

1. Let's start with a warm-up exercise for doing proofs where you need to use induction: Prove that for all  $n \in \mathbb{N}$

$$1 + 2 + 2^2 + 2^3 + \cdots + 2^n = 2^{n+1} - 1.$$

**Re-expressing the problem statement:**

Prove that  $\forall n \in \mathbb{N}$

$$1 + \sum_{i=1}^n 2^i = 2^{n+1} - 1$$

*Proof.* Base case:  $n=2$

$$1 + 2^1 + 2^2 = 2^3 - 1$$

$$7 = 7$$

Inductive Hypothesis:

$$P(k) = 1 + \sum_{i=1}^k 2^i = 2^{k+1} - 1$$

$P(k+1)$  :

$$1 + \sum_{i=1}^{k+1} 2^i = 2^{k+2} - 1$$

$$1 + \sum_{i=1}^k 2^i + 2^{k+1} = 2^{k+2} - 1$$

$$2^{k+1} - 1 + 2^{k+1} = 2^{k+2} - 1$$

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

$$2^{k+2} - 1 = 2^{k+2} - 1$$

□

2. And here is a second warm-up exercise: if  $x$  is a nonnegative real number show that  $(1+x)^n - 1 \geq nx$  for  $n = 0, 1, 2, \dots$

**Re-expressing the problem statement:**

let  $x \in \mathbb{R}, x \geq 0$ , Show that

$$(1+x)^n - 1 \geq nx, \forall n \in \mathbb{W}$$

*Proof.* Suppose  $x \in \mathbb{R}, x \geq 0$

$$(1+x)^n - 1 \geq nx$$

$$(1+x)^n \geq nx + 1$$

$$\sum_{k=0}^n \binom{n}{k} x^k \geq nx + 1$$

$$nx + 1 + \sum_{k=2}^n \binom{n}{k} x^k \geq nx + 1$$

$$\therefore (1+x)^n \geq nx + 1$$

Which implies

$$(1+x)^n - 1 \geq nx$$

□

3. Show that if  $p$  is a prime number, there do not exist nonzero integers  $a$  and  $b$  such that  $a^2 = pb^2$  (i.e.  $\sqrt{p}$  is not a rational number).

If  $p$  is a prime number then the only divisors of  $p$  are 1 and  $p$

Let  $a$  and  $b$  be expressed in the prime factorization:

$$a = \prod_{i=1}^k p_i^{\alpha_i}$$

$$b = \prod_{i=1}^k p_i^{\beta_i}$$

the original statement is then:

$$\left[ \prod_{i=1}^k p_i^{\alpha_i} \right]^2 = p \left[ \prod_{i=1}^k p_i^{\beta_i} \right]^2$$

$$\prod_{i=1}^k p_i^{2\alpha_i} = p \prod_{i=1}^k p_i^{2\beta_i}$$

If  $a^2 = b^2$  then they would have identical prime factorizations. Since the integer is raised to the second power this implies that for all prime factors, each has an even exponent.

if  $p$  is not a prime factor of  $b$  then it would have an odd exponent. If  $p$  was a prime factor of  $b$  then it would form an odd exponent when combined with the corresponding prime factor since the each prime factor in  $b^2$  has an even exponent. In either case  $p$  exists as a prime number with an odd exponent therefore it cannot be equal to  $a$  since  $a$  has a prime factorization that has even exponents for each prime factor.

4. Compute the gcd of the following pairs of integers:

i) 14 and 39;

$$39 = 14(2) + 11$$

$$14 = 11(1) + 3$$

$$11 = 3(3) + 2$$

$$3 = 2(1) + 1$$

$$2 = 1(2) + 0$$

$$\gcd(39, 14) = 1$$

ii) 234 and 165;

$$234 = 165(1) + 69$$

$$165 = 69(2) + 27$$

$$69 = 27(2) + 15$$

$$27 = 15(1) + 12$$

$$15 = 12(1) + 3$$

$$12 = 3(4) + 0$$

$$\gcd(234, 165) = 3$$

iii) 471 and 562.

$$562 = 471(1) + 91$$

$$471 = 91(5) + 16$$

$$91 = 16(5) + 11$$

$$16 = 11(1) + 5$$

$$11 = 5(2) + 1$$

$$5 = 1(5) + 0$$

$$\gcd(562, 471) = 1$$

5. Let  $a, b, c \in \mathbb{Z}$ . Prove that if  $\gcd(a, b) = 1$  and  $a \mid bc$  then  $a \mid c$ .

*Proof.* if  $a \mid bc$  then  $bc = ak, k \in \mathbb{Z}$

□

6. Let  $a$  and  $b$  be positive integers where

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} \quad \text{and} \quad a = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$$

with  $p_1, \dots, p_k$  distinct primes and  $\alpha_i, \beta_i \geq 0$  for  $i = 1, \dots, k$ . Show that

$$\text{lcm}(a, b) = p_1^{\max(\alpha_1, \beta_1)} p_2^{\max(\alpha_2, \beta_2)} \cdots p_k^{\max(\alpha_k, \beta_k)}.$$

*Proof.* Let a and b be expressed in a product form as follows:

$$a = \prod_{i=1}^k p_i^{\alpha_i}$$

$$b = \prod_{i=1}^k p_i^{\beta_i}$$

Let:

$$l = \prod_{i=1}^k p_i^{\max(\alpha_i, \beta_i)}$$

for l to be the least common multiple of a and b it must satisfy two conditions.

- (a)  $a|l$  and  $b|l$  (common multiple)
- (b) if there exists a multiple e such that  $a|e$  and  $b|e$  then  $l|e$  (least common multiple)

a) We must prove that  $l = ak, k \in \mathbb{Z}$  which can be done in the following way:

$$l = ak$$

$$\prod_{i=1}^k p_i^{\max(\alpha_i, \beta_i)} = \left[ \prod_{i=1}^k p_i^{\alpha_i} \right] k$$

$$\prod_{i=1}^k p_i^{\max(\alpha_i, \beta_i)} = \left[ \prod_{i=1}^k p_i^{\alpha_i} \right] \left[ \prod_{i=1}^k p_i^{\max(\alpha_i, \beta_i) - \alpha_i} \right]$$

By similar reasoning it can be shown that  $b|l$ .

b) We now prove that if there exists another common multiple that l must be smaller.

Suppose there exists another common multiple e, this is to say,  $a|e$ , and  $b|e$  to prove that l is the least common multiple we must show that  $e=lm, m \in \mathbb{Z}$ .

$$e = am, m \in \mathbb{Z}$$

$$e = an, n \in \mathbb{Z}$$

We will first express e in its prime factorization:

$$e = \prod_{i=1}^k p_i^{\delta_i}$$

$\delta_i > \max(\alpha_i, \beta_i)$  Due to the fact that e is composed of prime factors of a and also prime factors of b then the if :

$$l = \prod_{i=1}^k p_i^{\max\{\alpha_i, \beta_i\}}$$

then for each prime since  $\delta_i > \max(\alpha_i, \beta_i)$  this implies that l is smaller. □