CS 70 Worksheet: Midterm Review

1 Functions and Modular Arithmetic

1. Consider $f(x) = 3x \pmod 5$. Is this function bijective?

2. Consider $f(x) = 4x \pmod{14}$. Is this function bijective?

3. Take any modulus n. For $a \in \{1 \dots n-1\}$, when is $f(x) = ax$ bijective? When does a have an inverse in general?

4. If $a \cdot b \equiv 0 \pmod p$ for p prime, what can we say about a and b?

5. If $f(x) = ax$ is bijective mod n, what can we say about $1 \cdot 2 \cdot \dots (n-1)$ and $1 \cdot 2 \cdot \dots (n-1) \cdot a^{n-1}$.

6. Prove Fermat's little theorem: If p is a prime number, and $a \in \{1 \dots p-1\}$, then $a^{p-1} \equiv 1 \pmod p$..

7. The integer a is a quadratic residue of n if $gcd(a, n) = 1$ and $x^2 \equiv a \pmod n$ has a solution. Prove that if p is prime, $p > 2$, then there are $\frac{p-1}{2}$ quadratic residues of p among $\{1, \dots, p-1\}$.

2 Proofs and Previous Problems

1. Prove that if $n^2 \not\equiv 1 \pmod 7$, then $n \not\equiv 1 \pmod 7$.

2. Use induction to prove that $1 + \frac{1}{2} + \dots + \left(\frac{1}{2}\right)^n < 2$ for all n. (Hint: strengthen the inductive hypothesis)

3. Show that every natural number has a prime factorization.

4. Consider a fully connected directed graph where between every pair of vertices u, v, either u has an edge to v or v is has an edge to u. Prove that every vertex must be connected directly to the vertex with maximum in-degree with a path of length at most 2.

5. Consider a graph with n vertices that has a path of the form $v_1 \dots v_n$ involving all the vertices, and where v_1 and v_2 both have degree at least $n/2$. Show that the graph has a hamiltonian cycle (a cycle that visits every node in the graph at least once).

3 F2017 #6

1. Argue that any directed simple graph where every vertex has out-degree at least one has a directed cycle.

2. Consider the graph formed with vertices corresponding to the men and women in a stable marriage instance and edges according to two different stable pairings, S and S'. If a pair is in both pairings only include a single edge in G, which ensures it is a simple graph. Argue that there is a cycle of length strictly greater than 2.

3. Define a man m as feeling threatened by another man m' with respect to a pairing S if (m,w) is in S and w likes m' better than m. We define the male feeling threatened graph for a stable pairing S as the directed graph whose vertices are men and with a directed arc for each pair (m, m') where m is feeling threatened by m'. Show that the male feeling threatened graph for the male optimal pairing has a cycle if there is more than one pairing. (Hint: using the previous parts may be helpful.)