EECS 203: Discrete Mathematics
Winter 2024
Homework 2

Due **Thursday, Feb. 1st**, 10:00 pm

No late homework accepted past midnight.

Number of Problems: $8 + 2$ Total Points: $100 + 40$

- **Match your pages!** Your submission time is when you upload the file, so the time you take to match pages doesn't count against you.
- Submit this assignment (and any regrade requests later) on Gradescope.
- Justify your answers and show your work (unless a question says otherwise).
- By submitting this homework, you agree that you are in compliance with the Engineering Honor Code and the Course Policies for 203, and that you are submitting your own work.
- Check the syllabus for full details.

Grading of Groupwork 2

Using the solutions and Grading Guidelines, grade your Groupwork 2 Problems:

- Use the table below to grade your past groupwork submission and calculate scores.
- While grading, mark up your past submission. Include this with the table when you submit your grading.
- Write whether your submission achieved each rubric item. If it didn't achieve one, say why not.
- For extra credit, write positive comment(s) about your work.
- You don't have to redo problems correctly, but it is recommended!
- See "All About Groupwork" on Canvas for more detailed guidance, and what to do if you change groups.

	(i)	(ii)	(iii)	(iv)	(v)	(vi)	(vii)	(viii)	(ix)	(x)	(xi)	Total:
Problem 1	+4	+4	+2	+2	+2	+4	+2					20/20
Problem 2	+5	+0	+5	+0								10/20
Total:												30/40

Groupwork 2 Problems

1. Bézout's Identity [20 points]

In number theory, there's a simple yet powerful theorem called Bézout's identity, which states that for any two integers a and b (with a and b not both zero) there exist two integers r and s such that $ar + bs = \gcd(a, b)$. Use Bézout's identity to prove the following statements (you may assume all variables are integers):

(a) If $d \mid a$ and $d \mid b$, then $d \mid \gcd(a, b)$.

(b) If $a \mid bc$ and $\gcd(a, b) = 1$, then $a \mid c$.

Note: gcd is short for "greatest common divisor," so the value of $\gcd(a, b)$ is the largest integer that evenly divides a and b. You won't need to apply this definition, just know that $\gcd(a, b)$ is an integer.

Solution:

a) Assume $d \mid a \wedge d \mid b$	premise
$a = kd \wedge b = jd$, k and j are arbitary integers	definition of divide
$kdr + jds = gcd(a, b)$	Bezout's Identity
$gcd(a, b) = d(kr + js)$	factoring
Since $kr + js$ is also an integer, thus $d \mid gcd(a, b)$	definition of divide
Thus, $d \mid gcd(a, b)$.	
b) Assume $d \mid bc \wedge gcd(a, b) = 1$	premise
$bc = ka$	definition of divide
$ar + bs = 1$	Bezout's Identity
Since c is an non-zero integer, $arc + bsc = c$	equation
$arc + kac = c$	subsitution
$a(rc + kc) = c$	factoring
Since $rc + kc$ is also an integer, thus $a \mid c$	definition of divide
Thus, $a \mid c$	

2. Proposition Michigan [20 points]

Translate each of the following English statements into logic. You may define predicates as necessary.

Note: Your predicates should not trivialize the problem.

(a) Each pair of students at UMich has at least two mutual friends at UMich. The domain of discourse is all students at UMich.

(b) Nobody knows everyone's Wolverine Access password except the Wolverine Access administrators, who know all passwords. The domain of discourse is all people who have a Wolverine Access account (the administrators have Wolverine Access accounts).

Solution:

a) Let F(x) be UMich students who are friends
$\forall x \forall y [x \neq y \rightarrow \exists z \exists w [z \neq w \wedge F(x)]]$
I have a different predicate defined that should also work
b) Let A(x) be is administrator, P(x,y) be y knows someone's password
$\forall x (A(x) \iff \forall y P(x, y))$

Comments:
I did fine after camping at OH for 3 hours straight.