Staff Solutions to Problem Set 6


STAFF NOTE: Lectures covered: RSA, digraphs: Walks and Paths

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.

Solution. Either \( 10^{-200} \) or \( 10^{-199} \) is acceptable.

For \( m \in [0..pq) \),
\[
\gcd(m, pq) = p \iff p \mid m.
\]

The fraction of numbers divisible by \( p \) in an interval is \( 1/p \), and since \( 10^{199} \leq p < 10^{200} \), \( 1/p \) is on the order of \( 1/10^{200} \). The same logic holds for \( q \).

Because \( n = pq \), none of the messages \( m \in [0..n) \) can be divisible by both \( p \) and \( q \), so the total fraction of dangerous messages is approximately \( 1/p + 1/q \), which can be on the order of \( 10^{-200} \) or \( 10^{-199} \) depending on \( p \) and \( q \).

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 \( v \).

Solution. \( u \rightarrow w \rightarrow v \rightarrow w \rightarrow u \)

(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 \( v \).

Solution. By the WOP, there is a shortest positive length walk from \( v \) to \( v \). We claim this walk must be a cycle.

Suppose to the contrary that some vertex \( w \neq v \) occurred twice on the walk. Then removing the positive length walk from \( w \) to \( w \) would leave a shorter walk from \( v \) to \( v \), contradicting the choice of shortest walk. So if the shortest walk was not a cycle, the vertex \( v \) must have an occurrence that is not at the beginning or end of the walk. In that case, the walk from the initial \( v \) to the non-end occurrence of \( v \) would be a shorter walk from \( v \) to \( v \), again contradicting the choice of shortest walk.

Since both ways that the shortest positive length walk from \( v \) to \( v \) could fail to be a cycle led to contradictions, we conclude that this shortest walk must be a cycle.
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.

\[ \begin{array}{cccc}
\text{king} & a & b & \text{king} \\
\text{king} & d & e & \text{not a king}
\end{array} \]

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

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

**Solution.** 1 pecks 2 and 2 pecks 3–10 and 3–10 peck 1.

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

**Solution.** An example is illustrated in Figure 2.

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

Solution. Proof. By contradiction. Let $u$ be a node in a tournament graph $G = (V, E)$ with maximum outdegree and suppose that $u$ is not a king. Let $Y = \{v \mid (u \rightarrow v) \in E\}$ be the set of chickens that chicken $u$ pecks. Then $\text{outdeg}(u) = |Y|$. Since $u$ is not a king, there is a chicken $x \not\in Y$ (that is, $x$ is not pecked by chicken $u$) and that is not pecked by any chicken in $Y$. Since for any pair of chickens, one pecks the other, this means that $x$ pecks $u$ as well as every chicken in $Y$. This means that

$$\text{outdeg}(x) = |Y| + 1 > \text{outdeg}(u).$$

But $u$ was assumed to be the node with the largest degree in the tournament, so we have a contradiction. Hence, $u$ must be a king.

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.