CS174 Sp2001 **Homework 9** **due: April 12, 2001**

This homework is due by 5pm on Thursday April 12th. Please hand it to the CS174 homework box on the second floor of Soda Hall.

1. List all possible values of n such that the multiplicative group $\mathbb{Z}_n^*$ is cyclic and has order which is a power of 2, i.e. $\phi(n) = 2^k$.

2. If $n = 5^k$ so that $\mathbb{Z}_n^*$ is cyclic, what fraction of the elements of $\mathbb{Z}_n^*$ (the multiplicative group) are generators?

3. Suppose that a message M is encrypted using RSA twice, as $C_1 = M^{e_1} (\mathrm{mod}\ \ n)$ and $C_2 = M^{e_1} (\mathrm{mod}\ \ n)$. Note that the encryption keys are different, but the modulus n is the same in both cases. Show that M can be recovered from C_1 and C_2 in polynomial time.

4. If q is a prime, then $p = 2q + 1$ is also prime in some cases. Assuming q is large and p is prime, what fraction of the elements in $\mathbb{Z}_p^*$ are generators? Combinations like this are important in discrete-log crypto-systems.