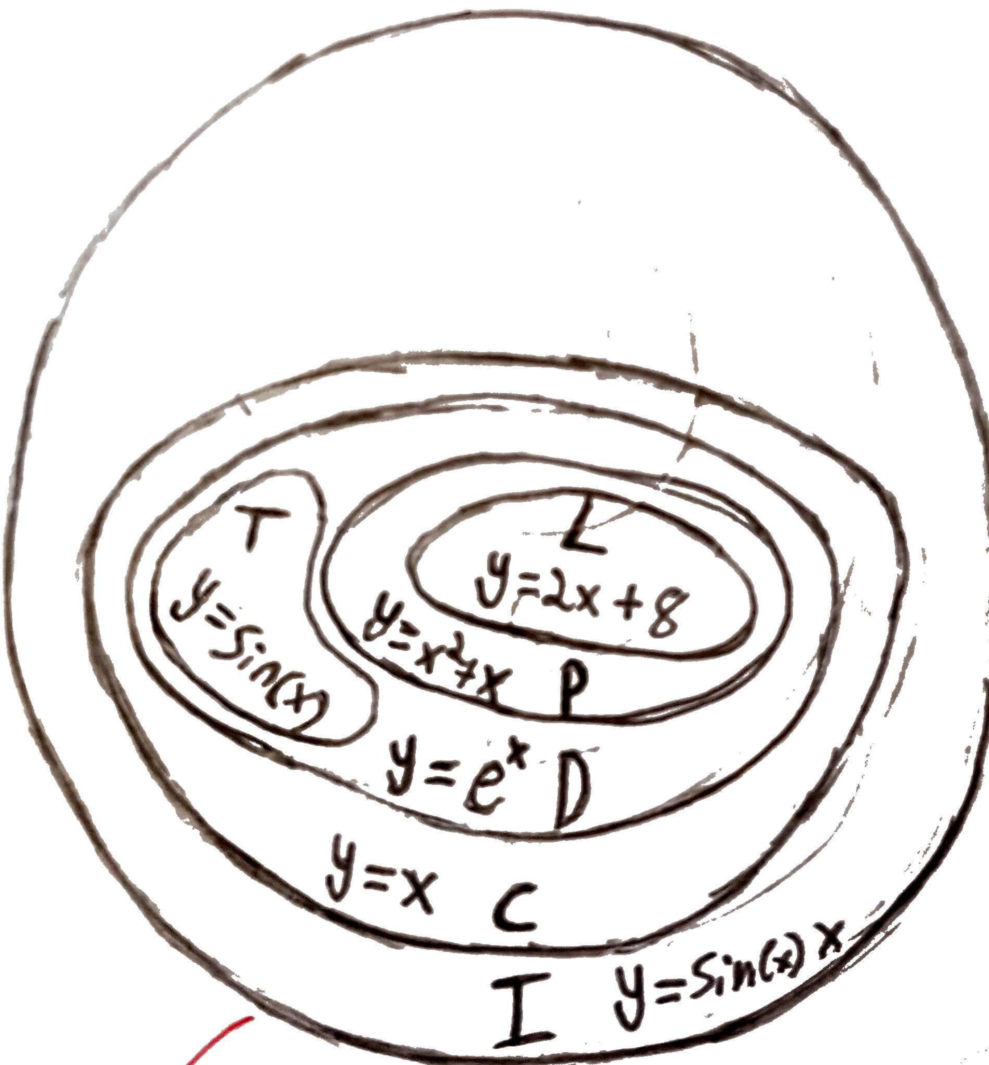
I = {m : m is an integrable function}
D = {x : x is a differentiable function}
L = {y : y is a linear function}
T = {z : z is a trigonometric function}
P = {a : a is a polynomial function}

(a)

(b)

(c)



(a)

(b) A

(c) A

(d) A C

the statement ... are not quazzit" is false,
or provide a counterexample in which a "glerby is a quazzit."

To prove the statement "Some rawkoy are quazzit" is false, you can provide a counterexample in which "∀rawkroy = quazzit." → ∀ is ... ... are

c) To prove the statement "No quazzit is fromulous" is false, you can provide a counterexample of "∃quazzit = fromulous."

) To prove the statement "for any $x>0$, there is a L where $f(x)>L$" is false, we can provide a counter example in which "for some $x>0$, there a limit when $f(x)<L$."

) To prove the statement "Most functions are continuous" is false, we can prove that "most functions are discontinuous."

) To prove the statement "Given any connected graph, and any two vertices, there is a path connecting the two vertices" is false, we can provide a counterexample like connected graph of 2 vertices with no path between them."

) To prove the statement "Every connected graph has a value k where any two vertices are no more than k units apart" is false, we can provide a counterexample in which "for a connected graph with value k, the vertices are more than k units apart."

) To prove the statement "Some diagnal matrices have nonzero eigenvalues" is false, we can provide a counter example in which "no diagnal matrices have nonzero eigenvalues."

4) a) The following are not ... glerbies:
- objects non-rawkoy
- rawkoys that are quazzit

b) The following are not glerbies:
- objects that are non-quazzit
- quazzits where 1 rawka lacks a flurion

(c) The following are not dependent sets:
- A vector set that holds a vector that's a linear combination of other vectors in the set.

(d) The following are not singularity matrices:
- ~~value~~ without

(e) The following are not groups:
- sets with no identity object
- sets where association fails for objects
- sets where 1 object has no inverse.

(f) The following are not objects that cartesian products
- Non-one to one cartesian products
- Non-onto cartesian ...

(a)

Logical Notation: $\forall n \in \mathbb{N}$ (n even & $n \geq 4$, ($\exists p, \exists q$ = prime #), where $n = p+q$).

Negation: $\exists n \in \mathbb{N}$ (n even & $n \geq 4$, ($\forall p, \forall q \neq$ prime #), where $n \neq p+q$).

(Negation in words) ⇒ (There exists at least one even number that is not the sum of a prime number.)

(b)

Logical Notation: $\forall \varepsilon > 0, \exists \phi > 0, \forall x \, (|x-a| < \phi \;\&\; |f(x)-L| < \varepsilon)$.

Negation: $\exists > 0, \forall \phi > 0, \exists x \, (|x-a| < \phi \;\&\; |f(x)-L| \geq \varepsilon)$.

(Negation in words) ⇒ (There exists some $\varepsilon > 0$ such that for every $\phi > 0$, there is at least one x with $|x-a| < \phi$ & $|f(x)-L| \geq \varepsilon$)

(c)

Logical Notation: $\forall \varepsilon > 0, \exists N \in \mathbb{N} \, \forall n \in \mathbb{N} \, (n > N \;\&\; |a_n - L| < \varepsilon)$.

Negation: $\exists \varepsilon > 0, \forall N \in \mathbb{N}, \exists n \in \mathbb{N} \, (n > N \;\&\; |a_n - L| < \varepsilon)$.

(Negation in Words)

↳ (There exists some $\varepsilon > 0$ such that for every N, there is at least one $n > N$ with $|a_n - L| \geq \varepsilon$)

(d)

Logical Notation: $\forall G$ (Euler Circuit(G) & $\exists H$ (Subgraph(H, G) = Hamiltonian(H)))

Negation: $\exists G$ (Euler Circuit(G) & $\forall H$ (Subgraph(H, G) $\neq$ Hamiltonian(H))).

(Negation In Words)

↳ (There exists a graph that has a Euler circuit but no subgraph that is Hamiltonian.)

conditionals

Quantifiers (Q)

- If a whole number is composite, then it can be expressed as a product of two smaller whole numbers. ✓

converse • If expressed as a product of two smaller whole numbers, then it's a composite whole number. ✓

Q: $\exists a, z \in \mathbb{N}, (1 < a < n \,\&\, 1 < z < n \,\&\, n = ab)$

(b) - If a quazzit is Scromulous, then all glerbys have at least one rawkoy.

converse - If all glerbys have at least one rawkoy, then a quazzit is Scromulous.

Q: $\forall g \, (g = \exists r)$

(c)

- If a function is continuos at $x=a$, then $\lim_{x \to a} f(x) = f(a)$

converse - If $\lim_{x \to a} f(x) = f(a)$, then said function is continuos at $x=a$. ✓

Q: $\forall \varepsilon > 0, \exists \delta > 0, \forall x \, (|x-a| < \delta \equiv |f(x) - f(a)|$

(d)

- If $\lim_{x \to a} f(x) = L$ & $\varepsilon > 0$ then there exists $\delta > 0$ where $|f(x) - L| < \varepsilon$ whenever $|x-a| < \delta$.

converse - If there exists $\delta > 0$ where $|f(x) - L| < \varepsilon$ whenever $|x-a| < \delta$, then $\lim_{x \to a} f(x) = L$ ✓

Q: $\forall \varepsilon > 0, \exists \delta > 0, \forall x \, (|x-a| < \delta \equiv |f(x) - L| < \varepsilon)$

(e)

- If $a_n = L$ & $\varepsilon > 0$ then there exists $N > 0$ where for all $n > N$, $|a_n - L| < \varepsilon$.

converse If there exists $N > 0$ where for all $n > N$, $|a_n - L| < \varepsilon$, then $a_n = L$ & $\varepsilon > 0$.

Q: $\forall \varepsilon > 0, \exists N \in \mathbb{N} \, \forall n > N \, (|a_n - L| < \varepsilon)$

* Eli

12S

Quantifiers and Definitions

1. For each definition, rewrite as a two conditionals; then rewrite using quantifiers. Note: All your answers should be "in words."

   (a) A composite whole number is a number that can be expressed as a product of two smaller whole numbers.

   (b) A quazzit is scromulous if for all glerbys, there is at least one rawkroy.

   (c) A function is continuous at $x = a$ provided $\lim_{x \to a} f(x) = f(a)$.

   (d) $\lim_{x \to a} f(x) = L$ if, for any $\epsilon > 0$, there exists $\delta > 0$ where $|f(x) - L| < \epsilon$ whenever $|x - a| < \delta$.

   (e) $\lim_{x \to \infty} a_n = L$ if for any $\epsilon > 0$, there exists $N > 0$ where for all $m > n$, $|a_m - L| < \epsilon$.

2. Rewrite the statement using logical notation, including logical quantifiers. Then write the negation of the statement, first using logical notation, then "in words."

   (a) Every even number is the sum of two prime numbers.

   (b) For any $\epsilon > 0$, there is a $\delta > 0$ where $|f(x) - L| < \epsilon$ whenever $|x - a| < \delta$.

   (c) For any $\epsilon > 0$, there is a N where for all $n > N$, $|a_n - L| < \epsilon$.

   (d) Any graph with an Euler circuit has a subgraph that is Hamiltonian.

3. In the following a statement is claimed. Assume that the statement is *false*. Describe how you could prove it false, either by providing a counterexample or proving a conditional. (Don't try to find the counterexample or prove the negation, but describe what you're looking for: "A counterexample to the statement would be a left handed framistat, if it existed" or "To prove the statement false, we could prove that all rawkroy are not fromulous")

   (a) All glerby are not quazzit.

   (b) Some rawkroy are quazzit.

(b) Let $\mathbb{A}$ be the set of Algebraic Numbers (roots of polynomials & rational coefficients).

Theorem: $|\mathbb{A}| = \aleph_0$.

Let $\mathbb{Q}_{surd}$ be the set of quadratic surds. By definition, $\mathbb{Q}_{surd} \subset \mathbb{A}$.

$\mathbb{Q}_{surd} \subset \mathbb{A} \wedge |\mathbb{A}| = \aleph_0 \Rightarrow |\mathbb{Q}_{surd}| \leq \aleph_0$

Since $\mathbb{Q}_{surd}$ is clearly infinite, $|\mathbb{Q}_{surd}| = \aleph_0$.

(b) Let $\mathbb{A}$ be the set of Algebraic Numbers (roots of polynomials & rational coefficients).

Theorem: $|\mathbb{A}| = \aleph_0$.

Let $\mathbb{Q}_{surd}$ be the set of quadratic surds. By definition, $\mathbb{Q}_{surd} \subset \mathbb{A}$.

$\mathbb{Q}_{surd} \subset \mathbb{A} \wedge |\mathbb{A}| = \aleph_0 \Rightarrow |\mathbb{Q}_{surd}| \leq \aleph_0$

Since $\mathbb{Q}_{surd}$ is clearly infinite, $|\mathbb{Q}_{surd}| = \aleph_0$.

$a_0 = 1,\ a_{n+1} = 3a_n$

Base Case:

$n = 0,\ a_0 = 3^0 = 1$

Assume $n \geq 0$ for $a_n = 3^n$

$$a_{k+1} = 3a_k$$

$$a_{k+1} = 3(3^k)$$

$$a_{k+1} = 3^{k+1} \quad ■$$

Thus $a_n = 3^n$ for all $n \geq 0$

(b) $a_0 = 1,\ a_{n+1} = a_n + 3$

Base Case:

$n = 0,\ a_0 = 1 + 3(0) = 1$

Assume $a_k = 1 + 3k$ for $\mathbb{Z}_{k \geq 0}$

$$a_{k+1} = a_k + 3$$

Substitute assumption

$$a_{k+1} = (1 + 3k) + 3$$

$$a_{k+1} = 1 + 3k + 3 = 1 + 3(k+1) \quad ■$$

Thus, $a_n = 1 + 3n$ for $\forall n \geq 0,\ n \in \mathbb{Z}$

(c) $a_0 = 1,\ a_{n+1} = 2a_n + 1$

$n = 0,\ 2^{0+1} - 1 = 2^1 - 1 = 1$ (Base Case)

Assume $a_k = 2^{k+1} - 1$ for $\mathbb{Z}_{k \geq 0}$

$$a_{k+1} = 2a_k + 1$$

Substitute assumption

$a_k = 2^{k+1} - 1,\ a_{k+1} = 2(2^{k+1} - 1) + 1 = 2^{k+2} - 1$ ■

Thus $a_n = 2^{n+1} - 1$ for $\forall n \geq 0,\ n \in \mathbb{Z}$

(d) $a_0 = 2,\ a_1 = 1,\ a_{n+2} = a_{n+1} + 6a_n$

(Base Case)

$n = 0,\ a_0 = 2,\ a_0 = 3^0 + (-2)^0 = 1 + 1 = 2$

$n = 1,\ a_1 = 1,\ a_1 = 3^1 + (-2)^1 = 3 - 2 = 1$

(Now assume for some integer $k \geq 0$ where $n = k$)

$$a_k = 3^k + (-2)^k$$

$$a_{k+1} = 3^{k+1} + (-2)^{k+1}$$

$$a_{k+2} = a_{k+1} + 6a_k$$

$$a_{k+2} = (3^{k+1} + (-2)^{k+1}) + 6(3^k + (-2)^k)$$

$$= (3^{k+1} + (-2)^{k+1} + 6 \times (3)^k + 6 \times (-2)^k)$$

$$= (3^{k+1} + 6 \cdot 3^k) + ((-2)^{k+1} + 6 \times (-2)^k)$$

$$= [3^{k+1} + 2 \cdot 3^{k+1}] + [(-2)^{k+1} - 3 \cdot (-2)^{k+1}]$$

$$= 3^{k+2} + (-2)^{k+2}$$

Thus $a_n = 3^n + (-2)^n$ for $\mathbb{Z}_{n \geq 0}$. ■

(e) $a_{n+2} = pa_{n+1} + qa_n$

Lets use substitution, but first find roots of $x^2 - px - q = 0$

$r_1^2 - pr_1 - q = 0 \rightarrow r_1^2 = pr_1 + q$

$r_2^2 - pr_2 - q = 0 \rightarrow r_2^2 = pr_1 + q$

$$pa_{n+1} + qa_n = p(\alpha r_1^{n+1} + \beta r_2^{n+1}) + q(\alpha r_1^n + \beta r_2^n)$$

$$= (p\alpha r_1^{n+1} + q\alpha r_1^n) + (p\beta r_2^{n+1} + q\beta r_2^n)$$

$$= \alpha r_1^n (pr_1 + q) + \beta r_2^n (pr_2 + q)$$

$$= \alpha r_1^n (r_1^2) + \beta r_2^n (r_2^2)$$

$$= \alpha r_1^{n+2} + \beta r_2^{n+2} \quad ■$$

Substitution

Proving with Induction

Base Case: $n=0$, $\int_0^\infty x^0 e^{-x} x = \int_0^\infty e^{-x} = -e^{-x}\Big|_0^\infty = -[\lim_{x\to\infty} e^{-x} - e^{(0)}]$

$= -[0-1] = 1 = 0!$

(Now we'll utilize integration by parts to present n+1 case)

$$\int_0^\infty x^{n+1} e^{-x} dx = (n+1)!$$

$$\left[\begin{array}{l} u = x^{n+1} \to du = (n+1)x^n dx \\ dv = e^{-x}dx \to v = -e^{-x} \end{array}\right]$$

$$\underbrace{-x^{n+1}e^{-x}\Big|_0^\infty}_{0} + (n+1)\underbrace{\int_0^\infty x^n e^{-x} dx}_{S_n} \quad \left[\begin{array}{ll} u = x^n & dv = e^{-x}dx \\ du = n x^{n-1}dx & v = -e^{-x} \end{array}\right]$$

$$(n+1)\underbrace{\left[-x^n e^{-x}\right]\Big|_0^\infty}_{0} + n\int_0^\infty x^{n-1} e^{-x} dx$$

$$\underline{S_n} = \underline{n\, S_{n-1}} = n(n-1)S_{n-2}$$

$$\cdots = n!\, S_0 = n!$$

Thus, $\int_0^\infty x^{n+1} e^{-x} dx = (n+1)n!$

$= (n+1)!$ ■

(b) Base Case:

$n=1$, $\cos\theta + i\sin\theta = \cos\theta + i\sin\theta$

(let's assume $n=z$, & use it to find $z+1$)

start $(\cos\theta + i\sin\theta)^z = \cos(z\theta) + i\sin(z\theta)$

$(\cos\theta + i\sin\theta)(\cos\theta + i\sin\theta)^z = \cos(z\theta) + i\sin(z\theta)(\cos\theta + i\sin\theta)$

$$(\cos\theta + i\sin\theta)^{z+1} = (\cos(z\theta)\cos\theta - \sin(z\theta)\sin\theta) + i[\sin(z\theta)\cos\theta + \cos(z\theta)\sin\theta]$$

$$= \underline{\underline{\cos((z+1)\theta) + i\sin((z+1)\theta)}}$$ ■

(using side/diagonal values to Approximate $\sqrt{2}$)

Utilizing $n=1$ to get $n=2$

$s_2 = s_1 + d_1 = 1+1 = 2$

$d_2 = 2s_1 + d_1 = 2(1)+1 = 3$

$(s_2, d_2) = (2,3)$, $\frac{d_2}{s_2} = \frac{3}{2} = \underline{1.5}$

Utilizing $n=2$ to get $n=3$

$s_3 = s_2 + d_2 = 2+3 = 5$

$d_3 = 2s_2 + d_2 = 2(2)+3 = 4+3 = 7$

$(s_3, d_3) = (5,7)$, $\frac{d_3}{s_3} = \frac{7}{5} = \underline{1.4}$

- utilizing $n=3$ to get $n=4$

$s_4 = s_3 + d_3 = 5+7 = 12$

$d_4 = 2s_3 + d_3 = 2(5)+7 = 10+7 = 17$

$(s_4, d_4) = (12,17)$, $\frac{d_4}{s_4} = \frac{17}{12} \approx \underline{1.417}$

(b) presenting $d_n^2 - 2s_n^2$ data

$n=1$, $d_1^2 - 2s_1^2 = 1^2 - 2(1^2) = 1-2 = -1$

$n=2$, $d_2^2 - 2s_2^2 = 3^2 - 2(2^2) = 9-8 = 1$

$n=3$, $d_3^2 - 2s_3^2 = 7^2 - 2(5^2) = 49-50 = -1$

$n=4$, $d_4^2 - 2s_4 = 17^2 - 2(12^2) = 289 - 2(144) = 289-288 = 1$

((conjecture) $d_n^2 - 2s_n^2 = (-1)^n$

Now let's prove it

(Base Case): $n=1$, $d_1^2 - 2s_1^2 = 1^2 - 2(1^2) = -1$

Assume $d_k^2 - 2s_k^2 = (-1)^k$ with $\mathbb{Z}\ k \geq 1$

$d_{k+1}^2 - 2s_{k+1}^2 = (2s_k + d_k)^2 - 2(s_k + d_k)^2$

$= (4s_k^2 + 4s_k d_k + d_k^2) - 2(s_k^2 + 2s_k d_k + d_k^2) = (4s_k^2 - 2s_k^2) + (4s_k d_k - 4s_k d_k) \ (d_k^2 - 2d_k^2 \ldots$

$= 2s_k^2 - d_k^2$

$= -(d_k^2 - 2s_k^2)$

$= -(\underbrace{(-1)^k}_{\text{substitute}})$

$= (-1)^1 \cdot (-1)^k = (-1)^{k+1}$

$\blacksquare$

(c) let's explain with calculus

$\lim_{n\to\infty} \frac{d_n}{s_n} = \sqrt{2}$

$\frac{d_n^2}{s_n^2} - \frac{2s_n^2}{s_n^2} = \frac{(-1)^n}{s_n^2}$

$\left(\frac{d_n}{s_n}\right)^2 - 2 = \frac{(-1)^n}{s_n^2}$

$\left(\frac{d_n}{s_n}\right)^2 = 2 + \left(\frac{(-1)^n}{s_n^2}\right)$

$\lim_{n\to\infty} \left(\frac{d_n}{s_n}\right)^2 = 2 + \lim_{n\to\infty} \left(\frac{(-1)^n}{s_n^2}\right)$

(let's identify $\lim_{n\to\infty} \frac{d_n}{s_n}$ as our limit L)

$L^2 = 2+0$

$L^2 = 2$

$L = \pm\sqrt{2}$

thus, $\lim_{n\to\infty} \frac{d_n}{s_n} = \sqrt{2}$

$\blacksquare$

Base Case:

$n=0,\ (1+x)^0 = \sum_{i=0}^{0} \binom{0}{i} x^i = 1$

Assume $n=j$ & find $j+1$

$(1+x)^j = \sum_{i=0}^{j} \binom{j}{i} x^i$

$(1+x)^{j+1} = (1+x)(1+x)^j = (1+x)\sum_{i=0}^{j} \binom{j}{i} x^i$

Distributed: $\sum_{i=0}^{j} \binom{j}{i} x^i + \sum_{i=0}^{j} \binom{j}{i} x^{i+1}$

$= \sum_{i=0}^{j} \binom{j}{i} x^i + \sum_{h=1}^{j+1} \binom{j}{h-1} x^h$

$= \binom{j}{0} + \sum_{i=1}^{j} \left[\binom{j}{i} + \binom{j}{i-1}\right] x^i + \binom{j}{j} x^{j+1}$

Now Pascal's identity

$\binom{j}{i} + \binom{j}{i-1} = \binom{j+1}{i}$

Thus, $(1+x)^{k+1} = \sum_{i=0}^{j+1} \binom{j+1}{i} x^i$ ■

(D)

Base Case:

$n=0,\ 2^0 = 1$, shows the empty set contains 1 subset.

let's assume $n=j$ & a set with j elements has 2^j subsets.

Now let's look at it with a $j+1$ constraint.

with this constraint set $A' = A \cup b$, b being an element

Thus A' is in either $\underset{2^j}{\underset{\uparrow}{b}}$ or $\underset{2^j}{\underset{\uparrow}{\overline{b}}}$ (# of subsets)

Therefore, $2^j + 2^j = 2^{j+1}$ ■

predicated from

$|A \cup B| = |A| + |B| - |A \cap B| = 2^j + 2^j - 0 =$

(b) Data Collection

let n = A set of ascending + integers ($\mathbb{Z}$) cubed & summed (starting at 1).

let CIS = cubed - Integer series shown. $\sum_{i=1}^{n}\left(\frac{i(i+1)}{2}\right)^2$

let S = Summation (series) result (output).

n	CIS	S
1	1^3	1
2	1^3+2^3	9
3	$1^3+2^3+3^3$	36
4	$1^3+2^3+3^3+4^3$	100
5	$1^3+2^3+3^3+4^3+5^3$	225
6	$1^3+2^3+3^3+4^3+5^3+6^3$	441

(c) Condensed Answer (quantified)

$$\forall n \in \mathbb{Z}^+, \left(S_n = \sum_{i=1}^{n} i^3\right) \Rightarrow \left(S_n = \left(\frac{n(n+1)}{2}\right)^2\right)$$

(b) Conjecture

This $\left[\sum_{i=1}^{n}(i)^3\right]$ is the sum of ($S_n = 1^3+2^3+\ldots+n^3$) cubes algoritmn when $n \in \mathbb{Z}^+$, & it can be quickly evaluated via $\left(\frac{n(n+1)}{2}\right)^2$

(c) If a summation follows $\left[\sum_{i=1}^{n}(i)^3\right]$ when $n \in \mathbb{Z}^+$ then it can be computed via $S_n = \left(\frac{n(n+1)}{2}\right)^2$, which is the sum of cubes algorithm

(d)

Step 1 Base Case: $n=1$ $\quad S_1 = \left(\frac{1*(1+1)}{2}\right)^2 = 1$

Step 2 Now let's assume we want S_n:

$$S_n = 1^3 + 2^3 + \cdots + n^3 = \left(\frac{n(n+1)}{2}\right)^2$$

Step 3 Now let's assume we wan S_{n+1}:

$$S_{n+1} = S_n + (n+1)^3 = \left(\frac{n(n+1)}{2}\right)^2 + (n+1)^3$$

Step 3 continued

$$S_n = \frac{n^2(n+1)^2}{4} + (n+1)^3$$

$$= \frac{n^2(n+1)^2}{4} + \frac{4(n+1)^3}{4}$$

added together & factored out $(n+1)^2$

$$= \frac{(n+1)^2(n^2+4(n+1))}{4}$$

$$= \frac{(n+1)^2(n^2+4n+4)}{4}$$

$$= \frac{(n+1)^2(n+2)^2}{4}$$

$$= \left(\frac{(n+1)(n+2)}{2}\right)^2$$

This proves the formula to be the Sum of cubes by induction $S_n = \left(\frac{n(n+1)}{2}\right)^2$ when

(a) Data Collection

($\mathbb{Z}^+$)

(n): A set of ascending odd + integers chosen, starting from 1.

(OIS): odd finite integer [sequence summation] (series). $\left(\sum_{i=1}^{n}(2i-1)\right)$

(S): Summation Result (output)

n	OIS	(S)
1	1	1
2	1+3	4
3	1+3+5	9
4	1+3+5+7	16
5	1+3+5+7+9	25
6	1+3+5+7+9+11	36

(c) Condensed Answer (quantified)

$\forall n \in \mathbb{Z}^+, \left(S_n = \sum_{i=1}^{n}(2i-1)\right) \Rightarrow (S_n = n^2)$

(b) Assuming you are summing a set of n odd positive integers starting from 1, i.e. (1+3+5+...+), its sum is equal to n^2.

(c) If this algorithm $\left(\sum_{i=1}^{n}(2i-1)\right)$ is produced for a series (indexed with $i=1$ being the first odd number) then its summation can be quickly computed with (n^2), which is the sum of odd numbers algorithm.

(d) Base case $n=1$

$$S_1 = 1 = 1^2$$

Now let's assume we want S_n,

$$S_n = 1+3+5+7+\dots(2n-1) = n^2$$

Now let's assume we want S_{n+1}

$n+1$

$$S_{n+1} = S_n + S_{n+1}$$

$$S_{n+1} = n^2 + (2(n+1)-1) = n^2 + (2n+1) = n^2 + 2n + 1 = (n+1)^2$$

Thus, by mathematical induction $S_n = n^2$ when $n \geq 1$, which is the sum of odd numbers algorithm. ∎

(c) $a_0 = 1$, $a_{n+1} = 2a_n + 1$. Prove: $a_n = 2^{n+1} - 1$,

(d) $a_0 = 2$, $a_1 = 1$, $a_{n+2} = a_{n+1} + 6a_n$. Prove: $a_n = 3^n + (-2)^n$.

(e) Suppose $a_{n+2} = pa_{n+1} + qa_n$, where p, q are constants, and a_1, a_0 are given values. Prove by induction: $a_n = \alpha r_1^n + \beta r_2^n$, where r_1, r_2 are the solutions to $x^2 - px + q = 0$.

5. The "side and diagonal" numbers provide a recursive approach to approximating $\sqrt{2}$. They are defined as follows: $s_1 = 1, d_1 = 1$. Then

$$s_{n+1} = s_n + d_n$$
$$d_{n+1} = 2s_n + d_n$$

and give the approximation $\sqrt{2} \approx \dfrac{d_n}{s_n}$.

(a) Find the next three pairs of side and diagonal numbers (in other words, find (s_2, d_2), (s_3, d_3), and (s_4, d_4).

(b) Make a conjecture about the value of $d_n^2 - 2s_n^2$, then prove it by induction.

(c) Using calculus, explain why $\lim_{n\to\infty} \dfrac{d_n}{s_n} = \sqrt{2}$. Hint: How can you determine that $\dfrac{d_n}{s_n} \approx \sqrt{2}$ without knowing the value of $\sqrt{2}$?

Christian Barden

20/30

Induction Proofs

1. We'll find and prove a formula for the sum of the first k odd numbers. **NOTE**: To get the most out of this problem, ignore anything you already know about this sum.

   (a) Collect data. (In other words, find the sum of the first two odd numbers; the first three; the first four; and so on)

   (b) Make a conjecture: "The sum of the first k odd numbers is ..."

   (c) Restate your conjecture in a provable form.

   (d) Prove your conjecture by induction.

2. We'll find and prove a formula for the sum of the cubes of the first k whole numbers. **NOTE**: To get the most out of this problem, ignore anything you already know about this sum.

   (a) Collect data.

   (b) Make a conjecture: "The sum of the cubes of the first k odd numbers is ..."

   (c) Restate your conjecture in a provable form.

   (d) Prove your conjecture by induction.

3. Prove using induction.

   (a) $\int_0^\infty x^n e^{-x}\, dx = n!$ for all $n \in \mathbb{N}$.

   (b) $(\cos\theta + i\sin\theta)^n = \cos n\theta + i\sin n\theta$ for all $n \in \mathbb{N}$, where $i = \sqrt{-1}$.

   (c) $(1+x)^n = \sum_{i=0}^{n} \binom{n}{i} x^i$.

   (d) Let S be a set with n elements. The number of distinct subsets of S is 2^n.

4. In the following, a recursive sequence is defined. Prove corect the given closed form expression for the nth term of the sequence.

   (a) $a_0 = 1$, $a_{n+1} = 3a_n$. Prove: $a_n = 3^n$

   (b) $a_0 = 1$, $a_{n+1} = a_n + 3$. Prove: $a_n = 1 + 3n$

(c) D^* is countable

The set of all describable numbers D^* is the union of descriptions of length n:

$$D^* = \bigcup_{n=1}^{\infty} D_n$$

The countable union of finite sets is countable.

$$\forall n \in \mathbb{N}, |D_n| < \infty \Rightarrow \left|\bigcup_{n=1}^{\infty} D_n\right| = \aleph_0$$

(d) Let T be the set of provable theorems.

A theorem is a finite string of symbols from a finite alphabet Σ.

The set of all finite strings is $\Sigma^k = \bigcup_{n=0}^{\infty} \Sigma^n$

From (c), $|\Sigma^*| = \aleph_0$

Since $T \subseteq \Sigma^*$, $\exists$ any subset of countable set is countable:

$$T \subseteq \Sigma^* \Rightarrow |T| \leq \aleph_0$$

3) (a) A quadratic surd x is a root of $ax^2 + bx + c = 0$ where $a, b, c \in \mathbb{Z}$, $a \neq 0$

Let S be the set of quadratic surds. Define a mapping

f: $f: \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \to$ polynomials

The cardinality of $\mathbb{Z}^3$ is $\aleph_0$ (since finite Cartesian product of countable sets is countable). So each polynomial has 2 roots

$|S| \leq 2 \cdot |\mathbb{Z}^3| = 2 \cdot \aleph_0 = \aleph_0$

Hence, is countable.

-continued on back of page. →

1) (a)

Assuming standard English naming for natural numbers:

1.) Eight

2.) Eighteen

3.) Eighty

(b)

Using Equivalence classes, let $\mathcal{L}$ be the set of all descriptions. We define a relation $\sim$ on $\mathcal{L}$ such that

$x \sim y \leftrightarrow \text{value}(x) = \text{value}(y)$. The set of unique mathematical objects is the quotient set $\mathcal{L}/\sim$.

(c)

Let $\mathcal{L}$ be the ordered list of descriptions.

Let $S_e = \{w \in D \mid w \text{ starts with 'e'}\}$. Since natural numbers are infinite, $|S_e| = \infty$ (e.g., eight, eighteen, ...). This is because 'f' comes after 'e', the index of 'five' would be $> |S_e|$. Since $|S_e|$ is infinite, "five" is never reached.

2) (a)

$$D_1 = \{d \in D^* \mid \text{length}(d) = 1\}$$

(b)

Let Σ be the finite alphabet of allowed symbols (letters, spaces, punctuation). Let $k = |\Sigma|$. The set of all strings length n is Σ^n.

$|D_n| \subseteq \Sigma^n \Rightarrow |D_n| \leq |\Sigma^n| = k^n$

Since k & n are finite, k^n is finite.

Thus, D_n is finite.

3. A **quadratic surd** is an irrational number that is the solution to a quadratic equation with integer coefficients. **Note:** In the following, it might be useful to consider quadratic surds as a subset of the numbers that are real solutions to quadratic equatioen with integer coefficients.

   (a) Prove: The number of quadratic surds is countably infinite.

   (b) Find a different proof. Suggestion: "If you're not using a definition, you're probabably not doing a proof." But there are different ways you could use the definition of a quadratic surd.

Christian G. Barden

Cardinality

1. Let $\mathcal{D}$ be the set of "describable numbers," which we define as any number that can be described in words. For example, 73 is describable, since we can write "seventy-three." Likewise, $\sqrt{17}$ is describable: "the square root of seventeen." We'll also allow series definitions: for example, since

$$\pi = \sum_{n=0}^{\infty} \frac{4(-1)^n}{2n+1}$$

then we can describe π as the sum of a series of terms with a particular form.

   (a) Since the elements of $\mathcal{D}$ are words, we can imagine putting them in alphabetical order. If you do that, what are the first three describable numbers? (If it makes it easier, focus on the natural numbers that can be written in words)

   (b) How could you account for the possibility that some numbers could be described in different ways? (In particular: What *mathematical* tool can we use to deal with the problem of multiple representations?)

   (c) Why can't we use the alphabetized list to prove the describable numbers are countable? Suggestion: Where is "five" on the alphabetical list?

2. Let $\mathcal{D}$ be the set of describable numbers, where $x \in \mathcal{D}$ is the shortest (by letter count) unambiguous definition of a number.[1] For example, while we could describe π as the sum of a series, we can also describe it as "pi" (the spelled out letter).

   (a) Let $\mathcal{D}$ be partitioned into subsets D_n, where D_n consists of the descriptions with n letters. What are the elements of D_1?

   (b) Prove: D_n is finite for all n.

   (c) Prove: The set of describable numbers is countably infinite.

   (d) Prove: The set of provable theorems is countably infinite.

[1] Interested students might look up "Berry's paradox." To avoid Berry's paradox, we disallow such definitions.

prove × is well-defined
Assume $(u,v) \sim (u',v')$ so
$u + v' = u' + v$.

$up + pv' = u'p + pv$ - multiply L/R by p

$uq + qv' = u'q + qv$ - multiply L/R by q

$up + pv' + uq + qv' = u'p + pv + u'q + qv$

rearrange by commutativity/associativity:

$(up + vq') + (uq + pv') = (u'p + vq) + (u'q + pv)$

Thus changing (u,v) to an equivalent pair does not change the class of the product. So multiplication is well defined.

5b) Show $[(u,v)] \times [(q,q)] = [(q,q)]$

$[(u,v)] \times [(q,q)] = [(uq + vq, vq + qv)]$

$[(q(u+v), q(u+v))]$

$[(u,v)] \times [(q,q)] = [(q,q)]$

5c) Show commutativity:

$[(u,v)] \times [(p,q)] = [(p,q)] \times [(u,v)]$

left side

$[(u,v)] \times [(p,q)] = [(up + vq, vq + pv)]$

right side

$[(p,q)] \times [(u,v)] = [(pu + qv, pv + qu)]$

By commutativity of multiplication

$up = pu,\ vq = qv,\ vq = qu,\ pv = vq$

So multiplication on classes is commutative.

5d) Distributivity

LHS: Left hand side

RHS: Right hand side

$[(u,v)] \times ([(p,q)] + [(r,s)]) = [(u,v)] \times [(p,q)] + [(u,v)] \times [(r,s)]$

$[(p,q)] + [(r,s)] = [(p+r, q+s)]$

Multiply $[(u,v)]$

$[(u,v)] \times [(p+r, q+s)] = [u(p+r) + v(q+s), u(q+s) + v(p+r)]$

first coordinate

$u(p+r) + v(q+s) = up + ur + vq + vs$

Second coordinate

$u(q+s) + v(p+r) = uq + us + vp + vr$

LHS class: $[(up + ur + vq + vs, uq + us + vp + vr)]$

RHS class: $[(u,v)] \times [(p,q)] = [(up + vq, uq + pv)]$

$[(u,v)] \times [(r,s)] = [(ur + vs, us + vr)]$

Add classes: $[(up + vq, uq + pv)] + [(ur + vs, us + vr)]$

$= [(up + ur + vq + vs, uq + us + vp + vr)]$

associativity/commutativity applied; it follows LHS so distributivity holds.

5e) let $[(u,v)]$ & $[(r,s)]$ be two guazzits

by def:

$[(u,v)]$ is a guazzit, so $u > v$.

$[(r,s)]$ is a guazzit, so $r > s$.

If we examine $(u-v)(r-s)$, $r - s > 0$, $u - v > 0$.

so $(u-v)(r-s) > 0$

expanding

$ur - us - vr + vs > 0$

thus $\boxed{ur + us > us + ur}$

resulting in equivalence class $[(ur + vs, us + vr)]$ is guazzit

But this is what you're proving

5f) let $[(u,v)]$ be a guazzit & $[(r,s)]$ be a glerby by def: $[(r,s)]$ is a glerby, so $u > v$

$[(u,v)]$ is a guazzit, so $r < s$

if we examine $(u-v)(r-s)$

$(u-v)(r-s) < 0$

Expand the left side

$ur - us - vr + vs < 0$

resulting in equivalence class glerby $[(ur + vs, us + vr)]$

rearrangement gives: $ur + us < us + ur$

5) Let $[(u,v)]$ & $[(r,s)]$ be two glerbys.
By def: $[(u,v)]$ is a glerby, so $u<v$.
$[(r,s)]$ is a glerby, so $r<s$.
First let's examine $(u-v)(r-s)$:
the product of 2 negatives give
$(u-v)(r-s)>0$ ($u<v$ & $r<s$) ← as well as this condition of class components.
Expanding the LHS gives $ur-us-vr+vs>0$, rearragment gives $ur+vs>us+vr$

$[(ur+vs, us+vr)]$ is a gua??it. since $ur+vs>us+vr$ class

6) What properties did we prove in problems 4 & 5?

Problem 4 Proven Properties

- Addition is well defined on integers.
- Addition is commutative & associative.
- every integer has an additive inverse.

Problem 5 Proven Properties

- Multiplication is well defined.
- Multiplication is commutative & associative.
- Multiplication distributes over addition.

The definition that corresponds to $(a,b)+(c,d)$ is:

$(a,b)+(c,d) \Rightarrow (a+c, b+d)$

2c) Assuming $w = xy$ an equation that satisfies $w+r=s$ would be:

$w + (ad+bc) = ac + bd$

2d) The definition that corresponds to $(a,b) \times (c,d)$:

$(a,b) \times (c,d) = (ad+bc, ac+bd)$

3a) (prove $\sim$ is an equivalence relation)

Reflexive

for $\forall (u,v)$,

$u+v = u+v$,

So $(u,v) \sim (u,v)$

Symmetry

If $(u,v) \sim (r,s)$, then $u+s = r+v$.

But, the same equality states $r+v = u+s$, so $(r,s) \sim (u,v)$

Transitive

Assume

$(u,v) \sim (r,s)$ & $(r,s) \sim (p,q)$

$u+s = r+v$, $r+q = p+s$

$u+s+q = r+v+q$

$r+q+v = p+s+v$

By associativity & commutativity

$u+s+q = u+q+s$, $r+v+q = r+q+v$,

$p+s+v = p+v+s$

thus, $u+q+s = r+q+v = p+v+s$

Now cancel s from both sides

$u+q = p+v$

Therefore $(u,v) \sim (p,q)$

(3b) Show $(x,y) \sim (x+z, y+z)$ for all $z \in \mathbb{N}$

$x + (y+z) = (x+z)+y$

$x+(y+z) = (x+y)+z = x+y+z$,

$(x+z)+y = x+z+y = x+y+z$

Since the two sides are equal

$(x,y) \sim (x+z, y+z)$ ∎

(4a) If $(u,v) \sim (u',v')$, prove $[[(u,v)]] = [[(u',v')]]$

by def

$[[(u,v)]] = \{(a,b) \in \mathbb{Z} : (a,b) \sim (u,v)\}$

& similarly for $[[(u',v')]]$

Assume $(u,v) \sim (u',v')$

If $(a,b) \in [[(u,v)]]$, then $(a,b) \sim (u,v)$.

Since $(u,v) \sim (u',v')$, transitivity gives $(a,b) \in [[(u',v')]]$.

Conversely if $(a,b) \in [[(u',v')]]$, then $(a,b) \sim (u',v')$.

By symmetry, $(u',v') \sim (u,v)$, & by transitivity $(a,b) \sim (u,v)$, so $(a,b) \in [[(u,v)]]$.

So the two classes contain the same pairs & are $=$. $[[(u,v)]] = [[(u',v')]]$

1e) $-3 + p = q$

$x + 3 = 0$
$x + 4 = 1$
$x + 5 = 2$

The three possible values are: $(3,0), (4,1), (5,2)$

(p is perpetually 3 more than q)

1a) we want a natural number x with $x+3=5$.

$2+3=5$, so $x=2$.

1b) There is no natural to identify with the operation of $x+5=3$, & the only logical value for said identity is $x=-2$

1c) $6+p=q$

$6+0=6 \rightarrow (0,6)$
$6+1=7 \rightarrow (1,7)$
$6+2=8 \rightarrow (2,8)$

The three pairs are $(0,6),(1,7),(2,8)$

1f) let's test $(3,0)$ & $(4,1)$

$0+4=4$, $1+3=4$

since $0+4=1+3$, our test says they give the same value. Same applies for

$(3,0)$ & $(5,2)$

$(0+5=5)$, $(2+3=5)$

$(0+5=2+3)$, true

1d) suppose we have 2 individual pairs of (p,q)

(p_1,q_1) (p_2,q_2)

$x+p_1=q_1$ $x+p_2=q_2$

we want to know when they equal the exact value

The solutions usually take the form $(q_1-p_1),(q_2-p_2)$

if we assume solutions to be equal then

$q_1+p_2=q_2+p_1$, which would result in a reflexive value for both sides.

2(a)

Given

$x+a=b$, $y+c=d$, $z=x+y$

(write an equation in form $z+p=q$.)

$x+a=b$, $y+c=d$

$(x+y)+(a+c)=b+d$

Since $z=x+y$, this gives

$\boxed{z+(a+c)=b+d}$

(c) Prove: $[(u,v)] + [(q,q)] = [(u,v)]$ for all $q \in \mathbb{N}$. Note: Don't use induction. (You can if you really want to, but that's cracking a walnut with a sledgehammer)

(d) Prove: $[(u,v)]+[(v,u)] = [(q,q)]$ for all $u, v, q \in \mathbb{N}$. (Again: Don't use induction!)

(e) Prove: $[(u,v)] + [(r,s)] = [(r,s)] + [(u,v)]$. Remember you can **ONLY** assume the properties of arithmetic of $\mathbb{N}$ and the preceding definitions.

(f) Prove: $([(u,v)] + [(p,q)]) + [(r,s)] = [(u,v)] + ([(p,q)] + [(r,s)])$.

5. Again, assuming only the properties of the arithmetic of the natural numbers, we define

$$[(u,v)] \times [(p,q)] = [(up + vq, uq + pv)]$$

(a) Prove: $\times$ is well-defined. (In other words, you get the same equivalence class regardless of which class representative you use)

(b) Prove: $[(u,v)] \times [(q,q)] = [(q,q)]$.

(c) Prove: $[(u,v)] \times [(p,q)] = [(p,q)] \times [(u,v)]$.

(d) Prove: $[(u,v)]([(p,q)]+[(r,s)]) = [(u,v)]\times[(p,q)]+[(u,v)]\times[(r,s)]$.

(e) We'll say $[(u,v)]$ is a quazzit if $u > v$, and a glerby if $u < v$. Prove: The product of two quazzits is quazzit.

(f) Prove: The product of a quazzit and a glerby is a glerby. Note: You can use the result of Problem 5c.

(g) Prove: The product of two glerbys is a quazzit.

6. (The punchline): We identify the equivalence class $[(u,v)]$ with the integer $u-v$. What properties of the integers did you prove in Problems 4 and 5?

(c) For a function mapping a finite set A to itself ($|A| = |A| = n$), a function is onto if & only if it is one to one.

since the set of onto functions is identical to the set of one-to-one functions in this specific context, the count is the same.

So there are $n!$ onto functions.

(d) Assume f is one-to-one. The image of f contains n distinct elements (since inputs are distinct). Since the codomain A has exactly n elements, the image must cover the entire codomain. Thus, f is onto.

Assume f is onto. The image of f is A, so the image has size n. If f were not one-to-one, at least two inputs would map to the same output. This would suggest that the image size is at max $n-1$. (pigeonhole principle). This contradicts that the image size is n. Therefore, f must be one to one.

In conclusion, since onto implies one to one for finite sets $A \to A$, the counting of onto functions is the same as counting permutations of A. So there are $n!$ onto functions.

3) (a) let $|A| = n$ & $|B| = m$, where $n > m$

- Suppose that $f: A \to B$ is one to one.
- If f is one-to-one, then f maps n distinct elements of A to n distinct elements in B.
- This implies that the codomain B must contain at least n elements.
- However, we know B has m elements & $m < n$.
- it is impossible to fit n distinct objects into m slots where $n > m$.

2 elements in A must map to the same B element, thus f isn't one to one

(b) - let $|A| = n$ & $|B| = m$, where $m > n$.

- The function g maps the n elements of A to elements in B.
- The image of g (the set of outputs) can have at most n elements (one output for each input).
- Since the size of the image is $\leq n$ & $|B| = m > n$, the image cannot all of B. There will be at least $m-n$ elements in B (unmapped).
- Thus, g cannot be onto.

- continued on

Christian Bardey

18/23

Equivalence Relations and Equivalence Classes: The Integers

In the following, you may assume all the usual properties of arithmetic of the natural numbers; you may NOT assume they extend to any other sets (so $a + b = b + a$ *provided* you are willing to guarantee, \$20 on the table, that a, b are natural numbers).

1. One way to define a number is to identify it with an equation it solves. Remember that the arithmetic of the natural numbers does NOT allow subtraction, only addition and multiplication.

   (a) What number do you identify with $x + 3 = 5$?

   (b) What number do you identify with $x + 5 = 3$?

   (c) Find three ordered pairs (p, q), with $p, q \in \mathbf{N}$, where the equation $x + p = q$ is identified with the number 6.

   (d) Suppose (p_1, q_1), (p_2, q_2) are two of the ordered pairs you've identified with the number 6. What "test" could you apply to p_1, p_2, q_1, q_2 that would tell you the ordered pairs correspond to the same number? (Remember: You only "know" the properties of arithmetic of the natural numbers, so you can't subtract or divide, and you can't introduce negative numbers!)

   (e) Find three ordered pairs (p, q), with $p, q \in \mathbf{N}$, where the equation $x + p = q$ is identified with the number -3.

   (f) Does the test you proposed in Problem 1d work for the pairs you found in 1e? In other words: The pairs you found should correspond to the same number; does your proposed test lead to that conclusion?

2. Now that we've associated each equation of the form $x + p = q$ with a number, let's introduce some arithmetic.

   (a) Consider the equations

$$x + a = b$$
$$y + c = d$$

   Let $z = x + y$. Write an equation of the form $z + p = q$.

(b) Remember we associate the equation $x + a = b$ with the ordered pair (a, b). What does the preceding suggest about how to define

$$(a, b) + (c, d)$$

NOTE: This isn't about proving things; it's about figuring what *to* prove. In particular: Do what you'd *like* to do, and don't worry about whether it's (logically) allowed: that comes later.

(c) Let $w = xy$. Write an equation of the form $w + r = s$ (based on the equations for x, y given above). **NOTE**: While, at this stage, you can do anything, the other problems will be easier if your final answer is based only on things you could do using $+$ and $\times$ of the natural numbers.

(d) What does the preceding suggest about how to define

$$(a, b) \times (c, d)$$

3. Let $Z = \{(x, y) : x, y \in \mathbb{N}\}$, and define the following:

$$(u, v) \sim (r, s) \text{ if and only if } u + s = r + v$$

(Use this definition for the remaining problems)

(a) Prove: $\sim$ is an equivalence relation.

(b) Prove: $(x, y) \sim (x + z, y + z)$ for all $z \in \mathbb{N}$.

4. Since $\sim$ is an equivalence relation, it induces a set of equivalence classes $[(x, y)]$ (where $x, y \in \mathbb{N}$). Define

$$[(u, v)] + [(r, s)] = [(u + r, v + s)]$$

(a) Suppose $(u, v) \sim (u', v')$. Prove: $[(u, v)] = [(u', v')]$.

(b) In this context, we say an operation is well defined if it gives the same results regardless of which class representative we use. Prove: If $[(u, v)] = [(u', v')]$, then

$$[(u, v)] + [(r, s)] = [(u', v')] + [(r, s)]$$

1.) Prove, or find a counterexample.

(a) If f, g are both one to one, then $f \circ g$ is also one-to-one.

Step 1 - Let's assume $(f \circ g)(x) = (f \circ g)(y)$
by definition of composition this means
$f(g(x)) = f(g(y))$.

Step 2 - Now let's apply f is 1-1; which means inputs with the same output must be equal (=). So, $g(x) = g(y)$.

Step 3 - Now let's apply g is 1-1; which means $g(x) = g(y)$, so it's implied that $x = y$.

Step 4 - As a result, $(f \circ g)(x) = (f \circ g)(y) \Rightarrow x = y$
& $f \circ g$ is one to one. ∎

(b) If f, g are both onto, then $f \circ g$ is also onto.

Note: let $g: A \to B$ & $f: B \to C$. Then $f \circ g: A \to C$.

(For function f) Step 1 Let z be any element in C. Since f is onto, then there exists some $y \in B$ such that $f(y) = z$.

(For function g) Step 2 Now let $y \in B$. Since g is onto, there exists some $x \in A$ such that $g(x) = y$.

Step 3 - Then substitute $y = g(x)$ into the first equation to produce: $f(g(x)) = z$

Step 4 - Therefore, we discovered an x for which $(f \circ g)(x) = z$.
So, $f \circ g$ is onto. ∎

- Continued on backside

(c) If $f \circ g$ is one-to-one, then f, g must both be one to one.

Concrete Counterexample

let $A = \{1\}, B = \{1,2\}, C = \{1\}$.

let's introduce function g such that $A \to C$ via $g(1) = 1$. (is 1 to 1)

Then introduce another function f such that $B \to C$ via $f(1) = 1$, & $f(2) = 1$. (Not 1 to 1)

Under composition, $(f \circ g)(1) = f(g(1)) = f(1) = 1$.

So the function $f \circ g$ maps $\{1\} \to \{1\}$, which is one to one.

✓ Our result is that $f \circ g$ is 1 to 1, however f is not. Thus, they don't both have to be one to one. So the statement is false. ∎

(d) If $f \circ g$ is onto, then f, g must both be onto. Another Concrete Counterexample

let $A = \{1,2\}, B = \{1,2,3\}, C = \{1,2\}$.

let's introduce function g such that $A \to B$ via $g(1) = 1, g(2) = 2$. (is not onto, & is missing 3)

Then introduce another function g such that $B \to C$ via $f(1) = 1, f(2) = 2, f(3) = 1$. (This is onto)

Under Composition $(f \circ g)$, $(f \circ g)(1) = f(1) = 1$

$(f \circ g)(2) = f(2) = 2$

✓ So the image of $f \circ g$ is $\{1,2\}$, which is equal to C. Thus, $f \circ g$ is onto, but not g. This means $f \circ g$ & f, g don't both have to be onto. Therefore our original statement is invalid. ∎

2.) (a) Prove: How many distinct function f are there? ($f: A \to A$, A has n elements)

let's assume the elements of domain A are $a_1, a_2, \ldots, a_n$.

For a_1, there are n possible choices in the codomain A.

It follows that a_2 has n possible choices. Now we multiply the choices for all n elements.

The choices are: $n \times n \times \ldots \times n$ (via method of counting)

Thus there are n^n distinct functions. ∎ ✓

(b) The first element a_1 has n choices. The second element a_2 has $n-1$ choices. For a_3, $n-2$ choices. (By method of counting)

Continuing the pattern: $n \times (n-1) \times n- \quad \times \ldots \times$

∎ (So, there are $n!$ one to one functions.)

- Continued on next pg

(c) For a function

Christian 9 Barden

20/20

Functions

We will (or have) introduced a more formal concept of the cardinality of a set, but for the following, treat things like "number of elements" or "one set has more elements than the other" in a set as a primitive concept that acts the way you think it should act. (But ... pigeons).

1. Prove, or find a counterexample.

   (a) If f, g are both one-to-one, then $f \circ g$ is also one-to-one.

   (b) If f, g are both onto, then $f \circ g$ is also onto.

   (c) If $f \circ g$ is one-to-one, then f, g must both be one-to-one.

   (d) If $f \circ g$ is onto, then f, g must both be onto.

2. Consider $f : A \to A$, and suppose A is a finite set with n elements.

   (a) How many distinct functions f are there? Prove it.

   (b) How many one-to-one functions f are there? Prove it.

   (c) How many onto functions f are there? Prove it.

   (d) Find a second proof for the number of onto functions. Suggestion: Any time two things are equal, it's worth asking "Is there a relationship?"

3. Suppose A, B are sets with a finite number of elements. (At this point, treat "number of elements" and "more" as a primitive concept)

   (a) Prove: If A has more elements than B, $f : A \to B$ **CANNOT** be one-to-one.

   (b) Prove: If B has more elements than A, $g : A \to B$ **CANNOT** be onto.

   (c) Suppose $h : A \to B$ is one-to-one and onto. What do you know about h? Prove it.

4. Suppose $f : A \to A$, where A has a finite number of elements. Suppose that f^{-1} is an inverse function for f.

   (a) Suppose f is onto. Prove: f^{-1} is onto.

   (b) Suppose f is *NOT* one-to-one. Prove: f^{-1} is *NOT* onto.

4)

Borden

(a) [Examples] → Back side has proofs for A, B, C

16

Proving: Naive factorization algorithm terminates

Assume $\mathbb{Z}_n$ is you divident & $\mathbb{Z}_k$ is your divisor value

✓ Set $n = 30$

* examples are not proofs

(# of divisors) $2 \leq k \leq \sqrt{n}$

upper bound $\approx \sqrt{30} \approx 5$

k	30/k	remainder	divides?	factor
2	15	0	Yes	(2, 15)
3	10	0	Yes	(3, 10)
4	7.5	0	No	// ∅ //
5	6	0	Yes	(5, 6)

as, a result $2 \times 3 \times 5$ are prime factors that produce 30 in a finite procedure.

(b) Proving: Division algorithm terminates

assuming $\mathbb{Z}_{a,b} > 0$, with remainder (r) & quotient (H)

& $a = 22, b = 5, H = 0$

(recur¹) $r \geq b\ (22 \geq 5)$
$r = 22 - 5 = 17,\ H = 1$

(recur²) $r \geq b\ (17 \geq 5)$
$r = 17 - 5 = 12,\ H = 2$

(recur³) $r \geq b\ (12 \geq 5)$
$r = 12 - 5 = 7,\ H = 3$

(recur⁴) $r \geq b\ (7 \geq 5)$
$r = 7 - 5 = 2,\ H = 4$

(recur 5) $r \geq b\ (2 \geq 5)$ Not true

Thus it stops with $H = 4,\ r = 2$

(c) Proving: Euclidean algorithm terminates

assuming $\mathbb{Z}_{a,b} > 0$ (computing $\gcd(\overset{A_0}{30}, \overset{A_1}{21})$)

& $A_0 = 30, A_1 = 21$

(recur¹) $A_1 \neq 0\ (21 \neq 0)$

$(30/21)$ gives $Q_0 = 1$ (quotient), remainder $(r_0) = 9$

Now $A_0 = 21$
$A_1 = 9$

(recur²) $A_1 \neq 0\ (9 \neq 0)$

$21/9$ gives $Q_1 = 2,\ r_1 = 3$

now $A_0 = 9$
$A_1 = 3$

(recur³) $A_1 \neq 0\ (3 \neq 0)$

$9/3$ gives $Q_2 = 3,\ r_2 = 0$

Set $A_0 = 3\ A_1 = 0$

(recur⁴) $A_1 \neq 0\ (0 \neq 0)$, Thus it breaks here

*NO Proof

(d) Proving: Collatz-like algorithm terminate

Assume $\mathbb{Z}_i > 0$

& let $n = 5$ (terminates at $n = 1$)

- If n is even, $n = n/2$
- If n is odd, $n = 3n + 1$

(This is the recurrence) $n = 5$

(n is odd) set $n = 3(5) + 1 = 16$, (n is even) set $n = 16/2 = 8$, (n is even) set $n = 8/2 = 4$, (n is even) set $n = 4/2$, (n is even) set $n = 2/2$ (terminated)

observation → I noticed that there's no definitive proof. Depending on your initial value(n) / functions for (n) it may approach / steer away from a "terminating"

Quantifiers & Definitions

Contrapositive & converse is true to a definition

Definitions can be written as 2 conditionals via converse

$P \to Q$

$Q \to P$

Composite is

$n = ab$, meaning being the product of 2 numbers a, b.

When you negate your quantified statement = becomes $\neq$, & $\exists_x$ switches to $\forall_x$ vice versa.

Know prime numbers are:

2, 3, 5, 7, 11, 13 . . .

Describe Failures of a definition:

Ex:

If you are strong then you are a man.

<u>when does this fail</u>

- When there is a strong child.
- When there is a strong woman.

You quantify your conditional (Definition) with logical notation.

(Quantifiers), (Predicate)

$\forall x, (P(x))$

$\exists x, (P(x))$

Ex: Every even integer is divisible by 2.

$\forall_x \in \mathbb{Z}, (\text{Even}(x) \to 2 \mid x)$

or

$\forall x \in \mathbb{Z} ((\exists k \in \mathbb{Z})(x = 2k) \to 2 \mid x)$

Proofs about Whole Numbers

More Equivalences

$(A \land B) \Rightarrow C \equiv B \Rightarrow (A \Rightarrow C) \equiv A \Rightarrow (B \Rightarrow C) \equiv \neg C \Rightarrow \neg(A \land B)$

$A \Rightarrow (B \lor C) \equiv (A \land \neg B) \Rightarrow C \equiv (A \land \neg C) \Rightarrow B \equiv (\neg B \land \neg C) = \neg A$

Proving divisors

- If b divides c then if a divides b? a must divide c.

  let's assum $b|c$, by def of division there exists
  $m \in \mathbb{Z}$ with, $c = bm$
  by the same def

  $\exists n \in \mathbb{Z}, b = an$

  $c = (an)m = a(nm)$ (substitution)
  ($\mathbb{Z}$ is closed under multiplication)

So $\mathbb{Z} \in m, n$, Now let $i = n * m$

then $c = ai$, by definition of divion this means $a|c$. ∎

Set Definitions

Subset: $A \subseteq B = (\forall x)(x \in A \rightarrow x \in B)$

ersection: $A \cap B = \{x \in U : x \in A \text{ \& } x \in B\}$

Complement: $\bar{B} = \{x \in U : x \notin B\}$

mpty set: $x \in A, x \notin B, A \cap B = \emptyset$

nion: $A \cup B = \{x \in U : x \in A \text{ or } x \in B\}$

quality: $A = B \leftrightarrow A \subseteq B \text{ \& } B \subseteq A$

Difference: $A - B = \{x \in U : x \in A \text{ \& } x \notin B\}$

Cartesian Product: $A \times B = \{(x, y) \in U : x \in A \text{ \& } y \in B\}$

$A = \{1, 2\}$

$B = \{a, b\}$

$A \times B = \{\{1, a\}, \{1, b\}, \{2, a\}, \{2, b\}\}$

U = Universal Set

A = Arbitrary Set 1

B = Arbitrary Set 2

$\Rightarrow (B \vee C) \equiv (A \wedge \neg B \Rightarrow C) \equiv (A \wedge \neg C) \Rightarrow B \equiv (\neg B \wedge \neg C) \Rightarrow \neg A$

Assume $n = 2i$ for some $i \in \mathbb{Z}$

any function in for $2 \cdot$ (integer) is even

$$n^2 = (2i)^2 = (4i^2) = 2(2i^2)$$

produces an integer

Therefore, if you have a square of an even # its even

$\Rightarrow (B \vee C) \equiv (A \wedge \neg B \Rightarrow C) \equiv (A \wedge \neg C) \Rightarrow B \equiv (\neg B \wedge \neg C) \Rightarrow \neg A$

Assume m, n are odd

$m = 2a + 1$, $n = 2b + 1$, a & b is some integer.
any # in this form is odd

$m \times n = (2a+1)(2b+1) = 4ab + 2a + 2b + 1$

factor out 2

$2(ab + a + b) + 1$

thus, $m \times n$ is odd.

Sets

How sets are denoted:

$S = \{x \mid x \text{ is squamish}\}$

$A = \{1, 2, 3\}$

$B = \{1, 2)$

$A - B = \{3\}$

$A + B = \{1, 2, 3\}$

$B \subseteq A$

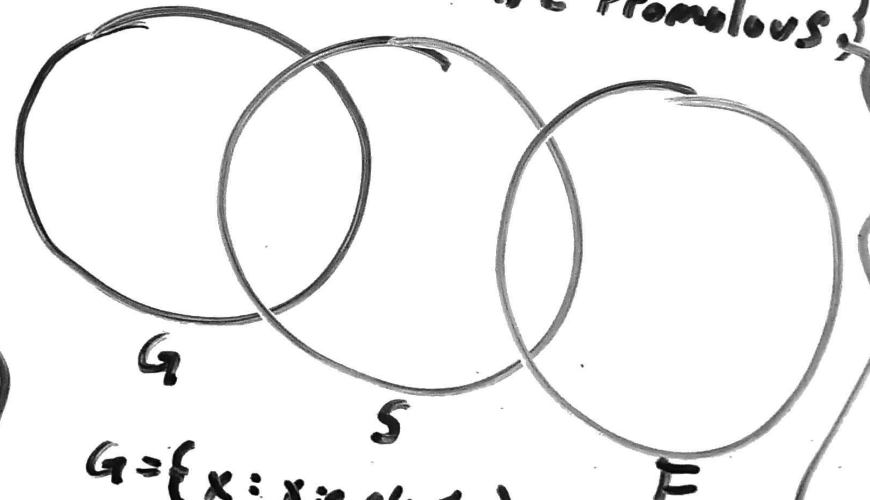
relationships: $\subseteq$, $<$, $=$, $\neq$

subset, proper subset

$A \subseteq B$ & $A \neq B$

graphical representation:

- Some glerby are squamish
- Some squamish are fromolous.



$G = \{x : x \text{ is glerby}\}$

$S = \{y : y \text{ is squamish}\}$

$F = \{z : z \text{ is fromolous}$

logical Equivalence

Different Equivalences

$P \to Q \equiv \neg P \to Q$

$P \to Q \equiv \neg P \vee Q$

$\neg(P \vee Q) \equiv \neg P \wedge \neg Q$

$\neg(P \wedge Q) \equiv \neg P \vee \neg Q$

Compound statements with 3 simple statements

$(A \wedge B) \Rightarrow C \equiv A \Rightarrow (B \Rightarrow C) \equiv (A \Rightarrow C) \vee (B \Rightarrow C)$

$(A \vee B) \Rightarrow C \equiv (A \Rightarrow C) \wedge (B \Rightarrow C)$

If 2 simple statements

A	B
T	T
T	F
F	T
F	F

If 3 simple statements

A	B	C
T	T	T
T	T	F
T	F	T
T	F	F
F	T	T
F	T	F
F	F	T
F	F	F

3 Main Rules

$P \wedge Q$
True if both are True

$P \vee Q$
False when both is false

$P \to Q$
False only when Q is false

Statements

Finding False & True statements.

$6+9=38$, False

$10+10=20$, True

$8\times 8=9$, False

⋮

rewrite statements as conditionals:

• No even # is prime

If your number is even then it's not prime.

Conditional: $P \rightarrow Q$

Converse: $\neg P \rightarrow \neg Q$

Inverse: $Q \rightarrow P$

Contrapositive: $\neg Q \rightarrow \neg P$

P = antecedant

Q = consequent

Types of Compound Statements:

Conjunctions: $P \wedge Q$

Disjunctions: $P \vee Q$

- At least one of the integers... (disjunct)
- 2 is an odd prime # (conjunct)

(a) $A \cap B \subseteq A \cup B$

$(x \in A \,\&\, x \in B) \subseteq (x \in A \text{ or } x \in B)$

union def intersection def

$\exists x \in (x \in A \,\&\, x \in B) \to \exists x \in (x \in A \text{ or } x \in B)$

True

Subset def

∎

(b) $A - B \subseteq A$.

$(x \in A \,\&\, x \notin B) \subseteq A$

$\exists x \in (x \in A \,\&\, x \notin B) \to \exists x \in (x \in A)$

True

∎

(c) $A - B \subseteq \bar{B}$.

$(x \in A \,\&\, x \notin B) \subseteq \bar{B}$

Since $\bar{A} = B$, with $x \notin B$

$\bar{B} = A$, with $x \in B$

$(x \in A \,\&\, x \notin B) \subseteq (x \notin B)$

$\exists x \in (x \in A \,\&\, x \notin B) \to \exists x \in (x \notin B)$

∎

3) $A \to (B \text{ or } C) = A \to (B \vee C) \equiv \neg A \vee (B \vee C)$

A	B	C	$B \vee C$	$A \to (B \vee C)$	$\neg A$	$\neg A \vee (B \vee C)$
T	T	T	T	T	F	T
T	T	F	T	T	F	T
T	F	T	T	T	F	T
T	F	F	F	F	F	F
F	T	T	T	T	T	T
F	T	F	T	T	T	T
F	F	T	T	T	T	T
F	F	F	F	T	T	T

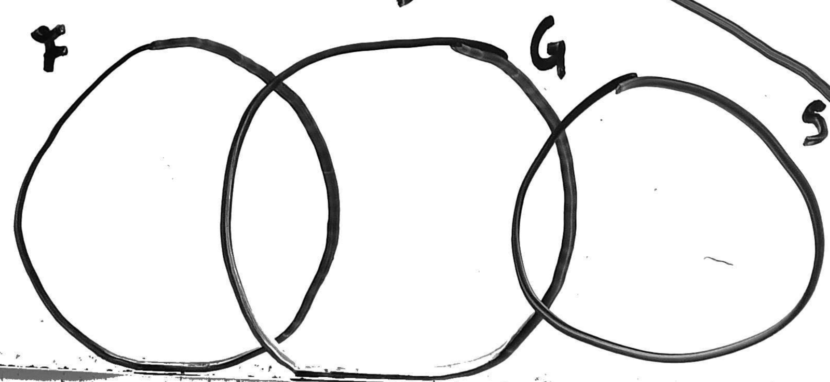
* Know 3 simple statement tables *

Equivalent: A flueron is not squamish or (it's not rawkoy or it is glerby).

4) $F = \{x \mid x \text{ is a flueron}\}$

$G = \{y \mid y \text{ is glerby}\}$

$S = \{z \mid z \text{ is squamish}\}$



New relationship

Some glerby are neither flueron or squamish

$G \setminus (F \cup S) = \emptyset$

at least 1 element of glerby outside F & S.

A→b	¬A→B	¬A→¬B	A→¬b	A	B	C
T	T	F	F	T	T	T
T	T	F	F	T	T	F
F	F	T	T	T	F	T
F	F	T	T	T	F	F
T	T	F	F	F	T	T
T	T	F	F	F	T	F
F	F	T	T	F	F	T
F	F	T	T	F	F	F

$P \land Q$	$P \lor Q$	$P \to Q$
Troc if both are trve	false when Both is false	false only when Q IS false.

Midterm

Must Know Tables

$A \to B$

A or b

$A \vee B$ or

$A \wedge B$

&

(a) $2+3=6$ unless $5\times 8=11$

(b) If $3\times 5=5$, then $4+8=32$

(c) $1+1=2$ & $2\times 3=8$, or $5+4=9$.

(d) $1+1=2$ & $2\times 3=8$ or $5+4=9$.

(a) $\neg Q \to P = \neg(\text{false}) \to \text{false} = \underline{\text{True} \to \text{False}}$

Statement Eval: <u>False</u>

b) $Q \to P = \underline{\text{True} \to \text{False}}$

Statement Eval: <u>False</u>

Compound statement

c) $(A \wedge b) \vee (c) = \underbrace{\underbrace{(T \wedge F)}_{\text{False}} \text{ or } (T)}_{\text{True}} = \underline{\text{True}}$

$(A \wedge B) \vee (c) = \underbrace{\underbrace{(T \wedge F)}_{\text{False}} \text{ or } T}_{\text{True}} = \underline{\text{True}}$