Theoretical Guide
Programadores Roblox

Arthur, Ana & João

1 Progressions

1. Soma dos n primeiros termos.

$$\sum_{k=1}^{n}(k) = \frac{n(n+1)}{2}$$

2. Soma dos n primeiros quadrados.

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

3. Soma dos n primeiros cubos.

$$\sum_{k=1}^{n}(k^3) = (\frac{n(n+1)}{2})^2$$

4. Soma dos n primeiros pares.

$$\sum_{k=1}^{n}(2k) = n^2 + n$$

5. Soma dos n primeiros ímpares.

$$\sum_{k=1}^{n}(2k-1) = n^2$$

6. Progressão Aritmética (PA)

   (a) Termo geral a partir do k-ésimo termo.

$$a_n = a_k + r(n-k)$$

   (b) Soma dos termos.

$$\sum_{i=1}^{n}(a_i) = \frac{n(a_1 + a_n)}{2}$$

7. Progressão Geométrica (PG)

   (a) Termo geral a partir do k-ésimo termo.

$$a_n = a_k r^{n-k}$$

   (b) Soma dos termos.

$$\sum_{k=1}^{n}(ar^{k-1}) = \frac{a_1(r^n - 1)}{r-1}, \quad \text{para } r \neq 1.$$

   (c) Soma dos termos de uma progressão infinita.

$$\sum_{k=1}^{\infty}(ar^{k-1}) = \frac{a_1}{1-r}, \quad \text{para } |q| < 1.$$

   (d) Produto dos termos.

$$\prod_{k=0}^{n}(ar^k) = a^{n+1} r^{\frac{n(n+1)}{2}}$$

8. Série Harmônica 1.

$$\sum_{i=1}^{n}\frac{1}{i} \approx \ln n$$

9. Série Harmônica 2.

$$\sum_{i=1}^{\infty}\frac{(-1)^{i+1}}{i} = \ln 2$$

2 Geometry

2.1 Equação da Reta (forma geral)

Os pontos (x, y) que pertencem a uma reta r devem satisfazer:

$$ax + by + c = 0$$

2.1.1 Geometria Básica

Produto Escalar. Geometricamente é o produto do comprimento do vetor a pelo comprimento da projeção do vetor b sobre a.

$$a \cdot b = \|a\| \cos\theta \|b\| = x_1x_2 + y_1y_2 + z_1z_2$$

Propriedades.

1. $a \cdot b = b \cdot a$.
2. $(\alpha \cdot a) \cdot b = \alpha \cdot (a \cdot b)$.
3. $(a + b) \cdot c = a \cdot c + b \cdot c$.
4. Norma de a (comprimento ao quadrado): $\|a\|^2 = a \cdot a$.
5. Projeção de a sobre o vetor b: $\frac{a \cdot b}{\|b\|}$.
6. Ângulo entre os vetores: $\cos^{-1} \frac{a \cdot b}{\|a\|\|b\|}$.
7. $a \cdot b$ é negativo se o ângulo entre a e b é agudo, positivo se obtusoe igual à 0 eles formam um ângulo reto.

Produto Vetorial. Dados dois vetores independentes linearmente a e b, o produto vetorial $a \times b$ é um vetor perpendicular ao vetor a e ao vetor b e é a normal do plano contendo os dois vetores.

$$a \times b = det \begin{vmatrix} e_x & e_y & e_z \\ x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \end{vmatrix}, \; a \cdot (b \times c) = det \begin{vmatrix} x_1 & y_1 & z_1 \\ x_2 & y_2 & z_2 \\ x_3 & y_3 & z_3 \end{vmatrix}$$

Propriedades.

1. $a \times b = -b \times a$.
2. $(\alpha \cdot a) \times b = \alpha \cdot (a \times b)$.
3. $a \cdot (b \times c) = b \cdot (c \times a) = -a \cdot (c \times b)$.

4. $(a+b) \times c = a \times c + b \times c$.
5. $\|a \times b\| = \|a\| \sin\theta \|b\|$.
6. Volume do paralelepípedo formado por a, b e c: $|a \cdot (b \times c)|$.
7. Área do paralelogramo formado por a e b: $|e_z \cdot (a \times b)| = |x_1 y_2 - y_1 x_2|$.
8. O sinal do coeficiente e_z do produto vetorial indica a orientação relativa dos vetores. Se positivo, o ângulo de a e b é anti-horário. Se negativo, o ângulo é horário e se for zero, os vetores são colineares.

Distância entre dois pontos. Dados dois pontos $a = (x_1, y_2)$ e $b = (x_2, y_2)$, a distância entre a e b é dada por:

$$d_{a,b} = \sqrt{(x_1 - x_2)^2 + (y_1 - y2)^2}$$

Condição de alinhamento de três pontos. Dados três pontos $a = (x_1, y_2)$, $b = (x_2, y_2)$ e $c = (x_3, y_3)$, os pontos a, b e c estão alinhados se:

$$det \begin{vmatrix} x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \\ x_3 & y_3 & 1 \end{vmatrix} = 0$$

Equação da Reta (forma geral). Os pontos (x, y) que pertencem a uma reta r devem satisfazer:

$$ax + by + c = 0$$

Equação da Reta (forma reduzida). A equação reduzida da reta, em que $m = \tan(a) = \frac{\Delta y}{\Delta x}$ é o coef. angular, e n é o coef. linear, isto é, o valor de y em que a reta intercepta o eixo y, é dada por:

$$y = mx + n = m(x - x_0) + y_0$$

Distância entre ponto e reta. Dados um pontos $p = (x_1, y_1)$ e uma reta r de equação $ax + by + c = 0$, a distância entre p e r é dada por:

$$d_{p,r} = \frac{|ax_1 + by_1 + c|}{\sqrt{a^2 + b^2}}$$

Interseção de retas. Para determinar os pontos de interseção é necessário resolver o seguinte sistema de equações lineares:

$$\begin{cases} a_1 x + b_1 y + c_1 = 0 \\ a_2 x + b_2 y + c_2 = 0 \end{cases}$$

A solução é dada por:

$$x = -\frac{c_1 b_2 - c_2 b_2}{a_1 b_2 - a_2 b_1}, \quad y = -\frac{a_1 c_2 - a_2 c_1}{a_1 b_2 - a_2 b_1}.$$

No caso do denominador for igual à 0, calculamos as seguintes determinantes, e se as duas são iguais à 0, as linhas são sobrepostas. Caso contrário, as linhas são paralelas e distintas.

$$det \begin{vmatrix} a_1 & c_1 \\ a_2 & c_2 \end{vmatrix}, det \begin{vmatrix} b_1 & c_1 \\ b_2 & c_2 \end{vmatrix}$$

Equação da Circuferência (forma reduzida). Os pontos (x, y) que pertencem a uma circuferência c devem satisfazer:

$$(x-a)^2 + (y-b)^2 = r^2,$$

onde (a, b) é o centro da circuferência e r o seu raio.

Equação da Circuferência (forma geral). A partir da equação reduzida da circuferência, encontramos a equação geral:

$$x^2 + y^2 - 2ax - 2by + (a^2 + b^2 - r^2) = 0$$

Interseção entre reta e circuferência. Para determinar o tipo de interseção é necessário resolver o seguinte sistema não-linear:

$$\begin{cases} ax + by + c = 0 \\ x^2 + y^2 - 2ax - 2by + (a^2 + b^2 - r^2) = 0 \end{cases}$$

Há três possibilidades como solução do sistema:

1. Reta exterior à circuferência: nenhuma solução. A reta não possui nenhum ponto de comum com a circuferência.
2. Reta tangente à circuferência: solução única. A reta possui apenas 1 ponto em comum com a circuferência.
3. Reta secante à circuferência: duas soluções. A reta cruza a circuferência em 2 pontos distintos.

2.1.2 Geometria Plana

Triângulos. Polígono com três vértices e três arestas. Uma aresta arbitrária é escolhida como a base e, nesse caso, o vértice oposto é chamado de ápice. Um triângulo com vértices A, B e C é denotado $\triangle ABC$.

- Comprimento dos lados: a, b, c
- Semiperímetro: $p = \frac{a+b+c}{2}$
- Altura:
  - Equilátero: $h = \frac{\sqrt{3}}{2} l$
  - Isósceles: $h = \sqrt{l^2 - \frac{b^2}{4}}$

- Área:
  - Equilátero: $A = \frac{l^2\sqrt{3}}{4}$
  - Isósceles: $A = \frac{1}{2}bh$
  - Escaleno: $A = \sqrt{p(p-a)(p-b)(p-c)}$
- Raio circunscrito: $R = \frac{1}{4A}abc$
- Raio inscrito: $r = \frac{1}{p}A$
- Tamanho da mediana: $m_a = \frac{1}{2}\sqrt{2b^2 + 2c^2 - a^2}$

Quadriláteros. Polígono de quatro lados, tendo quatro arestas e quatro vértices. Um quadrilátero com vértices A, B, C e D é denotado com $\Box ABCD$.

- Comprimento dos lados: a, b, c, d
- Semiperímetro: $p = \frac{a+b+c+b}{2}$
- Área:
  - Quadrado: a^2
  - Retângulo: $b \cdot h$
  - Losango: $\frac{1}{2}D \cdot d$
  - Trapézio: $\frac{1}{2}h(B+b)$
- Perímetro:
  - Quadrado: $4a$
  - Retângulo: $2(b+h)$
  - Losango: $4a$
  - Trapézio: $B + b + l_1 + l_2$
- Diagonal:
  - Quadrado: $a\sqrt{2}$
  - Retângulo: $\sqrt{b^2+h^2}$
  - Losango: $a\sqrt{2}$
  - Trapézio: $\sqrt{h^2 + \frac{(B-b)^2}{4h}}$

Círculos. Forma que consiste em todos os pontos de um plano que estão a uma determinada distância de um ponto dado, o centro. A distância entre qualquer ponto do círculo e o centro é chamada de raio.

- Área: $A = \pi r^2$
- Perímetro: $C = 2\pi r$
- Diâmetro: $d = 2r$
- Área do setor circular: $A = \frac{1}{2} r^2 \theta$
- Comprimento do arco: $L = r\theta$
- Perímetro do setor circular: $P = r(\theta + 2)$

Teorema de Pick. Suponha que um polígono tenha coordenadas inteiras para todos os seus vértices. Seja i o número de pontos inteiros no interior do polígono e b o número de pontos inteiros na sua fronteira (incluindo vértices e pontos ao longo dos lados). Então, a área A deste polígono é:

$$A = i + \frac{b}{2} - 1.$$

$$b = \gcd(|x_2 - x_1|, |y_2 - y_1|) + 1.$$

2.1.3 Geometria Espacial

- Área da Superfície:
  - Cubo: $6a^2$
  - Prisma: $A_l + 2A_b$
  - Esfera: $4\pi r^2$
  - Cilindro: $2\pi r(h + r)$
  - Cone: $\pi r(r + \sqrt{h^2 + r^2})$
  - Pirâmide: $A_b + \frac{1}{2} P_b \cdot g, \quad g = \text{geratriz}$
- Volume:
  - Cubo: a^3
  - Prisma: $A_b \cdot h$
  - Esfera: $\frac{4}{3}\pi r^3$
  - Cilindro: $\pi r^2 h$
  - Cone: $\frac{1}{3}\pi r^2 h$

– Pirâmide: $\frac{1}{3}A_b \cdot h$

Fórmula de Euler para Poliedros. Os números de faces, vértices e arestas de um sólido não são independentes, mas estão relacionados de uma maneira simples.

$$F + V - A = 2.$$

2.1.4 Trigonometria

Funções Trigonométricas.

$$\sin\theta = \frac{\text{cateto oposto a } \theta}{\text{hipotenusa}} \quad \cos\theta = \frac{\text{cateto adjacente a } \theta}{\text{hipotenusa}} \quad \tan\theta = \frac{\text{cateto oposto a } \theta}{\text{cateto adjacente a}\theta}$$

Ângulos notáveis.

θ	$0°$	$30°$	$45°$	$60°$	$90°$
$\sin\theta$	0	$\frac{1}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{\sqrt{3}}{2}$	1
$\cos\theta$	1	$\frac{\sqrt{3}}{2}$	$\frac{\sqrt{2}}{2}$	$\frac{1}{2}$	0
$\tan\theta$	0	$\frac{\sqrt{3}}{3}$	1	$\sqrt{3}$	∞

Propriedades.

1. $\sin(a+b) = \sin a \cos b + \cos a \sin b$
2. $\cos(a+b) = \cos a \cos b - \sin a \sin b$
3. $\tan(a+b) = \frac{\tan a + \tan b}{1 - \tan a \tan b}$
4. $a\sin x + b\cos x = r\sin(x+\phi)$, onde $r = \sqrt{a^2+b^2}$ e $\phi = \tan^{-1}\frac{b}{a}$
5. $a\cos x + b\sin x = r\cos(x-\phi)$, onde $r = \sqrt{a^2+b^2}$ e $\phi = \tan^{-1}\frac{b}{a}$
6. **Lei dos Senos**:
$$\frac{a}{\sin\hat{A}} = \frac{b}{\sin\hat{B}} = \frac{c}{\sin\hat{C}} = 2r.$$
7. **Lei dos Cossenos**:
$$a^2 = b^2 + c^2 + 2\cdot b\cdot c\cdot\cos\hat{A}$$
$$b^2 = a^2 + c^2 + 2\cdot a\cdot c\cdot\cos\hat{B}$$
$$c^2 = b^2 + a^2 + 2\cdot b\cdot a\cdot\cos\hat{C}$$

8. **Teorema de Tales**: A interseção de um feixe de retas paralelas por duas retas transversais forma segmentos proporcionais:

$$\frac{\overline{AB}}{\overline{BC}} = \frac{\overline{DE}}{\overline{EF}}$$

9. **Casos de semelhança**: dois triângulos são semelhantes se
   - dois ângulos de um são congruentes a dois do outro. Critério AA (Ângulo, Ângulo).
   - os três lados são proporcionais aos três lados do outro. Critério LLL (Lado, Lado, Lado).
   - possuem um ângulo congruente compreendido entre lados proporcionais. Critério LAL (Lado, Ângulo, Lado).

3 Math

4 Boolean Algebra

Álgebra booleana é a categoria da álgebra em que os valores das variáveis são os valores de verdade, verdadeiro e falso, geralmente denotados por 1 e 0, respectivamente.

4.0.1 Operações básicas

A álgebra booleana possui apenas três operações básicas: conjunção, disjunção e negação, expressas pelos operadores binários correspondentes E ($\wedge$) e OU ($\vee$) e pelo operador unário NÃO ($\neg$), coletivamente chamados de operadores booleanos.

Operador lógico	Operador	Notação	Definição
Conjunção	AND	$x \wedge y$	$x \wedge y = 1$ se $x = y = 1, x \wedge y = 0$ caso contrário
Disjunção	OR	$x \vee y$	$x \vee y = 0$ se $x = y = 0, x \wedge y = 1$ caso contrário
Negeação	NOT	$\neg x$	$\neg x = 0$ se $x = 1, \neg x = 1$ se $x = 0$

4.0.2 Operações secundárias

Operações compostas a partir de operações básicas incluem, dentro outras, as seguintes:

Operador lógico	Operador	Notação	Definição	Equivalência
Condicional material	$\rightarrow$	$x \rightarrow y$	$x \rightarrow y = 0$ se $x = 1$ e $y = 0, x \rightarrow y = 1$ caso contrário	$\neg x \vee y$
Bicondicional material	$\Leftrightarrow$	$x \Leftrightarrow y$	$x \Leftrightarrow y = 1$ se $x = y, x \Leftrightarrow y = 0$ caso contrário	$(x \vee \neg y) \wedge (\neg x \vee y)$
OR Exclusivo	XOR	$x \oplus y$	$x \oplus y = 1$ se $x \neq y, x \oplus y = 0$ caso contrário	$(x \vee y) \wedge (\neg x \vee \neg y)$

4.0.3 Leis

- Associatividade:

$$x \wedge (y \wedge z) = (x \wedge y) \wedge z$$

$$x \vee (y \vee z) = (x \vee y) \vee z$$

- Comutatividade:

$$x \wedge y = y \wedge x$$

$$x \vee y = y \vee x$$

- Distributividade:

$$x \wedge (y \vee z) = (x \wedge y) \vee (x \wedge z)$$

$$x \vee (y \wedge z) = (x \vee y) \wedge (x \vee z)$$

- Identidade: $x \vee 0 = x \wedge 1 = x$

- Aniquilador:

$$x \vee 1 = 1$$

$$x \wedge 0 = 0$$

- Idempotência: $x \wedge x = x \vee x = x$
- Absorção: $x \wedge (x \vee y) = x \vee (x \wedge y) = x$
- Complemento:

$$x \wedge \neg x = 0$$

$$x \vee \neg x = 1$$

- Negação dupla: $\neg(\neg x) = x$
- De Morgan:

$$\neg x \wedge \neg y = \neg(x \vee y)$$

$$\neg x \vee \neg y = \neg(x \wedge y)$$

5 Identities

6 Constants

7 Probability

7.0.1 Introdução à Probabilidade

Eventos. Um evento pode ser representado como um conjunto $A \subset X$ onde X contém todos os resultudos possíveis e A é um subconjunto de resultados.

Cada resultado x é designado uma probabilidade $p(x)$. Então, a probabilidade $P(A)$ de um evento A pode ser calculada como a soma das probabilidades dos resultados:

$$P(A) = \sum_{x \in A} p(x).$$

Complemento. A probabilidade do complemento $\overline{A}$, *i.e.* o evento A não ocorrer, é dado por:

$$P(\overline{A}) = 1 - P(A).$$

Eventos não mutualmente exclusivos. A probabilidade da união $A \cup B$ é dada por:

$$P(A \cup B) = P(A) + P(B) - P(A \cap B).$$

Se A e B forem eventos mutualmente exclusivos, *i.e.* $A \cup B = \emptyset$, a probabilidade é dada por:

$$P(A \cup B) = P(A) + P(B).$$

Probabilidade condicional. A probabilidade de A assumindo que B ocorreu é dada por:

$$P(A|B) = \frac{P(A \cap B)}{P(B)}.$$

Os eventos A e B são ditos **independentes** se, e somente se,

$$P(A|B) = P(A) \quad \text{e} \quad P(B|A) = P(B).$$

Teorema de Bayes. A probabilidade de um evento A ocorrer, antes e depois de condicionar em outro evento B é dada por:

$$P(A|B) = \frac{P(B|A)P(A)}{P(B)} \quad \text{ou} \quad P(A_i|B) = \frac{P(B|A_i)P(A_i)}{\sum_{j \in A} P(B|A_j)P(A_j)}$$

7.0.2 Variáveis Aleatórias

Seja X uma variável aleatória discreta com probabilidade $P(X = x)$ de assumir o valor x. Ela vai então ter um valor esperado (média)

$$\mu = E[X] = \sum_{i=1}^{n} x_i P(X = x_i)$$

e variância

$$\sigma^2 = V[X] = E[X^2] - (E[X])^2 = \sum_{i=1}^{n} (x - E[X])^2 P(X = x_i)$$

onde σ é o desvio-padrão.

Se X for contínua ela terá uma função de densidade $f_X(x)$ e as somas acima serão em vez disso integrais com $P(X = x)$ substituído por $f_X(x)$.

Linearidade do Valor Esperado.

$$E[aX + bY + c] = aE[X] + bE[Y] + c.$$

No caso de X e Y serem independentes, temos que:

$$E[XY] = E[X]E[Y]$$
$$V[aX + bY + c] = a^2 E[X] + b^2 E[Y].$$

7.0.3 Distribuições Discretas

Distribuição Binomial. Número de sucessor k em n experimentos independentes de sucesso/fracasso, cada um dos quais produz sucesso com probabilidade p é Bin(n,p), $n \in \mathbb{N}$, $0 \leq p \leq 1$.

$$P(X = k) = \binom{n}{k} p^k (1-p)^{n-k}$$
$$\mu = np, \quad \sigma^2 = np(1-p)$$

Bin(n,p) é aproximadamente Pois(np) para p pequeno.

Distribuição Geométrica. Número de tentativas k necessárias para conseguir o primeiro sucesso em experimentos independentes de sucesso/fracasso, cada um dos quais produz sucesso com probabilidade p é Geo(p), $0 \leq p \leq 1$.

$$P(X = k) = (1-p)^{k-1} p, \quad k \in \mathbb{N}$$
$$\mu = \frac{1}{p}, \quad \sigma^2 = \frac{1-p}{p}$$

Distribuição de Poisson. Número de eventos k ocorrendo em um período de tempo fixo t se esses eventos ocorrerem com uma taxa média conhecida r e independente do tempo já que o último evento é Pois(λ), $\lambda = tr$.

$$P(X = k) = e^{-k} \frac{\lambda^k}{k!}, \quad k \in \mathbb{N}_0$$
$$\mu = \lambda, \quad \sigma^2 = \lambda.$$

7.0.4 Distribuições Contínuas

Distribuição Uniforme. Se a função de densidade é constante entre a e b e 0 em outro lugar ela é Uni(a,b), $a < b$.

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

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

Distribuição Exponencial. Tempo entre eventos em um processo de Poisson é Exp(λ), $\lambda > 0$.

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

$$F(x) = \begin{cases} 1 - e^{-\lambda x}, & x \geq 0 \\ 0, & x < 0 \end{cases}$$

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

Distribuição Normal. Maioria das variáveis aleatórias reais com média μ e variância σ^2 são bem descritas por $N(\mu, \sigma^2)$, $\sigma > 0$.

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

8 Combinatorics

8.0.1 Permutação e Arranjo

Uma r-permutação de n objetos é uma seleção **ordenada** (ou arranjos) de r deles.

1. **Objetos distintos.**
$$P(n, r) = \frac{n!}{(n-r)!}$$

2. **Objetos com repetição.** Se temos n objetos com k_1 do tipo 1, k_2 do tipo 2,...,k_m do tipo m, e $\sum k_i = n$:
$$P(n; k_1, k_2, ..., k_m) = \frac{n!}{k_1! \cdot k_2! \cdot ... \cdot k_m!}$$

3. **Repetição ilimitada.** Se temos n objetos e uma quantidade ilimitada deles:
$$P(n, r) = n^r$$

Tabela de fatoriais.

n	0	1	2	3	4	5	6	7	8	9	10
$n!$	1	1	2	6	24	120	720	5040	40320	362880	3628800

8.0.2 Combinação

Uma r-combinação de n objetos é um seleção de r deles, sem diferenciação de ordem.

1. **Objetos distintos.**

$$C(n,r) = \frac{n!}{r!(n-r)!} = \binom{n}{r}.$$

Definimos também:

$$C(n,r) = C(n,n-r)$$
$$C(n,0) = C(n,n) = 1$$
$$C(n,r) = 0, \quad \text{para } r < 0 \text{ ou } r > n.$$

2. **Objetos com repetição (Stars and Bars).** Número de maneiras de dividir n objetos idênticos em k grupos:

$$C(n,k) = \binom{n+k-1}{n}$$

3. **Teorema Binomial.** Sendo a e b números reais quaisquer e n um número inteiro positivo, temos que:

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

4. **Triângulo de Pascal.** Triângulo com o elemento na n-ésima linha e k-ésima coluna denotado por $\binom{n}{k}$, satisfazendo:

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}, \quad \text{para } n > k \geq 1.$$

Propriedades.

1. **Hockey-stick (soma sobre n).**

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

2. **Soma sobre k.**

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

$$\sum_{k=0}^{n} \binom{n}{2k} = \sum_{k=0}^{n} \binom{n}{2k+1} = 2^{n-1}$$

3. **Soma sobre n e k.**

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

4. **Soma com peso.**

$$\sum_{k=0}^{n} k \cdot \binom{n}{k} = n2^{n-1}$$

5. **(n+1)-ésimo termo da sequência de Fibonacci.**

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

6. **Soma dos quadrados.**

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

8.0.3 Números de Catalan

O n-ésimo número de Catalan, C_n, pode ser calculado de duas formas:

1. **Fórmula recursiva:**

$$C_0 = C_1 = 1$$

$$C_n = \sum_{k=0}^{n-1} C_k C_{n-1-k}, \quad \text{para } n \geq 2.$$

2. **Fórmula analítica:**

$$C_n = \frac{1}{n+1}\binom{2n}{n} = \prod_{k=2}^{n} \frac{n+k}{k}, \quad \text{para } n \geq 0$$

Tabela dos 10 primeiros números de Catalan.

n	0	1	2	3	4	5	6	7	8	9	10
C_n	1	1	2	5	14	42	132	429	1430	4862	16796

Aplicações

O número de Catalan C_n é a solução para os seguintes problemas:

- Número de sequências de parênteses balanceados consistindo de n pares de parênteses.
- Números de árvores binárias enraizadas cheias com $n+1$ folhas (vértices não são numerados), ou, equivalentemente, com um total de n nós internos. Uma árvore binária enraizada é cheia se cada vértice tem dois filhos ou nenhum.
- Número de maneiras de colocar parênteses completamente em n+1 fatores.
- Número de triangularizações de um polígono convexo com $n+2$ lados.
- Número de maneiras de conectar $2n$ pontos em um círculo para formar n cordas disjuntas.
- Número de árvores binárias completas não isomórficas com $n+1$ nós.
- Número de caminhos monotônicos na grade de pontos do ponto $(0,0)$ ao ponto (n,n) em uma grade quadrada de tamanho nxn, que não passam acima da diagonal principal.

- Número de partições não cruzadas de um conjunto de n elementos.
- Números de manieras de se cobrir uma escada $1 \dots n$ usando n retângulos (a escada possui n colunas e a i-ésima coluna possui altura i).
- Número de permutações de tamanho n que podem ser *stack sorted*.

8.0.4 Princípio da Inclusão-Exclusão

Para calcular o tamanho da união de múltiplos conjuntos, é necessário somar os tamanhos desses conjuntos **separadamente**, e depois subtrair os tamanhos de todas as interseções **em pares** dos conjuntos, em seguida adicionar de volta o tamanho das interseções de **trios** dos conjuntos, subtrair o tamanho das interseções de **quartetos** dos conjuntos, e assim por diante, até a interseção de **todos** os conjuntos.

$$|\bigcup_{i=1}^{n} A_i| = \sum_{\emptyset \neq J \subseteq \{1,2,\dots n\}} (-1)^{|J|-1} |\bigcap_{j \in J} A_j|$$

8.0.5 Lema de Burnside / Teorema da Enumeração de Pólya

Para contar o número de classes de equivalência de um conjunto G, baseando-se na simetria interna, utilizamos a seguinte fórmula:

$$|\text{Classes}| = \frac{1}{|G|} \sum_{\pi \in G} k^{C(\pi)},$$

onde denotamos $C(\pi)$ como o número de ciclos em uma permutação π e k o número de valores que cada elemento de representação pode assumir.

9 Bitwise

10 Notes

11 Graph Theory

11.0.1 Caminhos

Caminho de Euler

Um caminho de Euler em um grafo é o caminho que visita cada aresta exatamente uma vez. Um ciclo de Euler, ou Tour de Euler, em um grafo é um ciclo que usa cada aresta exatamente uma vez.

Teorema: Um grafo conectado tem um ciclo de Euler se, e somente se, cada vértice possui grau par.

Caminho Hamiltoniano

Um caminho Hamiltoniano em um grafo é o caminho que visita cada vértice exatamente uma vez. Um ciclo Hamiltoniano em um grafo é um ciclo que visita cada vértice exatamente uma vez.

Teoremas:

- Teorema de Dirac: Um grafo simples com n vértices ($n \geq 3$) é Hamiltoniano se cada vértice tem grau $\geq \frac{n}{2}$.
- Teorema de Ore: Um grafo simples com n vértices ($n \geq 3$) é Hamiltoniano se, para cada par de vértices não-adjacentes, a soma de seus graus é $\geq n$.
- Ghouila-Houiri: Um grafo direcionado simples fortemente conexo com n vértices é Hamiltoniano se cada vértice tem um grau $\geq n$.
- Meyniel: Um grafo direcionado simples fortemente conexo com n vértices é Hamiltoniano se a soma dos graus de cada par de vértices não-adjacentes é $\geq 2n - 1$.

12 Matrices

12.0.1 Determinante

A determinante $det(A)$ de uma matriz A é definida se A é uma matriz quadrada. Se A é de tamanho 1×1, então $det(A) = A_{11}$. A determinante de matrizes maiores é calculada recursivamente usando a fórmula:

$$det(A) = \sum_{j=1}^{m} A_{1,j} C_{1,j},$$

onde $C_{i,j}$ é o **cofator** de A em i, j. O cofator é calculado usando a fórmula:

$$C_{i,j} = (-1)^{i+j} det(M_{i,j}),$$

onde $M_{i,j}$ é obtido ao remover a linha i e a coluna j de A.

A determinante de A indica se existe uma **matriz inversa** A^{-1} tal que $AA^{-1} = I$, onde I é uma matriz identidade. A^{-1} existe somente quando $det(A) \neq 0$, e pode ser calculada usando a fórmula:

$$A^{-1}_{i,j} = \frac{C_{i,j}}{det(A)}.$$

12.0.2 Aplicações

Contando caminhos. Quando V é a matriz de adjacência de um grafo sem peso, a matriz V^n contém o número de caminhos de n arestas entres os vértices do grafo.

Menores caminhos. Usando uma ideia similar para grafos com peso, podemos calcular para cada par de vértices a distância mínima para um caminho entre eles no qual contém exatos n arestas. Construímos a matriz de adjacência onde ∞ significa que uma aresta não existe, e outros valores correspondem ao peso da aresta. Utilizamos a fórmula

$$AB_{i,j} = \min_{k=1}^{n} A_{i,k} + B_{k,j}$$

na multiplicação de matriz. Após essa modificação, as potências da matriz correspondem aos menores caminhos no grafo.

Teorema de Kirchhoff. Para calcular o número de árvores geradoras de um grafo, construímos uma matrix laplaciana L, onde $L_{i,i}$ é o grau do vértice i e $L_{i,j} = -1$ se há uma aresta entre os vértices i e j, caso contrário $L_{i,j} = 0$. O número de árvores geradoras é igual à determinante da matriz que é obtida ao removermos qualquer linha e qualquer coluna de L.

13 C++

14 Counting Problems

15 Number Theory

15.0.1 Fundamentos

Maior Divisor Comum (MDC). Dados dois inteiros não-negativos a e b, o maior número que é um divisor de tanto de a quanto de b é chamado de MDC.

$$\gcd(a,b) = max\{d > 0 : (d|a) \wedge (d|b)\}$$

Menor Múltiplo Comum (MMC). Dados dois inteiros não-negativos a e b, o menor número que é múltiplo de tanto de a quanto de b é chamado de MMC.

$$lcm(a,b) = \frac{ab}{\gcd(a,b)}$$

Equação Diofantina Linear. Um Equação Diofantina Linear é uma equação de forma geral:

$$ax + by = c,$$

onde a,b,c são inteiros dados, e x,y são inteiros desconhecidos.

Para achar uma solução de uma equação Diofantina com duas incógnitas, podemos utilizar o algoritmo de Euclides. Quando aplicamos o algoritmo em a e b, podemos encontrar seu MDC d e dois números x_d e y_d tal que:

$$a \cdot x_d + b \cdot y_d = d.$$

Se c é divisível por $d = \gcd(a,b)$, logo a equação Diofantina tem solução, caso contrário ela não tem nenhuma solução.

Supondo que c é divisível por g, obtemos:

$$a \cdot (x_d \cdot \frac{c}{d}) + b \cdot (y_d \cdot \frac{c}{d}) = c.$$

Logo uma das soluções da equação Diofantina é:

$$x_0 = x_d \cdot \frac{c}{d}$$
$$y_0 = y_d \cdot \frac{c}{d}.$$

A partir de uma solução (x_0, y_0), podemos obter todas as soluções. São soluções da equação Diofantina todos os números da forma:

$$x = x_0 + k \cdot \frac{b}{d}$$
$$y = y_0 - k \cdot \frac{a}{d}.$$

Números de Fibonacci. A sequência de Fibonacci é definida da seguinte forma:

$$F_n = \begin{cases} 0, \text{se } n = 0 \\ 1, \text{se } n = 1 \\ F_{n-1} + F_{n-2}, \text{caso contrário} \end{cases}$$

Os 11 primerios números da sequência são:

n	0	1	2	3	4	5	6	7	8	9	10
F_n	0	1	1	2	3	5	8	13	21	34	55

Propriedades.

- Identidade de Cassini: $F_{n-1}F_{n+1} - {F_n}^2 = (-1)^n$
- Regra da adição: $F_{n+k} = F_k F_{n+1} + F_{k-1}F_n$
- Identidade do MDC: $\gcd(F_n, F_m) = F_{\gcd(n,m)}$

Fórmulas para calcular o n-ésimo número de Fibonacci.

- Forma matricial:

$$\begin{vmatrix} 1 & 1 \\ 1 & 0 \end{vmatrix}^n = \begin{vmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{vmatrix}$$

15.0.2 Funções

Função Totiente de Euler. A função-phi $\phi(n)$ conta o número de inteiros entre 1 e n incluso, nos quais são coprimos com n. Dois números são coprimos se o MDC deles é igual a 1.

Propriedades.

- Se p é primo, logo o $\gcd(p, q) = 1$ para todo $1 \leq q < p$. Logo,

$$\phi(p) = p - 1$$

- Se p é primo e $k \geq 1$, então há exatos p^k/p números entre 1 e p^k que são divisíveis por p. Portanto,

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

- Se a e b forem coprimos ou não, então:

$$\phi(ab) = \phi(a) \cdot \phi(b) \cdot \frac{d}{\phi(d)}, \quad d = \gcd(a, b)$$

- Fórmula do produto de Euler:

$$\phi(n) = n \prod_{p|n} (1 - \frac{1}{p})$$

- Soma dos divisores:

$$n = \sum_{d|n} \phi(d)$$

Aplicações:

- Teorema de Euler: Seja m um inteiro positivo e a um inteiro coprimo com m, então:

$$a^{\phi(m)} \equiv 1 \pmod{m}$$
$$a^n \equiv a^{n \pmod{\phi(m)}} \pmod{m}$$

- Generalização do Teorema de Euler: Seja x,m inteiros positivos e $n \geq \log_2 m$,

$$x^n \equiv x^{\phi(m)+[n \pmod{\phi(m)}]} \pmod{m}$$

- Teoria dos Grupos: $\phi(n)$ é a ordem de um grupo multiplicativo mod n $(\mathbb{Z}/n\mathbb{Z})^\times$, que é o grupo dos elementos com inverso multiplicativo (aqueles coprimos com n). A ordem multiplicativa de um elemento a mod m ($\text{ord}_m(a)$), na qual também é o tamanho do subgrupo gerado por a, é o menor $k > 0$ tal que $a^k \equiv 1 \pmod{m}$. Se a ordem multiplicativa de a é $\phi(m)$, o maior possível, então a é **raiz primitiva** e o grupo é cíclico por definição.

Número de Divisores. Se a fatoração prima de n é $p_1^{e_1} \cdot p_2^{e_2} \dots p_k^{e_k}$, onde p_i são números primos distintos, então o número de divisores é dado por:

$$d(n) = (e_1 + 1) \cdot (e_2 + 1) \dots (e_k + 1)$$

Um número altamente composto (HCN) é um número inteiro que possui mais divisores do que qualquer número inteiro positivo menor.

n	6	60	360	5040	83160	720720	735134400	74801040398884800
$d(n)$	4	12	24	60	128	240	1344	64512

Soma dos Divisores. Para $n = p_1^{e_1} \cdot p_2^{e_2} \dots p_k^{e_k}$ temos a seguinte fórmula:

$$\sigma(n) = \frac{p_1^{e_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{e_2+1} - 1}{p_2 - 1} \dots \frac{p_k^{e_k+1} - 1}{p_k - 1}$$

Contagem de números primos. A função $\pi(n)$ conta a quantidade de números primos menores ou iguais à algum número real n. Pelo Teorema do Número Primo, a função tem crescimento aproximado à $\frac{x}{\ln(x)}$.

n	10	10^2	10^3	10^4	10^5	10^6	10^7	10^8
$\pi(n)$	4	25	168	1229	9592	78489	664579	5761455

15.0.3 Aritmética Modular

Dado um inteiro $m \geq 1$, chamado módulo, dois inteiros a e b são ditos congruentes módulo m, se existe um inteiro k tal que

$$a - b = km,$$

Congruência módulo m é denotada: $a \equiv b \pmod{m}$

Propriedades.

- $(a \pm b) \pmod m = (a \mod m \pm b \mod m) \pmod m$.
- $(a \cdot b) \pmod m = (a \mod m) \cdot (b \mod m) \pmod m$.
- $a^b \pmod m = (a \mod m)^b \pmod m$.

- $a \pm k \equiv b \pm k \pmod m$, para qualquer inteiro k.
- $a \cdot k \equiv b \cdot k \pmod m$, para qualquer inteiro k.
- $a \cdot k \equiv b \cdot k \pmod{k \cdot m}$, para qualquer inteiro k.

Inverso Multiplicativo Modular. O inverso multiplicativo modular de um número a é um inteiro a^{-1} tal que

$$a \cdot a^{-1} \equiv 1 \pmod m.$$

O inverso modular existe se, e somente se, a e m são coprimos.

Um método para achar o inverso modular é usando o Teorema de Euler. Multiplicando ambos os lados da equação do teorema por a^{-1} obtemos:

$$a^{\phi(m)} \equiv 1 \pmod m \xrightarrow{\times(a^{-1})} a^{\phi(m)-1} \equiv a^{-1} \pmod m$$

Equação de Congruência Linear. Essa equação é da forma:

$$a \cdot x \equiv b \pmod m,$$

onde a,b e m são inteiros conhecidos e x uma incógnita.

Uma forma de achar uma solução é via achando o elemento inverso. Seja $g = \gcd(a, m)$, se b não é divisível por g, não há solução.

Se g divide b, então ao dividir ambos os lados da equação por g (a,b e m), recebemos uma nova equação:

$$a' \cdot x \equiv b' \pmod{m'}.$$

Como a' e m' são coprimo, podemos encontrar o inverso a', e multiplicar ambos os lados da equação pelo inverso, e então obtemos uma solução única.

$$x \equiv b' \cdot a'^{-1} \pmod{m'}$$

A equação original possui exatas g soluções, e elas possuem a forma:

$$x_i \equiv (x + i \cdot m') \pmod m, \quad 0 \le i \le g - 1.$$

Teorema do Resto Chinês. Seja $m = m_1 \cdot m_2 \cdot \cdots \cdot m_k$, onde m_i são coprimos dois a dois. Além de m_i, recebemos também um sistema de congruências

$$\begin{cases} a \equiv a_1 \pmod{m_1} \\ a \equiv a_2 \pmod{m_2} \\ \vdots \\ a \equiv a_k \pmod{m_k} \end{cases}$$

onde a_i são constantes dadas. O teorema afirma que o sistema de congruências dado sempre tem uma e apenas uma solução módulo m.

Seja $M_i = \prod_{i \neq j} m_j$, o produto de todos os módulos menos m_i, e N_i os inversos modulares $N_i = M_i^{-1} \pmod{m_i}$. Então, a solução do sistema de congruências é:

$$a \equiv \sum_{i=1}^{k} a_i M_i N_i \pmod{m_1 \cdot m_2 \cdot \ldots m_k}.$$

Para módulos não coprimos, o sistema de congruências tem exatas uma solução módulo $lcm(m_1, m_2, \ldots, m_k)$, ou tem nenhuma solução.

Uma única congruência $a \equiv a_i \pmod{m_i}$ é equivalente ao sistema de congruências $a \equiv a_i \pmod{p_j^{n_j}}$, onde $p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k}$ é a fatoração prima de m_i. A congruência com o maior módulo de potência prima será a congruência mais forte dentre todas as congruências com a mesma base prima. Ou dará uma contradição com alguma outra congruência, ou implicará já todas as outras congruências.

Se não há contradições, então o sistema de equações tem uma solução. Podemos ignorar todas as congruências, exceto aquelas com os módulos de maior potência de primo. Esses módulos agora são coprimos e, portanto, podemos resolver com o algoritmo do caso geral.

Logaritmo discreto. Sejam a, b, k, m inteiros, queremos encontrar x tal que a equação seja válida:

$$ka^x \equiv b \pmod{m}.$$

Para encontrá-lo:

1. Reescrevemos $x = np - q$, onde obteremos a seguinte equação:
$$ka^{np-q} \equiv b \pmod{m}, \quad n = \sqrt{m} + 1.$$
2. No caso de $g = \gcd(a, m) = 1$, obtemos:
$$ka^{np} \equiv ba^q \pmod{m}.$$
3. Caso contrário:
   (a) Se $g \nmid b$, a equação não possui solução.
   (b) Se $g \mid b$, escrevemos $a = g\alpha$, $b = g\beta$, $m = g\mu$, e obtemos a seguinte equação:
$$k(g\alpha)a^{x-1} \equiv g\beta \pmod{g\mu}$$
$$(k\alpha)a^{x-1} \equiv \beta \pmod{\mu}$$
4. Para todo $q \in [0, n]$, calculamos todos os valores possíveis de $f_1(q) = ba^q \pmod{m}$.
5. Por fim, para todo $p \in [0, n]$, calculamos todos os valores possíveis de $f_2(p) = ka^{np} \pmod{m}$ até encontrarmos um valor p tal que
$$f_1(q) = f_2(p).$$

Seguindo esses passos, iremos encontrar o menor x que tornará a equação válida.

Raiz primitiva. Um número g é raiz primitiva módulo m se e somente se para qualquer inteiro a tal que $\gcd(a, n) = 1$, existe um inteiro k tal que:

$$g^k \equiv a \pmod{m}.$$

k é chamado de índice ou logaritmo discreto de a na base g módulo m. g é chamado de generador do grupo multiplicativo dos inteiros módulo m.

A raiz primitiva módulo m existe se e somente se:

- m é 1,2,4, ou
- m é um potência de um primo ímpar ($m = p^k$), ou
- m é o dobro de uma potência de um primo ímpar ($m = 2 \cdot p^k$).

Para encontrar a raiz primitiva:

1. Encontrar $\phi(m)$ (Função Totiente de Euler) e fatorizá-lo.
2. Iterar por todos os números $g \in [1, m]$, e para cada número, para verificar se é raiz primitiva, fazemos:
   (a) Calcular todos $g^{\frac{\phi(m)}{p_i}} \pmod{m}$.
   (b) Se todos o valores são diferentes de 1, então g é uma raiz primitiva.

Raiz discreta. Sejam k, a inteiros e m um primo, queremos encontrar todo x tal que:

$$x^k \equiv a \pmod{m}.$$

Seja g a raiz primitiva módulo m, podemos representar a raiz discreta como uma potência de g. Assim, podemos reescrever a equação como:

$$x^k \equiv (g^y)^k \equiv a \pmod{m}$$

$$(g^k)^y \equiv a \pmod{m}.$$

Por fim, basta resolver o logaritmo discreto para descobrir uma solução.

Ao achar uma solução $x_0 = g^{y_0} \pmod{m}$, as demais soluções possuem a forma:

$$x_i = g^{y_0 + i\frac{\phi(m)}{\gcd(\phi(m),k)}}, \quad i \in \mathbb{Z}.$$