AM 106: Applied Algebra **Prof. Madhu Sudan**

Problem Set 3

Assigned: Wed. Sept. 20, 2017 Due: Tue. Sept. 26, 2017 (11:59 PM)

- You may submit your solutions via assignment page on the canvas website of the course.
- For collaboration and late days policy, see course website at `http://madhu.seas.harvard.edu/courses/Fall2017`
- Aim for clarity and conciseness in your solutions, emphasizing the main ideas over low-level details. Justify your answers except when otherwise specified.

Problem 1. (Cyclic groups) Which of the following are cyclic groups? For those that are not, justify your answers. For those that are, list all generators.

1. $\mathbb{Z}_{18}$.
2. $\mathbb{Z}_8^*$.
3. $\mathbb{Z}_{19}^*$.
4. D_5. (Please use the Rot_k and Ref_k notation for elements of D_n from lecture.)
5. $\mathbb{R}$.

Problem 2. (Subgroups) Draw the subgroup lattices for each of the following groups.

1. $\mathbb{Z}_{18}$
2. $\mathbb{Z}_8^*$.
3. $\mathbb{Z}_{19}^*$.
4. D_5. (Please use the Rot_k and Ref_k notation for elements of D_n from lecture.)

Problem 3. (Cauchy's Theorem) Let G be a finite group, and p a prime number. Let S be the set of all p-tuples of group elements $(g_0, \ldots, g_{p-1})$ whose product $g_0 g_1 \cdots g_{p-1}$ equals the identity e. Define an equivalence relation $\sim$ on S where $(g_0, \ldots, g_{p-1}) \sim (h_0, \ldots, h_{p-1})$ if the two p-tuples are cyclic shifts of each other, i.e. there is an $k \in \mathbb{Z}_p$ such that $h_i = g_{i+k \bmod p}$ for all $i \in \mathbb{Z}_p$.

1. Prove that all of the equivalence classes of $\sim$ are of size p or of size 1, and characterize all of the equivalence classes of size 1.

2. Show that if p divides $|G|$, then the number of equivalence classes of size 1 must be divisible by p. (Hint: analyze $|S|$.)

3. Deduce Cauchy's Theorem: if a prime p divides the order of a finite group G, then G has an element of order p.

Problem 4. (Diffie–Hellman in groups with small factors) Let $G = \langle g \rangle$ be a cyclic group of order q, and let d be a divisor of q. Recall that the Diffie-Hellman "key-exchange" protocol would definitely become insecure if there is a polynomial algorithm A that, given as inputs g^x and g^y for uniformly chosen x and y has a decent chance of outputting g^{xy}. (Formally, DH is insecure if $\Pr_{x,y}[A(g^x, g^y) = g(xy] \geq 1/\log q.)$ A stronger notion of security (weaker notion of insecurity) is the following, which says that the scheme is insecure if there is some polynomial time algorithm $B(a, b, c)$ that outputs "YES/NO" [1] such that B is more likely to output YES if the input triple is of the form (g^x, g^y, g^{xy}) than if the input is (g^x, g^y, g^z) for three independent and uniformly chosen x, y, z (so formally $\Pr_{x,y}[B(g^x, g^y, g^{xy}) = \text{YES}] \geq \Pr_{x,y,z}[B(g^x, g^y, g^z)] = \text{YES}] + 1/\log q$). The Decisional Diffie-Hellman assumption for a group G asserts that G is secure even in this stronger sense. Our goal is show that if the order of a group G has a small factor then the Decisional Diffie-Hellman assumption is not true for G.

1. For an element $a = g^x$ of G, show that d divides x if and only if $a^{q/d} = e$. Thus, one can efficiently test whether an element a is a d'th power in G by exponentiation.

2. Suppose we choose $x, y, z \in \mathbb{Z}_q$ uniformly at random. Calculate the probability that both g^x and g^{xy} are d'th powers, and the probability that both g^x and g^z are d'th powers.

3. Deduce that the Decisional Diffie–Hellman Assumption is false for G if the (known) order of G has a small factor (e.g. 2).

[1] YES for "Yes - this is a Diffie-Hellman triple" and NO for "No - this is not".