Algoritmos de división y Euclides

Dados a, b, c, d y m, con m $\neq$0. Si

$$a \mod m = c \mod m \qquad b \mod m = d \mod m$$

Entonces

$$(a+b) \mod m = (c+d) \mod m \qquad (ab) \mod m = (cd) \mod m$$

Algoritmo de Euclides para hallar $d = \text{mcd}(a, b)$.

1. Hallamos q_1 y r_1 tales que $a = bq_1 + r_1$
2. Seguimos con $b = r_1q_2 + r_2$
3. $r_1 = r_2q_3 + r_3$, etc.
4. Hasta que llegamos a un punto tal que $r_i = r_{i+1}q_{i+2} + 0$. En este punto tenemos que $d = \text{mcd}(a, b) = r_{i+1}$.

Si $d = \text{mcd}(a, b)$, entonces existen x e y tales que $d = ax + by$. Por tanto, si existen x' e y' tales que $ax' + by' = 1$, entonces a y b son primos entre sí.

Si $k > 0$, entonces $\text{mcd}(ka, kb) = k\text{mcd}(a, b)$.

Si $\text{mcd}(a, b) = d$, entonces $\text{mcd}(\frac{a}{d}, \frac{b}{d}) = 1$

Número primos y Teorema fundamental de la Aritmética

Lema de Euclides: sean a, b y c enteros. Si a y c son primos entre sí y $a|bc$, entonces $a|b$.

De aquí sacamos que si $p|a_1a_2a_3 \cdots a_k$, entonces $\exists i : p|a_i$.

Teorema fundamental de la Aritmética: Sea $n > 1$, entonces existen números primos $p_1, p_2, \cdots, p_i$ tales que $n = p_1p_2 \cdots p_i$. Además, esta factorización es única.

De ahí derivamos que la factorización única de n es de la forma:

$$|n| = p_1^{\alpha_1}p_2^{\alpha_2} \cdots p_t^{\alpha_t}$$

Dados $a = p_1^{\alpha_1}p_2^{\alpha_2} \cdots p_t^{\alpha_t}$ y $b = p_1^{\beta_1}p_2^{\beta_2} \cdots p_t^{\beta_t}$...

$$\text{mcd}(a, b) = p_1^{\min(\alpha_1,\beta_1)}p_2^{\min(\alpha_2,\beta_2)} \cdots p_t^{\min(\alpha_t,\beta_t)} \qquad \text{mcm}(a, b) = p_1^{\max(\alpha_1,\beta_1)}p_2^{\max(\alpha_2,\beta_2)} \cdots p_t^{\max(\alpha_t,\beta_t)}$$

Ecuaciones diofánticas

Ecuaciones del tipo $ax + by = n$.

- Hallamos $d = \text{mcd}(a, b)$ y ascendemos en el algoritmo de Euclides hasta obtener la expresión $aq_1^* + bq_2^* = d$.
- Entonces: $x_0 = \frac{nq_1^*}{d}$ e $y_0 = \frac{nq_2^*}{d}$.
- Las soluciones generales son: $x = x_0 + t\frac{b}{d}$ e $y = y_0 + t\frac{a}{d}$.

Ecuaciones del tipo $x^2 - y^2 = n$.

- Sólo puede solucionarse si n tiene una factorización de números $n = ab$ con igual paridad.
- Si es así, las soluciones son:

$$x = \frac{a+b}{2} \qquad y = \frac{a-b}{2}$$

Algoritmo de Factorizació de Fermat: si n es impar, y fuera compuesto, entonces se cumpliría que $n = \left(\frac{a+b}{2}\right)^2 - \left(\frac{a-b}{2}\right)^2 = x^2 - y^2$. Entonces, demostrar que n es compuesto es equivalente a resolver $x^2 - n = y^2$, con $\sqrt{n} \leq x \leq \frac{n+1}{2}$. Es decir, probar x en ese intervalo, y ver si el resultado de la resta es un número cuadrado. Si no lo es, entonces n es primo.

Ecuaciones que desenboquen en ternas pitagóricas.

- Asegurar que x, y y z son primos entre sí. Si no lo son, entonces hallar el mcd y dividir los números por el mcd.
- Alguno de los valores, es divisible por 2. Hacemos que este valor sea x.
- Entonces, existen s y t, de distinta paridad, tales que

$$x = 2st \qquad y = s^2 - t^2 \qquad z = s^2 + t^2$$

Congruencias

Recordemos que a y b son congruentes módulo m ($a \equiv b \mod m$) sii $m|(a - b)$.

Tenemos que si $a \equiv b \mod m$ y $c \equiv d \mod m$, entonces $a + c \equiv b + d \mod m$ y $ac \equiv bd \mod m$. También, si $d|m$, entonces, $a \equiv b \mod d$.

La ecuación $ax \equiv b \mod m$ tiene solucion sii $d|b$, $d = \text{mcd}(a, b)$. Además, sería el equivalente a resolver la ecuación diofántica $ax + my = b$.

Teorema chino del resto. Si tenemos un sistema de congruencias $a_i \equiv b_i \mod m_i$ con $\text{mcd}(m_i, m_j) = 1 \quad \forall i, j$ y $\text{mcd}(a_i, m_i) = 1 \quad \forall i$, el sistema tiene una solución x_0, única, y las demás soluciones son de la forma $x = x_0 + \lambda(m_1 m_2 \cdots m_k)$.

La solución x_0 es: $x_0 = \sum_{i=1}^{k} x_i t_i y_i$. Donde

- x_i es la solución trivial del sistema $a_i x \equiv b_i \mod m_i$.

- $t_i = \frac{m}{m_i} \quad m = \prod m_i$
- y_i es la solución de la ecuación $t_i y \equiv 1 \mod m_i$.
- Una vez tenemos x_0 la menor solución, x^* va a ser al solución de la congruencia $x_0 \equiv x^* \mod m$.

Función ϕ de Euler. Definimos $\phi(n)$ al numero de enteros positivos menores de n y primos con este. Tenemos que $\phi(p) = p - 1$, con p primo.

Dicho esto, $\phi(p^r) = p^r - p^{r-1} = p^r\,(1 - 1/p)$. Si $n = p_1^{r_1} p_2^{r_2} \cdots p_t^{r_t}$ entonces $\phi(n) = n \cdot (1 - 1/p_1)\,(1 - 1/p_2) \cdots (1 - 1/p_t)$.

Teorema de Euler. Sean a y m dos enteros con mcd$(a, m) = 1$, entonces $a^{\phi(m)} = 1 \mod m$. De aquí sacamos el pequeño teorema de Fermat: $a^{p-1} = 1 \mod p$.

Teorema de Wilson. Si p es primo, entonces $(p-1)! \equiv -1 \mod p$.

Criterios de divisibilidad

Teorema de la base. Si $b > 2$, entonces cualquier número n puede expresarse en la forma $n = a_0 + a_1 b + a_2 b^2 + a_3 b^3 + \cdots a_k b^k$.

Entonces, para hallar un criterio de divisibilidad empleamos los siguientes pasos:

- Si $n \equiv 0 \mod m$, entonces $a_0 + a_1 b + a_2 b^2 + a_3 b^3 + \cdots a_k b^k \equiv 0 \mod m$. Así, buscamos el criterio de divisibilidad para cada sumando, y sumamos todos los criterios.

Grafos, Digrafos y Multigrafos

Primer teorema de de la Teoría de Grafos. Sea $G = (V, E)$ un grafo. Se cumple que la suma de los grados de los vértices equivale al doble del número de aristas del grafo:

$$\sum_{i=1}^{p} \mathsf{gr}(v_i) = 2\#E$$

Definiciones:

- Multigrafo: dos vértices tienen dos o más aristas que los unan.
- Pseudografo: uno o más vértices tiene una arista consigo mismo.
- Digrafo: grafo que indica direccionalidad de las aristas.
- Grafos isomorfos: si existe una biyección entre G y G'.
- Regular: grafo que tiene el mismo número de aristas en todos los vértices.
- Completo: si el grafo con n vértices tiene $n - 1$ aristas para todos los vértices.

Grafos eulerianos y hamiltonianos

Más definiciones:

- Camino: sucesion de vertices y aristas conectados.

$$v_0, v_0v_1, v_1, v_1v_2, \cdots, v_{n-1}, v_{n-1}v_n, v_n$$

- Camino cerrado: camino donde $v_0 = v_n$.
- Camino simple: camino donde no se repiten aristas.
- Ciclo: camino cerrado donde no hay repetición de vértices (sólo el primero y el último).
- Circuito: camino cerrado que no repite aristas.
- Grafo conexo/desconexo: grafo donde todos los vertices tienen una conexión. En otras palabras, si para cada par de vértices u, v, existe un camino que conecte ambos vértices.
- Grafo euleriano: grafo donde todos los vértices pueden crear un camino que contenga una única vez todas las aristas.
- Grafo hamiltoniano: un grafo que admite un ciclo hamiltoniano, es decir, un ciclo que contiene todos los vértices del grafo.

Un grafo es euleriano si el grado de todos los vértices es par o si todos menos dos vértices tienen grado par. En este último caso, el camino tiene que empezar por uno de los vértices con grado impar y acabar por el otro. Si el grafo no cumple estas características no es euleriano.

Si para un grafo $G = (V, E)$ se cumple que, para todo v, $\text{gr}(v) \geq \frac{n-1}{2}$, entonces admite un camino hamiltoniano. Esto también es cierto si para todo par de vértices v, w, $v \neq w$, $\text{gr}(v) + \text{gr}(w) \geq n - 1$. Además, si para todo v, $\text{gr}(v) \geq \frac{n}{2}$, entonces G es hamiltoniano. Aviso: esto no quiere decir que si $\text{gr}(v) \leq \frac{n}{2}$ entonces G no sea hamiltoniano.

Exploración de grafos

Sea $\mathcal{M}$ la matriz de adyacencia de un grafo. $\mathcal{M}^n$ es la matriz que indica todos los caminos de longitud n disponibles entre los pares de vertices v_i, v_j del grafo.

La matriz $\mathcal{C} = \mathcal{M}^{p-1} + \mathcal{M}^{p-2} + \mathcal{M}^2 + \mathcal{M}$, con p el número de vértices del grafo, indica todos los posibles caminos de longitud $< p$. Si alguna entrada de $\mathcal{C}$ es nula, el grafo no es conexo.

Un arbol es un grafo conexo sin ciclos. Por tanto, un grafo es un árbol sii cada dos vértices distintos del árbol se conectan por un único camino simple. Si el árbol T es un subgrafi de un grafo conexo G, T es un subárbol conectante / maximal.

Sea (T, r) un árbol con raíz, y v y w dos vértices de T. Si dice que $v \geq w$ si el camino que une r con w pasa por v.

Mapas y coloraciones

Un grafo es plano si admite una representación gráfica en el plano de modo que cad arista corta únicamente a otra arista en un vértice que sea extremo de ambas. Un mapa es la representación de un grafo plano. Cada porción pintada de un mapa se denomina región. El grado de la región es la longitud del camino que la bordea.

La suma de los grados de la regiones de un mapa es igual al doble del número de aristas de este.

Teorema de Euler. Sea M un mapa conexo con $\#R$ regiones. Entonces se cumple que $\#V + \#R - \#E = 2$.

Si $G = (V, E)$ es un grafo plano conexo con $\#V \geq 2$, entonces $\#E \leq 3\#V - 6$. Si tenemos que en G no existe ningún grafo isomorfo al grafo completo K_3, entonces $\#E \leq 2\#V - 4$.

Teorema de Kurtakowski. Un grafo es plano si no contiene ninguna subdivisión de K_5 o $K_{3,3}$.

Un grafo es bipartito si admite una coloración con dos colores, $\gamma : V \to \{0, 1\}$. Un grafo es bipartito sii o ciclos de longitud impar.

Un clique es un conjunto de vértices tal que para cada par de vértices haya una arista que los conecte. Es decir, es un subgrafo completo.

Métodos combinatorios: técnicas básicas

Principio de adición: sean $A_1, A_2, \cdots, A_n$ conjuntos finitos tales que $A_i \cup A_j = \emptyset$, entonces $|\bigcup A_i| = \sum |A_i|$.

Principio de multiplicación: $A_1, A_2, \cdots, A_n$ conjuntos finitos, entonces $|A_1 \times A_2 \times \cdots \times A_n| = |A_1||A_2| \cdots |A_n|$.

Principio de distribución: dados n enteros $m_1, m_2, m_3, \cdots, m_n$ tales que $(\sum m_i)/n > p$, entonces existe un $m_i > p$.

Permutaciones, combinaciones y variaciones

- Variaciones = número de aplicaciones inyectivas: $\mathsf{V}(n, r) = \frac{n!}{(n-r)!}$
- Variaciones con repetición (n letras diferentes en r posiciones): $\mathsf{VR}(n, r) = n^r$.
- Combinaciones: $\mathsf{C}(n, r) = \frac{n!}{r!(n-r)!}$.
- Combinaciones con repetición, equivalente a resolver $x_1 + x_2 + \cdots + x_r = n$: $\mathsf{CR}(n, r) = \mathsf{C}(n + r - 1, n)$
- Permutaciones circulares de n objetos en r posiciones: $\mathsf{P}(n, r) = \mathsf{C}(n, r) \cdot (r - 1)!$.

Teorema del Binomio

Fórmula de Pascal.

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

Teorema del Binomio.

$$(x+y)^n = \sum_{i=0}^{n} \binom{n}{i} x^i y^{n-i} \qquad \rightarrow \qquad \sum_{i=0}^{n} \binom{n}{i} = 2^n$$

Para cada $m, k \in \mathbb{N} \cup \{0\}$ y para $k \leq m$ se tiene la igualdad.

$$\binom{m+1}{k+1} = \binom{k}{k} + \binom{k+1}{k} + \cdots + \binom{m}{k}$$

Coeficiente multinómico. Dados n objetos de k tipos, cuales el número de combinaciones con n_i objetos del tipo i.

$$P(n, n_1, n_2, \cdots, n_k) = \binom{n}{n_1}\binom{n-n_1}{n_2}\binom{n-n_1-n_2}{n_3}\cdots = \frac{n!}{n_1! n_2! \cdots n_k!}$$

Este es el mismo coeficiente que se aplicaria para un desarrollo de la fórmula de Leibniz: $(x_1 + x_2 + ... + x_k)^n$.

Principio de inclusión-exclusión

Sea S un conjunto finito y $P_1, P_2, \cdots, P_n$ propiedades de cada uno de los elementos de S, que pueden o no satisfacerse. Entonces, S_i es el conjunto de elementos que satisfacen la propiedad P_i, mientras que $\overline{S_i}$ es el conjunto de elementos que no la satisfacen. Dicho esto, definimos dos expresiones:

$$\left|\bigcap_{i=1}^{n} \overline{S_i}\right| = |S| - \sum_{i=1}^{n} |S_i| + \sum |S_{i1} \cap S_{i2}| + \cdots + (-1)^k \sum |S_{i1} \cap S_{i2} \cap \cdots \cap S_{ik}| + \cdots + (-1)^n \sum |S_1 \cap S_2 \cap \cdots \cap S_n|$$

$$\left|\bigcup_{i=1}^{n} \overline{S_i}\right| = \sum_{i=1}^{n} |S_i| - \sum |S_{i1} \cap S_{i2}| + \cdots + (-1)^{k-1} \sum |S_{i1} \cap S_{i2} \cap \cdots \cap S_{ik}| + \cdots + (-1)^{n-1} \sum |S_1 \cap S_2 \cap \cdots \cap S_n|$$

Desordenaciones. El número de permutaciones tales que ninguno de los elementos de la permutación coincide con el original es el número de desordenaciones, $d(n)$.

$$d(n) = n! \sum_{j=0}^{n} \frac{(-1)^j}{j!}$$

Recursividad y relaciones recurrentes

Una relación de recurrencia de la forma $r(n) = a_1 r(n-1) + a_2 r(n-2) + \cdots + a_t r(n-t) + k(n)$ es una relación de recurrencia lineal. Si $k(n) = 0$, entonces es lineal homogénea.

Sea $r(n) - a_1 r(n-1) - a_2 r(n-2) - \cdots - a_t r(n-t) = 0$ una relación de recurrencia lineal y homogénea. La expresión $x^t - a_1 x^{t-1} - a_2 x^{t-2} - \cdots - a_{t-1} x - a_t = 0$ es la ecuación característica asociada.

Sean $b_1, b_2, \cdots, b_t$ las soluciones a la ecuación característica, entonces, la expresión original de la recurrencia puede expresarse como $r(n) = c_1 b_1^n + c_2 b_2^n + \cdots + c_t b_t^n$, con $c_1, c_2, \cdots, c_t$ los coeficientes que se obtienen resolviendo los sistemas asociados a las t condiciones iniciales:

$$\begin{cases} r(1) = c_1 b_1 + c_2 b_2 + \cdots + c_t b_t \\ r(2) = c_1 b_1^2 + c_2 b_2^2 + \cdots + c_t b_t^2 \\ \vdots \\ r(t) = c_1 b_1^t + c_2 b_2^t + \cdots + c_t b_t^t \end{cases}$$

Si alguna de las raíces b_i aparece repetida la solución general de la recurrencia es de la forma:

$$r(n) = c_1 b_1^n + c_2 b_2^n + \cdots + (c_{i1} + c_{i2} n + c_{i3} n^2 + \cdots + c_{ik} n^{k-1}) b_i^n + \cdots + c_t b_t^n$$