

November 1, 2020

## Algebra.

### Principle of Mathematical Induction (continued).

Let  $\{P(n)\} = P(1), P(2), P(3), \dots$  be a sequence of propositions numbered by positive integers, which together constitute the general theorem  $P$ . In particular,  $P(n)$  can be some formula, or other property of positive integers.

**Theorem** (Principle of Mathematical Induction).

$$(P(1) \wedge (\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1))) \Rightarrow (P: \forall n \in \mathbb{N}, P(n)).$$

**Proof.** Assume the opposite. Recalling that,  $\sim(Q \Rightarrow P) \Leftrightarrow (Q \wedge \sim P)$ , we write, the negation of the above statement as,

$$(P(1) \wedge (\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1))) \wedge \sim(P: \forall n \in \mathbb{N}, P(n)),$$

Or,

$$(P(1) \wedge (\forall n \in \mathbb{N}, P(n) \Rightarrow P(n+1))) \wedge (\exists n \in \mathbb{N}, \sim P(n)).$$

Now, using the “principle of smallest integer” we arrive at a contradiction,

$$\left( \exists r \in \mathbb{N}, (P(r-1) \wedge \sim(P(r))) \right) \Leftrightarrow \sim(\forall r \in \mathbb{N}, P(r) \Rightarrow P(r+1)). \quad \square$$

**Example 1.** Prove that the sum of the  $n$  first odd positive integers is  $n^2$ ,

$$\text{i.e., } 1 + 3 + 5 + \dots + (2n-1) = n^2.$$

**Solution.** Let  $S(n) = 1 + 3 + 5 + \dots + (2n-1)$ .

We want to prove by induction that for every positive integer  $n$ ,  $S(n) = n^2$ .

(1) Verify Base Case. For  $n = 1$ , we have  $S(1) = 1 = 1^2$ , so the property holds for  $n = 1$ .

(2) Inductive Step. Assume (Induction Hypothesis) that the property is true for a positive integer  $n$ , i.e.:  $S(n) = n^2$ . We must prove that it is also true for

$n + 1$ , i.e.,  $S(n + 1) = (n + 1)^2$ , i. e.,  $\{S(n) = n^2\} \Rightarrow \{S(n + 1) = (n + 1)^2\}$ . In fact, we can verify this explicitly,

$$S(n + 1) = 1 + 3 + 5 + \cdots + (2n - 1) + (2n + 1) = S(n) + (2n + 1).$$

But, by induction hypothesis,  $S(n) = n^2$ . Hence,

$$S(n + 1) = n^2 + (2n + 1) = (n + 1)^2.$$

This completes the induction and shows that the property is true for all positive integers.  $\square$

### **Arithmetic and geometric mean inequality: Proof by induction.**

The **arithmetic mean** of  $n$  numbers,  $\{a_1, a_2, \dots, a_n\}$ , is, by definition,

$$A_n = \frac{a_1 + a_2 + \cdots + a_n}{n} = \frac{1}{n} \sum_{i=1}^n a_i \quad (1)$$

The **geometric mean** of  $n$  non-negative numbers,  $\{a_n \geq 0\}$ , is, by definition,

$$G_n = \sqrt[n]{a_1 \cdot a_2 \cdot \dots \cdot a_n} = \sqrt[n]{\prod_{i=1}^n a_i} \quad (2)$$

**Theorem.** For any set of  $n$  non-negative numbers, the arithmetic mean is not smaller than the geometric mean,

$$\frac{a_1 + a_2 + \cdots + a_n}{n} \geq \sqrt[n]{a_1 \cdot a_2 \cdot \dots \cdot a_n} \quad (3)$$

The standard proof of this fact by mathematical induction is given below.

**Induction basis.** For  $n = 1$  the statement is a true equality. We can also easily prove that it holds for  $n = 2$ . Indeed,  $(a_1 + a_2)^2 - 4a_1a_2 = (a_1 - a_2)^2 \geq 0 \Rightarrow a_1 + a_2 \geq 2\sqrt{a_1a_2}$ .

**Induction hypothesis.** Suppose the inequality holds for any set of  $n$  non-negative numbers,  $\{a_1, a_2, \dots, a_n\}$ .

**Induction step.** We have to prove that the inequality then also holds for any set of  $n + 1$  non-negative numbers,  $\{a_1, a_2, \dots, a_{n+1}\}$ .

**Proof.** If  $a_1 = a_2 = \dots = a_n = a_{n+1}$ , then the equality,  $A_{n+1} = G_{n+1}$ , obviously holds. If not all numbers are equal, then there is the smallest (smaller than the mean) and the largest (larger than the mean). Let these be  $a_{n+1} < A_{n+1}$ , and  $a_n > A_{n+1}$ . Consider new sequence of  $n$  non-negative numbers,  $\{a_1, a_2, \dots, a_{n-1}, a_n + a_{n+1} - A_{n+1}\}$ . The arithmetic mean for these  $n$  numbers is still equal to  $A_{n+1}$ ,

$$\frac{a_1 + a_2 + \dots + a_{n-1} + a_n + a_{n+1} - A_{n+1}}{n} = \frac{n+1}{n} A_{n+1} - \frac{1}{n} A_{n+1} = A_{n+1} \quad (4)$$

Therefore, by induction hypothesis,

$$(A_{n+1})^n \geq a_1 \cdot a_2 \cdot \dots \cdot a_{n-1} \cdot (a_n + a_{n+1} - A_{n+1}) \quad (5)$$

$$(A_{n+1})^{n+1} \geq a_1 \cdot a_2 \cdot \dots \cdot a_{n-1} \cdot (a_n + a_{n+1} - A_{n+1}) \cdot A_{n+1} \quad (6)$$

Wherein, using  $a_{n+1} < A_{n+1}$  and  $a_n > A_{n+1}$ , as assumed above, we get  $(a_n - A_{n+1})(A_{n+1} - a_{n+1}) > 0$ , or,  $a_n a_{n+1} < (a_n + a_{n+1} - A_{n+1})A_{n+1}$ , so we could substitute the last two terms in the product with  $a_n \cdot a_{n+1}$ , while keeping the inequality. This completes the proof.  $\square$

### Newton's binomial.

The **Newton's binomial** is an expression representing the simplest  $n$ -th degree factorized polynomial of two variables,  $P_n(x, y) = (x + y)^n$  in the form of the polynomial summation (i.e. expanding the brackets),

$$(x + y)^n = \binom{n}{0} x^n + \binom{n}{1} x^{n-1} y + \binom{n}{2} x^{n-2} y^2 + \dots + \binom{n}{k} x^{n-k} y^k + \dots + \binom{n}{n-1} x y^{n-1} + \binom{n}{n} y^n, \quad (1a)$$

$$(x + y)^n = C_n^0 x^n + C_n^1 x^{n-1} y + C_n^2 x^{n-2} y^2 + \dots + C_n^k x^{n-k} y^k + \dots + C_n^{n-1} x y^{n-1} + C_n^n y^n. \quad (1b)$$

For  $n = 1, 2, 3, \dots$ , these are familiar expressions,

$$(x + y) = x + y,$$

$$(x + y)^2 = x^2 + 2xy + y^2,$$

$$(x + y)^3 = x^3 + 3x^2y + 3xy^2 + y^3,$$

etc.

The Newton's binomial formula could be established either by directly expanding the brackets, or proven using the mathematical induction.

**Exercise.** Prove the Newton's binomial using the mathematical induction.

**Induction basis.** For  $n = 1$  the statement is a true equality,  $(x + y)^1 = C_1^0 x + C_1^1 y$ . We can also easily prove that it holds for  $n = 2$ . Indeed,  $(x + y)^2 = C_2^0 x^2 + C_2^1 xy + C_2^2 y^2$ .

**Induction hypothesis.** Suppose the equality holds for some  $n \in N$ , that is,

$$(x + y)^n = C_n^0 x^n + C_n^1 x^{n-1}y + C_n^2 x^{n-2}y^2 + \dots + C_n^k x^{n-k}y^k + \dots + C_n^{n-1} x y^{n-1} + C_n^n y^n$$

**Induction step.** We have to prove that it then also holds for the next integer,  $n + 1$ ,

$$(x + y)^{n+1} = C_{n+1}^0 x^{n+1} + C_{n+1}^1 x^n y + C_{n+1}^2 x^{n-1} y^2 + \dots + C_{n+1}^k x^{n+1-k} y^k + \dots + C_{n+1}^n x y^n + C_{n+1}^{n+1} y^{n+1}$$

**Proof.**  $(x + y)^{n+1} = (x + y)^n (x + y) =$

$$(C_n^0 x^n + C_n^1 x^{n-1}y + C_n^2 x^{n-2}y^2 + \dots + C_n^k x^{n-k}y^k + \dots + C_n^{n-1} x y^{n-1} + C_n^n y^n)(x + y) =$$

$$C_n^0 x^{n+1} + C_n^1 x^n y + C_n^2 x^{n-1} y^2 + \dots + C_n^k x^{n-k+1} y^k + \dots + C_n^{n-1} x^2 y^{n-1} + C_n^n x y^n + C_n^0 x^n y + C_n^1 x^{n-1} y^2 + C_n^2 x^{n-2} y^3 + \dots + C_n^k x^{n-k} y^{k+1} + \dots + C_n^{n-1} x y^n + C_n^n y^{n+1} =$$

$$C_n^0 x^{n+1} + (C_n^1 + C_n^0) x^n y + (C_n^2 + C_n^1) x^{n-1} y^2 + \dots + (C_n^k + C_n^{k-1}) x^{n-k+1} y^k + \dots + (C_n^n + C_n^{n-1}) x y^n + C_n^n y^{n+1} =$$

$$C_{n+1}^0 x^{n+1} + C_{n+1}^1 x^n y + C_{n+1}^2 x^{n-1} y^2 + \dots + C_{n+1}^k x^{n+1-k} y^k + \dots + C_{n+1}^n x y^n + C_{n+1}^{n+1} y^{n+1},$$

Where we have used the property of binomial coefficients,  $C_n^k + C_n^{k-1} = C_{n+1}^k$ .

□

## Properties of binomial coefficients

Binomial coefficients are defined by

$$C_n^k = {}_k C_n = \binom{n}{k} = \frac{n!}{k!(n-k)!}$$

Binomial coefficients have clear and important combinatorial meaning.

- There are  $\binom{n}{k}$  ways to choose  $k$  elements from a set of  $n$  elements.
- There are  $\binom{n+k-1}{k}$  ways to choose  $k$  elements from a set of  $n$  if repetitions are allowed.
- There are  $\binom{n+k}{k}$  strings containing  $k$  ones and  $n$  zeros.
- There are  $\binom{n+1}{k}$  strings consisting of  $k$  ones and  $n$  zeros such that no two ones are adjacent.

They satisfy the following identities,

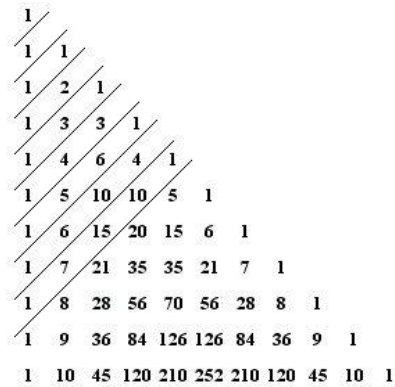
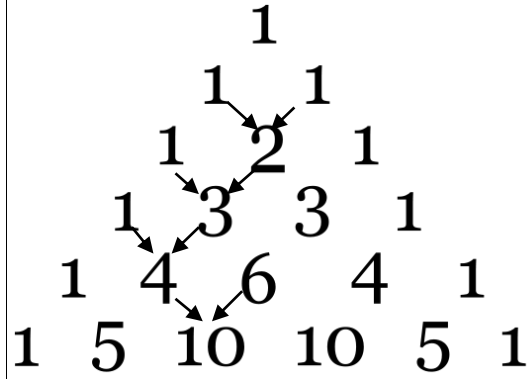
$$C_{n+1}^{k+1} = C_n^k + C_n^{k+1} \Leftrightarrow \binom{n+1}{k+1} = \binom{n}{k} + \binom{n}{k+1}$$

$$C_{n+1}^k = C_n^k + C_n^{k-1} \Leftrightarrow \binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$$

$$\sum_{k=0}^n C_n^k = \sum_{k=0}^n \binom{n}{k} = 2^n$$

## Patterns in the Pascal triangle

$C_n^k = C_{n-1}^{k-1} + C_{n-1}^k$	Fibonacci numbers (sum of the "shallow" diagonals:
-------------------------------------	--



**Exercise.** Find the sum of the top  $n$  rows in the Pascal triangle,

$$\sum_{m=0}^n (\sum_{k=0}^m C_m^k) = 2^{n+1} - 1.$$

### Review of selected homework problems.

**Problem 4.** Using mathematical induction, prove that

$$a. P_n: \sum_{k=1}^n k^2 = 1^2 + 2^2 + 3^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

**Solution.**

Basis:  $P_1: \sum_{k=1}^1 k^2 = 1 = \frac{1 \cdot (1+1) \cdot (2 \cdot 1 + 1)}{6}$

Induction:  $P_n \Rightarrow P_{n+1}$ , where  $P_{n+1}: \sum_{k=1}^{n+1} k^2 = 1^2 + 2^2 + 3^2 + \dots + (n+1)^2 = \frac{(n+1)(n+2)(2n+3)}{6}$

Proof:  $\sum_{k=1}^{n+1} k^2 = \sum_{k=1}^n k^2 + (n+1)^2 = \frac{n(n+1)(2n+1)}{6} + (n+1)^2 = \frac{(n+1)}{6} (n(2n+1) + 6n+6) = \frac{(2n+1)(2n^2+7n+6)}{6} = \frac{(n+1)(n+2)(2n+3)}{6},$

where we used the induction hypothesis,  $P_n$ , to replace the sum of the first  $n$  terms with a formula given by  $P_n$ .  $\square$

$$b. P_n: \sum_{k=1}^n k^3 = 1^3 + 2^3 + 3^3 + \dots + n^3 = \left[ \frac{n(n+1)}{2} \right]^2$$

**Solution.**

Basis:  $P_1: \sum_{k=1}^1 k^3 = 1 = \left[ \frac{1(1+1)}{2} \right]^2$

Induction:  $P_n \Rightarrow P_{n+1}$ , where  $P_{n+1}: \sum_{k=1}^{n+1} k^3 = 1^3 + 2^3 + 3^3 + \dots + (n+1)^3 = \left[ \frac{(n+1)(n+2)}{2} \right]^2$

Proof:  $\sum_{k=1}^{n+1} k^3 = \sum_{k=1}^n k^3 + (n+1)^3 = \left[ \frac{n(n+1)}{2} \right]^2 + (n+1)^3 = \left[ \frac{(n+1)}{2} \right]^2 (n^2 + 4n + 4) = \left[ \frac{(n+1)(n+2)}{2} \right]^2$ , where we used the induction hypothesis,  $P_n$ , to replace the sum of the first  $n$  terms with a formula given by  $P_n$ .  $\square$

c.  $P_n: \sum_{k=1}^n \frac{1}{k^2+k} = \frac{1}{1 \cdot 2} + \frac{1}{2 \cdot 3} + \frac{1}{3 \cdot 4} + \dots + \frac{1}{n \cdot (n+1)} = \frac{n}{n+1}$

**Solution.**

Basis:  $P_1: \sum_{k=1}^1 \frac{1}{k^2+k} = \frac{1}{2} = \frac{1}{1+1}$

Induction:  $P_n \Rightarrow P_{n+1}$ , where  $P_{n+1}: \sum_{k=1}^{n+1} \frac{1}{k^2+k} = \frac{n+1}{n+2}$

Proof:  $\sum_{k=1}^{n+1} \frac{1}{k^2+k} = \sum_{k=1}^n \frac{1}{k^2+k} + \frac{1}{(n+1)(n+2)} = \frac{n}{n+1} + \frac{1}{(n+1)(n+2)} = \frac{n^2+2n+1}{(n+1)(n+2)} = \frac{n+1}{n+2}$ .  $\square$

e.  $P_n: \forall n, \exists k, 5^n + 3 = 4k$

**Solution.**

Basis:  $P_1: n = 1, \exists k, 5^1 + 3 = 8 = 4k \Leftrightarrow k = 2$

Induction:  $P_n \Rightarrow P_{n+1}$ , where  $P_{n+1}: \forall n, \exists q, 5^{n+1} + 3 = 4q$

Proof:  $5^{n+1} + 3 = 5 \cdot 5^n + 3 = 5 \cdot (4k - 3) + 3 = 5 \cdot 4k - 12 + 3 = 4 \cdot (5k - 3)$ .

Where we used the induction hypothesis,  $P_n$ , to replace  $5^n$  with a formula,  $5^n = 4k - 3$ , given by  $P_n$ .  $\square$

e.  $P_n: \forall n \geq 2, \forall x > -1, (1+x)^n \geq 1+nx$

**Solution.**

Basis:  $P_2: \forall x > -1, n = 2, (1 + x)^2 = 1 + 2x + x^2 \geq 1 + 2x$

Induction:  $P_n \Rightarrow P_{n+1}$ , where  $P_{n+1}: \forall n \geq 2, \forall x > -1, (1 + x)^{n+1} \geq 1 + (n + 1)x$

Proof:  $(1 + x)^{n+1} = (1 + x) (1 + x)^n \geq (1 + x)(1 + nx) = 1 + (n + 1)x + x^2 \geq 1 + (n + 1)x. \square$



**Recap: Elements of number theory. Eucleadean algorithm and greatest common divisor.**

**Theorem 1.**  $\forall a, b \in \mathbb{Z}, b > 0, \exists q, r \in \mathbb{Z}, 0 \leq r < b: a = bq + r$

**Proof.** If  $a$  is a multiple of  $b$ , then  $\exists q \in \mathbb{Z}, r = 0: a = bq = bq + r$ . Otherwise,  $\exists q \in \mathbb{Z}: bq < a < b(q + 1)$ . Then,  $\exists r = a - bq \in \mathbb{Z}: 0 < r < b$ , which completes the proof.

**Definition.** A number  $d \in \mathbb{Z}$  is a common divisor of two integer numbers  $a, b \in \mathbb{Z}$ , if  $\exists n, m \in \mathbb{Z}: a = nd, b = md$ .

A set of all positive common divisors of the two numbers  $a, b \in \mathbb{Z}$  is limited because these divisors are smaller than the magnitude of the larger of the two numbers. The greatest of the divisors,  $d$ , is called the greatest common divisor (gcd) and denoted  $d = (a, b)$ .

**Theorem 2.**  $\forall a, b, q, r \in \mathbb{Z}, (a = bq + r) \Rightarrow ((a, b) = (b, r))$

**Proof.** Indeed, if  $d$  is a common divisor of  $a, b \in \mathbb{Z}$ , then  $\exists n, m \in \mathbb{Z}: a = nd, b = md \Rightarrow r = a - bq = (n - mq)d$ . Therefore,  $d$  is also a common divisor of  $b$  and  $r = a - bq$ . Conversely, if  $d'$  is a common divisor of  $b$  and  $r = a - bq$ , then  $\exists n', m' \in \mathbb{Z}: b = m'd, a - bq = n'd \Rightarrow a = (n' + m'q)d'$ , so  $d'$  is a common divisor of  $b$  and  $a$ . Hence, the statement of the theorem is valid for any divisor of  $a, b$ , and for gcd in particular.

**Eucleadean algorithm.** In order to find the greatest common divisor  $d = (a, b)$ , one proceeds iteratively performing successive divisions,

$$a = bq_1 + r_1, (a, b) = (b, r_1)$$

$$b = r_1q_2 + r_2, (b, r_1) = (r_1, r_2)$$

$$r_1 = r_2q_3 + r_3, (r_1, r_2) = (r_2, r_3), \dots$$

$$b > r_1 > r_2 > r_3 > \dots r_n > 0 \Rightarrow \exists n \leq b, r_n = d = (a, b)$$

The last positive remainder,  $r_n$ , in the sequence  $\{r_k\}$  is  $(a, b)$ , the gcd of the numbers  $a$  and  $b$ . Indeed, the Eucleadean algorithm ensures that

$$(a, b) = (b, r_1) = (r_1, r_2) = \cdots = (r_{n-1}, r_n) = (r_n, 0) = r_n$$

**Examples.**

- a.  $(385, 105) = (105, 70) = (70, 35) = (35, 0) = 35$
- b.  $(513, 304) = (304, 209) = (209, 95) = (95, 19) = (19, 0) = 19$

**Corollary.**  $(d = (a, b)) \Rightarrow (\exists k, l \in \mathbb{Z} : d = ka + lb)$

**Proof.** Consider the sequence of remainders in the Eucleadean algorithm,  $r_1 = a - bq_1, r_2 = b - r_1q_2, r_3 = r_1 - r_2q_3, \dots, r_n = r_{n-2} - r_{n-1}q_n$ . Indeed, the successive substitution gives,  $r_1 = a - bq_1, r_2 = b - (a - bq_1)q_2 = k_2a + l_2b, r_3 = r_1 - (k_2a + l_2b)q_3 = k_3a + l_3b, \dots, r_n = r_{n-2} - (k_{n-1}a + l_{n-1}b)q_n = k_na + l_nb = d = (a, b)$ .

**Exercise.** Find the representation  $d = ka + lb$  for the pairs  $(385, 105)$  and  $(513, 304)$  considered in the above examples.

**Continued fraction representation.** Using the Eucleadean algorithm, one can develop a continued fraction representation for rational numbers,

$$\frac{a}{b} = q_0 + \frac{1}{q_1 + \frac{1}{q_2 + \frac{1}{\dots + \frac{1}{q_{n-1} + \frac{1}{q_n}}}}}$$

This is accomplished by successive substitution, which gives,

$$\frac{a}{b} = q_1 + \frac{r_1}{b} = q_1 + \frac{1}{\frac{b}{r_1}}, \frac{b}{r_1} = q_2 + \frac{r_2}{r_1} = q_2 + \frac{1}{\frac{r_1}{r_2}}, \dots, \frac{r_{n-1}}{r_n} = q_{n+1}.$$

**Exercise.** Show the continued fraction representations for  $\frac{385}{105}, \frac{513}{304}, \frac{105}{385}, \frac{304}{513}$ .