AM 106/206: Applied Algebra	**Prof. Salil Vadhan**

Problem Set 3

Assigned: Mon. Sept. 25, 2010 — Due: Fri. Oct. 1, 2010 (2:10 PM sharp)

- You may submit your problem sets in the AM106 in the Maxwell–Dworkin basement, or electronically by email to `am106-hw@seas.harvard.edu`. If you use LaTeX, please submit both the source (`.tex`) and the compiled file (`.pdf`). Name your files `PS3-yourlastname`.
- Aim for clarity and conciseness in your solutions, emphasizing the main ideas over low-level details. Justify your answers except when otherwise specified.
- Problems marked [AM106] or [AM106-X] are for AM106 students (though AM206 students should confirm that they know how to do them), and those marked [AM206-X] are for AM206 students. However, AM106 students can do a problem marked [AM206-X] instead of one marked [AM106-X] (for the same value of X) if they wish (out of interest, or for a challenge). If you wish to keep the option of staying in either AM106 or AM206 open until add/drop date, then you should do all problems marked [AM106] and all problems marked [AM206-X].

Problem 1. (Cyclic groups [AM106-A]) 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 [AM206-A]) 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 [AM106-B]) Let $G = \langle g \rangle$ be a cyclic group of order q, and let d be a divisor of q.

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

Problem 5. (Discrete log in square-root time [AM206-B]) Let G be a cyclic group with a known generator g and known order q. Give a randomized algorithm[1] that, on input $a \in G$, with probability at least $1/4$ computes $x \in \mathbb{Z}_q$ such that $g^x = a$, using at most $O(\sqrt{q} \cdot \log q)$ multiplications of elements of G. (Hint: choose $x_1, \ldots, x_t, y_1, \ldots, y_t \in \mathbb{Z}_q$ uniformly at random for an appropriate choice of $t = O(\sqrt{q})$ and bound the probability that there is no intersection between the sets $\{g^{x_i}\}$ and $\{a \cdot g^{y_i}\}$. It may be convenient to first bound the probability that $2t$ uniformly random group elements are all distinct.)

[1] A randomized algorithm is one that can "toss coins," and more generally sample random numbers from any desired interval $\{0, \ldots, m-1\}$. Generally we only require such algorithms to compute a correct answer with high probability over their coin tosses. The success probability of a randomized algorithm can usually be amplified by repetition, e.g. repeating your algorithm 10 times will find the correct x with probability $1 - (3/4)^{10} > .94$.