Problem Set 6

Due: March 20

Reading: Chapter 8.11. *RSA Cryptosystem*. Chapter 9. *Directed Graphs* through 9.4. *Walk Relations*.

Problem 1.
Suppose the RSA modulus $n = pq$ is the product of distinct 200 digit primes p and q. A message $m \in [0..n)$ is called *dangerous* if $\gcd(m,n) = p$ or $\gcd(m,n) = q$, because such an m can be used to factor n and so crack RSA.

Estimate the fraction of messages in $[0..n)$ that are dangerous to the nearest order of magnitude.

Problem 2. **(a)** Give an example of a digraph with two vertices $u \neq v$ such that there is a path from u to v and also a path from v to u, but no cycle containing both u and v.

(b) Prove that if there is a positive length walk in digraph that starts and ends at node v, then there is a cycle that contains v.

Problem 3.
Suppose that there are n chickens in a farmyard. Chickens are rather aggressive birds that tend to establish dominance in relationships by pecking; hence the term "pecking order." In particular, for each pair of distinct chickens, either the first pecks the second or the second pecks the first, but not both. We say that chicken u *virtually pecks* chicken v if either:

- Chicken u directly pecks chicken v, or
- Chicken u pecks some other chicken w who in turn pecks chicken v.

A chicken that virtually pecks every other chicken is called a *king chicken*.

We can model this situation with a *chicken digraph* whose vertices are chickens with an edge from chicken u to chicken v precisely when u pecks v. In the graph in Figure 1, three of the four chickens are kings. Chicken c is not a king in this example since it does not peck chicken b and it does not peck any chicken that pecks chicken b. Chicken a *is* a king since it pecks chicken d, who in turn pecks chickens b and c.

In general, a *tournament digraph* is a digraph with exactly one edge between each pair of distinct vertices.

(a) Define a 10-chicken tournament graph with a king chicken that has outdegree 1.

(b) Describe a 5-chicken tournament graph in which every player is a king.

(c) Prove

Theorem (*King Chicken Theorem*)**.** *The chicken with the largest outdegree in an n-chicken tournament is a king.*

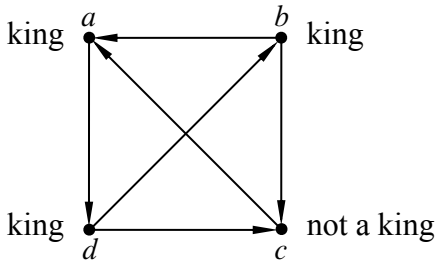

Figure 1 A 4-chicken tournament in which chickens a, b, and d are kings.

.

The King Chicken Theorem means that if the player with the most victories is defeated by another player x, then at least he/she defeats some third player that defeats x. In this sense, the player with the most victories has some sort of bragging rights over every other player. Unfortunately, as Figure 1 illustrates, there can be many other players with such bragging rights, even some with fewer victories.