Math 330-3 Number Systems Fall 2022 Final Exam Feingold

SHOW ALL WORK NECESSARY TO JUSTIFY YOUR ANSWERS.

$\mathbb{N}^+ = \mathbb{N}\backslash\{0\}$ and $\mathbb{Q}^+ = \{r \in \mathbb{Q} \mid r > 0\}$

(1) (20 Points) Write the **definition** for each of the following concepts.

(a) For a rational sequence, a_n, $n \in \mathbb{N}^+$, the **limit** $\lim_{n\to\infty} a_n = L$ when

(b) A rational sequence, a_n, $n \in \mathbb{N}^+$, is **Cauchy** when

(c) A relation $\sim$ on a set S is an **equivalence relation** when

(d) For $n \in \mathbb{N}$ let $P(n)$ be an assertion. The **Principle of Mathematical Induction** says that to prove $P(n)$ is true for all $n \in \mathbb{N}$ we must show that

---

(2) (20 Points) Prove each of the following statements by induction.

(a) For any $n \in \mathbb{N}$, we have $\displaystyle\sum_{k=0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$.

(b) For any $n \in \mathbb{N}$, we have $6|(2n^3 + 3n^2 + n)$.

---

(3) (20 Points) Define sets $A = \{n \in \mathbb{Z} \mid gcd(3, n) = 1\}$ and $B = \{n \in \mathbb{Z} \mid gcd(6, n) = 1\}$. For each assertion below prove it if it is true. If it is false, show why.

(a) $A \cap B = B$ (b) $A \cup B = \mathbb{Z}$ (c) $A \cup 3\mathbb{Z} = \mathbb{Z}$ (d) $B \cup 6\mathbb{Z} = \mathbb{Z}$

---

(4) (20 Points) For each of the following formulas, determine whether or not it defines a **function**, and if so, whether it is **injective**, **surjective**, **bijective**.

(a) $f : \mathbb{Z}_3 \to \mathbb{Z}_9$ by $f([a]_3) = [a]_9$ for all $a \in \mathbb{Z}$.

(b) $g : \mathbb{R} \to \mathbb{R}$ by $g(x) = 3x + 1$ for all $x \in \mathbb{R}$.

(c) $h : \mathbb{Q} \to \mathbb{Z}$ by $h(\frac{m}{n}) = m + n$ for all $\frac{m}{n} \in \mathbb{Q}$.

---

(5) (30 Points) Answer the following questions about rational sequences.

(a) Use the **definition** of limit to prove that $a_n = \dfrac{2n^2+3}{3n^2+4}$ has $\lim_{n\to\infty} a_n = \dfrac{2}{3}$.

(b) Use the **definition** of Cauchy to prove that $a_n = \dfrac{(-1)^n}{n}$ is Cauchy.

---

(6) (20 Points) We say sets S and T have the same **cardinality** when $\exists f : S \to T$ which is **bijective**. For any set S, the **power set** $\mathcal{P}(S) = \{A \mid A \subseteq S\}$ is the set of all subsets of S. For $n \in \mathbb{N}^+$ let $[1, n] = \{k \in \mathbb{N}^+ \mid 1 \le k \le n\} = \{1, \cdots, n\}$. We say set $S = \{s_1, \cdots, s_n\}$ has **finite cardinality** $|S| = n$ because the function $f : [1, n] \to S$ with $f(k) = s_k$ is bijective. Assume you know that for **disjoint** finite sets, $C \cap D = \emptyset$, that $|C \cup D| = |C| + |D|$.

Prove by induction on $n \in \mathbb{N}^+$ that the cardinality $|\mathcal{P}([1, n])| = 2^n$.

Hint: In the inductive step, for any subset $A \subseteq [1, n+1]$, either $n+1 \notin A$ or $n+1 \in A$.

---

(7) (20 Points) The Euler phi function is defined by $\phi(n) = |U(n)|$ where $U(n) = \{[a]_n \in \mathbb{Z}_n \mid gcd(a,n) = 1\}$. It can be proven that if $gcd(m,n) = 1$ then $\phi(mn) = \phi(m)\phi(n)$. We already know that $\phi(p) = p-1$ for p any prime, but it is also true that $\phi(p^k) = p^{k-1}(p-1)$, so from the Fundamental Theorem of Arithmetic, for any $2 \leq n \in \mathbb{N}$, if $n = \prod_{i=1}^{r} p_i^{k_i}$ then we get the famous Euler formula

$$\phi(n) = \prod_{i=1}^{r} \phi(p_i^{k_i}) = \prod_{i=1}^{r} p_i^{k_i-1}(p_i - 1) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

We have used Euler's theorem, $a^{\phi(n)} \equiv 1 \pmod{n}$ when $gcd(a,n) = 1$, to answer questions about the equivalence class of a high power of such an integer, a. Use this information to answer the following questions as efficiently as possible, without explicitly computing high powers.

(a) Find the last two digits of 9^{1002}, that is, find $1 \leq d \leq 99$ such that $9^{1002} \equiv d \pmod{100}$.

(b) Find the unique c with $1 \leq c < 23$ such that $18^{7064} \equiv c \pmod{23}$.

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

(1) (20 Points) Write the **definition** for each of the following concepts.

(a) For a rational sequence, a_n, $n \in \mathbb{N}^+$, the **limit** $\lim_{n\to\infty} a_n = L$ when
$\forall \epsilon \in \mathbb{Q}^+$, $\exists M_\epsilon \in \mathbb{N}^+$ such that if $n \geq M_\epsilon$ then $|a_n - L| < \epsilon$.

(b) A rational sequence, a_n, $n \in \mathbb{N}^+$, is **Cauchy** when
$\forall \epsilon \in \mathbb{Q}^+$, $\exists M_\epsilon \in \mathbb{N}^+$ such that if $m, n \geq M_\epsilon$ then $|a_m - a_n| < \epsilon$.

(c) A relation $\sim$ on a set S is an **equivalence relation** when
It is reflexive: $\forall s \in S$, $s \sim s$, symmetric: $\forall s_1, s_2 \in S$, $s_1 \sim s_2$ implies $s_2 \sim s_1$, transitive: $\forall s_1, s_2, s_3 \in S$, $s_1 \sim s_2$ and $s_2 \sim s_3$ implies $s_1 \sim s_3$.

(d) For $n \in \mathbb{N}$ let $P(n)$ be an assertion. The **Principle of Mathematical Induction** says that to prove $P(n)$ is true for all $n \in \mathbb{N}$ we must show that $P(0)$ is true (base case), and for any $n \in \mathbb{N}$, if $P(n)$ is true then $P(n+1)$ is true (inductive step).

---

(2) (20 Points) Prove each of the following statements by induction.

(a) For any $n \in \mathbb{N}$, we have $\displaystyle\sum_{k=0}^{n} k^2 = \frac{n(n+1)(2n+1)}{6}$

Solution: For any $n \in \mathbb{N}$ let $P(n)$ be the assertion of the formula. The base case $P(0)$ says $\displaystyle\sum_{k=0}^{0} k^2 = \frac{0(0+1)(2(0)+1)}{6}$, that is, $0^2 = \frac{0}{6}$ which is true. For the inductive step, assume that for some $n \in \mathbb{N}$, $P(n)$ is true, and show that implies $P(n+1)$. Starting with the left hand side of $P(n+1)$, using the inductive definition of summations and the inductive hypothesis, $P(n)$, we have

$$\sum_{k=0}^{n+1} k^2 = \sum_{k=0}^{n} k^2 + (n+1)^2 = \frac{n(n+1)(2n+1)}{6} + (n+1)^2 = \frac{n(n+1)(2n+1) + 6(n+1)^2}{6}$$

$$= \frac{(n+1)(n(2n+1) + 6(n+1))}{6} = \frac{(n+1)(2n^2 + 7n + 6)}{6} = \frac{(n+1)(n+2)(2n+3)}{6}$$

which is the right hand side of $P(n+1)$, completing the proof by induction.

(b) For any $n \in \mathbb{N}$, we have $6|(2n^3 + 3n^2 + n)$.

Solution: For any $n \in \mathbb{N}$ let $P(n)$ be the assertion that $6|(2n^3 + 3n^2 + n)$. $P(0)$ says $6|0$ which is true. Assuming $P(n)$ for some $n \in \mathbb{N}$, show that implies $P(n+1)$, that is, $6|(2(n+1)^3 + 3(n+1)^2 + (n+1))$. We have by basic algebra,

$$2(n+1)^3 + 3(n+1)^2 + (n+1) = 2(n^3 + 3n^2 + 3n + 1) + 3(n^2 + 2n + 1) + (n+1)$$

$$= (2n^3 + 3n^2 + n) + 6n^2 + 6n + 2 + 6n + 3 + 1 = (2n^3 + 3n^2 + n) + 6(n^2 + 2n + 1)$$

which is divisible by 6 since both terms are divisible by 6.

---

(3) (20 Points) $A = \{n \in \mathbb{Z} \mid gcd(3, n) = 1\}$ and $B = \{n \in \mathbb{Z} \mid gcd(6, n) = 1\}$. For each assertion below prove it if it is true. If it is false, show why.

(a) $A \cap B = B$ (b) $A \cup B = \mathbb{Z}$ (c) $A \cup 3\mathbb{Z} = \mathbb{Z}$ (d) $B \cup 6\mathbb{Z} = \mathbb{Z}$

(a) True. $A = \{n \in \mathbb{Z} \mid 3 \not| n\} = (3\mathbb{Z} + 1) \cup (3\mathbb{Z} - 1)$ and $B = \{n \in \mathbb{Z} \mid n \equiv \pm 1 \pmod 6\} = (6\mathbb{Z}+1) \cup (6\mathbb{Z}-1)$. So $n \in B$ iff $n = 6m \pm 1 = 3(2m) \pm 1$ for some $m \in \mathbb{Z}$ says $n \in A$. Since B is a subset of A, $A \cap B = B$.

(b) False. From part (a), we have $A \cup B = A \neq \mathbb{Z}$. No multiple of 3 is in $A \cup B$.

(c) True. $A \cup 3\mathbb{Z} = (3\mathbb{Z}+1) \cup (3\mathbb{Z}-1) \cup 3\mathbb{Z} = \mathbb{Z}$ since it is the union of all three equivalence classes mod 3.

(d) False. $B \cup 6\mathbb{Z} = (6\mathbb{Z}+1) \cup (6\mathbb{Z}-1) \cup 6\mathbb{Z} \neq \mathbb{Z}$ since it is only three of the six equivalence classes mod 6. In particular, 2, 3 and 4 are not in $B \cup 6\mathbb{Z}$.

---

(4) (20 Points) For each of the following formulas, determine whether or not it defines a **function**, and if so, whether it is **injective**, **surjective**, **bijective**.

(a) (5 Pts) $f : \mathbb{Z}_3 \to \mathbb{Z}_9$ by $f([a]_3) = [a]_9$ for all $a \in \mathbb{Z}$.

Solution: This is not a function since $[0]_3 = [3]_3$ in $\mathbb{Z}_3$ but $f([0]_3) = [0]_9 \neq [3]_9 = f([3]_3)$.

(b) $g : \mathbb{R} \to \mathbb{R}$ by $g(x) = 3x + 1$ for all $x \in \mathbb{R}$.

Solution: (10 Pts) This is a function since for every $x \in \mathbb{R}$, $3x + 1 \in \mathbb{R}$ is defined by the operations of multiplication and addition in $\mathbb{R}$. g is injective because $g(x_1) = g(x_2)$ means $3x_1 + 1 = 3x_2 + 1$ which implies $3x_1 = 3x_2$ and after dividing by 3, $x_1 = x_2$. g is surjective because for any $y \in \mathbb{R}$ we can find $x \in \mathbb{R}$ such that $g(x) = y$. To do so, just solve $3x + 1 = y$ to get $x = (y - 1)/3$. g is bijective since it is both injective and surjective.

(c) (5 Pts) $h : \mathbb{Q} \to \mathbb{Z}$ by $h(\frac{m}{n}) = m + n$ for all $\frac{m}{n} \in \mathbb{Q}$.

Solution: This is not a function since $\frac{1}{2} = \frac{2}{4} \in \mathbb{Q}$ but $h(\frac{1}{2}) = 1+2 = 3 \neq 6 = 2+4 = h(\frac{2}{4})$.

(5) (30 Points) Answer the following questions about rational sequences.

(a) Use the **definition** of limit to prove that $a_n = \dfrac{2n^2+3}{3n^2+4}$ has $\lim_{n\to\infty} a_n = \dfrac{2}{3}$.

Solution: We need to show that $\forall \epsilon \in \mathbb{Q}^+$, $\exists M_\epsilon \in \mathbb{N}^+$ such that if $n \ge M_\epsilon$ then $|a_n - L| < \epsilon$. We know that $\left|\dfrac{2n^2+3}{3n^2+4} - \dfrac{2}{3}\right| = \left|\dfrac{3(2n^2+3)-2(3n^2+4)}{3(3n^2+4)}\right| = \dfrac{1}{3(3n^2+4)} < \dfrac{1}{9n^2}$. Let's find $M_\epsilon \in \mathbb{N}^+$ such that if $n \ge M_\epsilon$ then $\dfrac{1}{9n^2} < \epsilon$ which is true iff $\dfrac{1}{9\epsilon} < n^2$ iff $\dfrac{1}{3\sqrt{\epsilon}} < n$. Using the Archimedean Lemma, for $x = \frac{1}{3\sqrt{\epsilon}} \in \mathbb{R}$ there is an $N_x \in \mathbb{N}^+$ such that $x < N_x$, so for $n \ge M_\epsilon = N_x$ we have $\frac{1}{3\sqrt{\epsilon}} < M_\epsilon \le n$ implies $\frac{1}{9n^2} < \epsilon$.

(b) Use the **definition** of Cauchy to prove that $a_n = \dfrac{(-1)^n}{n}$ is Cauchy.

Solution: We need to show that $\forall \epsilon \in \mathbb{Q}^+$, $\exists M_\epsilon \in \mathbb{N}^+$ such that if $m, n \ge M_\epsilon$ then $|a_m - a_n| < \epsilon$. From the Triangle Inequality we know

$$\left|\frac{(-1)^m}{m} - \frac{(-1)^n}{n}\right| \le \left|\frac{(-1)^m}{m}\right| + \left|-\frac{(-1)^n}{n}\right| = \frac{1}{m} + \frac{1}{n}.$$

The condition $m \ge M_\epsilon$ is equivalent to $\frac{1}{m} \le \frac{1}{M_\epsilon}$ so we want $\frac{1}{M_\epsilon} < \frac{\epsilon}{2}$, which is the same as $\frac{2}{\epsilon} < M_\epsilon$. Using the Archimedean Lemma, for $x = \frac{2}{\epsilon} \in \mathbb{R}$ there is an $N_x \in \mathbb{N}^+$ such that $x < N_x$, so for $m, n \ge M_\epsilon = N_x$ we have $\frac{2}{\epsilon} < M_\epsilon \le m, n$ implies $\frac{1}{m} + \frac{1}{n} < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon$.

---

(6) (20 Points) We say sets S and T have the same **cardinality** when $\exists f : S \to T$ which is **bijective**. For any set S, the **power set** $\mathcal{P}(S) = \{A \mid A \subseteq S\}$ is the set of all subsets of S. For $n \in \mathbb{N}^+$ let $[1, n] = \{k \in \mathbb{N}^+ \mid 1 \le k \le n\} = \{1, \cdots, n\}$. We say set $S = \{s_1, \cdots, s_n\}$ has **finite cardinality** $|S| = n$ because the function $f : [1, n] \to S$ with $f(k) = s_k$ is bijective. Assume you know that for **disjoint** finite sets, $C \cap D = \emptyset$, that $|C \cup D| = |C| + |D|$.

Prove by induction on $n \in \mathbb{N}^+$ that the cardinality $|\mathcal{P}([1, n])| = 2^n$.

Solution: For the base case $n = 1$, $\mathcal{P}([1, 1]) = \{\emptyset, \{1\}\}$ has $2 = 2^1$ elements. For the inductive step suppose $|\mathcal{P}([1, n])| = 2^n$ and try to prove $|\mathcal{P}([1, n+1])| = 2^{n+1} = 2^n \cdot 2$. Write $\mathcal{P}([1, n+1]) = C \cup D$ where $C = \{A \subseteq [1, n+1] \mid n+1 \notin A\} = \{A \subseteq [1, n]\} = \mathcal{P}([1, n])$ and $D = \{A \subseteq [1, n+1] \mid n+1 \in A\}$. These are disjoint subsets of $\mathcal{P}([1, n+1])$ since any subset of $[1, n+1]$ either contains $n+1$ or it doesn't. By the inductive hypothesis, $|C| = |\mathcal{P}([1, n])| = 2^n$, and we know $|\mathcal{P}([1, n+1])| = |C \cup D| = |C| + |D| = 2^n + |D|$. So it only remains to show that $|D| = |C|$ because that would say $|\mathcal{P}([1, n+1])| = 2^n + 2^n = 2^n \cdot 2 = 2^{n+1}$. To get $|D| = |C|$ we just need to find a bijective map $f : C \to D$. For any $A \in C$ define $f(A) = A \cup \{n+1\} \in D$. This map is surjective by the definitions of C and D. It is injective since $f(A) = f(B)$ means $A \cup \{n+1\} = B \cup \{n+1\}$ so $A = B$ in C.

(7) (20 Points) The Euler phi function is defined by $\phi(n) = |U(n)|$ where $U(n) = \{[a]_n \in \mathbb{Z}_n \mid gcd(a,n) = 1\}$. It can be proven that if $gcd(m,n) = 1$ then $\phi(mn) = \phi(m)\phi(n)$. We already know that $\phi(p) = p-1$ for p any prime, but it is also true that $\phi(p^k) = p^{k-1}(p-1)$, so from the Fundamental Theorem of Arithmetic, for any $2 \le n \in \mathbb{N}$, if $n = \prod_{i=1}^{r} p_i^{k_i}$ then we get the famous Euler formula

$$\phi(n) = \prod_{i=1}^{r} \phi(p_i^{k_i}) = \prod_{i=1}^{r} p_i^{k_i-1}(p_i - 1) = n \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

We have used Euler's theorem, $a^{\phi(n)} \equiv 1 \pmod{n}$ when $gcd(a,n) = 1$, to answer questions about the equivalence class of a high power of such an integer, a. Use this information to answer the following questions as efficiently as possible, without explicitly computing high powers.

(a) Find the last two digits of 9^{1002}, that is, find $1 \le d \le 99$ such that $9^{1002} \equiv d \pmod{100}$.

Solution: We know that $\phi(100) = \phi(2^2)\phi(5^2) = 2^1(2-1)5^1(5-1) = (2)(5)(4) = 40$ so from Euler's Theorem, $9^{40} \equiv 1 \pmod{100}$. But $1002 = (40)(25) + 2$ so

$$9^{1002} = 9^{(40)(25)+2} = (9^{40})^{25}\ 9^2 \equiv 1^{25}\ 9^2 \equiv 81 \pmod{100} \quad \text{gives} \quad d = 81.$$

In fact, $9^{10} \equiv 1 \pmod{100}$ gives the same answer but takes too much time to calculate.

(b) Find the unique c with $1 \le c < 23$ such that $18^{7064} \equiv c \pmod{23}$.

Solution: Since 23 is prime, $\phi(23) = 22$ so from Euler's Theorem, or Fermat's Little Theorem, $18^{22} \equiv 1 \pmod{23}$. But $7064 = (22)(321) + 2$ so

$$18^{7064} = 18^{(22)(321)+2} = (18^{22})^{321}\ 18^2 \equiv 1^{321}\ 18^2 \equiv 324 \equiv (23)(14) + 2 \equiv 2 \pmod{23}$$

gives $c = 2$. The last steps could have been done as $18^2 \equiv (-5)^2 = 25 \equiv 2 \pmod{23}$.
