **1**

Problem 5

a. $7^{2015346001} \bmod 11$.

Using the formula on the powerpoint lectures we get:

$7^{(201534600*10)+1}$ with α being $0 \leq 1\alpha = 1 \leq 10$

$7^{(201534600*10)} * 7^1$

$= 7^1$

b. $15^{23}(mod 1051)$ and use repeated squaring.

We first find the powers of 2 that make up 23 which are:

16, 4, 2, and 1.

So we have $15^{16+4+2+1}(modulo 1051)$

Split up: $15^{16}(modulo 1051) * 15^{4}(modulo 1051) * 15^{2}(modulo 1051) * 15^{1}(modulo 1051)$

$15^{1}(modulo 1051) = 15$. Then we take $15^{2}(modulo 1051) = 225$.

Now we take $225^{2}(modulo 1051)$ to get $15^{4}(modulo 1051)$ which is 177.

To get $15^{8}(modulo 1051)$ we take $15^{4}(modulo 1051)$ and then square it then take the (modulo 1051) which is $177^{2}(modulo 1051) = 850$.

To get $15^{16}(modulo 1051)$, we take $850^{2}(modulo 1051) = 463$.

Now we take the values 15, 225, 177, and 463 for the respective square 1, 2, 4, 16 and we multiply them together and take the modulo 1051:

$(15 * 225 * 177 * 463)(modulo 1051) = 312$.

So $15^{23}(modulo 1051) = 312$.

Problem 6

The elements with $p = 35$ are {1, 2, 3, 4, 5, 6, 7, 8, 9, 10 , 11, 12,13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33, 34}. Basically 1 to p-1.

Problem 7

The order of a group G is defined as the size of $|G|$ of the set G

Assume there exists an element $a \in G$ with order greater than k. Consider the set $\{a, a^2, ...a^k\}$ - by our assumption, since the order of a is greater than k, none of these elements are unity, therefore there exist $i,j \leq k, i \neq j$ such that $a^i = a^j$.

If there exists an element $a > k$, for example lets say the order of a group G is $k = 15$ and that there exists an element a that is 18, which is $> k$. This is a straigh contradiction of the definition of order of a group which is the cardinality of the group G, meaning the elements of the group G are from 0 to 15 and that the element a which is 18 is not included. Therefore, there cannot be an element a that is $> k$.

Problem 8

I really enjoy private key encryption because its simplistic and

only requires one key to be shared between the users and not different keys making it more straight forward than public key encryption.