

# Contents

<b>1 Boolean Algebra (Logic)</b>	<b>5</b>
1.1 Symbols . . . . .	5
1.1.1 Implication ( $\rightarrow$ ) . . . . .	5
<b>2 Geometry</b>	<b>5</b>
2.1 Trigonometry . . . . .	5
2.2 Line . . . . .	5
2.2.1 General equation . . . . .	5
2.2.2 General equation from two points . . . . .	6
2.2.3 Line inclination from two points . . . . .	6
2.2.4 Check if a point belongs to the line . . . . .	6
2.2.5 Distance from a point to a line . . . . .	6
2.3 Convex and Concave Polygons . . . . .	7
2.3.1 Regular polygon circumradius . . . . .	7
2.3.2 Regular polygon inscribed circle radius . . . . .	8
2.3.3 Area of regular polygons . . . . .	8
2.3.4 Sum of internal angle of a regular polygon . . . . .	8
2.4 Triangle . . . . .	8
2.4.1 Semiperimeter . . . . .	9
2.4.2 Area . . . . .	9
2.4.3 Circumradius . . . . .	9
2.4.4 Inradius . . . . .	9
2.4.5 Length of bisector . . . . .	9
2.4.6 Law of sines . . . . .	9
2.4.7 Law of cosines . . . . .	9
2.4.8 Law of tangents . . . . .	10
2.5 Quadrilaterals . . . . .	10
2.6 Trapezium . . . . .	10
2.6.1 Area, knowing base and height . . . . .	10
2.6.2 Area knowing only sides . . . . .	10
2.7 Sphere . . . . .	11
2.7.1 Equation . . . . .	11
2.7.2 Equation in spherical coordinate system . . . . .	11
2.7.3 Area . . . . .	11
2.7.4 Volume . . . . .	11
2.8 Cube . . . . .	12
2.8.1 Facial & Body diagonal . . . . .	12
2.8.2 Area . . . . .	12

2.8.3	Volume . . . . .	12
2.8.4	Circumscribed sphere . . . . .	12
2.8.5	Inscribed Sphere . . . . .	12
2.8.6	Tangent Sphere . . . . .	13
2.9	Parallelepiped . . . . .	13
2.9.1	Area delimited by two vectors . . . . .	13
2.9.2	Volume . . . . .	13
2.10	Cylinder . . . . .	13
2.10.1	Area . . . . .	14
2.10.2	Volume . . . . .	14
2.11	Cone . . . . .	14
2.11.1	Area . . . . .	14
2.11.2	Volume . . . . .	14
2.12	Truncated Cone . . . . .	14
2.12.1	Area . . . . .	15
2.12.2	Volume . . . . .	15
2.13	Dot product . . . . .	15
2.14	Magnitude . . . . .	15
<b>3</b>	<b>Algebra</b>	<b>15</b>
3.1	Absolute Value . . . . .	15
3.1.1	Definition . . . . .	15
3.1.2	Properties and Theorems . . . . .	16
3.2	Sums . . . . .	16
<b>4</b>	<b>Graphs</b>	<b>17</b>
4.0.1	Bipartite Graph . . . . .	17
4.1	Topological Sorting . . . . .	17
4.2	Strongly Connected Components . . . . .	17
4.3	Minimum spanning tree . . . . .	18
4.3.1	Properties . . . . .	18
4.4	Eulerian path . . . . .	18
4.5	Network . . . . .	19
4.6	Flow network . . . . .	19
4.6.1	Properties . . . . .	19
4.7	Prüfer Code . . . . .	19
4.8	Prüfer's Sequence . . . . .	20

<b>5</b>	<b>Trees</b>	<b>21</b>
5.1	Centroid . . . . .	21
5.2	Centroid decomposition . . . . .	21
<b>6</b>	<b>Number Theory</b>	<b>21</b>
6.1	Fermat's Theorems and Lemmas . . . . .	21
6.2	Goldbach's Conjecture . . . . .	22
6.3	Linear Diophantine Equations . . . . .	22
6.3.1	Solution(s) . . . . .	22
6.4	Wilson's theorem . . . . .	23
6.5	Fundamental theorem of arithmetic . . . . .	23
6.5.1	LCM and GCD . . . . .	24
6.6	Taking modulo at the exponent . . . . .	24
<b>7</b>	<b>Identities</b>	<b>24</b>
<b>8</b>	<b>Linear Algebra</b>	<b>24</b>
8.1	Matrix Multiplication . . . . .	24
<b>9</b>	<b>Probability Theory</b>	<b>25</b>
9.1	Discrete distributions . . . . .	25
9.1.1	Binomial distribution . . . . .	25
9.1.2	First success distribution . . . . .	26
9.1.3	Poisson distribution . . . . .	26
9.2	Continuous distributions . . . . .	26
9.2.1	Uniform distribution . . . . .	26
9.2.2	Exponential distribution . . . . .	26
9.2.3	Normal distribution . . . . .	27
9.3	Markov chains . . . . .	27
9.3.1	Stationary distribution . . . . .	27
9.3.2	Ergodicity . . . . .	28
9.3.3	Absorption . . . . .	28
<b>10</b>	<b>Polynomial</b>	<b>28</b>
10.1	Bhaskara . . . . .	28
10.2	Pascal's Triangle . . . . .	28
10.3	N-th first terms of P-th column in Pascal Triangle . . . . .	28
10.4	Number of odd numbers in the N-th line of pascal triangle . . . . .	28

<b>11 Trees</b>	<b>29</b>
11.1 Heavy-Light Decomposition . . . . .	29
<b>12 Combinatorics</b>	<b>29</b>
12.1 Binomial Coefficients . . . . .	29
12.1.1 Odd numbers in the $i$ -th line . . . . .	30
12.1.2 Properties . . . . .	30
12.2 4 fundamental problems of distribution . . . . .	31
12.2.1 $N$ equal balls in $K$ equal boxes . . . . .	31
12.2.2 $N$ equal balls in $K$ distinct boxes . . . . .	31
12.2.3 $N$ distinct balls in $K$ equal boxes . . . . .	32
12.2.4 $N$ distinct balls in $K$ distinct boxes . . . . .	32
<b>13 Bitwise</b>	<b>32</b>
13.1 Binary to gray code . . . . .	32
13.2 Gray code to binary . . . . .	32
<b>14 Game Theory</b>	<b>32</b>
14.1 Impartial Games . . . . .	32
14.2 Sprague-Grundy Theorem . . . . .	33
14.3 Nim variation Subtract game . . . . .	34
<b>15 Group Theory</b>	<b>34</b>
15.1 Permutations . . . . .	34
15.1.1 Odd permutations . . . . .	34
15.1.2 Even permutations . . . . .	34
<b>16 Others</b>	<b>34</b>
16.1 Unimodal Functions . . . . .	34
16.2 Critérios de divisibilidade . . . . .	35
16.2.17 . . . . .	35
16.2.211 . . . . .	36
16.2.313 . . . . .	36
16.2.417 . . . . .	36
16.2.519 . . . . .	37
16.2.623 . . . . .	37

# 1 Boolean Algebra (Logic)

## 1.1 Symbols

### 1.1.1 Implication ( $\rightarrow$ )

$$a \rightarrow b \Leftrightarrow \neg a \vee b \quad (1)$$

# 2 Geometry

## 2.1 Trigonometry

$$\sin(v + w) = \sin v \cos w + \cos v \sin w \quad (2)$$

$$\cos(v + w) = \cos v \cos w - \sin v \sin w \quad (3)$$

$$\tan(v + w) = \frac{\tan v + \tan w}{1 - \tan v \tan w} \quad (4)$$

$$\sin v + \sin w = 2 \sin \frac{v + w}{2} \cos \frac{v - w}{2} \quad (5)$$

$$\cos v + \cos w = 2 \cos \frac{v + w}{2} \cos \frac{v - w}{2} \quad (6)$$

$$(V + W) \tan(v - w)/2 = (V - W) \tan(v + w)/2 \quad (7)$$

where  $V, W$  are lengths of sides opposite angles  $v, w$ .

$$\begin{aligned} a \cos x + b \sin x &= r \cos(x - \phi) \\ a \sin x + b \cos x &= r \sin(x + \phi) \end{aligned} \quad (8)$$

where  $r = \sqrt{a^2 + b^2}$ ,  $\phi = \text{atan2}(b, a)$ .

## 2.2 Line

### 2.2.1 General equation

$$ax + by + c = 0 \quad (9)$$

Note that a same line can have multiple representations (just multiply the equation by any real number), so to make each line have a single equation divide everything by  $a$ , or  $b$  if  $a$  is zero.

### 2.2.2 General equation from two points

Let  $P$  and  $Q$  be the points that define the line.

$$\begin{aligned}a &= P_y - Q_y \\b &= Q_x - P_x \\c &= P_x Q_y - P_y Q_x\end{aligned}$$

### 2.2.3 Line inclination from two points

Let  $P$  and  $Q$  be two points that belongs to the line, such that  $P_x < Q_x$  the inclination  $m$  or angular coefficient is given by:

$$m = \frac{Q_y - P_y}{Q_x - P_x} \quad (10)$$

### 2.2.4 Check if a point belongs to the line

Let  $r$  be a line such that  $ax + by + c = 0$  and  $P$  a point.  $P \in r$  if and only if :

$$aP_x + bP_y + c = 0$$

### 2.2.5 Distance from a point to a line

The distance from a point  $P$  and a line  $r$  is defined as the shortest distance possible between every point that belongs to  $r$  and  $P$ . Such distance will be the distance from  $P$  and the intersection between  $r$  and the orthogonal projection from  $P$  to  $r$ , and can be found by:

$$\frac{|aP_x + bP_y + c|}{\sqrt{a^2 + b^2}}$$

The coordinates of the point Q are given by:

$$Q_x = \frac{b(bP_x - aP_y) - ac}{a^2 + b^2}$$
$$Q_y = \frac{a(-bP_x + aP_y) - bc}{a^2 + b^2}$$

2.3 Convex and Concave Polygons

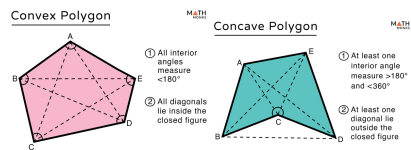
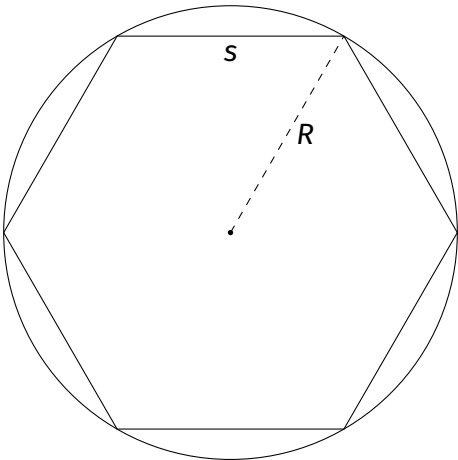


Figure 1: Convex Polygon      Figure 2: Concave Polygon

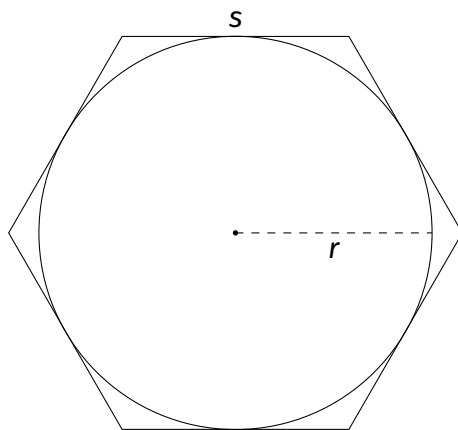
Figure 3: Two Types of Polygons

2.3.1 Regular polygon circumradius



$$R = \frac{S}{2} \csc \frac{\pi}{n}$$

### 2.3.2 Regular polygon inscribed circle radius



$$r = R \cos \frac{\pi}{n}$$

### 2.3.3 Area of regular polygons

- Let  $n$  be the number of sides of the regular polygon, the area can be found using one of the values below:
  - the length of one of the sides ( $s$ )
  - apothem, the radius of the inscribed circle ( $r$ )
  - the radius of the circumscribed circle ( $R$ )

$$A = \frac{1}{2} nrs = \frac{1}{4} ns^2 \cot \frac{\pi}{n} = nr^2 \tan \frac{\pi}{n} = \frac{1}{2} nR^2 \sin \frac{2\pi}{n}$$

### 2.3.4 Sum of internal angle of a regular polygon

A regular polygon with  $n$  sides have  $(n - 2)180$  degrees as sum of it's internal angle.

## 2.4 Triangle

Let the length of the sides of the triangle be  $a$ ,  $b$ ,  $c$ .



**2.4.1 Semiperimeter**

Let  $p$  be the semiperimeter defined as:

$$p = \frac{a + b + c}{2} \quad (11)$$

**2.4.2 Area**

Let  $A$  be the area defined as:

$$\sqrt{p(p - a)(p - b)(p - c)} \quad (12)$$

**2.4.3 Circumradius**

$$R = \frac{abc}{4A} \quad (13)$$

**2.4.4 Inradius**

$$r = \frac{A}{p} \quad (14)$$

**2.4.5 Length of bisector**

$$s_a = \sqrt{bc \left[ 1 - \left( \frac{a}{b+c} \right)^2 \right]} \quad (15)$$

**2.4.6 Law of sines**

$$\frac{\sin \alpha}{a} = \frac{\sin \beta}{b} = \frac{\sin \gamma}{c} = \frac{1}{2R} \quad (16)$$

**2.4.7 Law of cosines**

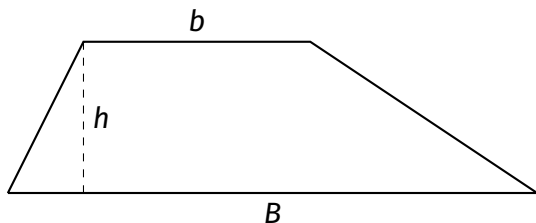
$$a^2 = b^2 + c^2 - 2bc \cos \alpha \quad (17)$$

**2.4.8 Law of tangents**

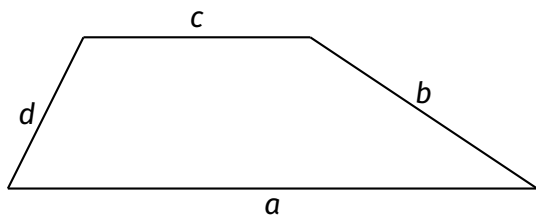
$$\frac{a+b}{a-b} = \frac{\tan \frac{\alpha+\beta}{2}}{\tan \frac{\alpha-\beta}{2}} \quad (18)$$

**2.5 Quadrilaterals**

Let it's sides lenght be  $a, b, c, d$

**2.6 Trapezium****2.6.1 Area, knowing base and height**

$$A = \frac{(B+b)h}{2}$$

**2.6.2 Area knowing only sides**

$$e = \frac{d^2 - b^2 + a^2 - 2ac + c^2}{2a - 2c}$$

$$h = \sqrt{d^2 - e^2}$$

$$A = \frac{h(a+c)}{2}$$

## 2.7 Sphere

### 2.7.1 Equation

$$(x - x_0)^2 + (y - y_0)^2 + (z - z_0)^2 = r^2$$

### 2.7.2 Equation in spherical coordinate system

$r$  is the radius,  $\theta$  is an angle that goes from 0 to  $2\pi$ , and  $\varphi$  is an angle that goes from 0 to  $\pi$ .

$$\begin{aligned}x &= x_0 + r \cos \theta \sin \varphi \\y &= y_0 + r \sin \theta \sin \varphi \\z &= z_0 + r \cos \varphi\end{aligned}$$

### 2.7.3 Area

$A = 4\pi r^2$ , where  $r$  is the radius, comes from :

$$A = \int_0^\pi \int_0^{2\pi} r^2 \sin(\varphi) d\theta d\varphi$$

### 2.7.4 Volume

$$V = \frac{4}{3}\pi r^3$$

comes from :

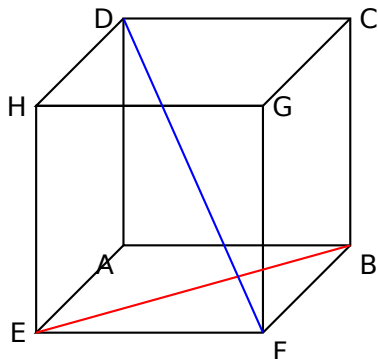
$$V = \int_0^R \int_0^\pi \int_0^{2\pi} r^2 \sin(\varphi) d\theta d\varphi dR$$

## 2.8 Cube

### 2.8.1 Facial & Body diagonal

Facial diagonal join two vertices at the same face.

Body diagonal join two vertices from opposite faces.



$$\text{Facial diagonal} = L\sqrt{2}$$

$$\text{Body diagonal} = L\sqrt{3}$$

### 2.8.2 Area

$$A = 6L^2$$

### 2.8.3 Volume

$$V = L^3$$

### 2.8.4 Circumscribed sphere

Pass through the 8 vertices, radius equal to  $L(\frac{\sqrt{3}}{2})$ .

### 2.8.5 Inscribed Sphere

Tangent to the 6 faces, radius equal to  $\frac{L}{2}$ .

**2.8.6 Tangent Sphere**

Tangent to the edges, radius equal to  $\frac{L}{\sqrt{2}}$ .

**2.9 Parallelepiped**

Let it be defined by three linear independent vectors

$$\vec{u}, \vec{v}, \vec{w}$$

**2.9.1 Area delimited by two vectors**

$$A = |\vec{u} \times \vec{v}|$$

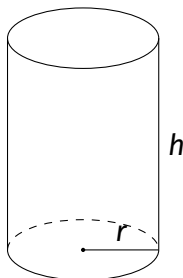
**2.9.2 Volume**

$$V = |(\vec{u} \times \vec{v}) \cdot \vec{w}|,$$

$$(\vec{u} \times \vec{v}) \cdot \vec{w} = \det \begin{bmatrix} u_x & u_y & u_z \\ v_x & v_y & v_z \\ w_x & w_y & w_z \end{bmatrix}$$

or if you know the sides  $a, b, c$ , and the angles  $\alpha, \beta, \gamma$ :

$$V = abc \sqrt{1 + 2 \cos \alpha \cos \beta \cos \gamma - \cos^2 \alpha - \cos^2 \beta - \cos^2 \gamma}$$

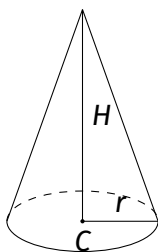
**2.10 Cilinder**

**2.10.1 Area**

$$A = 2\pi rh + 2\pi r^2 = 2\pi r(h + r),$$

**2.10.2 Volume**

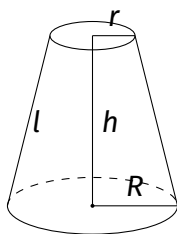
$$A = \pi r^2 h$$

**2.11 Cone****2.11.1 Area**

$$A = \pi r^2 + \pi r\sqrt{r^2 + H^2}$$

**2.11.2 Volume**

$$V = \frac{1}{3}\pi r^2 H$$

**2.12 Truncated Cone**

**2.12.1 Area**

$$l = \sqrt{h^2 + r^2}$$

$$A = \pi(R + r)l + \pi(R^2 + r^2)$$

**2.12.2 Volume**

$$V = \frac{1}{3}\pi h(R^2 + Rr + r^2),$$

**2.13 Dot product**

The dot product of vectors  $\mathbf{u}$  and  $\mathbf{v}$  in  $n$  dimensions is given by:

$$\langle \mathbf{u}, \mathbf{v} \rangle = u_1 \cdot v_1 + u_2 \cdot v_2 + \dots + u_n \cdot v_n$$

**2.14 Magnitude**

The magnitude of a vector  $\mathbf{v}$  in  $n$  dimensions is given by:

$$|\mathbf{v}| = \sqrt{v_1^2 + v_2^2 + \dots + v_n^2}$$

The dot product of two Euclidean vectors  $\mathbf{u}$  and  $\mathbf{v}$  is defined by

$$\langle \mathbf{u}, \mathbf{v} \rangle = |\mathbf{u}| \cdot |\mathbf{v}| \cdot \cos(\theta)$$

**3 Algebra****3.1 Absolute Value****3.1.1 Definition**

The absolute value of  $x$ , denoted by  $|x|$  is defined by:

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases} \quad (19)$$

**3.1.2 Properties and Theorems**

$$|x| < a \iff -a < x < a, \text{ where } a > 0 \quad (20)$$

$$|x| \leq a \iff -a \leq x \leq a, \text{ where } a > 0 \quad (21)$$

$$|x| > a \iff (x > a) \vee (x < -a), \text{ where } a > 0 \quad (22)$$

$$|x| \geq a \iff (x \geq a) \vee (x \leq -a), \text{ where } a > 0 \quad (23)$$

$$|ab| = |a| \cdot |b|, \text{ where } a, b \in \mathbb{R} \quad (24)$$

$$\left| \frac{a}{b} \right| = \frac{|a|}{|b|}, \text{ where } a, b \in \mathbb{R}, \text{ and } b \neq 0 \quad (25)$$

$$|a + b| \leq |a| + |b|, \text{ where } a, b \in \mathbb{R} \quad (26)$$

$$|a - b| \leq |a| + |b|, \text{ where } a, b \in \mathbb{R} \quad (27)$$

$$|a| - |b| \leq |a - b|, \text{ where } a, b \in \mathbb{R} \quad (28)$$

**3.2 Sums**

$$\begin{aligned} c^a + c^{a+1} + \dots + c^b &= \frac{c^{b+1} - c^a}{c - 1}, c \neq 1 \\ 1 + 2 + 3 + \dots + n &= \frac{n(n+1)}{2} \\ 1^2 + 2^2 + 3^2 + \dots + n^2 &= \frac{n(2n+1)(n+1)}{6} \\ 1^3 + 2^3 + 3^3 + \dots + n^3 &= \frac{n^2(n+1)^2}{4} \\ 1^4 + 2^4 + 3^4 + \dots + n^4 &= \frac{n(n+1)(2n+1)(3n^2+3n-1)}{30} \end{aligned} \quad (29)$$



## 4 Graphs

### 4.0.1 Bipartite Graph

Bipartite Graph is a special graph with the following characteristics: the set of vertices  $V$  can be partitioned into two disjoint sets  $V_1$  and  $V_2$  and all undirected edges  $(u, v) \in E$  have the property that  $u \in V_1$  and  $v \in V_2$ . This makes a Bipartite Graph free from odd-length cycle. Not that by this definition is possible to have isolated vertices.

### 4.1 Topological Sorting

**Definition:** You are given a **directed** graph with  $n$  vertices and  $m$  edges. You have to find an order of the vertices, so that every edge leads from the vertex with a smaller index to a vertex with a larger one.

Topological order can be non-unique !

A Topological order **may not exist** at all. It only exists, if the directed graph **contains no cycles**. Otherwise because there is a contradiction: if there is a cycle containing the vertices  $a$  and  $b$ , then  $a$  needs to have a smaller index than  $b$  (since you can reach  $b$  from  $a$ ) and also a bigger one (as you can reach  $a$  from  $b$ ). Every acyclic directed graph contains at least one topological order.

### 4.2 Strongly Connected Components

You are given a directed graph  $G$  with vertices  $V$  and edges  $E$ . It is possible that there are loops and multiple edges. Let's denote  $n$  as number of vertices and  $m$  as number of edges in  $G$ .

Strongly connected component is a maximal subset of vertices  $C$  such that any two vertices of this subset are reachable from each other, i.e. for any  $u, v \in C$ :

$$u \mapsto v, v \mapsto u$$

where  $\mapsto$  means reachability, i.e. existence of the path from first vertex to the second.

The most important property of the condensation graph is that it is a **DAG**. Indeed, suppose that there is an edge between  $C$  and  $C'$ , let's prove that there is no edge from  $C'$  to  $C$ . Suppose that  $C' \mapsto C$ . Then there are two vertices  $u' \in C$  and  $v' \in C'$  such that  $v' \mapsto u'$ . But since  $u$  and  $u'$  are in the same strongly connected component then there is a path between them; the same for  $v$  and  $v'$ . As a result, if we join these paths we have that  $v \mapsto u$  and at the same time  $u \mapsto v$ . Therefore  $u$  and  $v$  should be at the same strongly connected component, so this is contradiction. This completes the proof.

## 4.3 Minimum spanning tree

### 4.3.1 Properties

- A minimum spanning tree of a graph is unique, if the weight of all the edges are distinct. Otherwise, there may be multiple minimum spanning trees. (Specific algorithms typically output one of the possible minimum spanning trees).
- Minimum spanning tree is also the tree with minimum product of weights of edges. (It can be easily proved by replacing the weights of all edges with their logarithms)

## 4.4 Eulerian path

A Eulerian path is a path in a graph that passes through all of its edges exactly once. A Eulerian cycle is a Eulerian path that is a cycle.

An Eulerian cycle exists if and only if the degrees of all vertices are even

And an Eulerian path exists if and only if the number of vertices with odd degrees is two (or zero, in the case of the existence of a Eulerian cycle).

## 4.5 Network

A **network** is a directed graph  $G$  with vertex  $V$  and edges  $E$  combined with a function  $c$ , which assigns each edge  $e \in E$  a non-negative integer value, the *capacity* of  $e$ .

## 4.6 Flow network

Is a **network** with two vertices labeled as **source** and **sink**.

### 4.6.1 Properties

- The flow of an edge cannot exceed the capacity

$$f(e) \leq c(e)$$

- And the sum of the incoming flow of a vertex  $u$  has to be equal to the sum of the outgoing flow of  $u$  except in the source and sink vertices.
- The source vertex  $s$  only has an outgoing flow, and the sink vertex  $t$  has only incoming flow.

## 4.7 Prüfer Code

The Prüfer code is a way of encoding a labeled tree with  $n$  vertices using a sequence of  $n - 2$  integers in the interval  $[0; n - 1]$ . This encoding also acts as a bijection between all spanning trees of a complete graph and the numerical sequences.

The Prüfer code is constructed as follows. We will repeat the following procedure  $n - 2$  times: we select the leaf of the tree with the smallest number, remove it from the tree, and write down the number of the vertex that was connected to it. After  $n - 2$  iterations there will only remain 2 vertices, and the algorithm ends.

Thus the Prüfer code for a given tree is a sequence of  $n - 2$  numbers, where each number is the number of the connected vertex, i.e. this number is in the interval  $[0, n - 1]$ .

The algorithm for computing the Prüfer code can be implemented easily with  $O(n \log n)$  time complexity, simply by using a data structure to extract the minimum (for instance `set` or `priority_queue` in C++), which contains a list of all the current leafs.

After constructing the Prüfer code two vertices will remain. One of them is the highest vertex  $n - 1$ , but nothing else can be said about the other one.

Each vertex appears in the Prüfer code exactly a fixed number of times - its degree minus one. This can be easily checked, since the degree will get smaller every time we record its label in the code, and we remove it once the degree is 1. For the two remaining vertices this fact is also true.

## 4.8 Prüfer's Sequence

The Prüfer sequence is a bijection between labeled trees with  $n$  vertices and sequences with  $n - 2$  numbers from 1 to  $n$ . To get the sequence from the tree:

- While there are more than 2 vertices, remove the leaf with smallest label and append it's neighbour to the end of the sequence.

To get the tree from the sequence:

- The degree of each vertex is 1 more than the number of occurrences of that vertex in the sequence. Compute the degree  $d$ , then do the following: for every value  $x$  in the sequence (in order), find the vertex with smallest label  $y$  such that  $d(y) = 1$  and add an edge between  $x$  and  $y$ , and also decrease their degrees by 1. At the end of this procedure, there will be two vertices left with degree 1; add an edge between them.

## 5 Trees

### 5.1 Centroid

A centroid of a tree is defined as a node such that when the tree is rooted at it, no other nodes have a subtree of size greater than  $\frac{N}{2}$ .

Every tree have a centroid.

### 5.2 Centroid decomposition

The centroid decomposition of a tree is another tree defined recursively as:

- Its root is the centroid of the original tree.
- Its children are the centroid of each tree resulting from the removal of the centroid from the original tree.

Properties:

- A vertex belongs to the component of all its ancestors.

## 6 Number Theory

### 6.1 Fermat's Theorems and Lemmas

Let  $p$  be a prime number and  $a, b \in \mathbb{Z}$ :

$$a^p \equiv a \pmod{p} \quad (30)$$

$$a^{p-1} \equiv 1 \pmod{p} \quad (31)$$

$$(a + b)^p \equiv a^p + b^p \pmod{p} \quad (32)$$

$$a^{-1} \equiv a^{p-2} \pmod{p} \quad (33)$$

## 6.2 Goldbach's Conjecture

"Every pair number greater than 2 can be written as the sum of two primes"

Valid for every integer in range from 4 to  $10^{18}$ , but without proof

For an odd  $x$  number it can be written as the sum of two primes if  $x - 2$  is also prime, or three primes, 3 and the two primes that results in  $x - 3$ .

## 6.3 Linear Diophantine Equations

A Linear Diophantine Equation (in two variables) is an equation of the general form:

$$ax + by = c$$

Where  $a, b, c$  are given integers, and  $x, y$  are unknown integers.

If  $a = b = 0$ , we have infinite solutions if  $c = 0$ , and 0 otherwise.

### 6.3.1 Solution(s)

Let  $g = \gcd(a, b)$  such that  $ax_g + by_g = g$ , then we only have a solution if and only if  $g \mid c$ , and if it have a solution it have infinite.

The solutions will be of the form :

$$\begin{aligned} x_0 &= x_g \cdot \frac{c}{g}, y_0 = y_g \cdot \frac{c}{g}. \\ a \cdot x_0 + b \cdot y_0 &= c \end{aligned} \quad (34)$$

With the initial solution, we can can find every solution, with :

$$x = x_0 + k \cdot \frac{b}{g}, y = y_0 - k \cdot \frac{a}{g} \quad (35)$$

To find the solution that minimize  $x + y$  we use the fact that:

$$x' = x + k \cdot \frac{b}{g},$$

$$y' = y - k \cdot \frac{a}{g}.$$

Note that

$x + y$  change as follows:

$$x' + y' = x + y + k \cdot \left( \frac{b}{g} - \frac{a}{g} \right) = x + y + k \cdot \frac{b - a}{g}$$

If  $a < b$ , we need to select smallest possible value of  $k$ . If  $a > b$ , we need to select the largest possible value of  $k$ . If  $a = b$ , all solution will have the same sum  $x + y$ .

## 6.4 Wilson's theorem

Wilson's theorem states that a natural number  $n > 1$  is a **prime number** if and only if the product of all the positive integers less than  $n$  is one less than a multiple of  $n$ .

That is :

$$(n - 1)! \equiv -1 \pmod{n} \quad (36)$$

In other words, any integer  $n > 1$  is a prime number if, and only if,  $(n - 1)! + 1$  is divisible by  $n$

## 6.5 Fundamental theorem of arithmetic

Every integer greater than 1 can be represented uniquely as a product of prime numbers, up to the order of the factors.

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} \quad (37)$$

### 6.5.1 LCM and GCD

$$\begin{aligned}
 a &= p_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k} \\
 b &= p_1^{\beta_1} p_2^{\beta_2} \dots p_k^{\beta_k} \\
 (a, b) &= p_1^{\min \alpha_1, \beta_1} p_2^{\min \alpha_2, \beta_2} \dots p_k^{\min \alpha_k, \beta_k} \\
 [a, b] &= p_1^{\max \alpha_1, \beta_1} p_2^{\max \alpha_2, \beta_2} \dots p_k^{\max \alpha_k, \beta_k}
 \end{aligned} \tag{38}$$

## 6.6 Taking modulo at the exponent

If  $\gcd(a, m) = 1$  then:

$$a^m \equiv a^{n \bmod \varphi(m)} \pmod{m} \tag{39}$$

## 7 Identities

$$\begin{aligned}
 \sum_{i=1}^n i &= \frac{n(n+1)}{2} \\
 \sum_{i=1}^n i^2 &= \frac{n(n+1)(2n+1)}{6} \\
 \sum_{i=1}^n i^3 &= \frac{n^2(n+1)^2}{4} = \left( \sum_{i=1}^n i \right)^2
 \end{aligned}$$

## 8 Linear Algebra

### 8.1 Matrix Multiplication

Let  $A \in \mathbb{R}^{m \times n}$  and  $B \in \mathbb{R}^{n \times p}$ . The product  $C = AB \in \mathbb{R}^{m \times p}$  is defined as:

$$c_{ij} = \sum_{k=1}^n a_{ik} b_{kj}$$



for  $i = 1, \dots, m$  and  $j = 1, \dots, p$ .

Matrix multiplication is associative and distributive, but not commutative:  $AB \neq BA$  in general.

## 9 Probability Theory

Let  $X$  be a **discrete random** variable with probability  $p_X(x)$  of assuming the value  $x$ .

It will then have an **expected value** (mean)

$$\mu = \mathbb{E}(X) = \sum_x x p_X(x)$$

**Variance**  $\sigma^2 = V(X) = \mathbb{E}(X^2) - (\mathbb{E}(X))^2 = \sum_x (x - \mathbb{E}(X))^2 p_X(x)$  where  $\sigma$  is the standard deviation.

If  $X$  is instead continuous it will have a probability density function  $f_X(x)$  and the sums above will instead be integrals with  $p_X(x)$  replaced by  $f_X(x)$ .

Expectation is linear:

$$\mathbb{E}(aX + bY) = a\mathbb{E}(X) + b\mathbb{E}(Y)$$

For independent  $X$  and  $Y$ ,

$$V(aX + bY) = a^2 V(X) + b^2 V(Y).$$

### 9.1 Discrete distributions

#### 9.1.1 Binomial distribution

The number of successes in  $n$  independent yes/no experiments, each which yields success with probability  $p$  is  $\text{Bin}(n, p)$ ,  $n = 1, 2, \dots$ ,  $0 \leq p \leq 1$ .

$$p(k) = \binom{n}{k} p^k (1-p)^{n-k}$$

$$\mu = np, \sigma^2 = np(1-p)$$

$\text{Bin}(n, p)$  is approximately  $\text{Po}(np)$  for small  $p$ .

### 9.1.2 First success distribution

The number of trials needed to get the first success in independent yes/no experiments, each which yields success with probability  $p$  is  $Fs(p)$ ,  $0 \leq p \leq 1$ .

$$p(k) = p(1 - p)^{k-1}, k = 1, 2, \dots$$

$$\mu = \frac{1}{p}, \sigma^2 = \frac{1 - p}{p^2}$$

### 9.1.3 Poisson distribution

The number of events occurring in a fixed period of time  $t$  if these events occur with a known average rate  $\kappa$  and independently of the time since the last event is  $Po(\lambda)$ ,  $\lambda = t\kappa$ .

$$p(k) = e^{-\lambda} \frac{\lambda^k}{k!}, k = 0, 1, 2, \dots$$

$$\mu = \lambda, \sigma^2 = \lambda$$

## 9.2 Continuous distributions

### 9.2.1 Uniform distribution

If the probability density function is constant between  $a$  and  $b$  and 0 elsewhere it is  $U(a, b)$ ,  $a < b$ .

$$f(x) = \begin{cases} \frac{1}{b-a} & a < x < b \\ 0 & \text{otherwise} \end{cases}$$

$$\mu = \frac{a+b}{2}, \sigma^2 = \frac{(b-a)^2}{12}$$

### 9.2.2 Exponential distribution

The time between events in a Poisson process is  $Exp(\lambda)$ ,  $\lambda > 0$ .

$$f(x) = \begin{cases} \lambda e^{-\lambda x} & x \geq 0 \\ 0 & x < 0 \end{cases}$$

$$\mu = \frac{1}{\lambda}, \sigma^2 = \frac{1}{\lambda^2}$$

### 9.2.3 Normal distribution

Most real random values with mean  $\mu$  and variance  $\sigma^2$  are well described by  $N(\mu, \sigma^2)$ ,  $\sigma > 0$ .

$$f(x) = \frac{1}{\sqrt{2\pi\sigma^2}} e^{-\frac{(x-\mu)^2}{2\sigma^2}}$$

If  $X_1 \sim N(\mu_1, \sigma_1^2)$  and  $X_2 \sim N(\mu_2, \sigma_2^2)$  then

$$aX_1 + bX_2 + c \sim N(\mu_1 + \mu_2 + c, a^2\sigma_1^2 + b^2\sigma_2^2)$$

## 9.3 Markov chains

A *Markov chain* is a discrete random process with the property that the next state depends only on the current state. Let  $X_1, X_2, \dots$  be a sequence of random variables generated by the Markov process. Then there is a transition matrix  $\mathbf{P} = (p_{ij})$ , with  $p_{ij} = \Pr(X_n = i | X_{n-1} = j)$ , and  $\mathbf{p}^{(n)} = \mathbf{P}^n \mathbf{p}^{(0)}$  is the probability distribution for  $X_n$  (i.e.,  $p_i^{(n)} = \Pr(X_n = i)$ ), where  $\mathbf{p}^{(0)}$  is the initial distribution.

### 9.3.1 Stationary distribution

is a stationary distribution if  $\pi = \mathbf{P} \pi$ . If the Markov chain is *irreducible* (it is possible to get to any state from any state), then  $\pi_i = \frac{1}{\mathbb{E}(T_i)}$  where  $\mathbb{E}(T_i)$  is the expected time between two visits in state  $i$ .  $\pi_j / \pi_i$  is the expected number of visits in state  $j$  between two visits in state  $i$ . For a connected, undirected and non-bipartite graph, where the transition probability is uniform among all neighbors,  $\pi_i$  is proportional to node  $i$ 's degree.

### 9.3.2 Ergodicity

A Markov chain is *ergodic* if the asymptotic distribution is independent of the initial distribution. A finite Markov chain is ergodic iff it is irreducible and *aperiodic* (i.e., the gcd of cycle lengths is 1).  $\lim_{k \rightarrow \infty} \mathbf{P}^k = \mathbf{1}\pi$ .

### 9.3.3 Absorption

A Markov chain is an A-chain if the states can be partitioned into two sets **A** and **G**, such that all states in **A** are absorbing ( $p_{ii} = 1$ ), and all states in **G** leads to an absorbing state in **A**. The probability for absorption in state  $i \in \mathbf{A}$ , when the initial state is  $j$ , is  $a_{ij} = p_{ij} + \sum_{k \in \mathbf{G}} a_{ik} p_{kj}$ . The expected time until absorption, when the initial state is  $i$ , is  $t_i = 1 + \sum_{k \in \mathbf{G}} p_{ki} t_k$ .

## 10 Polynomial

### 10.1 Bhaskara

$$x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a} \quad (40)$$

### 10.2 Pascal's Triangle

### 10.3 N-th first terms of P-th column in Pascal Triangle

$$\binom{p}{p} + \binom{p+1}{p} + \dots + \binom{p+n}{p} = \binom{p+n+1}{p+1} \quad (41)$$

### 10.4 Number of odd numbers in the N-th line of pascal triangle

There is a mathematical relation which gives the number of odd numbers in the N-th row of pascal's triangle. The theorem states that the number of odd numbers in N-th row

is equal to 2 raised to the number of ones in the binary representation of  $N$ .

## 11 Trees

### 11.1 Heavy-Light Decomposition

Heavy-Light Decomposition (HLD) is a technique to decompose a tree into a set of disjoint paths. This technique is particularly useful to deal with problems which require us to do some path-queries in a tree which seemingly complicated but easy enough to be solved for a line-graph. The idea is to decompose the tree into several paths (line-graph) of disjoint vertices. Then, each path-query in the original tree might be able to be answered by queries in one or more of those paths.

An edge  $(a, b)$  is heavy if and only if  $\text{size}(b) \geq \text{size}(a)/2$ ; otherwise, it is light

## 12 Combinatorics

### 12.1 Binomial Coefficients

Binomial coefficients  $\binom{n}{k}$  are the number of ways to select a set of  $k$  elements from  $n$  different elements without taking into account the order of arrangement of these elements (i.e., the number of unordered sets).

Binomial coefficients are also the coefficients in the expansion of  $(a + b)^n$  (so-called binomial theorem):

$$(a + b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \dots + \binom{n}{k}a^{n-k}b^k + \dots + \binom{n}{n}b^n$$

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

**Recurrence** formula\*\* (which is associated with the famous "Pascal's Triangle"):

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$$

### 12.1.1 Odd numbers in the i-th line

O número de elementos ímpares na  $n$ -ésima linha do triângulo de pascal é  $2^c$ , onde  $c$  é o número de bits na representação binária de  $n$ .

### 12.1.2 Properties

Binomial coefficients have many different properties. Here are the simplest of them:

- Symmetry rule:

$$\binom{n}{k} = \binom{n}{n-k}$$

- Factoring in:

$$\binom{n}{k} = \frac{n}{k} \binom{n-1}{k-1}$$

- Sum over  $k$ :

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

- Sum over  $n$ :

$$\sum_{m=0}^n \binom{m}{k} = \binom{n+1}{k+1}$$

- Sum over  $n$  and  $k$ :

$$\sum_{k=0}^m \binom{n+k}{k} = \binom{n+m+1}{m}$$

- Sum of the squares:

$$\binom{n}{0}^2 + \binom{n}{1}^2 + \dots + \binom{n}{n}^2 = \binom{2n}{n}$$

- Weighted sum:

$$1\binom{n}{1} + 2\binom{n}{2} + \dots + n\binom{n}{n} = n2^{n-1}$$

- Connection with the [Fibonacci numbers](../algebra/fibonacci-numbers.md):

$$\binom{n}{0} + \binom{n-1}{1} + \dots + \binom{n-k}{k} + \dots + \binom{0}{n} = F_{n+1}$$

## 12.2 4 fundamental problems of distribution

### 12.2.1 N equal balls in K equal boxes

### 12.2.2 N equal balls in K distinct boxes

Equivalent to count the number of solutions for the equation:

$$\begin{aligned} x_1 + \dots + x_K &= N \\ \text{where } x_i &> 0, i \in [1, K], N > 0 \end{aligned} \quad (42)$$

It's given by the formula:

$$\binom{N+1}{K-1} \quad (43)$$

If some boxes may be **empty** ( $x_i \geq 0$ ), then it's given by:

$$\binom{N+K-1}{N}$$

**12.2.3  $N$  distinct balls in  $K$  equal boxes****12.2.4  $N$  distinct balls in  $K$  distinct boxes****13 Bitwise****13.1 Binary to gray code**

$$\begin{aligned}
 G_n &= B_n \\
 G_{n-1} &= B_n \oplus B_{n-1} \\
 G_i &= B_i \oplus B_{i-1} \\
 &\dots \\
 G_1 &= B_2 \oplus B_1
 \end{aligned}$$

**13.2 Gray code to binary**

$$\begin{aligned}
 B_n &= G_n \\
 B_{n-1} &= B_n \oplus G_{n-1} = G_n \oplus G_{n-1} \\
 &\dots \\
 B_1 &= B_2 \oplus G_1 = G_n \oplus G_1
 \end{aligned}$$

**14 Game Theory****14.1 Impartial Games**

To be considered a impartial game following rules must be true:

1. The available moves win/lose depends only on the state of the game, in other words, the only difference between the two players is that one of them moves first
2. Additionally, we assume that the game has perfect information, i.e. no information is hidden from the players (they know the rules and the possible moves).
3. It is assumed that the game is finite, i.e. after a certain number of moves, one of the players will end up in a losing position — from which they can't move to another position. On the other side, the player who set



up this position for the opponent wins. Understandably, there are no draws in this game.

Such games can be completely described by a directed acyclic graph: the vertices are game states and the edges are transitions (moves). A vertex without outgoing edges is a losing vertex (a player who must make a move from this vertex loses).

Since there are no draws, we can classify all game states as either winning or losing. Winning states are those from which there is a move that causes inevitable defeat of the other player, even with their best response. Losing states are those from which all moves lead to winning states for the other player. Summarizing, a state is winning if there is at least one transition to a losing state and is losing if there isn't at least one transition to a losing state.

Our task is to classify the states of a given game.

## 14.2 Sprague-Grundy Theorem

The Sprague-Grundy Theorem states that every impartial game is equivalent to a pile of a certain size in Nim. In other words, every impartial game can be solved as Nim by finding their corresponding game.

Basically, for a game situation  $A$  and its SG function value  $g(A)$ :

1.  $g(A) = 0$  if and only if  $A$  is a must-lose situation.  
Otherwise,  $g(A) \in \mathbb{Z}^*$
2. If  $A$  can be divided into  $n$  sub-situations  $x_1, x_2, \dots, x_n$ , then  $g(A) = g(x_1) \oplus g(x_2) \oplus \dots \oplus g(x_n)$
3. If  $A$  can be converted to situation  $B_1$  or  $B_2$  or ... or  $B_n$  by only one operation, then  $g(A) = \text{mex}(g(B_1), g(B_2), \dots, g(B_n))$  where function  $\text{mex}(S)$  is defined as the smallest non-negative integer that does not appear in  $S$ . For example,  $\text{mex}(0, 1, 2, 4) = 3$ ,  $\text{mex}(\emptyset) = 0$ ,  $\text{mex}(0, 1, 2, 4) = 3$ ,  $\text{mex}(\emptyset) = 0$

### 14.3 Nim variation Subtract game

Work just like nim but instead remove any number of objects you can remove at most  $K$ , this game can be seen as a nim game but before computing the num-sum you need to take the size of each pile module  $K + 1$ , the optimal way to play it is by taking  $K$  at each turn.

## 15 Group Theory

### 15.1 Permutations

A permutation is an arrangement of elements. A permutation of  $N$  elements can be represented by an arrangement of the numbers  $1, 2, \dots, N$  in some order. Eg.  $5, 1, 4, 2, 3$ .

#### 15.1.1 Odd permutations

A permutation is called odd if it can be expressed as a product of odd number of transpositions.  
A sorted permutation is an even permutation

#### 15.1.2 Even permutations

A permutation is called even if it can be expressed as a product of even number of transpositions.

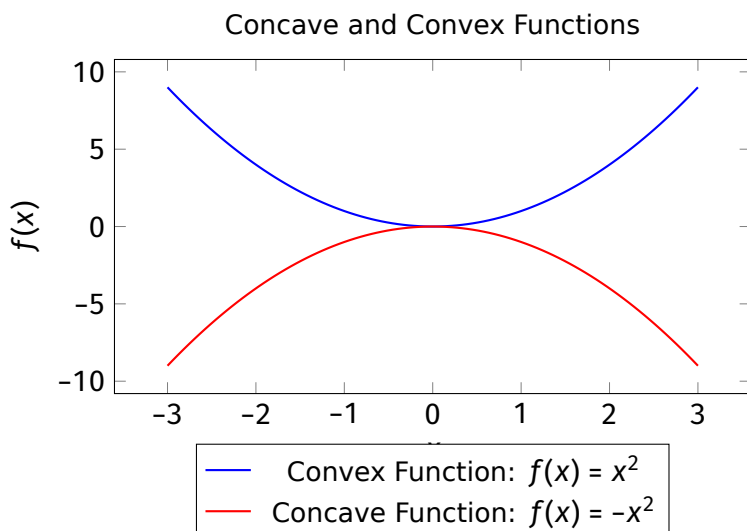
## 16 Others

### 16.1 Unimodal Functions

By unimodal function, we mean one of two behaviors of the function:

- The function strictly increases first, reaches a maximum (at a single point or over an interval), and then strictly decreases.

- The function strictly decreases first, reaches a minimum, and then strictly increases.



## 16.2 Critérios de divisibilidade

### 16.2.1 7

Para verificar a divisibilidade de um número por 7, siga a seguinte regra:

1. Pegue o número em questão.
2. Remova o último dígito (unidade) do número.
3. Dobre o valor removido no passo anterior.
4. Subtraia o valor dobrado do número restante.
5. Se o resultado da subtração for divisível por 7, o número original é divisível por 7.

Exemplo:

Suponha que desejamos verificar a divisibilidade do número 413 por 7.

1. Remova o último dígito (3) e dobre-o, obtendo 6.
2. Subtraia 6 do número restante ( $41 - 6 = 35$ ).

**16.2.2 11**

$$n \text{ é divisível por } 11 \iff \sum_{i=1}^k a_{2i-1} - \sum_{i=1}^j a_{2i} \text{ é divisível por } 11$$

onde  $a_i$  é o  $i$ -ésimo dígito do número  $n$ ,  $k$  é a quantidade de dígitos ímpares,  $j$  é a quantidade de dígitos pares.

Exemplo:

Suponha que desejamos verificar a divisibilidade do número  $n = 7923$  por 11.

$$k = 2, \quad j = 2$$

$$\text{Soma dos dígitos ímpares: } 7 + 3 = 10$$

$$\text{Soma dos dígitos pares: } 9 + 2 = 11$$

$$\text{Subtração: } 10 - 11 = -1$$

Como  $-1$  não é divisível por 11, o número 7923 não é divisível por 11.

**16.2.3 13**

$$13|x \equiv 13|4 \cdot (x\%10) + \lfloor x/10 \rfloor \quad (44)$$

Em outras palavras 13 divide  $x$  se o quádruplo do último algarismo somado com o número sem este algarismo for divisível por 13.

**16.2.4 17**

$$17|x \equiv 17|\lfloor x/10 \rfloor - 5 \cdot (x\%10) \quad (45)$$

Em outras palavras 17 divide  $x$  se o a diferença entre o quádruplo do último algarismo e o número sem este algarismo for divisível por 17.

**16.2.5 19**

$$19|x \equiv 19|[x/10] + 2 \cdot (x \bmod 10) \quad (46)$$

Em outras palavras 19 divide x se o dobro do último algarismo de x somado a o número restante de x é divisível por 19.

**16.2.6 23**

$$23|x \equiv 23|x/10 + 7 \cdot (x \bmod 10) \quad (47)$$