EE 8372 CRYPTOGRAPHY & DATA SECURITY

Homework 9
31 March 2020

Professor Dunham
Due: 7 April 2020

Review Text: Chapter 8.

1. For the following multiplicative groups, determine the order of all elements in the group. Create a table with two rows for each group, where the top row contains each element a and the order ord(a) is in the row immediately below it.

   (a) $\mathbb{Z}_3^*$.

   (b) $\mathbb{Z}_{11}^*$.

   (c) $\mathbb{Z}_{17}^*$.

2. We now study the groups from Problem 1.

   (a) How many elements does each of the multiplicative groups have?

   (b) Do all orders from above divide the number of elements in the corresponding multiplicative group?

   (c) Which of the elements are primitive elements?

   (d) Verify for the groups that the number of primitive elements is given by $\varphi(|\mathbb{Z}_p^*|) = \varphi(\varphi(p))$.

3. Consider the group $\mathbb{Z}_{67}^*$. What are the possible element orders? How many elements exist for each order?

4. In this exercise we want to identify primitive elements (generators) of a multiplicative group since they play a big role in the Diffie-Hellman Key Exchange (DHKE) and in many other public-key schemes based on the Discrete Logarithm (DL) problem. You are given a prime $p = 5557$ and the corresponding multiplicative group $\mathbb{Z}_{5557}^*$.

   (a) Determine how many generators exist in $\mathbb{Z}_{5557}^*$.

   (b) What is the probability of a randomly chosen element $a \in \mathbb{Z}_{5557}^*$ being a generator?

   (c) Determine the smallest generator $a \in \mathbb{Z}_{5557}^*$ with $a \geq 1060$. *Hint:* The identification can be done naively through testing all possible factors of the group cardinality $p-1$, or more efficiently by checking the premise that $a^{(p-1)/q_i} \neq 1 \bmod p$ for all prime factors q_i with $p-1 = \Pi q_i^{e_i}$. You can simply start with a = 1060 and repeat these steps until you find a respective generator of $\mathbb{Z}_{5557}^*$. Note that this algorithm is equivalent to the Random Primitive Root Modulo Prime given in Topic #11.

   (d) What measures can be taken in order to simplify the search for generators for arbitrary multiplicative groups $\mathbb{Z}_p^*$?

5. Let α be a primitive root of $\mathbb{Z}_p$ where p is a prime number. Show that

$$L_\alpha(\beta_1\beta_2) \equiv L_\alpha(\beta_1) + L_\alpha(\beta_2) \pmod{(p-1)}.$$

Use the fact for integers j and k that $\alpha^j \equiv \alpha^k \pmod{p}$ if and only if $j \equiv k \pmod{(p-1)}$.

6. Consider the finite field $\mathbb{Z}_{13}$.

   (a) Show that 2 is a primitive root of $\mathbb{Z}_{13}$.

   (b) Compute $\log_2(9)$ and $\log_2(7)$.

   (c) Apply the results of problem 5 above to compute $\log_2(9 \times 7)$.

7. A positive integer is called B-smooth if none of its prime factors is greater than B. How many 3-smooth numbers are there less than 113? Note that 1 is a unit and not a prime number.

8. Consider $\mathbb{Z}_{7777727}$, the finite field for prime $7,777,727_{10}$ (base 10 number), along with the primitive root 5. Let $FB(n)$ denote the Factor Base for the number n and consists of the first n primes. For example, $FB(5) = \{2,3,5,7,11\}$. Use the Index Calculus Algorithm to find the discrete logarithm of $7,654,321$ over $FB(40)$. The table on the next page provides the discrete logarithm for the primes in $FB(40)$. *Note:* You can use a subset of $FB(40)$, keeping in mind that the larger the Factor Base, the higher the probability that a randomly chosen number will be p-smooth for the largest prime p in your factor base. For example, there are $464,693$ 173-smooth number less than $7,777,727$, about 6%. Also, use the result of Problem 5 to keep your discrete logarithm to a reasonable size. I point out that some people chose to add "-1" which is congruent to "$p-1$" into the factor base.; but it is not necessary. Finally, be sure to provide the random exponent and factorization of the associated B-smooth number you generated.

Prime - p	Discrete Logarithm - $log_5(p)$
2	4695286
3	4282940
5	1
7	2398772
11	1446375
13	608610
17	6300817
19	6976405
23	2656693
29	4885159
31	5315314
37	4528331
41	1919109
43	4803635
47	1830814
53	6565675
59	2776250
61	4467465
67	459688
71	1763611
73	6431281
79	7494069
83	2437332
89	3400986
97	2998612
101	2510138
103	1870726
107	2853045
109	5303601
113	372144
127	1551795
131	4592492
137	491320
139	1770767
149	2227560
151	544225
157	6975397
163	1214128
167	2689843
173	4647953