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

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

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

$$\left.\begin{array}{l} P(1) \text{ true} \\ P(k) \text{ true} \Rightarrow P(k+1) \text{ true} \end{array}\right] \Longrightarrow P(n) \text{ true } \forall n \in \mathbb{Z}^+$$

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

Therefore, $\sum_{i=1}^{1} i^2 = \frac{1(1+1)(2(1)+1)}{6}$ & so P(1) true.

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

$$\sum_{i=1}^{k+1} i^2 = 1^2 + \cdots + (k+1)^2 = \left(1^2 + \cdots + k^2\right) + (k+1)^2$$

$$= \frac{k(k+1)(2k+1)}{6} + (k+1)^2$$ ---- by Ind$^{\underline{n}}$ hypothesis (P(k) true).

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

$$= \frac{(k+1)\left[k(2k+1) + 6(k+1)\right]}{6}$$

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

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

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 $a \equiv b \pmod{m}$.

$a \equiv b \pmod{m}$ means $m \mid (b-a)$

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 $aa' \equiv bb' \pmod{m}$.

<u>Sum</u>: $a \equiv b \pmod{m} \Rightarrow m \mid (b-a) \Rightarrow b - a = km$ for some $k \in \mathbb{Z}$.

$a' \equiv b' \pmod{m} \Rightarrow m \mid (b'-a') \Rightarrow b' - a' = k'm$ for some $k' \in \mathbb{Z}$.

Thus
$$\begin{aligned}(b+b') - (a+a') &= (b-a) + (b'-a') \\ &= km + k'm \\ &= (k+k')m\end{aligned}$$

and so $m \mid (b+b') - (a+a')$

$\Rightarrow a + a' \equiv b + b' \pmod{m}$ done!

<u>Product</u>: See <u>class notes</u>.

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

$10 \equiv 3 \pmod{7} \Rightarrow 10^2 \equiv 3^2 \equiv 9 \equiv 2 \pmod{7}$

$\Rightarrow 123 \equiv (1)10^2 + 2(10) + 3 \equiv (1)(2) + (2)(3) + 3 \equiv 11 \equiv 4 \pmod{7}$

Now $4^2 \equiv 16 \equiv 2 \pmod{7}$ and so $4^3 \equiv (4)(2) \equiv 8 \equiv 1 \pmod{7}$

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

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

$\boxed{\text{Ans: } 1}$

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 <u>bijective map</u> $h: A \to B$.

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

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

$f: (0,1) \to (0,1)^2 : x \mapsto (x, \frac{1}{2})$ is clearly injective

$g: (0,1)^2 \to (0,1)$

$: (0.a_1a_2a_3\ldots, 0.b_1b_2b_3\ldots) \longmapsto 0.a_1b_1a_2b_2\ldots$

where $0.a_1a_2\ldots$ and $0.b_1b_2\ldots$ do not end in ∞ string of 9's

is injective.

S-B $\Rightarrow$ $\exists$ bijection $h: (0,1) \to (0,1)^2$.

$\mathcal{P}(\mathbb{Z}^+) \cong \{\infty \text{ binary strings}\} \xrightarrow{f} (0,1)$

STRING $\longmapsto 0.a_1a_2\ldots$ ∞ decimal

where $a_i = \begin{cases} 3 & \text{if } i^{th} \text{ position of string} = 0 \\ 4 & \text{if } i^{th} \text{ position of string} = 1 \end{cases}$

<u>Claim</u>: f injective.

$g: (0,1) \to \{\infty \text{ binary strings}\} \cong \mathcal{P}(\mathbb{Z}^+)$

$: x \longmapsto$ <u>truncated</u> base 2 representation of x

→ Remove 0 & . from start.

→ Use representations which do not have ∞ string of 1's.

g is injective.

S-B $\Rightarrow$ $\mathcal{P}(\mathbb{Z}^+) \cong (0,1)$

Q4]... [10 points] Give the definition of the greatest common divisor, $\gcd(a, b)$, of two integers a and b.

$\gcd(a,b)$ divides a & divides b

If $d|a$ and $d|b$, then $d \le \gcd(a,b)$.

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

$180 = 1(96) + 84$

$96 = 1(84) + 12$

$84 = 7(12) + 0$

$84 = (-1)(96) + 1(180)$

$12 = (-1)(84) + (96)$

$\Rightarrow 12 = (-1)\big((-1)(96) + (1)(180)\big) + (1)(96)$

$= (2)(96) - (1)180$

$\Rightarrow \gcd(180, 96) = \gcd(96, 84) = \gcd(84, 12) = \boxed{12}$

$$\boxed{12 = (2)(96) + (-1)(180)}$$

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

$\gcd(a,b) = 1 \Rightarrow \exists$ integers x, y so that $1 = xa + yb$.

Multiply by $c \Rightarrow c = 1.c = xac + ybc$

Now $a | xac$ by def^{n}

and $a | ybc$ since $a|bc$ by hypothesis

$\Rightarrow a|(xac + ybc) \Rightarrow a|c$ ☒

Prove that if p is a prime number, and $p|ab$ for integers a and b, then $p|a$ or $p|b$.

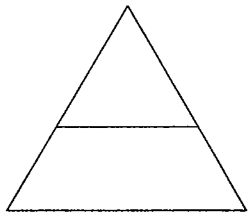
$p|a$ or $p \nmid a$.

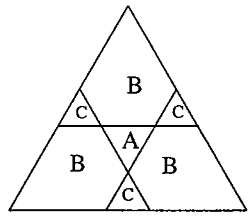
If $p \nmid a$ then $\gcd(a,p) = 1$ since p is prime.

Previous result $\Rightarrow p|b$

Thus $p|a$ or $p|b$. ☒

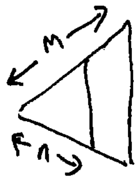
Q5]... [10 points] Consider a pair of equilateral triangles such that the area of the larger is 3 times the area of the smaller. Take three copies of the smaller triangle inside the larger. A copy of the smaller triangle is based at each of the three vertices of the larger triangle. These overlap to 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 Area of equilateral Δ = constant $(\text{edge})^2$ ..... $\left(\text{Constant} = \frac{\sqrt{3}}{4}\right)$.



Thus $3 = \dfrac{\text{Area Large } \Delta}{\text{Area Small } \Delta} = \dfrac{|\text{Large edge}|^2}{|\text{Small edge}|^2} = \dfrac{M^2}{N^2}$

$$\boxed{\frac{M^2}{N^2} = 3}$$

② Note $\text{Area}(\text{Large } \Delta) = A + 3B + 3C$

$\text{Area}(\text{small } \Delta) = B + 2C$

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

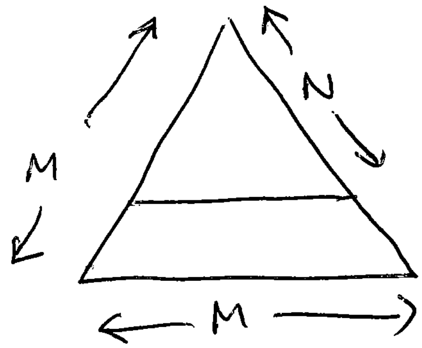
$\cancel{3B} + \underset{3C}{\cancel{6C}} = A + \cancel{3B} + \cancel{3C}$

$$\boxed{A = 3C}$$

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 <u>Least</u> such integer (Well-ordering).

Form the large & smaller Δ's with sidelengths M & N



But then the new smaller Δ's will have (also) + integer edge lengths M' & N' (say)

& we've seen in 1 & 2 above that

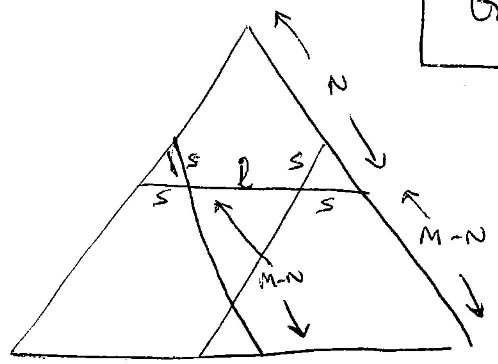
$$\left(\frac{M'}{N'}\right)^2 = \text{Ratio of areas} = 3$$

in 1   in 2

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

$\Rightarrow$ contradiction.

Thus $\sqrt{3}$ must be <u>irrational</u>. $\blacksquare$



Geometry ⇝ Algebra

⟵ EXTRA NOTES ⟶

$(M-N) + s = N$ ... look at inner Δ on left.

$\Rightarrow \boxed{s = 2N - M}$

$l + 2s = N$

$l = N - 2s = N - 2(2N-M) = 2M - 3N$

$\boxed{l = 2M - 3N}$

This is the basis for our purely algebra proof:

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

Thm $\sqrt{3}$ is irrational

Pf (By Well-Ordering, ∞-descent). We argue (painfully!) by contradiction.

Suppose that $\sqrt{3}$ is rational. Thus there exists an expression of the form

$$\sqrt{3} = \frac{M}{N} \qquad \text{——— } (*)$$

where (i) $M, N \in \mathbb{Z}^+$, and
(ii) N is least among all positive integers M, N satisfying $(*)$.

Now $\quad 1 < \sqrt{3} < 2$.

$\Rightarrow \quad 1 < \frac{M}{N} < 2$

N positive $\Rightarrow \quad N < M < 2N$

$N < M$

$\Rightarrow \quad N - M < M - M = 0$

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

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

$M < 2N$

$\Rightarrow \quad 0 = M - M < 2N - M$

$\Rightarrow \quad 0 < 2N - M$

$$\boxed{0 < 2N - M < N}$$

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

Claim

$$\boxed{\frac{2M-3N}{2N-M} = \frac{M}{N}} \qquad \text{——— } (**)$$

Cross multiply to get--

$$(**) \text{ true } \iff \cancel{2MN} - 3N^2 = \cancel{2NM} - M^2$$

$$\iff 3N^2 = M^2$$

$$\iff 3 = \left(\frac{M}{N}\right)^2$$

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

Now $2N - M$ is $\oplus$ $\Rightarrow$ $2M - 3N$ is also $\oplus$
(since Ratio $= \sqrt{3}$ is $\oplus$)

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 $\oplus$ integers.

$\Rightarrow \sqrt{3}$ is irrational $\boxed{/\!/}$