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

Problem Set 5

Assigned: Sat. Oct. 16, 2010 Due: Fri. Oct. 22, 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 `PS5-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. (Cosets [AM106]) Let $H = \{e, (12)(34), (13)(24), (14)(23)\} \leq S_4$.

1. List the left-cosets of H in S_4.
2. We can also view H as a subgroup of S_6. How many left-cosets does H have in S_6?

Problem 2. (Subgroups of $\mathbb{C}^*$) Determine all of the finite subgroups of $\mathbb{C}^*$. Justify your answer. (Hint: what are the solutions to $a^n = 1$ in $\mathbb{C}^*$?)

Problem 3. (Orbits and Stabilizers for the Cube) Let G be the group of rotational symmetries of a regular cube in $\mathbb{R}^3$. (We do not include reflections in G.)

1. Among points s on the surface of the cube (including edges and corners), what are the possible orbit sizes? For each answer a you give, provide an example of a point s with with $|\mathrm{orb}_G(s)| = a$.
2. For each point s above, describe $\mathrm{stab}_G(s)$.

Problem 4. (Classification of Abelian Groups [AM106-A]) Determine which of the following groups are isomorphic to each other:

1. $\mathbb{Z}_{40}$.
2. $\mathbb{Z}_8 \times \mathbb{Z}_5$.

3. $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_5$.

4. $\mathbb{Z}_{55}^*$.

5. $\mathbb{Z}_{88}^*$.

6. $\mathbb{Z}_{100}^*$.

Problem 5. (Richness of $\mathbb{Z}_n^*$ [AM206-A]) Dirichelet's Theorem says that if a and b are relatively prime integers, then the arithmetic progress $\{a + tb : t \in \mathbb{Z}\}$ contains infinitely many prime numbers. Use this to show that for every finite abelian group G, there is an $n \in \mathbb{N}$ such that $G \lesssim \mathbb{Z}_n^*$. (This result is similar in spirit to Cayley's Theorem, which says that for every finite group (even non-abelian), there is an $n \in \mathbb{N}$ such that $G \lesssim S_n$.)

Problem 6. (Testing Squares)

1. Provide an efficient (polynomial-time) algorithm that given the prime factorization of an odd number N and an element $x \in \mathbb{Z}_N^*$, decides whether x is a square in $\mathbb{Z}_N^*$ (i.e. whether there exists a $y \in \mathbb{Z}_N^*$ such that $y^2 \bmod N = x$). (You may use the solution to Problem 4 on Problem Set 3.)

2. [AM106-B] Use your algorithm to determine which of the following elements of $\mathbb{Z}_{495}^*$ are squares: 122, 124, 211. (You don't need to show all calculations, but enough to indicate that you are using your algorithm.)

3. [AM206-B] When $N = pq$ for distinct primes p, q that are both congruent to 3 modulo 4, provide a polynomial-time algorithm that, given p, q, and a square $x \in \mathbb{Z}_N^*$, finds all of the square roots of x in $\mathbb{Z}_N^*$. (Hint: first show that $x^{(p+1)/4}$ is a square root of x modulo p.)

There is no known polynomial-time algorithm for testing squareness (aka quadratic residuosity) modulo N without being given the factorization of N, and indeed a number of cryptographic protocols are built upon the assumption that this problem is inherently intractable.