Problem 1 [12pts] Finish stating the definitions below by completing the sentences below:

a. Let A and B be sets then $A \subseteq B$ iff...

$x \in A \Rightarrow x \in B$ for each $x \in A$.

b. Let $x, y \in \mathbb{Z}$ and $n \in \mathbb{N}$ then $x = y$ modulo n iff...

$\exists k \in \mathbb{Z}$ such that $x = y + nk$.

c. Cantor's Theorem states that if $\overline{\overline{S}}$ is the cardnality of a set S and $\mathcal{P}(S)$ is the power set of S then...

$\overline{\overline{S}} < \overline{\overline{\mathcal{P}(S)}}$.

d. Let $a, b \in \mathbb{Z}_n$ and $n \in \mathbb{N}$ then we say that a and b are zero-divisors iff...

$a \neq 0$ and $b \neq 0$ yet $ab = 0$.

e. Let $a, b \in \mathbb{Z}$ such that $b \leq a$, the division algorithm states...

(Oops, sorry folks should have said $a, b \in \mathbb{N}$.)

f. If $a, b \in \mathbb{Z}$ then we say a, b are relatively prime iff...

$\gcd(a, b) = 1$.

Problem 2 [6pts] Provide examples (no need to prove they work)

a. a function $f : \mathbb{R} \to \mathbb{R} \times \mathbb{R}$

$f(x) = (x, x)$.

b. a function $f : \mathbb{R} \times \mathbb{R} \to \mathbb{R} \times \mathbb{R}$

$f(r, \theta) = (r\cos\theta, r\sin\theta)$

c. a function $f : \mathbb{R} \to \mathbb{R}$ such that the fiber of 3 is $\mathbb{R}$.

$f(x) = 3$ has $f^{-1}\{3\} = \mathbb{R}$.

Problem 3 [3pts] True or False?. A set which is denumerable is also called countably infinite. A countably infinite set cannot be finite. The cardnality of a countably infinite set is defined to be $\aleph_o$. Cantor showed that rational numbers and natural numbers have the same cardnality.

Problem 4 [3pts] True or False?

$$\aleph_o = \overline{\overline{\mathbb{N}}} = \overline{\overline{\mathbb{Z}}} = \overline{\overline{\mathbb{Q}}} < \overline{\overline{\mathbb{R}}} = c$$

Problem 5 [8pts] Let $f : \mathbb{Z}_5 \to \mathbb{Z}_{10}$ be defined by $f(\overline{x}) = [2x]$. Show that f is well-defined. Show that f is one-one. Show that f is not onto.

Notice $\overline{x} = \overline{x+5k}$ and $[y] = [y+10k]$ for any $k \in \mathbb{Z}$.
Consider then, for $k \in \mathbb{Z}$,

$$
\begin{aligned}
f(\overline{x+5k}) &= [2(x+5k)] \\
&= [2x+10k] \\
&= [2x]
\end{aligned}
$$

$\therefore f(\overline{x}) = f(\overline{x+5k})\ \forall k \in \mathbb{Z}$.
Hence f is well-defined.

Suppose $f(\overline{x}) = f(\overline{y})$ then $[2x] = [2y]$ hence $\exists k \in \mathbb{Z}$ such that $2x = 2y + 10k \Rightarrow x = y + 5k \Rightarrow \overline{x} = \overline{y}$.
Thus f is injective.

$f(\mathbb{Z}_5) = \{[0], [2], [4], [6], [8]\}$ thus $[1] \notin \text{range}(f)$ yet $[1] \in \text{codomain}(f)$ $\therefore f$ is not onto.

Problem 6 [4pts] Find all the zero divisors in $\mathbb{Z}_6$. $= \{0, 1, 2, 3, 4, 5\}$

$\gcd(x, 6) = 1 \Rightarrow x^{-1} \in \mathbb{Z}_6$ So we can ignore 1, 5.

also 0 is not a zero divisor. However, modulo 6,

$2 \cdot 3 = 0$ and $3 \cdot 4 = 0$

Thus $\boxed{2, 3 \text{ and } 4 \text{ are zero divisors in } \mathbb{Z}_6}$

Problem 7 [12pts] Let $f : (1, \infty) \to \mathbb{R}$ with $f(x) = \ln(x - 1) + 3$. Show that f is a bijection.

<u>1-1</u> Let $x, y \in (1, \infty)$ then suppose $f(x) = f(y)$ this yields,

$$\ln(x-1) + 3 = \ln(y-1) + 3$$
$$\ln(x-1) = \ln(y-1)$$
$$x - 1 = y - 1 \Rightarrow \underline{x = y}. \therefore f \text{ is 1-1.}$$

<u>onto</u> Let $z \in \mathbb{R}$ observe that $x = 1 + e^{z-3} \in (1, \infty)$ and $f(x) = \ln(1 + e^{z-3} - 1) + 3 = z - 3 + 3 = z$ thus f is onto.

$\therefore$ <u>f is a bijection</u>.

Problem 8 [4pts] Solve $x^3 + x^2 + x = 2$ in $\mathbb{Z}_3$. $= \{0, 1, 2\}$

$0 + 0 + 0 = 0 \neq 2 \quad \therefore 0$ not a sol^{n}.

$1 + 1 + 1 = 3 = 0 \neq 2 \quad \therefore 1$ not a sol^{n}.

$2^3 + 2^2 + 2 = 14 = 2 \quad \therefore \boxed{x = 2 \text{ is the sol}^{n}}$

Problem 9 [8pts] Use the Euclidean algorithm to find the multiplicative inverse of 17 modulo 217; that is find $17^{-1} \in \mathbb{Z}_{217}$.

$$217 = 17(12) + 13$$
$$17 = 13(1) + 4$$
$$13 = 4(3) + \boxed{1} \leftarrow \gcd(17, 217).$$
$$3 = 3(1) + 0$$

$$\begin{aligned} 1 &= 13 - 4(3) \\ &= 13 - 3[17 - 13] \\ &= 217 - 17(12) - 3[17 - 217 + 17(12)] \\ &= 4 \cdot 217 + 17[-12 - 39] \\ &= 4 \cdot 217 + 17(-51) \end{aligned}$$

Thus, modulo 217, we find, $-51 \equiv 166$,

$$1 \equiv_{217} 166 \cdot 17 \quad \therefore \quad \boxed{17^{-1} = 166}$$

Problem 10 [8pts] Let $f : \mathbb{R}^3 \to \overset{[0,\infty)}{\cancel{\mathbb{R}}}$ with $f(x, y, z) = \sqrt{x^2 + y^2 + z^2}$. Show that f is onto $\mathbb{R}$. Find the fiber of 1. ~~Find the fiber of -1.~~ Find the inverse image $f^{-1}([0, 1])$.

① Let $a \in [0,\infty)$ observe that $f(a,0,0) = \sqrt{a^2+0+0} = \sqrt{a^2} = |a|$

and $|a| = a$ since $a \geq 0$. Thus f is onto.

② fiber of 1 $= f^{-1}(\{1\}) = \{(x,y,z) \in \mathbb{R}^3 \mid f(x,y,z) = 1\}$

$$= \boxed{\{(x,y,z) \in \mathbb{R}^3 \mid \sqrt{x^2+y^2+z^2} = 1\}}$$

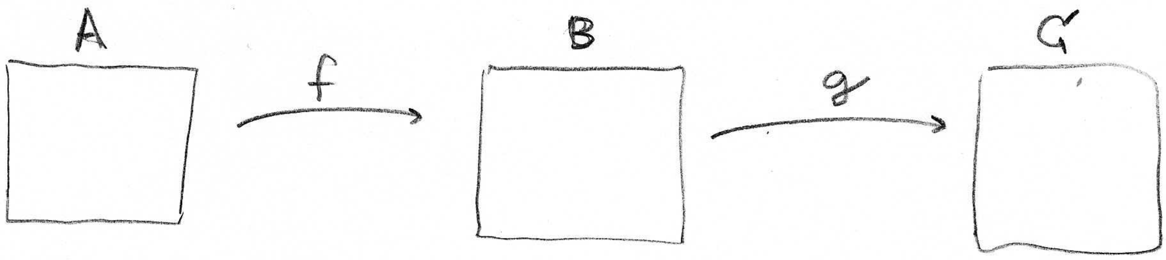
(spherical shell $\rho = 1$)

③ $f^{-1}([0,1]) = \{(x,y,z) \in \mathbb{R}^3 \mid f(x,y,z) \in [0,1]\}$

$$= \boxed{\{(x,y,z) \in \mathbb{R}^3 \mid 0 \leq \sqrt{x^2+y^2+z^2} \leq 1\}}$$

(solid sphere $\rho \leq 1$)

Problem 11 [8pts] Prove that: If f, g are surjective functions $f : A \to B$ and $g : B \to C$ then $g \circ f$ is surjective.



Notice $g \circ f : A \to C$. Let $c \in C$. Since $g : B \to C$ is onto, we know $\exists\, b \in B$ such that $g(b) = c$. Since $f : A \to B$ is onto, we know $\exists\, a \in A$ such that $f(a) = b$. Thus,

$$
\begin{aligned}
(g \circ f)(a) &= g(f(a)) = a \\
&= g(b) \\
&= c.
\end{aligned}
$$

$\therefore$ <u>$g \circ f$ is a surjection</u> //

do not consult others for help, you may use your notes and the text but that is all. (Due Wednesday by 4pm, slide under my door or give it to me directly, thanks!), there are 6 bonus points built into this test.

Problem 12 [7pts] Let $m, p \in \mathbb{N}$. If $f : \mathbb{Z}_m \to \mathbb{Z}_p$ with $f(\overline{x}) = [x]$ then what condition(s) must we place on m, p in order that f be a well-defined function?

If $m < p$ then $\bar{0} = \bar{m}$ but $[0] \neq [m]$ thus $f(\bar{x}) = [x]$ will not be single-valued. So we can assume $m \geq p$ if we wish $f(\bar{x}) = [x]$ to define a function $f : \mathbb{Z}_m \to \mathbb{Z}_p$.

Assume $m \geq p$. Consider then $\bar{x} = \overline{x + mk}$ $\forall k \in \mathbb{Z}$.

We want $f(\bar{x}) = f(\overline{x+mk}) = [x]$ this means we need

$$[x] = [x + mk] \quad \forall k \in \mathbb{Z}. \quad ([x] \in \mathbb{Z}_p)$$

$$\Leftrightarrow \quad x \equiv_p x + mk$$

$$\Leftrightarrow \quad (x + mk) - x = lp \text{ for some } l \in \mathbb{Z}.$$

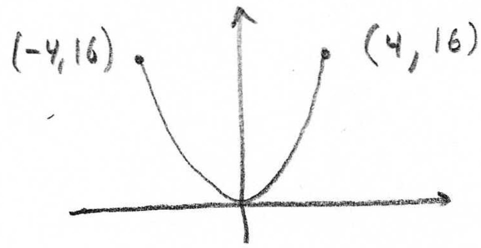
$$\Leftrightarrow \quad mk = lp \quad \text{for each } k \in \mathbb{Z},\ \exists l \in \mathbb{Z} \text{ such that the eq}^{\underline{n}} \text{ holds.}$$

Consider $k = 1$, $m = lp \Rightarrow$ <u>p is a factor of m</u>.

$$\boxed{f : \mathbb{Z}_m \to \mathbb{Z}_p \text{ is a function iff } p \mid m. \quad f(\bar{x}) = [x]}$$

Problem 13 [8pts] Let $f : [-4, 4] \to \mathbb{R}$ with $f(x) = x^2$. Find the codomain and range of f. Find an injective function g which is a restriction of f.

Note $\text{dom}(f) = [-4,4]$ and $\text{codomain}(f) = \mathbb{R}$ since we are given $f: [-4,4] \longrightarrow \mathbb{R}$. The range of $f(x)$ clear from the graph of f,



$\boxed{\text{range}(f) = [0,16]}$

Choose $g = f\big|_{[0,4]}$ then $g(x) = g(y)$ for $x, y \in [0,4]$

$\Rightarrow f(x) = f(y)$

$\Rightarrow x^2 = y^2$

$\Rightarrow x = \pm y$ but $x, y \geq 0$

hence $x = y$ $\therefore g$ is 1-1.

(Remark: there are many choices)

Problem 14 [15pts] Use an induction argument to prove $n^3 + 5n + 6$ is divisible by 3 for all $n \in \mathbb{N}$.

oops. see sol$^{\underline{n}}$ from the other test. Or,

Let $P(n)$ be the statement $n^3 + 5n^2 + 6$ is divisible by 3.

Note $P(1)$ is true since $1 + 5 + 6 = 12 = 4(3)$.

Assume $P(n)$ true, then $\exists k \in \mathbb{Z}$ such that

$n^3 + 5n + 6 = 3k$. Consider then

$$(n+1)^3 + 5(n+1) + 6 = \underline{n^3} + 3n^2 + 3n + 1 + \underline{5n} + 5 + \underline{6}$$
$$= \underline{n^3} + \underline{5n} + \underline{6} + 3(n^2 + n + 2)$$
$$= 3(k + n^2 + n + 2)$$

thus $P(n+1)$ is true. It follows that $P(n)$ is true $\forall n \in \mathbb{N}$ by PMI.