WORKSHEET #7 – MATH 2200
SPRING 2018

NOT DUE

This should help you prepare for the final.

1. Short answer questions.

(a) Define what it means for a function $f : A \longrightarrow B$ to be surjective.

Solution: For every $b \in B$, there exists $a \in A$ such that $f(a) = b$.

(b) Give an example of a function that is not injective (make sure to specify the domain and codomain).

Solution: Consider the function $f : \{1, 2\} \longrightarrow \{3\}$ sending both 1 and 2 to 3.

(c) What is $\{1, 2, 3, 23\} \cap \{3, 2, 1\}$?

Solution: $\{1, 2, 3\}$

(d) What is $\varphi(75)$ where φ is Euler's phi function

Solution: $\varphi(75) = \varphi(3) \cdot \varphi(25) = 2 \cdot 20 = 40$.

(e) Suppose $P(x, y)$, $Q(x), R(y)$ are logical propositions. Rewrite the statement

$$\neg(\forall x, \exists y, (P(x, y) \longrightarrow (Q(x) \vee \neg R(y))))$$

so that no negation symbol appears outside a logical operator ($\longrightarrow$, $\vee$, $\wedge$).

Solution:

$$\exists x, \forall y, (P(x, y) \wedge (\neg Q(x) \wedge R(y)))$$

(f) Consider the function $f(x) = 3^x + x^3$. True or false, $f(x)$ is $O(2^x)$.

Solution: False. We really need to show that 3^x can't be bounded above by $C \cdot 2^x$ (the x^3 is irrelevant) for *xlarge*. If it could be then there would exist C such that $(C \cdot 2^x)/3^x \geq 1$ for $x \gg 0$. But this can be rewritten as $C \cdot (2/3)^x$, which is obviously arbitrarily close to 0 for $x \gg 0$ no matter what C is.

(g) Consider the system of congruences $x \equiv_5 2$ and $x \equiv_7 3$. How many solutions does this system have between 0 and $104 = (35 \cdot 3) - 1$?

Solution: 3.

(h) Compute $\gcd(35, 55)$.

Solution: 5.

(i) Give an example of a relation that is not an equivalence relation.

Solution: The relation $>$ on $\mathbb{Z}$. It is neither symmetric or reflexive.

(j) Give an example of a function $f : \mathbb{Z} \longrightarrow \mathbb{Z}$ that is injective but not surjective.

Solution: There's no single correct answer, but $f(x) = 2x$ works.

(k) Write the number 33 in base 7.

Solution: $(45)_7$

(l) Consider the set $S = \{-5, -2, -1, 2, 3, 5, 6\}$. Define an equivalence relation on S as $x \sim y$ if $x^2 = y^2$ (you don't need to show this is an equivalence relation). Compute $[2]$, the equivalence class of 2.

Solution: $[2] = \{-2, 2\}$

(m) Is the open interval $(2, 4) = \{x \in \mathbb{R} \mid 2 < x < 4\}$ finite, countably infinite, or uncountable?

Solution: uncountable

(n) Briefly describe the all comparisons that would be done when doing a binary search on the list $\{1, 3, 4, 5, 7, 8, 9, 9.5, 10\}$, searching for the number 4.

Solution: We first compare the middle number 7 to 4, 7 is bigger so we restrict our list to $\{1, 3, 4, 5\}$. Let's say we are rounding down, and so the middle entry in our list is 3. We see that 3 is less than 4, and so we restrict our list to $\{4, 5\}$. Since we are rounding down, the middle entry is 4, and that equals 4.

(o) Find an integer n so that the statement $2^{n-1} \equiv_n 1$ is false.

Solution: $n = 0$ works, as does $n = 6$.

(p) Rewrite the following statement using (nested) quantifiers and logical propositions.

For every problem on the final, there exists some student in our class who will get full credit on that problem.

Solution: Set $P(x, y)$ to be the statement "student x gets full credit on problem y". Then our statement becomes.

$$\forall y, \exists x, P(x, y).$$

(q) What does the pigeonhole principal say?

Solution: If you have a set of pigeons and a set of holes, and you have more pigeons than holes, then some pigeons need to share.

(r) If I have N socks, how many ways are there to choose 3 socks (where order doesn't matter)? What about if order does matter?

Solution: For the first problem, the formula is $N \cdot (N-1) \cdot (N-2)/6$. For the second it is $N \cdot (N-1) \cdot (N-2)$.

(s) Is it true that $-8 \equiv_6 16$?

Solution: True. $16 - (-8) = 24$. Furthermore, 24 is divisible by 6, and so the true is indeed correct.

(t) Is the statement $\neg p \implies (\neg p \vee q)$ a tautology?

Solution: Yes.

(u) What is the inverse of 3 modulo 7?

Solution: 5 is the inverse. If found this by inspection since $3 \cdot 5 = 15$ which has remainder 1 modulo 7.

(v) Suppose $f : A \longrightarrow B$ and $g : B \longrightarrow C$ are functions. Which of the following notations make sense: $f \circ g$ or $g \circ f$.

Solution: $g \circ f$.

2. Run the extended Euclidean algorithm on the integers 63 and 77 and use it to find integers s and t such that $s \cdot 63 + t \cdot 77 = 7$. Make sure to explain each step.

Solution: We first form a table. We'll go down the table filling out the a, b, q, r first. Then we'll work our way up filling out the s, t.

a	b	q	r	s	t
77	63	1	14	-4	5
63	14	4	7	1	-4
14	7	2	0	0	1

I will describe working our way backwards up the table. Starting with the bottom line, we notice that $0 \cdot a_3 + 1 \cdot b_3 = 7$ which is the gcd. So we set $s_3 = 0, t_3 = 1$.

Notice that $a_2 = 4 \cdot b_2 + r_2$ where $7 = r_2 = b_3$, and $4 = q_2$. Hence solving for r_2 we obtain $7 = a_2 - 4 \cdot b_2 = 1 \cdot a_2 + (-4) \cdot b_2$. Thus we can set $s_2 = 1$ and $t_2 = -4$.

Finally, we notice that $a_1 = 1 \cdot b_1 + r_1$ or in other words $r_1 = a_1 - 1 \cdot b_1$. Also $b_1 = a_2$ as well as $r_1 = b_2$. We know $7 = 1 \cdot a_2 + (-4) \cdot b_2 = 1 \cdot b_1 + (-4) \cdot r_1$. Plugging in we get

$$7 = 1 \cdot b_1 + (-4) \cdot (a_1 - 1 \cdot b_1) = (-4) \cdot a_1 + 5 \cdot b_1.$$

Thus we set $s_1 = -4$ and $t_1 = 5$.

3. Solve the system of congruences

$$x \equiv_7 0$$
$$2x \equiv_5 1$$
$$x \equiv_4 2$$

Solution: We first turn the second equation into $x \equiv_5 ?$. We find the inverse of 2 modulo 5, that inverse is 3. So we multiply the equation by 3, and obtain $x \equiv_5 3$. So we have 3 equations

$$x \equiv_7 0$$
$$x \equiv_5 3$$
$$x \equiv_4 2$$

We first handle the first two equations. We write $1 = 3 \cdot 7 + (-4) \cdot 5$. Then we first notice that $x \equiv_{35} 3 \cdot 3 \cdot 7 + 0 \cdot (-4) \cdot 5 = 63 \equiv_{35} -7$ hence solves the first two equations. Now we have

$$x \equiv_{35} -7$$
$$x \equiv_4 2$$

We write $1 = (-1) \cdot 35 + 9 \cdot 4$. Hence we can set $x \equiv_{140} 2 \cdot (-1) \cdot 35 + (-7) \cdot 9 \cdot 4 = -70 - 252 = -322 \equiv_{140} 98$. Finally, we see that

$$x \equiv_{140} 98$$

solves the system.

4. Suppose $S = \{1, 2, 3\}$. Compute $\mathcal{P}(S) \cap \{\emptyset, 1, 2, \{3\}, S\}$.

Solution: We ask which elements of $\{\emptyset, 1, 2, \{3\}, S\}$ are subsets of S. Those are $\emptyset, \{3\}, S$. Hence the intersection is

$$\{\emptyset, \{3\}, S\}$$

5. Write down a bijective function between $\mathbb{Z}_{>0}$ and $S = \{x \in \mathbb{Z} \mid x \text{ is odd }\}$ (the odd integers). Prove carefully that your function is bijective.

Solution: The function

$$f(x) = \begin{cases} x & \text{if } x \text{ odd} \\ -x+1 & \text{if } x \text{ is even} \end{cases}$$

will work. We show first that f is surjective. Choose $y \in S$ so y is odd. If $y > 0$, then $y = f(y)$. If $y < 0$ is in S, then notice that $x = -y + 1$ is both positive and even. Hence $f(x) = f(-y+1) = -(-y+1) + 1 = y$ and so f is surjective.

Next we show that f is injective. Suppose $f(x_1) = f(x_2)$. Since odd x are sent to positive numbers and even are sent to negative, we must have that both x_1 and x_2 have the same parity if they have the same image under x. But if they have the same parity, then either $x_1 = f(x_1) = f(x_2) = x_2$ (if both are odd) or if both are even, then $-x_1 + 1 = -x_2 + 1$ and so again $x_1 = x_2$. Hence in either case $x_1 = x_2$ and so f injects.

6. Prove carefully that if $\phi : U \longrightarrow V$ is injective and $\psi : V \longrightarrow W$ is injective, that $\psi \circ \phi$ is also injective.

Solution: Suppose that $x_1, x_2 \in U$ are such that $\psi \circ \phi(x_1) = \psi \circ phi(x_2)$. Thus $\psi(\phi(x_1)) = \psi(\phi(x_2))$. Since ψ is injective, we deduce that $\phi(x_1) = \phi(x_2)$. Then since ϕ is injective we conclude that $x_1 = x_2$ as desired, hence $\psi \circ phi$ is injective.

7. Prove carefully by induction that $9^n - 1$ is divisible by 8 for all integers $n \geq 1$.

Solution: We begin with the base case of $n = 1$. Then $9^n - 1 = 9 - 1 = 8$, which is divisible by 8 and thus proves the base case. Now for the induction step, suppose that $9^k - 1$ is divisible by 8. Then

$$9^{k+1} - 1 = 9^{k+1} - 9 + 9 - 1 = 9(9^k - 1) + 8.$$

By the induction hypothesis, 8 divides $9^k - 1$ and hence it divides $9(9^k - 1)$ and finally it also divides $9(9^k - 1) + 8 = 9^{k+1} - 1$. This completes the proof of the induction step.

8. Use the well ordering principal to give a careful proof of the fact that

$$\gcd(a, b) = \min\{sa + tb > 0 \mid s, t \in \mathbb{Z}\}.$$

Solution: Let $c = \gcd(a, b)$ and $d = \min\{sa + tb > 0 \mid s, t \in \mathbb{Z}\}$. Note $d = sa + tb$ by definition for some choice of $s, t \in \mathbb{Z}$. Since $c|a$ and $c|b$, we see immediately that $c|d$, and so $c \leq d$. We will now prove that $d|a$ and $d|b$, which proves that $d|c$ since c is the *greatest* common divisor on a and b. Without loss of generality, suppose d does not divide a, then we can write $a = qd + r$ where $d > r > 0$. Since $d = sa + tb$ we obtain that

$$a = q(sa + tb) + r \text{ and so } r = (qs - 1)a + tb.$$

It follows that $r \in \{sa + tb > 0 \mid s, t \in \mathbb{Z}\}$ but $r < d$ which contradicts the minimality of d. Thus we see that d must divide both a and b and thus $d \leq c$. In conclusion, $d = c$ as desired.

9. Write down a recursive algorithm (pseudo-code is fine) which computes the gcd of two numbers a and b.

Solution: The following should work.

```
gcd(a,b){
    if (a == 0) return b;
    if (b == 0) return a;
    if (a == b) return a;
    r = a % b;
    return gcd(b, r);
}
```

The above is basically `C`.

10. Suppose that A and B are countable infinite sets such that $A \cap B = \emptyset$. Prove that $A \cup B$ and $A \times B$ are also countably infinite.

Solution: First we suppose that $f : \mathbb{Z}_{>0} \longrightarrow A$ and $g : \mathbb{Z}_{>0} \longrightarrow B$ are bijections. We first produce a function

$$h : \mathbb{Z}_{>0} \longrightarrow A \cup B \text{ defined by } h(x) = \begin{cases} f(x/2) & \text{if } x \text{ even} \\ g((x+1)/2) & \text{if } x \text{ odd} \end{cases}$$

We show carefully that $h : \mathbb{Z}_{>0} \longrightarrow A \cup B$ is bijective. To see it is surjective, choose $y \in A \cup B$. If $y \in A$, then there exists $x \in A$ such that $f(x) = y$. Thus $h(2x) = f(x) = y$. If $y \in B$ then there exists $x \in B$ such that $g(x) = b$ Then $h(2x-1) = g(x) = b$. Hence h surjects.

To show that h injects suppose $h(x) = h(x')$. If x and x' have different parities, then h of one is in A and h of the other is in B, so if $h(x) = h(x')$ then $h(x) \in A \cap B = \emptyset$, which is impossible. Hence we may assume that x and x' have the same parity. If both are even, then it follows that $f(x/2) = f(x'/2)$ and since f is injective, we see that $x/2 = x'/2$ and thus $x = x'$. If both are odd then $g((x+1)/2) = g((x'+1)/2)$ and so since g is injective, $(x+1)/2 = (x'+1)/2$ and hence $x = x'$ again. Thus no matter what $x = x'$.

For the second statement, we have already seen that $\mathbb{Z}_{>0} \times \mathbb{Z}_{>0}$ has the same cardinality of $\mathbb{Z}_{>0}$ (by chasing the same shape as we did for $\mathbb{Q}$) and so let $m : \mathbb{Z}_{>0} \longrightarrow \mathbb{Z}_{>0} \times \mathbb{Z}_{>0}$ be such a bijection. Next let $n : \mathbb{Z}_{>0} \times \mathbb{Z}_{>0} \longrightarrow A \times B$ be the bijection $n = f \times g$ (in other words, $n((u,v)) = (f(u), g(v))$). To show that n is bijective, we first show it is surjective. Choose $(a,b) \in A \times B$. Then there is $x, y \in \mathbb{Z}_{>0}$ so that $f(x) = a$ and $g(y) = b$ and so $n((x,y)) = (a,b)$. Next we show it is injective. Suppose $(f(x), g(y)) = n((x,y)) = n((x',y')) = (f(x'), g(y'))$. Thus $f(x) = f(x')$ and so $x = x'$ since f is injective. Likewise $g(y) = g(y')$ and so $y = y'$ since g is injective. Thus $(x,y) = (x',y')$ and so n is injective. Consider the composition

$$n \circ m : \mathbb{Z}_{>0} \longrightarrow A \times B.$$

This is a composition of bijections and hence also a bijection. Thus $A \times B$ is countable.

11. Suppose that S is the set of current math majors at the University of Utah. We define a relation $\sim$ on S where $a \sim b$ if a and b got the same grade in Math 2200. Is $\sim$ an equivalence relation? If so, what is the equivalence class of Alice who got an `A` in 2200?

Solution: Before we can answer this, we notice that there is a choice we can make. If a student does not take 2200, do they have the same grade as someone else who didn't take 2200? We interpret the answer to this question as "yes". (But other choices would be reasonable if they were clearly stated). We likewise don't worry about students who take the class multiple times (we only *count* the most recent attempt). Again, another choice would also be ok. With these conventions...

Yes, it is an equivalence relation. We show this. Notice that a student gets the same grade as themselves, which proves reflexivity. If student A and student B get the same grade in 2200, then so do students B and A. Thus the relation is symmetric. Finally, if students A and B have the same grade, as do students B in C, then students A and C also have the same grade in 2200. Thus the relation is transitive.

We finally describe the equivalence class:

$$[\text{Alice}]_\sim = \{\text{math majors at Utah} \mid \text{ who got an A in 2200}\}.$$

12. Suppose that $S = \{f : \{1,2,3\} \longrightarrow \{1,2,3\}\}$ is the set of functions from $\{1,2,3\}$ to $\{1,2,3\}$. Define a relation on S where $f \sim g$ if $|f(x) - g(x)| \leq 1$ for all $x \in \{1,2,3\}$. Is $\sim$ an equivalence relation? How many functions are related to the constant function $h(x) = 3$?

Solution: No, it is not an equivalence relation. Consider three functions, $f(x) = 1$, $g(x) = 2$ and $h(x) = 3$. Notice that $f \sim g$ and $g \sim h$ but f is not related to h, and so the relation is not transitive. Hence we don't have to do any equivalence classes either :-)