

CSCI 381 - Advanced Cryptography - Fall 2005
George Washington University

Homework I

due 7 September

10%

Show all work. You will be graded almost entirely on how you get to the solution, and not on whether you get there. More efficient and elegant solutions will receive higher marks.

1. For each of the following sets (a) the roots of $x^3 - 1$ and (b) the roots of $x^4 - 1$, answer the following:
 - (i) Is the set a group under multiplication?
 - (ii) If so, is the set a cyclic group under multiplication? If so, list all generators of the group.
2. When, if ever, is the set of roots of $x^n - 1$ (the n^{th} roots of unity) a group under multiplication? When, if ever, is it a cyclic group? If it is a cyclic group, list all generators.
3. A quarter of the numbers in a set of numbers are square numbers. Randomly picking five numbers from the set (with replacement) find the probability for the majority of the picked numbers being squares.
4. Show that the smallest group - under regular addition - containing integers m and n is the cyclic group generated by $h = \gcd(m, n)$, i.e. that the smallest group containing both m and n is $\{\dots - 2h, -h, 0, h, 2h, \dots\}$.
5. Show that the intersection of the cyclic group generated by m : $\{\dots - 2m, -m, 0, m, 2m, \dots\}$ and that generated by n : $\{\dots - 2n, -n, 0, n, 2n, \dots\}$ is a group and that it is generated by the lowest common multiple (lcm) of m and n . The lcm of m and n is defined as follows: $g = \text{lcm}(m, n)$, if and only if, for all integers j such that $m|j$ and $n|j$, $g|j$.