Math 330-3 Number Systems Fall 2022 Exam 1 Feingold

SHOW ALL WORK NECESSARY TO JUSTIFY YOUR ANSWERS. $\mathbb{N}^+ = \mathbb{N}\backslash\{0\}$

1. (20 Points) Write each of the following statements P as a logically equivalent statement Q so that the word "not" does not occur anywhere in Q. Whether the statement is true or false is not the issue.

(a) not($\exists m \in \mathbb{Z}$ such that $\forall n \in \mathbb{Z}$, $m > n$)
(b) not($\forall a \in \mathbb{Z}$, $\exists b \in \mathbb{N}$ such that $b \leq a$)
(c) not(if $x^2 \leq y^2$ then $x \leq y$)
(d) not($x < y$ and $xy = 8$)

---

2. (20 Points) For $m \in \mathbb{N}^+$ we defined $\mathbb{Z}_m = \{[a]_m \mid a \in \mathbb{Z}\}$ consisting of m distinct equivalence classes, $[a]_m = \{x \in \mathbb{Z} \mid x \equiv a \ (mod\ m)\}$. We have also defined binary operations $+$ and $\cdot$ on $\mathbb{Z}_m$ which make it a ring. For $m, n \in \mathbb{N}^+$, **try to define** a function $f : \mathbb{Z}_m \to \mathbb{Z}_n$ by $f([a]_m) = [a]_n$ for any $a \in \mathbb{Z}$.

(a) (5 pts) Determine whether or not $f : \mathbb{Z}_5 \to \mathbb{Z}_7$ is **well-defined** and **justify** your answer.
(b) (5 pts) What relationship between m and n would **guarantee** that $f : \mathbb{Z}_m \to \mathbb{Z}_n$ is a well-defined function?

(c) (10 pts) Assuming that m and n satisfy that relationship so f is a well-defined function, prove that f is a ring homomorphism, that is, $f([a]_m + [b]_m) = f([a]_m) + f([b]_m)$ and $f([a]_m \cdot [b]_m) = f([a]_m) \cdot f([b]_m)$.

---

3. (20 Points) Determine whether each assertion is true or false. Prove your answer by any method.

(a) $\forall m \in \mathbb{Z}$, $\exists n \in \mathbb{Z}$ such that $m^2 - n^2$ is divisible by 4.
(b) $\exists n \in \mathbb{Z}$, $\forall m \in \mathbb{Z}$ such that $m^2 - n^2$ is divisible by 4.

---

4. (20 Points) Prove each of the following statements rigorously. You may use that for $n, m, p, q \in \mathbb{Z}$, if $0 \leq m \leq n$ and $0 \leq p \leq q$ then $0 \leq mp \leq nq$. You may also use the recursive definition of $k!$: $0! = 1$ and for any $k \in \mathbb{N}$, $(k+1)! = (k+1) \cdot k!$, and the recursive definition of powers: For any $n \in \mathbb{Z}$ and for any $k \in \mathbb{N}$, n^k is defined recursively by: $n^0 = 1$ and $n^{k+1} = n^k \cdot n$.

(a) If $a, b \in \mathbb{Z}$ satisfy $0 \leq a \leq b$ then $\forall k \in \mathbb{N}^+$ we have $a^k \leq b^k$.
(b) For any $k \in \mathbb{N}^+$ we have $k! \leq k^k$.

---

5. (20 Points) Prove each of the following **by induction**. Direct proofs are not acceptable.

(a) For any $n \in \mathbb{N}^+$ we have $\displaystyle\sum_{j=1}^{n}(2j-1) = n^2$.

(b) For any $k \in \mathbb{N}$ we have $5|(6^k - 1)$.

Math 330-3 Number Systems Fall 2022 Exam 1 Solutions Feingold

1. (20 Points) Write each of the following statements P as a logically equivalent statement Q so that the word "not" does not occur anywhere in Q. Whether the statement is true or false is not the issue.

(a) not($\exists m \in \mathbb{Z}$ such that $\forall n \in \mathbb{Z}$, $m > n$) is equivalent to
$\forall m \in \mathbb{Z}$, $\exists n \in \mathbb{Z}$ such that $m \leq n$.
(b) not($\forall a \in \mathbb{Z}$, $\exists b \in \mathbb{N}$ such that $b \leq a$) is equivalent to $\exists a \in \mathbb{Z}$ such that $\forall b \in \mathbb{N}$, $b > a$.
(c) not(if $x^2 \leq y^2$ then $x \leq y$) is equivalent to $x^2 \leq y^2$ and $x > y$.
(d) not($x < y$ and $xy = 8$) is equivalent to $x \geq y$ or $xy \neq 8$ (and to $x < y$ implies $xy \neq 8$).

---

2. (20 Points) For $m \in \mathbb{N}^+$ we defined $\mathbb{Z}_m = \{[a]_m \mid a \in \mathbb{Z}\}$ consisting of m distinct equivalence classes, $[a]_m = \{x \in \mathbb{Z} \mid x \equiv a \ (mod\ m)\}$. We have also defined binary operations $+$ and $\cdot$ on $\mathbb{Z}_m$ which make it a ring. For $m, n \in \mathbb{N}^+$, **try to define** a function $f : \mathbb{Z}_m \to \mathbb{Z}_n$ by $f([a]_m) = [a]_n$ for any $a \in \mathbb{Z}$.

(a) (5) Determine whether or not $f : \mathbb{Z}_5 \to \mathbb{Z}_7$ is **well-defined** and **justify** your answer.

Proof: This f is not a well-defined function because, for example, $[0]_5 = [5]_5$ but $f([0]_5) = [0]_7 \neq [5]_7 = f([5]_5)$.

(b) (5) What relationship between m and n would **guarantee** that $f : \mathbb{Z}_m \to \mathbb{Z}_n$ is a well-defined function?

Proof: In order for this f to be well-defined, we would have to know that $[a]_m = [b]_m$ implies $f([a]_m) = f([b]_m)$, that is, $[a]_n = [b]_n$. We would need to know that $m|(a-b)$ implies $n|(a-b)$. The relationship $n|m$ would be needed to guarantee that since transitivity of "divides" would say that $n|m$ and $m|(a-b)$ implies $n|(a-b)$.

(c) (10 pts) Assuming that m and n satisfy that relationship so f is a well-defined function, prove that f is a ring homomorphism, that is, $f([a]_m + [b]_m) = f([a]_m) + f([b]_m)$ and $f([a]_m \cdot [b]_m) = f([a]_m) \cdot f([b]_m)$.

Proof: We have
$f([a]_m + [b]_m) = f([a+b]_m) = [a+b]_n = [a]_n + [b]_n = f([a]_m) + f([b]_m)$, and
$f([a]_m \cdot [b]_m) = f([a \cdot b]_m) = [a \cdot b]_n = [a]_n \cdot [b]_n = f([a]_m) \cdot f([b]_m)$.

---

3. (20 Points) Determine whether each assertion is true or false. Prove your answer by any method.

(a) $\forall m \in \mathbb{Z}$, $\exists n \in \mathbb{Z}$ such that $m^2 - n^2$ is divisible by 4.

True. Proof: For any $m \in \mathbb{Z}$, the obvious choice of $n = m \in \mathbb{Z}$ gives $m^2 - n^2 = m^2 - m^2 = 0$ which is divisible by 4.

(b) $\exists n \in \mathbb{Z}$ such that $\forall m \in \mathbb{Z}$ we have $m^2 - n^2$ is divisible by 4.

False. Proof: By contradiction, suppose such an integer n exists, then in particular for $m = 1$ we would have $4|(1 - n^2)$ and for $m = 0$ we would have $4|(-n^2)$, so 4 would divide the difference $(1 - n^2) - (-n^2) = 1$. But 4 does not divide 1.

---

4. (20 Points) Prove each of the following statements rigorously. You may use that for $n, m, p, q \in \mathbb{Z}$, if $0 \leq m \leq n$ and $0 \leq p \leq q$ then $0 \leq mp \leq nq$. You may also use the recursive definition of $k!$: $0! = 1$ and for any $k \in \mathbb{N}$, $(k+1)! = (k+1) \cdot k!$, and the recursive definition of powers: For any $n \in \mathbb{Z}$ and for any $k \in \mathbb{N}$, n^k is defined recursively by: $n^0 = 1$ and $n^{k+1} = n^k \cdot n$.

(a) If $a, b \in \mathbb{Z}$ satisfy $0 \leq a \leq b$ then $\forall k \in \mathbb{N}^+$ we have $a^k \leq b^k$.

Proof: Let $a, b \in \mathbb{Z}$ satisfy $0 \leq a \leq b$, and for $k \in \mathbb{N}^+$ let $P(k)$ be the assertion that $a^k \leq b^k$. $P(1)$ is true since $a^1 = a \leq b = b^1$. Assume for some $k \in \mathbb{N}^+$ that $P(k)$ is true. Then $a^{k+1} = a^k \cdot a \leq b^k \cdot a \leq b^k \cdot b = b^{k+1}$ so $P(k+1)$ is true. Done by induction.

(b) For any $k \in \mathbb{N}^+$ we have $k! \leq k^k$.

Proof: For $k \in \mathbb{N}^+$ let $P(k)$ be the assertion $k! \leq k^k$. $P(1)$ is true since $1! = 1 = 1^1$. For some $k \in \mathbb{N}^+$ assume $P(k)$ is true. Show $P(k+1)$, that is, $(k+1)! \leq (k+1)^{(k+1)}$. By definition of factorial and by $P(k)$, we know that $(k+1)! = (k+1) \cdot (k!) \leq (k+1) \cdot (k^k)$. By problem 4(a), since $0 \leq k < k+1$, we have $0 \leq k^k \leq (k+1)^k$, so we get $(k^k) \cdot (k+1) \leq (k+1)^k \cdot (k+1) = (k+1)^{(k+1)}$ by definition. By transitivity of $\leq$, we have shown that $(k+1)! \leq (k+1)^{(k+1)}$, that is, $P(k+1)$ is true. Done by induction.

---

5. (20 Points) Prove each of the following **by induction**. Direct proofs are not acceptable.

(a) For any $n \in \mathbb{N}^+$ we have $\sum_{j=1}^{n}(2j-1) = n^2$.

Proof: For $n \in \mathbb{N}^+$ let $P(n)$ be the assertion of the formula for n. $P(1)$ is true since $\sum_{j=1}^{1}(2j-1) = 2(1) - 1 = 1 = 1^2$. Assume $P(n)$. Then

$$\begin{aligned}
\sum_{j=1}^{n+1}(2j-1) &= \sum_{j=1}^{n}(2j-1) + (2(n+1)-1) && \text{by definition of summation} \\
&= n^2 + 2(n+1) - 1 && \text{by } P(n) \\
&= n^2 + 2n + 2 - 1 && \text{by distributive law in } \mathbb{Z} \\
&= n^2 + 2n + 1 && \text{by simple arithmetic} \\
&= (n+1)^2 && \text{by definition of powers and simple algebra}
\end{aligned}$$

so $P(n+1)$ is true. We are done by induction.

(b) For any $k \in \mathbb{N}$ we have $5|(6^k - 1)$.

Proof: For $k \in \mathbb{N}$ let $P(k)$ be the assertion $5|(6^k - 1)$. $P(0)$ is true since $6^0 - 1 = 1 - 1 = 0$ and we know $5|0$ since $0 = (5)(0)$. Assume $P(k)$. Then $6^{k+1} - 1 = 6^k 6 - 1 = 6^k(5+1) - 1 = 6^k 5 + (6^k - 1)$. But $5|(6^k 5)$ and by $P(k)$ we know $5|(6^k - 1)$ so $5|(6^k 5 + (6^k - 1))$ gives us $5|(6^{k+1} - 1)$ which is $P(k+1)$. Done by induction.
