

2/2/2021

Part 1

1. Show $n^3 \equiv n \pmod{6}$.

Proof (by cases):

To show that $n^3 \equiv n \pmod{6}$, there exists an integer k , such that $n = 6k$, $n = 6k+1$, $n = 6k+2$, $n = 6k+3$, $n = 6k+4$, and $n = 6k+5$.

Case 1: $n = 6k$

$$n^3 = 216k^3$$

By definition, $n^3 - n = 216k^3 - 6k$.

Factoring out a 6: $n^3 - n = 6(36k^3 - k)$. Therefore, $6 \mid (n^3 - n)$ and for this case $n^3 \equiv n \pmod{6}$

Case 2: $n = 6k+1$

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

By definition, $n^3 - n = (216k^3 + 108k^2 + 18k + 1) - (6k + 1)$

Factoring out a 6: $n^3 - n = 6(36k^3 + 18k^2 + 2k)$. Therefore, $6 \mid (n^3 - n)$ and for this case $n^3 \equiv n \pmod{6}$

Case 3: $n = 6k+2$

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

By definition, $n^3 - n = (216k^3 + 216k^2 + 72k + 8) - (6k + 2)$

Factoring out a 6: $n^3 - n = 6(36k^3 + 36k^2 + 11k + 1)$. Therefore, $6 \mid (n^3 - n)$ and for this case $n^3 \equiv n \pmod{6}$

Case 4: $n = 6k+3$

$$n^3 = (6k+3)^3$$

By definition, $n^3 - n = (216k^3 + 324k^2 + 162k + 27) - (6k + 3)$

Factoring out a 6: $n^3 - n = 6(36k^3 + 54k^2 + 26k + 4)$. Therefore, $6 \mid (n^3 - n)$ and for this case $n^3 \equiv n \pmod{6}$

Case 5: $n = 6k+4$

$$n^3 = (6k+4)^3$$

By definition, $n^3 - n = (216k^3 + 432k^2 + 288k + 64) - (6k + 4)$

Factoring out a 6: $n^3 - n = 6(36k^3 + 72k^2 + 47k + 10)$. Therefore, $6 \mid (n^3 - n)$ and for this case $n^3 \equiv n \pmod{6}$

Case 6: $n = 6k+5$

$$n^3 = (6k+5)^3$$

By definition, $n^3 - n = (216k^3 + 540k^2 + 450k + 125) - (6k + 5)$

Factoring out a 6: $n^3 - n = 6(36k^3 + 90k^2 + 74k + 20)$. Therefore, $6 \mid (n^3 - n)$ and for this case $n^3 \equiv n \pmod{6}$

After analyzing all possible cases, we can conclude that $n^3 \equiv n \pmod{6}$ ■

2. Show that if $y^3 + yx^2 \leq x^3 + xy^2$, then $y \leq x$.

$p \rightarrow q$

contrapositive: $\neg q \rightarrow \neg p$

$$p = y^3 + yx^2 \leq x^3 + xy^2 \quad \neg p = y^3 + yx^2 > x^3 + xy^2$$

$$q = y \leq x$$

$$\neg q = y > x$$

Proof (by contrapositive):

Suppose that $y \leq x$ is not true, and in fact, $y > x$.

Therefore, $y - x > 0$

$$\begin{aligned} \text{Multiplying both sides by } (x^2 + y^2) \quad & (x^2 + y^2)(y - x) > (x^2 + y^2)(0) \\ & yx^2 + y^3 - x^3 - xy^2 > 0 \end{aligned}$$

$$\text{Rearranging:} \quad y^3 + yx^2 > x^3 + xy^2$$

Therefore, if $y > x$, then $y^3 + yx^2 > x^3 + xy^2$. By contrapositive, this means that if $y^3 + yx^2 \leq x^3 + xy^2$, then $y \leq x$ ■

3. Prove or disprove this statement: If a divides b and b divides c , then a divides c .

Proof:

Assume that $a|b$ and $b|c$, and that a , b , and c are $\in \mathbb{Z}$.

By definition of divisibility, there exists some $k \in \mathbb{Z}$ such that $ak = b$ and there exists some $j \in \mathbb{Z}$ such that $bj = c$.

Substitute: $(ak)j = c$

$$a(kj) = c$$

Since k and j are $\in \mathbb{Z}$, we can conclude that $a|c$ ■

4. Find $411^{-1} \pmod{421}$

$411(x \cdot \text{mod} 421) = 1$ (goal is to find x) to get the modular inverse of $411 \pmod{421}$

By Euclidean algorithm:

$$421 = 411(1) + 10$$

$$411 = 10(41) + 1$$

Rearranging:

$$411 + 10(-41) = 1$$

$$421 + 411(-1) = 10$$

Substituting $(421 + (411(-1)))$ for 10:

$$411 + (421 + (411(-1)))(-41) = 1 \pmod{421}$$

$$411 + (-41)(421) + 41(411) = 1 \pmod{421}$$

$(-41 \cdot 421) \pmod{421}$ cancels out:

$$411 + 41(411) = 1 \pmod{421}$$

$$42(411) = 1 \pmod{421}$$

$$\mathbf{411^{-1} \pmod{421} = 42}$$

5. Prove or disprove this statement: If a divides bc , then a divides b or a divides c .

Proof:

Suppose that $a|bc$ and that a , b and c are $\in \mathbb{Z}$.

This means that by the definition of divisibility, there exists some $k \in \mathbb{Z}$ such that $bc = ka$.

For an integer x , $bcx = (ka)x = (kx)a$, where $kx \in \mathbb{Z}$, so $a|b$ or $a|c$ ■

6. Suppose you have 3 containers, one with 17 deciliter capacity, one with 27 deciliter capacity, and one large container of unknown capacity. You have a water source and a drain. The goal is to have 1 measured deciliter in the large container. You may fill containers, pour contents or partial contents of one container into another, and empty containers. Each container should always hold a known amount of water. Please show how to achieve the goal, or prove that it can't be done.

Yes, this can be done because the $\gcd(17, 27)=1$.

$27 = 17(1) + 10$ *fill 17bucket, transfer 17dL to the 27 container, remainder 10dL space. 17 bucket is empty

$17 = 10(1) + 7$ *fill 17 bucket, transfer 10 to the 27dL container to fill it up. 17dL bucket now has 7dL remainder 10dL space.

dump out the 27dL bucket

$10 = 7(1) + 3$ *transfer 7dL from 17 bucket to 27dL container. 17dL container is empty and the 27dL container has 7dL with 20dL empty space.

*Fill the 17 bucket and add 17 to the 27 bucket, resulting in 24dL in the 27 container with 3dL remainder of empty space.

$7 = 3(2) + 1$ * fill the 17bucket, and add 3 dL to fill up the 27 container. The 17dL bucket has 14dL water with 3dL empty space.

dump out the 27dL bucket

*fill the 27bucket with the 14dL left in the 17dL bucket. 27 bucket now has 14dL water, remainder 13 empty space.

*fill the 17bucket and transfer 13dL to the 27bucket. The 17bucket now has 4dL water, 13dL empty space.

dump out the 27dL bucket

*fill the 27 container with 4dL water from the 17dL container. Now the 27 container has 4dL water with 23dL empty space remaining. 17bucket is empty.

*fill the 17dL container and transfer 17dL to the 27dL container. Now, the 17dL

container is empty and the 27dL container is 21dL full with 6dL empty space remaining.

*fill the 17dL container and transfer 17dL to the 27dL container. Now, the 17dL container is empty and the 27dL container is 21dL full with 6dL remaining

$3 = 2(1) + 1$ fill the 17dL container, transfer the water to fill the remaining 6dL space in the 27dL container. The 17dL container has 11dL of water with 6dL empty space.

dump out the 27dL bucket

*fill the empty 27dL container with 11dL water. Now, the 27dL container has 11dL water with 16dL empty space. The 17dL container is empty

*Finally, fill the 17dL container and transfer 16dL to the 27dL container. The 17dL container now has 1dL water remaining, which can be transferred to the large container. ■

7. (a) Show that a number is divisible by 3 if and only if the sum of the digits is divisible by 3. (for example, 4329 is divisible by 3, since $4+3+2+9=18$ is a multiple of 3, but 2123 is not divisible by 3 because $2+1+2+3=8$ is not a multiple of 3.)

Proof:

Assume x is a number composed of k digits in base 10 representation. x can therefore be written as $x = b_k b_{k-1} b_{k-2} \dots b_2 b_1$ where $b_i \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, since b is in base 10.

Since we are in base 10, x can be written as:

$$x = b_1 \cdot 10^0 + b_2 \cdot 10^1 + b_3 \cdot 10^2 + \dots + b_k \cdot 10^{k-1}$$

We know that $10 \equiv 1 \pmod{3}$. $10^n \equiv 1 \pmod{3}$, n is $\in \mathbb{Z}$

Therefore, x can be re-written as:

$$x \equiv b_1 \cdot 1 + b_2 \cdot 1 + b_3 \cdot 1 + \dots + b_k \cdot 1 \pmod{3}$$

Simplified:

$$x \equiv b_1 + b_2 + b_3 + \dots + b_k \pmod{3}$$

Suppose that $b_1 + b_2 + b_3 + \dots + b_k = 3j$ where $j \in \mathbb{Z}$

Substitute

$$\begin{aligned} x &\equiv b_1 + b_2 + b_3 + \dots + b_k \equiv 3j \pmod{3} \\ &\equiv 0 \pmod{3} \quad (\text{because } 3j \text{ is equivalent to } 0 \text{ in mod } 3) \end{aligned}$$

This tells us that x is an integer multiple of 3, i.e. x is divisible by 3. Therefore, x is divisible by 3 if its digits add to a multiple of 3 ■

(b) There is one other value of a digit for which finding divisibility follows the exact rule as for the digit 3. Find it, and prove the rule holds.

Proof:

Assume x is a number composed of k digits in base 10 representation. x can therefore be written as $x = b_k b_{k-1} b_{k-2} \dots b_2 b_1$ where $b_i \in \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$, since b is in base 10.

Since we are in base 10, x can be written as:

$$x = b_1 \cdot 10^0 + b_2 \cdot 10^1 + b_3 \cdot 10^2 + \dots + b_k \cdot 10^{k-1}$$

We know that $10 \equiv 1 \pmod{9}$. $10^n \equiv 1 \pmod{9}$, $n \in \mathbb{Z}$

Therefore, x can be re-written as:

$$x \equiv b_1 \cdot 1 + b_2 \cdot 1 + b_3 \cdot 1 + \dots + b_k \cdot 1 \pmod{9}$$

Simplified:

$$x \equiv b_1 + b_2 + b_3 + \dots + b_k \pmod{9}$$

Suppose that $b_1 + b_2 + b_3 + \dots + b_k = 9j$ where $j \in \mathbb{Z}$

Substitute

$$\begin{aligned} x &\equiv b_1 + b_2 + b_3 + \dots + b_k \equiv 9j \pmod{9} \\ &\equiv 0 \pmod{9} \quad (\text{because } 9j \text{ is equivalent to } 0 \text{ in mod } 9) \end{aligned}$$

This tells us that x is an integer multiple of 9, i.e. x is divisible by 9. Therefore, x is divisible by 9 if its digits add to a multiple of 9 ■

(c) Develop and prove a rule involving combining of the digits to determine if a number is divisible by 11.

	Base 10	Mod 11 remainder	Congruence remainder
1	10^0	1	1
10	10^1	10	-1
100	10^2	1	1
1000	10^3	10	-1
10000	10^4	1	1

Since we are in base 10, x can be written as:

$$x = b_1 \cdot 10^0 + b_2 \cdot 10^1 + b_3 \cdot 10^2 + \dots + b_k \cdot 10^{k-1}$$

Based on the table above, we know that base 10 remainder alternates positive and negative remainders of 1. We know that $10 \equiv -1 \pmod{11}$. $10^n \equiv (-1)^n \pmod{11}$, $n \in \mathbb{Z}$

Therefore, x can be re-written as:

$$x \equiv b_k - b_{k-1} + b_{k-2} - b_{k-3} + \dots + b_1 \pmod{11}$$

Rule: if the alternating sum of a number's digits is divisible by 11, then the number is also divisible by 11.

(d) Find $43^{117} \pmod{19}$. Show your work.

Binary of 117 = 1110101 (computed for problem 1, part 2).

$$43^1 \cdot 43^4 \cdot 43^{16} \cdot 43^{32} \cdot 43^{64} \pmod{19}$$

$$43^1 \pmod{19} = 5$$

$$43^2 \pmod{19} = (43^1 \pmod{19} \cdot 43^1 \pmod{19}) \pmod{19} = (5 \cdot 5) \pmod{19} = 6$$

$$43^4 \pmod{19} = (43^2 \pmod{19} \cdot 43^2 \pmod{19}) \pmod{19} = (6 \cdot 6) \pmod{19} = 17$$

$$43^8 \pmod{19} = (43^4 \pmod{19} \cdot 43^4 \pmod{19}) \pmod{19} = (17 \cdot 17) \pmod{19} = 4$$

$$43^{16} \pmod{19} = (43^8 \pmod{19} \cdot 43^8 \pmod{19}) \pmod{19} = (4 \cdot 4) \pmod{19} = 16$$

$$43^{32} \pmod{19} = (43^{16} \pmod{19} \cdot 43^{16} \pmod{19}) \pmod{19} = (16 \cdot 16) \pmod{19} = 9$$

$$43^{64} \pmod{19} = (43^{32} \pmod{19} \cdot 43^{32} \pmod{19}) \pmod{19} = (9 \cdot 9) \pmod{19} = 5$$

$$43^1 \cdot 43^4 \cdot 43^{16} \cdot 43^{32} \cdot 43^{64} \pmod{19} = (5 \cdot 17 \cdot 16 \cdot 9 \cdot 5) \pmod{19}$$

$$= (61200) \pmod{19}$$

$$= 1$$

8. Show that $41 \mid (3^{20} + 1)$ (without actually computing 3^{20}).

$$3^4 = 81 \text{ and } 81 + 1 = 82 \text{ which is also divisible by 41.}$$

$$3^{30} + 1 = (3^{16}(3^4 + 1))$$

$$3^4 + 1 = 82$$

$$41 \mid 82$$

$$\text{So, } 41 \mid 3^{20} + 1$$

9. Show that $A \cup B = (A \setminus B) \cup (A \cap B) \cup (B \setminus A)$. Show also that these three sets are mutually exclusive.

A	B	$A \cup B$	$(A \setminus B)$	$(A \cap B)$	$(A \setminus B) \cup (A \cap B)$	$(B \setminus A)$	$(A \setminus B) \cup (A \cap B) \cup (B \setminus A)$
T	T	T	F	T	T	F	T
T	F	T	T	F	T	F	T
F	T	T	F	F	F	T	T
F	F	F	F	F	F	F	F

*columns shaded in green are logically equivalent

*yellow, orange, and blue columns are mutually exclusive because they do not share any common truth values

10. Show that $A = (A \setminus B) \cup (A \cap B)$.

A	B	$\setminus B$	$(A \setminus B)$	$(A \cap B)$	$(A \setminus B) \cup (A \cap B)$
T	T	F	F	T	T
T	F	T	T	F	T
F	T	F	F	F	F
F	F	T	F	F	F

*columns shaded in green are logically equivalent

11. For each of the following statements, either prove it is true, or provide a counter-example:

(a) $A \setminus (B \cup C) = (A \setminus B) \cup (A \setminus C)$

A	B	C	$B \cup C$	$A \setminus B \cup C$	$(A \setminus B)$	$(A \setminus C)$	$(A \setminus B) \cup (A \setminus C)$
T	T	T	T	F	F	F	F
T	T	F	T	F	F	T	T
T	F	T	T	F	T	F	T

T	F	F	F	T	T	T	T
F	T	T	T	F	F	F	F
F	T	F	T	F	F	F	F
F	F	T	T	F	F	F	F
F	F	F	F	F	F	F	F

Counter example is shown in orange because there is a different truth value between the columns for the proposed logical equivalence.

(b) If $B \neq \emptyset$ and $A \times B \subseteq B \times C$, then $A \subseteq C$

$p = B \neq \emptyset$

$q = A \times B \subseteq B \times C$

$r = A \subseteq C$

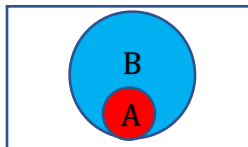
if p and q then r

p	q	r	$p \wedge q$	$p \wedge q \rightarrow r$
T	T	T	T	T
T	T	F	T	F
T	F	T	F	T
T	F	F	F	T
F	T	T	F	T
F	T	F	F	T
F	F	T	F	T
F	F	F	F	T

Counter example is shown in orange: the premise true, but the conclusion is false.

(c) $A \subseteq B$ if and only if $A \setminus B = \emptyset$

For A to be related to B , $\forall x(x \in A \rightarrow x \in B)$. $A \subseteq B$ holds if and only if $A \setminus B = \emptyset$.



$p = A \subseteq B$

$q = A \setminus B = \emptyset$

p	q	$p \leftrightarrow q$
T	T	T
T	F	F
F	T	F
F	F	T

Part 2

- Write the decimal number 117 as a binary number. In an earlier problem you computed $43^{117} \pmod{19}$. How does the binary representation of 117 related to the computation you did?

117_{10} as a binary number:

2^7	2^6	2^5	2^4	2^3	2^2	2^1	2^0
128	64	32	16	8	4	2	1

$$117 = 1 \cdot 64 + 53$$

$$53 = 1 \cdot 32 + 21$$

$$21 = 1 \cdot 16 + 5$$

$$5 = 0 \cdot 8 + 5$$

$$5 = 1 \cdot 4 + 1$$

$$1 = 0 \cdot 2 + 1$$

$$1 = 1 \cdot 1 + 0$$

$$117_{10} = 1110101_2$$

1110101 is the binary representation for 117 in decimal.

$$43^{117} = (43^{64} + 43^{32} + 43^{16} + 43^4 + 43^1)$$

2. Prove that $\sqrt{5}$ is irrational.

Proof(contradiction): By way of contradiction, assume that $\sqrt{5}$ is rational.

By definition of real numbers, x is called rational if there exists integers p and q such that $x = \frac{p}{q}$.

So, we can choose $p, q \in \mathbb{Z}$ such that $\sqrt{5} = \frac{p}{q}$. We may assume that the fraction is in its simplest form, and that p and q are not both even.

Squaring both sides, we see that $5 = \frac{p^2}{q^2}$, so $5q^2 = p^2$. This means that 5 divides p^2 , which means that 5 also divides p . So, we have $p = 5k$ for some $k \in \mathbb{Z}$ and we can substitute $5k$ for p .

We have $5q^2 = (5k)^2$, so $5q^2 = 25k^2$, and thus, $q^2 = 5k^2$. This means that 5 also divides q^2 , which means that 5 also divides q .

So, 5 is a common factor for both p and q , which is a contradiction. Thus $\sqrt{5}$ must be irrational ■

3. Take a standard deck, draw a random card and write down what you drew. Return the card, shuffle again, and draw again, and so forth, until you have an ordered list of 5 cards. How many outcomes are there for which the first card is an Ace or the second card is an Ace? How many outcomes are there that include a four-of-a-kind?

Case 1: how many outcomes are there for which the first card is an Ace?

There are 4 aces in a deck, so on the first draw, there are 13 outcomes for that case.

Case 2: how many outcomes are there for which the second card is an Ace? (with replacing the first card?) With replacement, there are 4 aces in the deck for both draws, so there are 13^2 outcomes for drawing an ace on the first draw and drawing an ace on the second draw.

Case 3: how many outcomes include a four-of-a-kind?

$$\binom{n}{r} = {}_nC_r = \frac{n!}{r!(n-r)!}$$

Possible arrangement of cards: ${}_{52}C_4 = 270,725$

The possible locations of non-four of a kind fifth card is 48

Therefore, there are $(48)({}_{52}C_4)$ outcomes which include a four-of-a-kind. Note, this does not include the case for "5 of a kind", due to card replacement.

4. A set X has 35 four-element subsets. What is $|X|$?

$$\binom{n}{r} = {}_nC_r = \frac{n!}{r!(n-r)!}$$

$${}_nC_4 = 35, \text{ solve for } n$$

$$35 = \frac{n!}{4!(n-4)!}$$

$$840 = \frac{n!}{(n-4)!}$$

$$840 = \frac{n(n-1)(n-2)(n-3)(n-4)!}{(n-4)!}$$

$$840 = n(n-1)(n-2)(n-3)$$

$$0 = n^4 - 6n^3 + 11n^2 - 6n - 840$$

$$0 = (n+4)(n-7)(n^2 - 3n + 30)$$

$$n > 4, \text{ so } n = 7$$

Therefore, the cardinality of set X is 7.

5. How many 5-digit postal codes have exactly 3 zeros?

Set of digits = $\{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$

For example, 00012 is different than 00102, so order matters

The possible locations of non-zero digits is $9 \times 9 = 81$

The possible arrangement of codes is $\binom{5}{2} = {}_5C_2 = \frac{5!}{2!(3!)} = 10$

Therefore, there are $(81)(10) = 810$ 5-digit postal codes with exactly 3 zeros.

6. Define the relation R on \mathbb{R} by xRy if and only if $x-y \in \mathbb{Z}$. Show R is an equivalence relation.

*is R reflexive? Yes, since $x-x=0 \forall x \in \mathbb{Z}$. $0 \in \mathbb{Z}$, so R is reflexive.

*is R symmetric? Yes, $x-y = k$ for some $k \in \mathbb{Z}$

$y-x = -k$, $-k \in \mathbb{Z}$, so R is symmetric.

*is R transitive? Yes, take $x, y, z \in \mathbb{Z}$ such that $x-y = j$, $y-z = k$ with $j, k \in \mathbb{Z}$

$(x-y) + (y-z) = j+k$

$x-z = j+k$ and $j, k \in \mathbb{Z}$. So xRz , which is transitive.

A relation R on a set \mathbb{R} is an equivalence relation if it is reflexive, symmetric, and transitive. Because this relation fulfills reflexive, symmetric, and transitive properties, it is an equivalence relation. ■

7. Complete the proof by induction that for all $n \geq 0$, $3|(n^3 + 3n^2 + 2n)$.

Proof (by induction)

Step 1: base case: let $n = 0$

$$3|(0^3 + 3(0^2) + 2(0))$$

$$3|(0 + 0 + 0)$$

$$3|0$$

So, the formula holds for $n=0$.

Step 2 (inductive step):

Suppose $k \in \mathbb{N}$ and assume that $3|(k^3+3k^2+2k)$ (inductive hypothesis)

Note that we want to show that $3|((k+1)^3+3(k+1)^2+2(k+1))$

$$=k^3+3k^2+3k+1+3k^2+6k+3+2k+2$$

$$(\text{rearrange terms}) = (k^3+3k^2+2k) + 3k^2+9k+6$$

(factor, and notice that by inductive hypothesis) $= k + (3k^2+9k+6)$

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

Step 3(conclusion):

Therefore, by induction, the formula holds for all $n \in \mathbb{N}$ ■

8. Prove that $n! > 2^n$ for natural numbers $n \geq 4$.

Proof(by induction)

Step 1: base case: let $n=4$

Is $4! > 2^4$

$$4! = 4 \cdot 3 \cdot 2 \cdot 1 = 24 \quad 2^4 = 16$$

$24 > 16$, so the formula holds for $n=4$.

Step 2 (inductive step):

Suppose $k \in \mathbb{N}$ and $k \geq 4$. Assume that $k! > 2^k$ (inductive hypothesis)

Note that we want to show that $(k+1)! > 2^{k+1}$

$$(k+1)! - 2^{k+1} > 0 \text{ (rearranging terms)}$$

$$(k+1)k! - 2^{k+1} > 0$$

$$(k+1)k! - 2^{k+1} > 0 \text{ by inductive hypothesis } k! > 2^k$$

$$(k+1)2^k - (2^{k+1}) > (k+1)k! - 2^{k+1} > 0$$

By transitive property,

$$(k+1)2^k - (2^{k+1}) > 0$$

$$(k+1)2^k > 2^{k+1} \text{ again, by inductive hypothesis } k! > 2^k$$

$$(k+1)! > 2^{k+1}$$

Step 3(conclusion):

Therefore, by induction, the formula holds for all $n \in \mathbb{N}$ where $n \geq 4$ ■

9. In calculus we used the summation formula

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

Prove this formula is correct for all natural numbers n .

Proof(by induction):

Step 1(base case): let $n=1$.

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

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

and so the formula holds for $n=1$.

Step 2 (inductive step):

Suppose $k \in \mathbb{N}$ and assume that

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

Note that we want to show:

$$\sum_{i=1}^{k+1} i^2 = \frac{(k+1)(k+2)(2k+3)}{6}$$

$$1^2 + 2^2 + \dots + k^2 + (k+1)^2 = \frac{(k+1)(k+2)(2k+3)}{6}$$

$$\frac{k(k+1)(2k+1)}{6} + (k+1)^2 = \frac{(k+1)(k+2)(2k+3)}{6}, \text{ by inductive hypothesis}$$

$$\frac{k(k+1)(2k+1)(6(k+1)^2)}{6}$$

$$\frac{(k+1)(k(2k+1))(6(k+1)^2)}{6}$$

$$\frac{(k+1)(2k^2 + k + 6k + 6)}{6}$$

$$\frac{(k+1)(2k^2 + 7k + 6)}{6}$$

$$\frac{(k+1)(2k+3)(k+2)}{6} = \frac{(k+1)(k+2)(2k+3)}{6}, \text{ thus the formula holds for } n=k+1$$

Step 3 (conclusion):

Therefore, by induction, the formula holds for all $n \in \mathbb{N}$ ■

10. Prove that for $n \geq 0$, $\int_0^\infty x^n e^{-x} dx = n!$

Proof (by induction):

Step 1 (base case): let $n=0$

$$\int_0^\infty x^n e^{-x} dx = 0!$$

$$= \int_0^\infty x^0 e^{-x} dx$$

$$= \int_0^\infty e^{-x} dx$$

$$= -[e^{-\infty} - e^0]$$

$$= -\left[\frac{1}{e^{-\infty}} - 1\right]$$

$$= -[0 - 1]$$

$$= 1$$

$$0! = 1$$

And so the formula holds for $n=0$.

Step 2 (inductive step): assume the statement is true for $n=k$

$$\int_0^{\infty} x^n e^{-x} dx = k!$$

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

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

$$= -x^{k+1} e^{-x} - \int_0^{\infty} x^{k+1} e^{-x} dx$$

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

$$= -x^k (1) - (k+1) \int_0^{\infty} x^k e^{-x} dx \text{ *notice that } \int_0^{\infty} x^k e^{-x} dx = k!$$

$$= -x^k - (k+1)(k!)$$

Step 3(conclusion):

Therefore, by induction, the formula holds for all $n \in \mathbb{N}$ ■