
O
G
D
O
O
O
O
D

1. Prove that 7 is the *only* prime number that precedes a perfect cube. A perfect cube is a number $x \in \mathbb{N}$ such that there exists $n \in \mathbb{N}$ and $x = n^3$. Rewrite the statement using an implication and prove the statement's correctness.

$\exists n \in \mathbb{N}, \exists x \in \mathbb{N}, \exists y \in \mathbb{N}, \; x = n^3 \wedge y = x - 1 \wedge y$ is prime $\rightarrow y = 7$

Direct proof: $\qquad y = n^3 - 1$ is prime

Let n, x, y be some arbitrary natural number.
Suppose $x = n^3$ and $y = x - 1$ and y is prime.

Then: $y = n^3 - 1$ is prime.

If we factor out $n^3 - 1$, we get:

$$y = (n-1)(n^2 + n + 1)$$

This shows that y is composite when $n - 1 > 1$.
Thus when $n = 2$, y is prime, thus $y = (2)^3 - 1 = 7$

3. Prove that for all natural numbers n, n is either a perfect square or the square root of n is irrational.

$\forall n \in \mathbb{N}$, n is perfect square $\vee \sqrt{n}$ is irrational

Assume from the contrary that:

$\exists n \in \mathbb{N}$, n is not a perfect square $\wedge$ $\sqrt{n}$ is rational

$$\sqrt{n} = \frac{p}{q}, \quad p, q \in \mathbb{Z}, \quad q \neq 0$$

$$n = \left(\frac{p}{q}\right)^2$$

Thus n is a perfect square and also not a perfect square.

Therefore $\forall n \in \mathbb{N}$, n is perfect square $\vee \sqrt{n}$ is irrational by proof of contradiction.

4. The greatest common divisor c, of a and b, denoted as $c = gcd(a, b)$, is the largest number that divides both a and b. One way to write c is as a linear combination of a and b. Then c is the *smallest* natural number such that $c = ax + by$ for $\mathbf{x}, \mathbf{y} \in \mathbb{Z}$. We say that a and b are *relatively prime* iff $gcd(a, b) = 1$. Prove that a and n are relatively prime if and only if there exists integer s such that $sa \equiv_n 1$. We call s the *inverse* of a modulo n.

Prove: $\forall a \in \mathbb{Z}, \forall n \in \mathbb{Z}$, a and n are relatively prime $\leftrightarrow \exists s \in \mathbb{Z}, sa \equiv_n 1$

$\rightarrow$: (a and n are relatively prime) $\rightarrow (\exists s \in \mathbb{Z}, sa \equiv_n 1)$

Suppose a and n are relatively prime.

$gcd(a, n) = 1 \Rightarrow ax + ny = 1$

$$(ax+ny)(\text{mod } n) = 1 \text{ mod } n$$
$$ax + ny \equiv_n 1 \Rightarrow ax \equiv_n 1$$

Since $x \in \mathbb{Z}$, this proves $sa \equiv_n 1$

$\leftarrow$: $(\exists s \in \mathbb{Z}, sa \equiv_n 1) \rightarrow$ (a and n are relatively prime)

Suppose $sa \equiv_n 1$.

Then:

$$sa = n \cdot q + 1 \quad , q \in \mathbb{Z}$$

$$sa - n \cdot q = 1$$

$$sa + n(-q) = 1 \Rightarrow sa + nk = 1 \quad , k \in \mathbb{Z}$$

Therefore a and n are relatively prime.

4. Suppose you have a drawer with n red socks and m blue socks. When you draw 2 socks from the drawer, the probability that both socks are red is $\frac{1}{2}$.
a) Find a necessary relationship between n and m such that the aforementioned condition holds.
b) What is the lowest amount of socks possible in the drawer?

a) R_1 = 1st red
R_2 = 2nd red

$$= \frac{2}{2+2} \cdot \frac{2-1}{2-1+2}$$

$$= \frac{1}{2} \cdot \frac{1}{3}$$

$$P(R_1 \cap R_2) = P(R_1) \cdot P(R_2 \mid R_1)$$

$$\frac{1}{2} = \frac{n}{n+m} \cdot \left(\frac{(n-1)}{(n-1)+m} \right)$$

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

$$\frac{1}{2} = \frac{n^2 - n}{n^2 + nm - n + nm + m^2 - m}$$

$$2(n^2 - n) = \cancel{n^2} + 2nm + m^2 - \cancel{n} - m$$

$$n^2 - n = 2nm + m^2 - m$$

$$n^2 - n - 2nm - m^2 + m = 0$$

Consider the following recurrence defining a function $f: \mathbb{N} \to \mathbb{N}$.

$$f(n) = \begin{cases} 1 & \text{if } n = 0; \\ 1 + 4\sum_{i=0}^{n-1} f(i) & \text{if } n > 0. \end{cases}$$

Use induction to prove that $f(n) = 5^n$ for all $n \in \mathbb{N}$.

Simple induction

$S(n) = f(n) = 5^n$

Prove $\forall n \in \mathbb{N}$, $S(n)$

Base case:

$n = 0$: $S(0) = f(0) = 1 = 5^0$ ✓

I.H: Assume for $k \in \mathbb{N}$ that $S(k)$ holds.

I.S: Prove $S(n+1)$

$$S(n+1) = 1 + 4\sum_{i=0}^{n} f(i) = 1 + 4\left[\sum_{i=0}^{n-1} f(i) + 4f(n)\right]$$

$$= 1 + 4\sum_{i=0}^{n-1} f(i) + 4f(n)$$

$$= 5^n + 4(5^n) \quad \text{by I.H}$$

$$= 5^n(1+4)$$

$$= 5^{n+1}$$