MATH 540: EXAM I

You must show all work to receive full credit. Each of the problems 1-5 is worth 20 points.

Name:

1. Consider the statement $\sum_{i=1}^{n}(2i-1) = n^2$. Prove this statement in two ways: First by induction and then by using the Well Ordering Principle.

Induction: Base Case $n=1$: $\sum_{i=1}^{1} 2i-1 = 2\cdot 1-1 = 1 = 1^2$.

Assume $\sum_{i=1}^{n}(2i-1) = n^2$. Add $2(n+1)-1$ to both sides to get

$$\sum_{i=1}^{n+1}(2i-1) = n^2 + 2(n+1)-1 = n^2+2n+1 = (n+1)^2 \quad //$$

Well Ordering: Let $S =$ all $k \in \mathbb{N}$ s.t $\sum_{i=1}^{k}(2i-1) \neq k^2$. Claim: $S = \phi$. If so, the eq$^{\underline{n}}$ holds. Suppose $S \neq \phi$. Let $r \in S$ be the least element - by the Well Ordering principle. Note $r \neq 1$.

Then $\sum_{i=1}^{r}(2i-1) \neq r^2$.

On the other hand, $r-1 \notin S$, so $\sum_{i=1}^{r-1}(2i-1) = (r-1)^2$.

Add $2r-1$ to both sides $\Rightarrow \sum_{i=1}^{r} 2i-1 = (r-1)^2 + 2r-1 = r^2$ #

Contradiction. Thus $S = \phi$, as required.

2. Let $S = \mathbb{R}^2$ be the set of ordered pairs of real numbers. Define $(a, b) \sim (c, d)$ to mean that the distance from (a, b) to $(0, 0)$ is the same as the distance from (c, d) to $(0, 0)$.

(i) Prove that $\sim$ is an equivalence relation.

Note $(a,b) \sim (c,d)$ if and only if $\sqrt{a^2+b^2} = \sqrt{c^2+d^2}$.

(a) $\sqrt{a^2+b^2} = \sqrt{a^2+b^2} \Rightarrow (a,b) \sim (a,b)$ – Reflexivity

(b) $\sqrt{a^2+b^2} = \sqrt{c^2+d^2} \Rightarrow \sqrt{c^2+d^2} = \sqrt{a^2+b^2} \Rightarrow (c,d) \sim (a,b)$ – symmetry

If $(a,b) \sim (c,d)$

(c) $\left.\begin{array}{l} (a,b) \sim (c,d) \Rightarrow \sqrt{a^2+b^2} = \sqrt{c^2+d^2} \\ (c,d) \sim (e,f) \Rightarrow \sqrt{c^2+d^2} = \sqrt{e^2+f^2} \end{array}\right\} \Rightarrow \sqrt{a^2+b^2} = \sqrt{e^2+f^2} \Rightarrow$ $(a,b) \sim (e,f)$ – Transitivity

(ii) Give a concise description of the equivalence class $[(\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2})]$.

$\sqrt{\left(\frac{\sqrt{2}}{2}\right)^2 + \left(\frac{\sqrt{2}}{2}\right)^2} = 1$. Thus $(a,b) \sim \left(\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}\right) \Leftrightarrow \sqrt{a^2+b^2} = 1$

$\Leftrightarrow$ (a,b) lies on the unit circle centered at $(0,0)$.

$\therefore \left[\left(\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2}\right)\right]$ = unit circle, centered at $(0,0)$.

(iii) Let X denote the set of equivalence classes of $\sim$. Define $f : X \to \mathbb{R}$ by $f([(a, b)] = a^2 + b^2 + 2$. Prove that f is well-defined.

If $[(a,b)] = [(c,d)] \Rightarrow \sqrt{a^2+b^2} = \sqrt{c^2+d^2} \Rightarrow a^2+b^2 = c^2+d^2$

$\Rightarrow a^2+b^2+2 = c^2+d^2+2$

$\Rightarrow f([(a,b)]) = f([(c,d)])$, so f is well-defined.

3. Provide all details for the following:

(i) Use the divison algorithm to find GCD(24,58).

$$58 = 2 \cdot 24 + 10$$

$$24 = 2 \cdot 10 + 4$$

$$10 = 2 \cdot 4 + 2 \longrightarrow \text{GCD of } 24, 58$$

$$4 = 2 \cdot 2 + 0$$

(ii) Use your calculation in (i) to write the GCD in terms of 24 and 58, as required by Bezout's principle.

$$2 = -2 \cdot 4 + 10$$

$$2 = -2(24 - 2 \cdot 10) + 10 = -2 \cdot 24 + 5 \cdot 10$$

$$2 = -2 \cdot 24 + 5(58 - 2 \cdot 24)$$

$$2 = -12 \cdot 24 + 5 \cdot 58$$

(iii) Use the Fundamental Theorem of Arithmetic to find the LCM of 2,800 and 11,000.

$$2800 = 100 \cdot 28 = 2^2 \cdot 5^2 \cdot 2^2 \cdot 7 = 2^4 \cdot 5^2 \cdot 7$$

$$11{,}000 = 11 \cdot 10^3 = 2^3 \cdot 5^3 \cdot 11$$

$$LCM = 2^4 \cdot 5^3 \cdot 7 \cdot 11 = 154{,}000$$

4. Consider the integers with congruence modulo 24.

(i) List the elements in [11], the equivalence class of 11.

$$[11] = \{ 11 + 24n \mid n \in \mathbb{Z} \}$$

(ii) List the equivalence classes that have multiplicative inverses modulo 24. Justify your answer.

We need the classes whose representatives are relatively prime to 24: $[1], [5], [7], [11], [13], [17], [19], [23]$.

(iii) Solve the congruence $13x \equiv 8$ (modulo 24).

Note: $13 \cdot 13 \equiv 169 \equiv 1 \pmod{24}$. Thus:

$$13 \cdot 13 x \equiv 13 \cdot 8 \pmod{24}$$
$$x \equiv 104 \bmod (24) \equiv 8 \pmod{24}$$

(iv) Is your solution in (iii) unique as an element of $\mathbb{Z}_{24}$? Explain.

The sol$^{\underline{n}}$ in $\mathbb{Z}_{24}$ is unique,

since if $[a]$ is a sol$^{\underline{n}}$

$13 \cdot [a] \equiv 8 \bmod 24$

mult by 13 as before $\Rightarrow [a] \equiv 8$

5. Let $p \in \mathbb{Z}$ be a prime number. Prove that if $p|ab$, then $p|a$ or $p|b$.

If $p|a$, we are done. If $p \nmid a$, then $GCD(p,a)=1$.

Thus: $1 = sp + ta$, some $s,t \in \mathbb{Z}$. Therefore:

$b = spb + tab$. Since $p|spb$ and $p|tab \Rightarrow p|b$ //

Bonus. Let $a, b \geq 2$ be relatively prime. Prove that if $a|n$ and $b|n$, then $ab|n$. (10 points.)

Write $n = an_1$, $n = bn_2$. We may also write $1 = sa + tb$, for $s,t \in \mathbb{Z}$. Thus

$n = san + tbn$

$n = sabn_2 + tban_1 = (sn_2 + tn_1)ab$

$\therefore$ $ab | n$.