Math 105, Fall 2010, HW2

1. If p is an odd prime and $p-1=2^j k$, where k is odd, show that there is an element in $\mathbb{F}_p^*$ of order 2^j, and that any such element is a quadratic nonresidue modulo p.

2. With the same notation as the previous problem, show that $\alpha \in \mathbb{F}_p^*$ has order 2^j if and only if $\alpha^{2^{j-1}} = -1$.

3. Continuing with these thoughts, describe a deterministic, polynomial-time algorithm to produce a quadratic nonresidue modulo p given the "super power" of being able to take square roots of quadratic residues modulo p. (That is, each call to this super power of yours counts as just one step in the final tally of bit operations.)

4. If G is a cyclic group (under multiplication) of order n and $3 \nmid n$, show that every element of G is a cube. Give a deterministic algorithm for finding cube roots in G that takes $O(\log n)$ group operations.

5. If G is a cyclic group of order n and $3 \mid n$, show that exactly $1/3$ of the elements of G are cubes and give a criterion akin to Euler's criterion for squares that recognizes cubes.

6. Continuing with this thought, describe a random algorithm that quickly can find a cube root of a cube in G.