Q1]...[10 points] State the Principle of Induction.

\[ P(n) \] is a statement about the positive integer \( n \).

- \( P(n) \) true
- \( P(k) \) true \( \Rightarrow \) \( P(k+1) \) true

\[ \Rightarrow \] \( P(n) \) true \( \forall n \in \mathbb{Z}^+ \)

Give a proof by induction that

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

Proof by Induction.

- \( P(1) \) true. \( \sum_{i=1}^{1} i^2 = 1^2 = 1 \), and \( \frac{(1+1)(2(1)+1)}{6} = \frac{6}{6} = 1 \)

Therefore,

\[ \sum_{i=1}^{1} i^2 = \frac{(1+1)(2(1)+1)}{6} \quad \text{& so} \quad P(1) \text{ true.} \]

- \( P(k) \) true \( \Rightarrow \) \( P(k+1) \) true.

\[ \sum_{i=1}^{k+1} i^2 = \sum_{i=1}^{k} i^2 + (k+1)^2 = \left( \sum_{i=1}^{k} i^2 \right) + (k+1)^2 \]

\[ \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \quad \text{by Ind Hypothesis} \quad (P(k) \text{ true}). \]

Thus \( P(k+1) \) true.

That is \( P(k) \) true \( \Rightarrow \) \( P(k+1) \) true.

Finally, Principle of Induction implies that \( P(n) \) true for all \( n \in \mathbb{Z}^+ \).
Q2] [10 points] Give the definition of \( a \equiv b \pmod{m} \).

\[
a \equiv b \pmod{m} \quad \text{means} \quad m \mid (b-a)
\]

Suppose that \( a \equiv b \pmod{m} \), and that \( a' \equiv b' \pmod{m} \). Prove one of the following conclusions. \( a + a' \equiv b + b' \pmod{m} \), and \( aa' \equiv bb' \pmod{m} \).

\[
\text{Sum:} \quad a \equiv b \pmod{m} \implies m \mid (b-a) \implies b-a = km \quad \text{for some } k \in \mathbb{Z},
\]
\[
a' \equiv b' \pmod{m} \implies m \mid (b'-a') \implies b'-a' = k'm \quad \text{for some } k' \in \mathbb{Z}.
\]

Thus \( (b+b') - (a+a') = (b-a) + (b'-a') \)
\[
= km + k'm
\]
\[
= (k+k')m
\]

and so \( m \mid (b+b') - (a+a') \)
\[
\implies a+a' \equiv b+b' \pmod{m} \quad \text{done!}
\]

\[
\text{Product:} \quad \text{See class notes.}
\]

Find the remainder when \(123^{456} \) is divided by 7. That is, compute \(123^{456} \pmod{7}\).

\[
10 \equiv 3 \pmod{7} \implies 10^3 \equiv 3^3 \equiv 9 \equiv 2 \pmod{7}
\]
\[
\implies 123 \equiv (1)10^2 + 2(10) + 3 \equiv (1)(2) + (2)(3) + 3 \equiv 11 \equiv 4 \pmod{7}
\]

Now \(4^3 \equiv 64 \equiv 2 \pmod{7} \) and so \(4^3 \equiv (4)(2) \equiv 8 \equiv 1 \pmod{7}\)

Note that \(3 \mid 456\) (actually \(456 = (3)(152)\))

Thus \(123^{456} \equiv 4^{456} \equiv (4^3)^{152} \pmod{7}
\]
\[
\equiv 1^{152} \equiv 1 \pmod{7}
\]

\[
\text{Ans: 1}
\]
Q3]...[10 points] State the Schröder-Bernstein Theorem.

If there is an injective map \( f : A \to B \) and an injective map \( g : B \to A \), then there is a bijective map \( h : A \to B \).

Use the Schröder-Bernstein Theorem to prove one of the following (your choice).

- \( P(\mathbb{Z}^+) \) and \( (0, 1) \) have the same cardinality.
- \( (0, 1) \) and \( (0, 1)^2 \) have the same cardinality.

\[ f : (0, 1) \to (0, 1)^2 : x \mapsto (x, x) \text{ is clearly injective} \]

\[ g : (0, 1)^2 \to (0, 1) \]

\[ : (a_1a_2a_3..., 0.b_1b_2b_3...) \mapsto 0.a_1b_1b_2b_3... \]

where \( a_1a_2... \) and \( 0.b_1b_2... \) do not end in \( \infty \) string.

\( g \) is injective.

\[ S : B \to \exists \text{ bijection } h : (0, 1) \to (0, 1)^2 \]

\[ P(\mathbb{Z}^+) \equiv \{ \text{infinite binary strings} \} \]

\[ f : \text{string} \to 0.a_1a_2... \text{ in decimal} \]

where \( a_i = \begin{cases} 3 & \text{if } \text{ith position} \text{ string } = 0 \\ 4 & \text{otherwise} \end{cases} \)

Claim: \( f \) is injective.

\( g : (0, 1) \to \{ \text{infinite binary strings} \} \equiv P(\mathbb{Z}^+) \)

\[ : x \mapsto \text{truncated base 2 representation of } x \]

\( \rightarrow \text{ remove } 0 \text{ b. s. from start.} \\ \rightarrow \text{ use representation which do not have } \infty \text{ string.} \)

\( g \) is injective.

\[ S : B \to P(\mathbb{Z}^+) \equiv (0, 1) \]
Q4]...[10 points] Give the definition of the greatest common divisor, \( \gcd(a, b) \), of two integers \( a \) and \( b \).

\[ \gcd(ab) \text{ divides } a \text{ and divides } b \]

- If \( d \mid a \) and \( d \mid b \), then \( d \leq \gcd(a, b) \).

Compute \( \gcd(180, 96) \) and show how to express your answer as an integer linear combination of 180 and 96.

\[
\begin{align*}
180 &= 1(96) + 84 \\
96 &= 1(84) + 12 \\
84 &= 7(12) + 0
\end{align*}
\]

\[
\begin{align*}
84 &= (-1)(96) + 1(180) \\
12 &= (-1)(84) + 1(96) \\
&= (2)(96) - (1)(180)
\end{align*}
\]

\( \Rightarrow \gcd(180, 96) = \gcd(96, 84) = \gcd(84, 12) = 12 \)

\[
\boxed{12 = (2)(96) - (1)(180)}
\]

Prove that if \( a \mid bc \) and \( \gcd(a, b) = 1 \), then \( a \mid c \).

\[
\gcd(a, b) = 1 \quad \Rightarrow \quad \exists \text{ integers } x, y \text{ so that } 1 = xa + yb.
\]

Multiply by \( c \) \( \Rightarrow \quad c = 1 \cdot c = xac + ybc \)

Now \( a \mid xac \) by def\( \Rightarrow \)

and \( a \mid ybc \) since \( a \mid bc \) by hypothesis

\( \Rightarrow \quad a \mid (xac + ybc) \quad \Rightarrow \quad a \mid c \]

Prove that if \( p \) is a prime number, and \( p \mid ab \) for integers \( a \) and \( b \), then \( p \mid a \) or \( p \mid b \).

\[
P \mid a \quad \Leftrightarrow \quad p \nmid a.
\]

If \( p \nmid a \) then \( \gcd(a, p) = 1 \) since \( p \) is prime.

Previous result \( \Rightarrow \quad p \mid b \)

Thus \( p \mid a \) or \( p \mid b \). 

\( \square \)
Q5]...[10 points] Consider a pair of equilateral triangles such that the area of the larger is 3 times the area of the smaller. Take three copies of the smaller triangle inside the larger. A copy of the smaller triangle is based at each of the three vertices of the larger triangle. These overlap to form regions with area $A$, $B$ and $C$ as shown.

Show how to turn this into a proof by infinite descent (well-ordering) that $\sqrt{3}$ is irrational. Give a detailed algebra proof of the irrationality of $\sqrt{3}$ using infinite descent.

1. Note \( \text{Area } \triangle = \text{Constant } (\text{edge})^2 \),
   Thus \( 3 = \frac{\text{Area large } \triangle}{\text{Area small } \triangle} = \frac{(\text{large edge})^2}{(\text{small edge})^2} = \frac{M^2}{N^2} \)
   \( \frac{M^2}{N^2} = 3 \)

2. Note \( \text{Area (large } \triangle) = A + 3B + 3C \)
   \( \text{Area (small } \triangle) = B + 2C \)

   So \( 3(B + 2C) = A + 3B + 3C \)
   \( 3B + 3C = A + 3B + 3C \)

   \( A = 3C \)

   of the two newly created triangles, the area of the larger is exactly 3 times the area of the smaller.

3. If $\sqrt{3}$ is rational $\Rightarrow$ exists rational expression $\frac{M}{N} = \sqrt{3}$
   where $M, N \in \mathbb{Z}^+$ and $N$ is least such integer (well-ordering).
Form the large & smaller $\Delta$s with sidelengths $M$ & $N$

But then the new smaller $\Delta$s will have (also) $
\Theta$ integer edge lengths $M'$ & $N'$ (say)

& we re seen in 0 & 0 above that

\[
\left(\frac{M'}{N'}\right)^2 = \text{Ratio of areas} = \frac{3}{4}
\]

in 0

\[\text{in 2}\]

Thus $\frac{M'}{N'} = \sqrt{3}$ & $N'$ is smaller $\Theta$ integer than $N$

$\Rightarrow$ contradiction.

Thus $\sqrt{3}$ must be irrational.
\[(M-N)+s = N\]  ... look at inner \(\Delta\) on left.

\[\Rightarrow s = 2N-M\]

\[l + 2s = N\]

\[l = N - 2s = N - 2(2N-M) = 2M - 3N\]

\[l = 2M - 3N\]

This is the basis for our purely algebra proof:

- No geometry
- No odd/evenness
- No divisibility/non-divisibility by 3

\[\text{Thm} \quad \sqrt{3} \text{ is irrational}\]

\[\text{Pf} \quad (\text{By Well-Ordering, \(\infty\)-descent}). \quad \text{We argue by contradiction.}\]
Suppose that $\sqrt{3}$ is rational. Thus there exists an expression of the form
\[\sqrt{3} = \frac{M}{N}\] (**)
where (i) $M, N \in \mathbb{Z}^+$, and
(ii) $N$ is least among all positive integers $M, N$ satisfying (**).

Now
\[1 < \sqrt{3} < 2\]
\[\Rightarrow\]
\[1 < \frac{M}{N} < 2\]

$N$ positive $\Rightarrow$ \[N < M < 2N\]

$N < M$ \[\Rightarrow \]
$N-M < M-M = 0$

$\Rightarrow \]
$N+N-M < N+0 = N$

$\Rightarrow \]
$2N-M < N$

Thus ($2N-M$) is a positive integer which is strictly smaller than $N$.\[H.\]

Claim
\[\frac{2M-3N}{2N-M} = \frac{M}{N}\]

\[\text{(**)}\]
Cross multiply to get --

\[(***) \text{true} \implies 2MN - 3N^2 = 2NM - M^2\]

\[\implies 3N^2 = M^2\]

\[\implies 3 = \left(\frac{M}{N}\right)^2\]

This is true, since \(\frac{M}{N} = \sqrt{3}\) by (***).

Now \(2N-M\) is \(\Theta\) \iff \(2M-3N\) is also \(\Theta\)

(since ratio = \(\sqrt{3}\) is \(\Theta\))

Thus (****) gives a way of expressing \(\sqrt{3}\) as a ratio of two positive integers, where the denominator, \((2M-N)\), is strictly less than \(N\).

This contradicts the fact that \(N\) was least.

Contradiction comes from assumption that \(\sqrt{3}\) has expressions as ratio of \(\Theta\) integers.

\[\implies \sqrt{3}\text{ is irrational }\]