TEORÍA Y ESTRATEGIAS DE RESOLUCION DE PROBLEMAS

1.- Esquema teórico para problemas bloque de aritmética

Rigor en matemáticas, principales definiciones:

- Axioma: es una proposición o enunciado tan evidente que se considera que no requiere demostración.
- Lema: una afirmación demostrable que forma parte de un teorema más amplio.
- Corolario: una afirmación fácilmente demostrable a partir a un teorema.
- Proposición: una afirmación demostrable o resultado no asociado a ningún teorema en particular. Muchos expertos usan proposición como sinónimo de teorema.
- Conjetura o hipótesis, una afirmación que se supone verdadera, aún no demostrada.

Tipos de demostraciones más comunes en matemáticas:

- Principio de inducción: Es un método de probar proposiciones que dependen de un número n (que normalmente está dentro de un conjunto o subconjunto de los números naturales, pero que es posible que sean un número entero a partir de un número fijo).
    - Se demuestra para un valor dado, al que llamaremos $\boldsymbol{P_1}$
    - Suponemos que se cumple para P_n, a lo que llamaremos hipótesis de inducción, y utilizándolo debemos demostrar que se cumple para P_{n+1}
- Reducción al absurdo: este método de demostración consiste en suponer una hipotética la veracidad o falsedad, y se llega a una contradicción lógica, un absurdo, con lo cual se concluye que la hipótesis de partida ha de ser falsa.
- Por contraposición: Esta regla se infiere una sentencia condicional a partir de su contraposición. En otras palabras, la conclusión «si A, entonces B» se extrae de la premisa simple «si no B, entonces no A.
- Doble implicación: Para probar que dos condiciones $P_1 \ y \ P_2$ son equivalentes, se puede demostrar que $P_1 \Rightarrow P_2 \ \ y \ P_2 \Rightarrow P_1$, y con ello, estarán demostradas ambas.
- Conjunto contenido en otro: Para demostrar que un conjunto A está contenido en otro B se procede a coger un elemento cualquiera de A y se procederá a ver que está contenido en B. Así, si un elemento cualquiera de A está en B, significa que todos lo están y será $A \subseteq B$.

Conjuntos numéricos:

- Números naturales: Nacen para contar, $1, 2, 3, \ldots$.
- Números enteros: Nacen para poder representar y operar con los números que representan las restas que no son naturales, $-1, -2, \ldots$

- Números racionales: Nacen para poder representar y operar con los números que representan las divisiones de los anteriores que no resultan un número entero, $\frac{1}{2}, -\frac{2}{3}, \ldots$
- Números reales: Nacen para completar los anteriores de tres maneras:
  - Numéricamente aquellos números decimales no periódicos con infinitos decimales
  - Geométricamente para representar diagonales de cuadrados, relación entre el radio y el área de un círculo
  - Algebraicamente para resolver ecuaciones como $x^2 - 2 = 0$
  - Axiomáticamente para que cualquier conjunto de los números anteriores tenga un supremo.

  Se dividen en algebraicos o trascendentes si son solución de un polinomio no nulo con coeficientes racionales o no.
- Números complejos: Nacen para representar y operar con los números que son soluciones de todas las ecuaciones de una incógnita. La definición de sus operaciones (en particular el producto y la división) hace que sea muy útil su representación como vectores de $\mathbb{R}^2$.
- Cuaterniones: La interpretación geométrica de los complejos llevo a Hamilton a pensar como extender esa idea a $\mathbb{R}^3$ y creo los cuaterniones con operaciones similares a los complejos…

En ejercicios con **divisores y múltiplos** hay varios teoremas que nos son de gran utilidad:

- Relación entre mcd y mcm: $a \cdot b = mcm(a,b) \cdot mcd(a,b)$
- Algoritmo de Euclides: $\mathrm{a, b, c, d} \in \mathbb{Z}$ y $\mathrm{a = bq + r}$, siguiendo la división Euclidea, entonces: $mcd\ (a,b) = mcd\ (b,r)$
- Lema de Euclides: Sea p primo y a, b € $\mathbb{Z}$, si p/ab => p/a ó p/b
- Identidad de Bezout: sean $a_1, a_2, \ldots, a_n \in \mathbb{Z}$, d$\in \mathbb{Z}$ su m.c.d. entonces $\exists\ c_1, c_2, \ldots \ldots c_n \in \mathbb{Z}$ tal que $d = a_1c_1 + a_2c_2 + \cdots \ldots + a_nc_n$. Ojo, esta identidad no se cumple en $\mathbb{N}$.
- $\mathbb{Z}$ es un dominio de factorización única
- El número de divisores del número $n = p_1^{k_1} \cdot p_2^{k_2} \cdots\cdots p_r^{k_r}$ así descompuesto en números primos es $(k_1 + 1) \cdot (k_2 + 1) \cdot \ldots . (k_r + 1)$
- La suma de todos los divisores anteriores, utilizando la suma de una serie geométrica, será:

$$s = \frac{p_1^{k_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{k_2+1} - 1}{p_2 - 1} \cdot \ldots . \cdot \frac{p_r^{k_r+1} - 1}{p_r - 1}$$

Para entender muchos de los temas del bloque de Teoría de números conviene entender bien en matemáticas que es una **relación de equivalencia y de orden**, porque se utiliza principalmente para la construcción de muchos tipos de números:

- Relación de orden R: Es una relación binaria que cumple las propiedades:
  - Reflexiva: aRa

- Antisimétrica: $aRb \ y \ bRa \Rightarrow a = b$
- Transitiva: $aRb \ y \ bRc \Rightarrow aRc$

- Relación de equivalencia, Es una relación binaria que cumple las propiedades:
  - Reflexiva: aRa
  - Simétrica; $aRb \Rightarrow bRa$
  - Transitiva: $aRb \ y \ bRc \Rightarrow aRc$

  Una clase de equivalencia, son todos los elementos que se relacionan con uno dado.

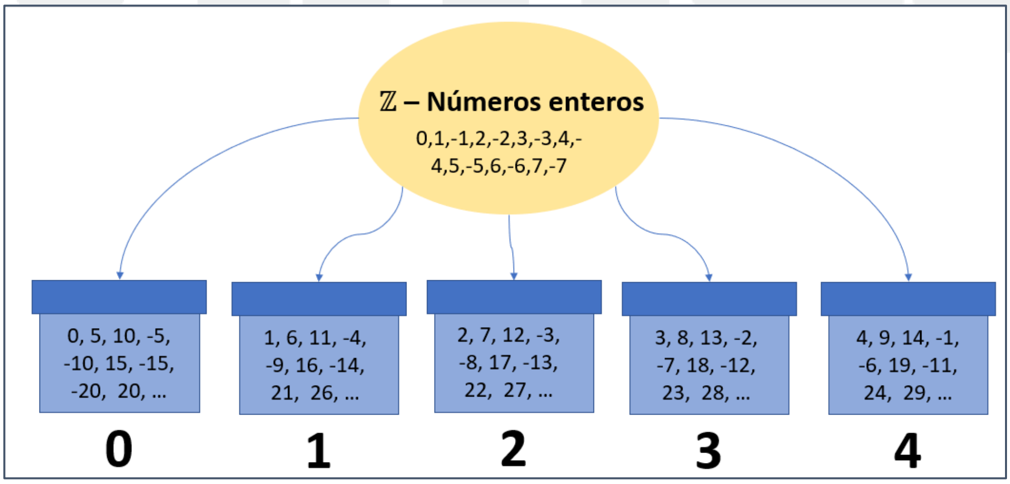
Recordemos que la descomposición de un número en el sistema de numeración de base b)

$$a_n a_{n-1} a_{n-2} \dots . a_1 a_{0 \ k)} = a_n b^n + a_{n-1} b^{n-1} + \cdots a_1 b + a_0$$

En muchos casos puede verse esta suma como la suma de una serie geométrica, y ayudarnos de eso en la resolución de problemas. $\sum_{k=1}^{n} b^n = \frac{b^{n+1}-1}{b-1}$

Congruencias:

- Números congruentes: $a \equiv b\big(mod(n)\big) \Leftrightarrow (a-b) \equiv 0\big(mod(n)\big) \rightarrow Relación \ de \ equivalencia$



- Propiedades: $a(modp) + b(modp) = a + b \ (modp) \ y \ \ a(modp) \cdot b(modp) = a \cdot b \ (modp)$
- Hay p clases distintas módulo p
- Elemento Inverso Un elemento a de $\mathbb{Z}_p$ admite inverso si, y sólo si, y a y p son primos entre sí.
- Pequeño teorema de Fermat: Sea p primo, y $a > 0 \ \ => \ \ a^p \equiv a(modp)$ o $a^{p-1} \equiv 1(modp)$
- Teorema de Wilson: Si p es un número primo, entonces $(p \ - \ 1)! \ \equiv \ -1 \ (mod \ p)$

Criterios de divisibilidad/Restos potenciales:

- Sea n un entero positivo, y sea $n = \sum_{i=0}^{k} a_i 10^i$ su representación decimal, y sean r_i los restos de la división de 10^i para $p \geq 2, i = 1,2, . . k$, entonces:

  n es divisible por p si, y sólo lo es $\sum_{i=0}^{k} a_i r_i$

- Definición: Los restos potenciales de n módulo m, son los restos de las divisiones de n^i entre m.
- Hay como máximo m restos potenciales.
- Si un resto potencial se anula, lo hacen los sucesivos
- Si dos restos potenciales se igualan, entonces se repite la serie subsecuentemente, el periodo es llamado Gaussiano.

Números combinatorios/Binomio de Newton:

Se define como número combinatorio $n\ sobre\ k$: $\binom{n}{k} = \frac{n!}{k!(n-k)!}$

Recordemos que el **binomio de Newton** es muy útil en multitud de problemas y que es una generalización de las identidades notables "cuadrado de una suma o diferencia".

$$(a+b)^n = \binom{n}{0} a^n b^0 + \binom{n}{1} a^{n-1} b^1 + \cdots \ldots \ldots .. + \binom{n}{n} a^0 b^n$$

Cuadrados perfectos:

- Son aquellos números que son cuadrado de un número natural.
- Los cuadrados perfectos acaban en 0,1,4,5,6 y 9
- En la descomposición factorial, todos los exponentes son pares.
- Son congruentes con $0,1(mod 4)$
- De hecho, el cuadrado de un número par siempre es múltiplo de 4, ya que $(2n)^2 = 4n^2$. El cuadrado de un número impar siempre es impar, ya que $(2n + 1)^2 = 4(n^2 + n) + 1$.

2.- Estrategias para resolver problemas de aritmética

1	Cuando habla de demostrar alguna característica de teoría de números en referencia a n, intentar siempre como una opción probarlo por **inducción. Si habla de múltiplo o divisible,** también es una opción tomar congruencias. Ej: Demostrar que $3n - 2n^2 - 1$ es múltiplo de 8
2	**Acotar** las posibilidades en problemas de sistemas de numeración y tantear las posibilidades acotadas. Ej.: Calcula la suma de los dígitos de la suma de los dígitos de la suma de los dígitos de 4444^{4444} Sol 7
3	Utilizar el **pequeño Teorema de Fermat,** cuando tengamos potencias, intentando que el exponente sea o le falte 1 para ser un número primo. Ej: Probar que la diferencia $(27^4)^9 - (25^3)^6$ es múltiplo de 37.
4	Tomar **congruencias apropiadas** eligiendo bien el número natural para probar problemas de múltiplos y divisores. Ej: Demostrar que, para p primo, $3^p + (-2)^p + (-1)^p$ es divisible por p.
5	Utilizar el **algoritmo de Euclides** para reducir el criterio de números grandes a números pequeños puesto que el m.c.d. coincide al hacer la división Ej; $mcd(2n, 2n+2) = 2, mcd(2n-1, 2n+1) = 1$ $mcd(n, n+1) = 1$
6	**Descomponer un número en potencias como una sucesión o serie** para poder más tarde convertirlo en producto o suma de varios Ej: Demostrar que en cualquier sistema de numeración 10101, 101010101, 1010101010101, ….. no son primos.
7	Razonamiento de factores en **números consecutivos** o múltiplos consecutivos. Ej: Sean $a, b, c, d \in \mathbb{Z}$, probar que $abcd(a^2 - b^2)(a^2 - c^2)(a^2 - d^2)(b^2 - c^2)(b^2 - d^2)(c^2 - d^2)$ es divisible entre 7
8	Utilizar la estrategia **par/impar y aumentarla hasta congruencias tipo 4** para poder discriminar las posibilidades. Ej. Encontrar todos los $n \in \mathbb{N}$, tal que $3^n - 8$ es un cuadrado perfecto.
9	Utilizar el **binomio de Newton** siempre que tengamos una potencia para desarrollarlo Ej. Sea X un conjunto de n elementos. Probar que el número de parejas (A, B) con A y B subconjuntos de X, A subconjunto de B y $A \neq B$ es igual a $3^n - 2^n$.
10	**Problemas que tratar con cifras de un número siempre conviene hacer la descomposición polinómica y tratarlo con múltiplos y divisores y basados en la suma de sus cifras:** Ej: Demostrar que no existe ningún número natural que resulte ser la mitad del número que se obtiene al pasar su cifra inicial a la final.
11	Cuando habla de cuadrados o cubos perfectos, se puede jugar con **la suma de las cifras del número general**, porque un cuadrado o cubo perfecto tiene que ser múltiplo de 4 o 1 mod(4). También intentar

	expresarlo en caso de que existiera y pasar el -1 al otro lado, pero lo importante aquí es jugar siempre con **suma por diferencia.** Ej. Encontrar todos los $n \in \mathbb{N}$, tal que $3^n - 8$ es un cuadrado perfecto.
12	Cuando tengamos dos variables, crea una **tabla de doble entrada con todas las posibilidades** para entender el problema. Ej. Demostrar que $\sum_{i,j=1}^{p+1} i^j$ es múltiplo de p
13	**La suma de las cifras de un número y ese número son congruentes módulo 9**. Lo mismo con el 3. Este resultado nos sirve para acotar y descartar muchos números. Ej: Calcula la suma de los dígitos de la suma de los dígitos de la suma de los dígitos de 4444^{4444} Sol 7.
14	Aunque sean problemas de números naturales o enteros, como los números reales los contienen, podemos definir una **función de variable real que conozcamos** que nos ayude a resolver un problema de acotación de números, que podamos **derivar y calcular sus mínimos y máximos**. Ej: establecer cuando $a^b\ es\ mayor\ que\ b^a\ y\ viceversa$
15	Calcular el polinomio mínimo de una raíz cúbica, utilizar $(x+y)^3 = x^3 + y^3 + 3xy(x+y)$ Ej: Ver si $\sqrt[3]{45+29\sqrt{2}} + \sqrt[3]{45-29\sqrt{2}}$ si es un número natural
16	Utilizar el **lema de Euclides** para establecer relaciones de divisores entre varios números en una ecuación Ej: Demostrar que no existe ningún número natural que resulte ser la mitad del número que se obtiene al pasar su cifra inicial a la final.