## MATH 13 WINTER 2017 PRACTICE PROBLEMS FOR WEEK 6

First review the set-theoretic definition of a function. The important point is that $y=f(x)$ means the same as $(x, y) \in f$. This plays role in analyzing properties of functions such as for instance injectivity and surjectivity. For injectivity, we have any of the following two equivalent conditions characterizing injectivity of a function $f: A \rightarrow B$.
(a) $a \neq a^{\prime} \Longrightarrow f(a) \neq f\left(a^{\prime}\right)$.
(b) $f(a)=f\left(a^{\prime}\right) \Longrightarrow a=a^{\prime}$.

For $f$ to be injective, these must hold for all $a, a^{\prime} \in A$. Set theoretically, these can be rephrased as follows:
(a1) $\left(a \neq a^{\prime} \wedge(a, b) \in f \wedge\left(a^{\prime}, b^{\prime}\right) \in f\right) \Longrightarrow b \neq b^{\prime}$.
(b1) $\left((a, b) \in f \wedge\left(a^{\prime}, b\right) \in f\right) \Longrightarrow a=a^{\prime}$.
This time these statements must hold for all $a, a^{\prime} \in A$ and $b, b^{\prime} \in B$. Note that $b^{\prime}$ does not occur in (b1).

Important: Recall once again, that when we write characterzation of injectivity using any of the statements above, we need to put universal quantifiers in front, that is $(\forall a \in A)$ etc. These statements do not say that something exists, and this is important as sometimes they may be true vacuously, which we want.

Important: On the other hand, if we want to prove that $f$ is not injective, then we have to verify a statement with existential quantifier, as a negation of a statement starting with $\forall$ starts with $\exists$. In this case we need to show an existence/find some $a, a^{\prime}$ (and for (a1, b 1 ) also some $\left.b, b^{\prime}\right)$ violating these conditions.

For $m, n \in \mathbb{Z}$ we define the greatest common divisor $\operatorname{gcd}(m, n)$. Recall first that a number $e \in \mathbb{Z}$ is a divisor of $m$ iff $e \mid m$, or equivalently $m=k \cdot e$ for some $e \in \mathbb{Z}$.

The number $d \in \mathbb{Z}$ is a common divisor of $m, n$ iff $d$ is a divisor of both $m, n$, symbolically iff $d|m \wedge d| n$.

The number $d \in \mathbb{N}$ is the greatest common divisor of $m, n$ iff the following two clauses are satisfied.
(g1) $d$ is a common divisor of both $m, n$.
(g2) If $d^{\prime}$ is a common divisor of both $m, n$ then $d \mid d^{\prime}$.

## Imoprtant remarks.

(i) Notice that "greatest" in the definition is not with respect to the natural ordering of numbers $\leq$, but with respect to divisibility. This is important in algebra, where one defines the notion of greates common divisor for objects other than numbers, where there is no ordering analogic to the natural ordering of numbers (think of polynomials for instance).
(ii) We chose the greatest common divisor to be a positive number. It is not hard to see that if $d=\operatorname{gcd}(m, n)$ then the number $-d \in \mathbb{Z}$ also satisfies clauses (g1) and (g2). In algebra one defines the set of greatest common divisors to be all objects satisyfing clauses (g1) and (g2), we will not do this here.
(iii) The fact that we chose $\operatorname{gcd}(m, n)$ positive makes $\operatorname{gcd}(m, n)$ the largest common divisor of $m, n$ with respect to the natural ordering of numbers $\leq$.

However, we prefer to define $\operatorname{gcd}(m, n)$ as above not only as a preparation for the algebra course, but also because this way the definition is conceptually more natural: In general, one should not expect to have some ordering of the objects whose divisibility we study, other than the ordering given by divisibility itself.

## SUGGESTED PRACTICE PROBLEMS.

1. Composition of relations/functions. Let $R$ be the divisibility relation on $\mathbb{Z}$ and $S$ be the natural ordering $\leq$ on $\mathbb{Z}$ and $T$ be the strict ordering $<$ on $\mathbb{Z}$. Also $P$ is a binary relation from $X$ to $Y$ and $Q$ is a binary relation from $Y$ to $Z$.
(a) Prove that $S \circ R \subseteq S, R \circ S \subseteq S, R \circ R=R$ and $S \circ S=S$.
(b) Determine whether the following are true and prove that your answer is correct: $T \circ T \subseteq T, T \circ R \subseteq R, R \circ T \subseteq R, R \circ T \subseteq T$.
(c) Prove that $(Q \circ P)^{-1}=P^{-1} \circ Q^{-1}$ and $\left(P^{-1}\right)^{-1}=P$.
2. Images and inverse images. The relations considered here are the ones from Item 1 above.
(a) In Homework 3 there is a question asking you to prove that $Q[A \cup B]=$ $Q[A] \cup Q[B]$. Argue that the analogous conclusion holds for inverse images. Do you need to repeat the proof?
(b) Assume $f: X \rightarrow Y$. Prove that if $B, B^{\prime} \subseteq Y$ then

$$
f^{-1}\left[B \cap B^{\prime}\right]=f^{-1}[B] \cap f^{-1}\left[B^{\prime}\right]
$$

Is $f\left[B \cap B^{\prime}\right]=f[B] \cap f\left[B^{\prime}\right]$ ? What if $f$ is injective?
(c) Prove that $(Q \circ P)[A]=Q[P[A]]$.
3. Injections, surjections and bijections. In each case decide whether the given function is injection or surjection. Always justify your answer by a proof. Review Theorems 4.15 and 4.16 from the book.
(a) Fix $y^{*} \in Y$. $f: X \rightarrow X \times Y$ is given by $f(x)=\left(x, y^{*}\right)$.
(b) $f: \mathbb{N} \backslash\{1\} \rightarrow \mathbb{N}$ is given by

$$
f(n)=\text { the largest divisor of } n \text { which is discinct from } n \text {. }
$$

(c) $f: \mathbb{Z} \times \mathbb{Z} \rightarrow \mathbb{Z}$ is given by $f(m, n)=\operatorname{gcd}(m, n)$.
(d) Given a set $A^{*} \subseteq X$, the map $f: \mathcal{P}(X) \rightarrow \mathcal{P}(X)$ given by $f(A)=A \cap A^{*}$.
(e) $f: \mathcal{P}(X) \times \mathcal{P}(X) \rightarrow \mathcal{P}(X)$ is given by $f\left(A, A^{\prime}\right)=A \cap A^{\prime}$.
(f) Find a bijection between $A \times B$ and $B \times A$.
(g) Given a number $q \in \mathbb{N}$, the $\operatorname{map} f_{q}: \mathbb{Z} \rightarrow \mathbb{Z}$ is given by

$$
f_{q}(n)=\text { the reminder of } n \text { when divided by } q \text {. }
$$

(h) Theorem 4.16 in the book tells us that the impliction

$$
g \circ f \text { is injective } \Longrightarrow f \text { is injective }
$$

holds whenever $f: X \rightarrow Y$ and $g: Y \rightarrow Z$. What about $g$ ? Must $g$ be injective if $g \circ f$ is injective?
(i) Similarly to (h), from Theorem 4.16 we have

$$
g \circ f \text { is surjective } \Longrightarrow g \text { is surjective }
$$

whenever $f: X \rightarrow Y$ and $g: Y \rightarrow Z$. What can we say about $f$ ? Must $f$ be surjective if $g \circ f$ is surjective?
(j) Let $g: Y \rightarrow Z$. Prove that the (i) and (ii) below are equivalent.
(i) $g$ is injective.
(ii) If $f, f^{\prime}: X \rightarrow Y$ are such that $g \circ f=g \circ f^{\prime}$ then $f=f^{\prime}$.

Write (ii) symbolically using logical connectives and quantifiers so that you understand it better.

Reformulate (ii) in that you form its contraposition. Give a proof of that contraposition independently of the proof of the original statement.
(k) Let $f: X \rightarrow Y$. Prove that the (i) and (ii) below are equivalent.
(i) $f$ is surjective.
(ii) If $g, g^{\prime}: Y \rightarrow Z$ are such that $g \circ f=g^{\prime} \circ f$ then $g=g^{\prime}$.

Write (ii) symbolically using logical connectives and quantifiers so that you understand it better.

Reformulate (ii) in that you form its contraposition. Give a proof of that contraposition independently of the proof of the original statement.
(l) $f:(0,1) \rightarrow \mathbb{R}$ is given by

$$
f(x)=\frac{x-1 / 2}{1-x^{2}}
$$

(m) $f: \mathcal{P}(X \times Y) \rightarrow \mathcal{P}(Y \times X)$ is given by $f(R)=R^{-1}$.

