Your Name

Solutions

Your Signature

Wording highlighted in yellow is "boiler-plate" language.

Problem	Total Points	Score
1	20	
2	20	
3	20	
4	20	
5	20	
extra credit	10	
Total	100	

Remember: The point of this class and of this exam is to learn to craft rigorous, formal mathematical proofs, and NOT to convince yourself (or me) that the statements are true. We probably all believe their truth without writing anything.

- You have 1 hour.
- If you have a cell phone with you, it should be turned off and put away. (Not in your pocket)
- You may not use a calculator, book, notes or aids of any kind.
- In order to earn partial credit, you must show your work.
- All proofs on this exam are expected to be concise, mathematically rigorous, and formal. Thus, you must use of complete sentences, correct grammar and punctuation. Unless prescribed by the problem, you may use any proof technique you like; however, *you must explicitly state the method you are using.*

1. (a) (5 points) Complete the following *formal* definition:

Given sets A and B, we write $A \subseteq B$ if

$\forall a \in A,\ a \in B.$

(b) (15 points) Suppose $A = \{12a + 4b : a, b \in \mathbb{Z}\}$ and $B = \{4c : c \in \mathbb{Z}\}$. Prove $A = B$.

Proof: First we show $A \subseteq B$.

Let $x \in A$. Then, by the definition of A, $x = 12a + 4b$ for some $a, b \in \mathbb{Z}$. Now, $x = 4(3a+b)$ where we know $3a+b \in \mathbb{Z}$. So $x = 4c$ for some $c \in \mathbb{Z}$. Thus, $x \in B$. Since $x \in A$ implies $x \in B$, it follows that $A \subseteq B$.

Next we show $B \subseteq A$.

Let $x \in B$. Then, by the definition of B, $x = 4c$ for some $c \in \mathbb{Z}$. Observe that $4 = 12 - 8 = 12(1) + 4(-2)$. Substituting in for 4 we obtain:

$$x = 4c = (12(1)+4(-2))c = 12(c) + 4(-2c) \text{ where}$$

$c, -2c \in \mathbb{Z}$. Thus, $x \in A$. Since $x \in B$ implies $x \in A$, it follows that $B \subseteq A$.

Since $A \subseteq B$ and $B \subseteq A$, it follows that $A = B$.

2. (a) (5 points) Complete the following *formal* definition:

The integer a is *even* if $a=2n$ for some $n\in\mathbb{Z}$.

The integer a is *odd* if $a=2n+1$ for some $n\in\mathbb{Z}$.

(b) (15 points) Suppose a and b are integers. Use Proof by Contrapositive to prove that if $a^3(3-b)$ is odd, then a is odd and b is even.

Proof: Suppose $a,b\in\mathbb{Z}$.

We will show that if a is even or b is odd, then $a^3(3-b)$ is even.

Suppose a is even or b is odd. We will proceed by cases.

Case 1 Assume a is even.

Then by the definition of even, $a=2n$ for some $n\in\mathbb{Z}$. Thus, $a^3(3-b)=8n^3(3-b)=2[4n^3(3-b)]$, where $4n^3(3-b)\in\mathbb{Z}$. Thus, it follows that $a^3(3-b)$ is even.

Case 2: Assume b is odd.

Then by definition of odd, $b=2n+1$ for some $n\in\mathbb{Z}$. Thus $a^3(3-b)=a^3(3-(2n+1))=2[a^3(1-n)]$ where $a^3(1-n)\in\mathbb{Z}$. Thus, it follows that $a^3(3-b)$ is even.

Thus, in both cases, $a^3(3-b)$ is even.

3. (20 points) Use the method of Proof by Contradiction to the statement below.

Suppose $a, b \in \mathbb{R}$. If a is rational and ab is irrational, then b is irrational.

Pf: (contradiction)

Suppose $a, b \in \mathbb{R}$ such that a is rational, ab is irrational and b is not irrational. Thus b is rational.

Since $a, b \in \mathbb{Q}$, there exist integers l, m, n, p so that $a = \frac{l}{m}$, $b = \frac{n}{p}$ and $m \neq 0$ and $p \neq 0$.

Thus, $ab = \frac{l}{m} \cdot \frac{n}{p} = \frac{ln}{mp}$ where $ln, mp \in \mathbb{Z}$ and $mp \neq 0$. Thus $ab \in \mathbb{Q}$.

Now we have a contradiction since ab cannot be rational and irrational. Thus, the assumption that b is rational is false. Thus, b is irrational.

4. (20 points) Suppose $x, y \in \mathbb{R}$. Prove $(x+y)^2 = x^2 + y^2$ if and only if $x = 0$ or $y = 0$.

Proof: Suppose $x, y \in \mathbb{R}$.

($\Rightarrow$:) First we prove if $(x+y)^2 = x^2+y^2$, then $x=0$ or $y=0$.
Suppose $(x+y)^2 = x^2+y^2$. Then $x^2+2xy+y^2 = x^2+y^2$. Thus $2xy=0$.
Since $2xy=0$, it follows that either $x=0$ or $y=0$.

($\Leftarrow$:) Next we show that if $x=0$ or $y=0$, then $(x+y)^2 = x^2+y^2$.
Suppose $x=0$ or $y=0$. Thus, $xy=0$ and consequently $2xy=0$.
Since $2xy=0$, we know $x^2+2xy+y^2 = x^2+y^2$. Thus, $(x+y)^2 = x^2+y^2$.

Note: Think carefully about why this argument is faulty:

($\Leftarrow$:) Show that if $x=0$ or $y=0$, then $(x+y)^2 = x^2+y^2$.

Case 1: Assume $x=0$

Then $(x+y)^2 = x^2+y^2$ implies $(0+y)^2 = 0^2+y^2$
which implies $y^2 = y^2$ which is true.
Thus when $x=0$, $(x+y)^2 = x^2+y^2$.

Moreover, this is different from the following argument:

Case 1: Suppose $x=0$.
Then $(x+y)^2 = (0+y)^2 = y^2$ and $x^2+y^2 = 0^2+y^2 = y^2$.
Thus, we have shown that when $x=0$, it follows that $(x+y)^2 = x^2+y^2$.

5. (a) (5 points) Complete the following *formal* definition:

Given $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$, we write $a \equiv b \mod n$ if $n \mid (a-b)$.

(b) (15 points) If $a \in \mathbb{Z}$, then $a^3 \equiv a (\text{mod } 3)$.

What am I thinking? This is the product of 3 consecutive integers.

Proof: Let $a \in \mathbb{Z}$.

Observe that $a^3 - a = a(a^2-1) = a(a-1)(a+1)$.

We will proceed by cases.

Case 1: Suppose $a = 3n$ for $n \in \mathbb{Z}$.
Then $a(a-1)(a+1) = 3n(3n-1)(3n+1)$, which is divisible by 3.
Thus $a^3 \equiv a \mod 3$ in this case.

Case 2: Suppose $a = 3n+1$ for $n \in \mathbb{Z}$
Then $a(a-1)(a+1) = (3n+1)(3n)(3n+2) = 3n(3n+1)(3n+2)$,
which is divisible by 3. So $a^3 \equiv a \mod 3$ in this case.

Case 3: Suppose $a = 3n+2$ for $n \in \mathbb{Z}$
Then $a(a-1)(a+1) = (3n+2)(3n+1)(3n+3) = 3(n+1)(3n+2)(3n+1)$,
which is divisible by 3. Thus, $a^3 \equiv a \mod 3$ in this case.

Since $a^3 \equiv a \mod 3$ in all cases, the result follows.

boiler plate wording if unable to produce a proof:

Note: It is at this point in the "work backwards" method that one realizes one MUST play with the expression $a^3 - a$. The only thing I know to do with it is factor.

Thus, $a^3 - a = 3k$, for some $k \in \mathbb{N}$.

Thus, $3 \mid (a^3 - a)$.

Thus, $a^3 \equiv a \mod 3$.

Extra Credit (10 points) Suppose $n \in \mathbb{Z}$. Prove that $\gcd(n, n+2) \in \{1, 2\}$.

Proof: Let $n \in \mathbb{Z}$ and let $d = \gcd(n, n+2)$.

Then, by the definition of gcd, $d \mid n$ and $d \mid n+2$.

By definition of divides, it follows that

$$n = dk_1 \text{ and } n+2 = dk_2 \text{ for } k_1, k_2 \in \mathbb{Z}.$$

Thus, by algebra,

$$2 = (n+2) - (n) = k_2 d - k_1 d = (k_1 - k_2) d,$$

where $k_1 - k_2 \in \mathbb{Z}$.

Thus, we have demonstrated that $d \mid 2$. The only positive divisors of 2 are 1 and 2. Thus $d \in \{1, 2\}$.