HOMEWORK 3 MATHS 141 WINTER 2018

1. Introduction

This assignment mainly focuses on equivalence relations and its applications in modular arithmetic.

2. Problems

Problem 1. Using modular arithmetic show for integers x, y and $n \geq 0$

$$(x - y)|(x^n - y^n)$$

Problem 2. Let A be a set and R, S are two equivalence relations on A. Prove the following:
(a) $R \cap S$ is an equivalence relation on A

(b) $R \cup S$ may not be an equivalence relation on A. Give a counterexample to show how this fails.

(c) Now consider $A = \mathbb{Z}$ and consider the two equivalence relations:

$$nRm \iff 2|(n-m)$$
$$nSm \iff 3|(n-m)$$

What is the relation $R \cap S$?
(d) If R has n equivalence classes and S has m equivalence classes, how many equivalence classes does $R \cap S$ have?

Problem 3. Consider the set $A = \mathbb{Z} \times \mathbb{Z}$. Let $n, m \in \mathbb{Z} - \{0\}$ be nonzero integers. Consider the relations $R_{n,m}$ given by

$$(a, b)R_{n,m}(c, d) \iff na + md = nc + mb$$

(a) Let's start with the easy case. Show $R_{1,1}$ is an equivalence relation on $\mathbb{Z} \times \mathbb{Z}$.

(b) What is the equivalence class in $R_{1,1}$ of $[(1, 0)]$?

(c) What are the equivalence classes of $R_{1,1}$?

(d) Show for any nonzero n, m that $R_{n,m}$ is an equivalence relation on $\mathbb{Z} \times \mathbb{Z}$.

(e) What is the equivalence class of $[(1, 0)]$?

(f) Draw the equivalence class of $[(1, 0)]$ in several (4 or so, you can do more if you like) cases $R_{n,m}$. Geometrically speaking, what are these equivalence classes?

Problem 4. Let G be an undirected graph. Consider the relation T on the set $V(G)$ of vertives given by:

$$vTw \iff \exists \text{ a walk of even length connecting } v \text{ to } w.$$

(a) Show that T is an equivalence relation. Hint: Think inductively.

(b) Show that any complete bipartite graph $K_{n,m}$ has exactly two equivalence classes.

(c) Show that any cyclic graph with an odd number of vertives C_{2n+1} has only one equivalence class.

(d) The maximum number of equivalence classes for a connected graph is 2. Why?

Problem 5. Use modular arithmetic to prove the following divisibility:

$$19|(77777^{4994} + 44444^{9889})$$

Hint: This problem can be done in four or five lines depending on how large or small one's handwriting is. You'll want to use modular arithmetic on 19 to reduce the bases, and Fermat's little theorem, which we proved in one of our induction homeworks to solve this. The relevant piece of information you need is that 19 is prime and therefore:

$$a^{19} \equiv a \mod 19 \implies a^{18} \equiv 1 \mod 19$$

Problem 6. (a) Find the inverse of $137 \mod 237$.

(b) Find an integer $0 < k < 237$ so that

$$137k \equiv 37 \mod 237$$

3. Notes

Problem one is our old friend. We first proved it in the form

$$\sum_{j=0}^{n} r^j = \frac{r^{n+1}-1}{r-1}$$

Then substituting $r = \frac{x}{y}$. In the second case we proved it directly by induction on integer divisibility:

$$x^{n+1} - y^{n+1} = x(x^n - y^n) + (x-y)y^n$$

In this homework we're thinking about equivalence relations in the form of

$$nRm \iff d|(n-m)$$

And in this case we let $d = x - y$. This gives a third proof of this statement. So it had better be true!

Problem two makes us think about equivalence relations geometrically. The intersection of equivalence relations is, in fact, an equivalence relation, but its applications are far reaching. One application that we'll see shortly is the so called Chinese Remainder Theorem. On the other hand, the union of equivalence relations certainly maintains reflexivity and symmetry, but fails at transitivity. While the intersection in problem two tells us something about the $\gcd(n,m)$ the union, does not, conversely tell us anything about $\text{lcm}(n,m)$.

Problem three is intimately related to the equivalence relation on $\mathbb{Z} \times \mathbb{Z} - \{0\}$ which allows us to build up rationals. The equivalence relation on rationals, of course, is that two pairs of integers are related if, and only if they have a constant ratio. In our case, we're looking at constant differences, but with slop n/m or m/n depending on one's outlook. When we draw the equivalence classes we can see this quite clearly.

Problem four allows us to determine whether or not a graph is bipartite. Part (d) is interesting in that this type of relation on an undirected graph will not tell us about tripartite or k-partite graphs. Any equivalence relation on a graph defined by connectivity will pick up the connected components of a graph, unless otherwise specifically defined. On a directed graph things get a lot trickier. A directed graph must have cycles or a relation defined by walks will be transitive only. Without cycles we lose relfexivity and symmetry.

Problem five is a problem I made up just to show that in many cases we can handle extraordinarily large numbers. The number we're trying to divide has 45963 digits. In order to perform the actual division, one would need an arbitrary precision calculator and a lot of RAM. Here, we can do this by hand using a few powerful tricks. This problem is just an upgrade of an old problem from the Soviet Mathematical Olympiad which we've seen in class:

$$7|(2222^{5555} + 5555^{2222})$$

Problem six is a good practice problem computing inverses in modular arithmetic. This is particularly useful when it comes to factoring integers. Many techniques in this style involve finding modular inverses. If a number N has a modular inverse with every prime up to $\sqrt{N}$ then we can conclude that N is prime. Each step is done in logarithmic time, which means modular arithmetic reduces our time to check the primality to $O(\sqrt{N}\log(N))$ The original "techniques" were to try each long division by hand. No thanks! We'll use the techniques of problem 6 to build up discrete logarithms, solve Chinese Remainder Theorem problems, and eventually give the analysis of run-time of some number theoretic algorithms.