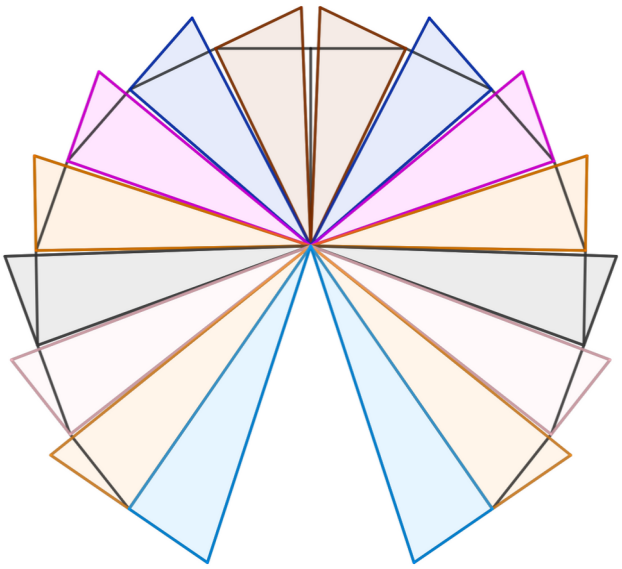
JORGE MORRA

Tema 4. Números Enteros. Divisibilidad. Números Primos. Congruencias.

OPOSICIONES
MATEMÁTICAS

JORGE MORRA

Tema 4. Números Enteros. Divisibilidad. Números Primos. Congruencias.



OPOSICIONES
MATEMÁTICAS

Prólogo

Tiene delante el lector el cuarto cuadernillo de la serie "Oposiciones Matemáticas", concretamente el de números enteros, divisibilidad, números primos y congruencias..

Como ya expuse en prólogos anteriores, para poder enfrentarse con cierta solvencia al examen de oposición de Matemáticas, la construcción de cada tema debe contener y diferenciar tres partes: una presentación, un nudo y un desenlace. Parecen las mismas tres partes que encontramos en una película o un libro, sí, lo son, pero es que cuando contamos algo necesitamos que *"ese algo"* tenga entidad por sí solo. Pensemos que un tribunal no es más que nuestro público, y si queremos aprobar tenemos que *"entretenerlos"*. ¿Qué mejor forma de gustarles que contarles un cuento?

De las tres partes, la primera la utilizaremos para presentar el tema, justificar todo el contenido que vamos a exponer y encuadrarlo dentro de la Historia y dentro de nuestra propuesta.

En la segunda debemos ordenar todos los contenidos de acuerdo a los resultados que vayamos a mostrar, aunque no probemos todo porque no va a ser posible con todas las proposiciones, teoremas, lemas o corolarios que enunciemos. Pero, insisto, es necesario que al menos se expongan en el orden correcto. Sobre esto los matemáticos somos bastante exigentes, los lemas preceden a los teoremas, y los corolarios los suceden, por poner un ejemplo.

Acabaremos poniendo la "guinda" al pastel en la tercera y última parte. Bueno..., así dicho parece más una receta de cocina que el desarrollo de un tema de Matemáticas. Básicamente debemos acabar con un resultado importante, demostrado o no, eso importa menos, pero sí relevante.

Para que las tres partes puedan funcionar y constituirse como un todo, es imprescindible que sepamos a priori lo que tenemos tiempo de escribir, presentar o exponer; y para ello es también preciso que nos preparemos el tema *"a conciencia"*.

Las oposiciones de Matemáticas no son fáciles, como tampoco lo son las Matemáticas. *"A conciencia"* significa que hay que conocer todo o casi todo de lo que estamos tratando, porque controlando el tema evitamos que él nos controle a nosotros. Cuando sabemos de lo que hablamos, podemos improvisar en cualquier momento; no importa que no recordemos un paso en un teorema porque sabemos dónde queremos llegar, saltamos el teorema o el paso correspondiente dándolo por demostrado y añadimos algún otro apartado para completar el desarrollo. Todo depende de lo que lo dominemos.

Pero preparar o prepararse un tema de oposición no es nada sencillo. Debemos *saber* Matemáticas, y además las *mínimas* del tema que escribamos. Pero si no es así porque nos ha tocado uno de los peor preparados, tenemos que dar a entender al Tribunal que *sí las sabemos*, y que las cosas que no contamos no es porque las desconozcamos sino porque nos falta tiempo.

No quiero extenderme más, espero que la lectura y el trabajo con este cuarto cuadernillo

sea productivo para todos aquellos que quieran o bien conocer algo más de esta ciencia o bien convertirse en profesores de Secundaria..., o ambas cosas.

Por último agradecer al lector el trabajo que está a punto de comenzar y mencionarle que todos aquellos comentarios que considere oportunos, bien de profundización de algunos puntos, bien de inconsistencias, errores o erratas en algunas demostraciones, o bien sugiriendo nuevos apartados o secciones, puede hacérmelos llegar a través de mi correo electrónico: jorgemorra@outlook.es. Si bien es cierto que aunque no pueda asegurar contestarlos, sí puedo asegurar leerlos.

Jorge Morra

Madrid, septiembre de 2019

Índice

Página

1. ¿Cómo preparar este tema?

Es este el primer tema de Teoría de Números, aunque no esté definido como tal. Cuando se habla de divisibilidad o se habla del máximo común divisor, entramos de lleno en conceptos de ecuaciones en números enteros, o por lo menos en conceptos que se utilizan para resolver dichas ecuaciones.

Es, sin duda, uno de los temas más amplios de todo el temario. La definición de los enteros, así como de sus propiedades y de la estructura algebraica que tienen, ya podría llenar fácilmente todo su contenido; pero además se añade la divisibilidad, de la que se han escrito libros enteros; los números primos, a la sazón los grandes desconocidos, y acabamos con la congruencia, que es el preludio de todas las ecuaciones diofánticas o en números enteros.

Es claro que nos encontramos ante un dilema: presentar y demostrar todo lo interesante, o bien presentar solamente, demostrar lo imprescindible y enunciar lo que se considere básico al menos para que el tema pueda desarrollarse decentemente.

El dilema no es fácil. Por una parte soy de los que creen que los resultados importantes hay que enunciarlos y demostrarlos; y por otra pienso que en el tiempo que tiene el lector de desarrollo en la oposición no tiene sentido perderlo en la prueba de algunos teoremas.

Como en todos los temas hasta ahora es importante leer y entender todo el contenido al completo, desde la primera hasta la última línea. Siempre insisto en lo mismo porque en ocasiones tendemos a saltarnos partes de un texto ya que lo consideramos poco importante, o porque creemos que lo conocemos; en este caso le pido al lector que no lo haga.

Cuando lo haya leído y entendido, ya tendrá una idea de lo que le quiero contar, ahora viene la parte más difícil, que es la de sintetizar, resumir y concretar lo que quiere escribir.

En ese momento puede optar por una de dos alternativas, o lo hace por sí mismo, que es posiblemente la mejor propuesta puesto que de esta forma aprenderá todo del tema; o bien se deja aconsejar por mí y se estudia lo que yo le propongo, siempre por supuesto con posibilidades de cambiar lo que estime oportuno.

Es necesario también que tenga claro que lo que le voy a proponer es lo que le debe dar tiempo a desarrollar. Si puede escribir más tendrá que añadir más, y si escribe menos, tendrá que eliminar parte del tema; todo a su criterio.

Pues bien, comencemos:

- La **Introducción** es al completo. Es importante justificar lo que se va a exponer a continuación.
- De la sección 3, la de los **números enteros**, tenemos que definir $\mathbb{Z}$, enunciando al menos las propiedades de la relación de equivalencia. Después tenemos que definir ambas operaciones internas y demostrar que no dependen de los representantes elegidos. Finalmente tenemos que describir la estructura que tiene el conjunto de los enteros. Debemos enunciar las propiedades que cumplen: asociativa, conmutativa, etc., aunque sin demostración. Cuando lleguemos al orden no es necesario demostrar la relación de orden que se puede definir en $\mathbb{Z}$.

- De la sección de **divisibilidad y números primos entre sí**, hay que definir dichos conceptos y luego enunciar solamente los teoremas previos a la *Regla de la División*, que debe enunciarse y demostrarse. El concepto de *máximo común divisor* debe definirse, así como enunciarse los resultados previos al Algoritmo de Euclides, que debe demostrarse al igual que la Identidad de Bezout. Es interesante que los resultados posteriores se enuncien y se demuestren. Sobre el *mínimo común múltiplo*, debe definirse así como enunciarse y demostrarse las proposiciones que tiene esta sección.
- De la sección de los **números primos**, se define el concepto de *primo* y se enuncia y demuestra el Teorema de Euclides. La proposición posterior puede solamente enunciarse para justificar el procedimiento de la Criba de Eratóstenes. El Teorema Fundamental de la Aritmética debe enunciarse y demostrarse, aunque los lemas previos solamente se mencionen. La parte del teorema de los números primos debe incluirse al completo. Puede omitirse la demostración de Euler sobre el producto que lleva su nombre o sobre la suma de los inversos de los primos, pero toda la parte histórica y su relación con la conjetura de Riemann debe incluirse.
- De la última sección, la de **congruencias**, debe definirse el concepto y enunciar los resultados previos a las propiedades. Es importante introducir el conjunto de clases a partir de la relación de equivalencia, y definir $\mathbb{Z}_m$. La introducción de las operaciones en dicho conjunto, es también necesaria, demostrando que se encuentran bien definidas. La prueba de sus propiedades no es necesaria, solamente se enuncian. Por último debe dotarse a $\mathbb{Z}_m$ de una estructura algebraica y demostrar que es cuerpo si y solamente si m es primo. Los dos últimos teoremas, de Euler y Fermat no es necesario demostrarlos.

Si con esta síntesis del tema llena las dos horas de examen perfecto, en caso contrario lo dicho anteriormente, se deja a su criterio aumentar o disminuir contenidos.

2. Introducción

La definición de los números enteros como el conjunto de las clases de equivalencia de una relación, resuelve el problema de la resolución de ecuaciones dentro del conjunto de los números naturales. Tenga en cuenta el lector que las ampliaciones o extensiones que tienen los números desde los naturales a los complejos, pueden verse como consecuencia de la resolución de algunas ecuaciones que en sus conjuntos originales no encontraban solución.

El primer caso lo tenemos delante al intentar resolver en $\mathbb{N}$ la ecuación $n + 4 = 3$. El conjunto de los números enteros surge, independientemente de ser una consecuencia de la axiomatización de la Aritmética, (uno de los objetivos de Hilbert), como solución al problema de la resolución de cualquier ecuación con números naturales[1].

Esta extensión consigue ampliar la estructura de $\mathbb{N}$ a una de grupo conmutativo con la adición, añadiendo incluso un elemento neutro (el cero[2]). Además con la operación "pro-

[1] El caso de los racionales, $\mathbb{Q}$, de los reales, $\mathbb{R}$ o de los complejos, $\mathbb{C}$ se tratará en temas posteriores.

[2] En algunos textos se incluye al cero como número natural, en éste particulamente no lo estamos haciendo.

ducto" (ya definida sobre $\mathbb{N}$), y la demostración de algunas de sus propiedades, el conjunto de los enteros obtendrá una nueva estructura que será la de *Dominio de Integridad*.

La definición de divisibilidad permite introducirnos dentro del mundo de los números primos y del Teorema Fundamental de la Aritmética, así como de la demostración del Teorema de Euclides.

La parte más interesante del tema se encuentra al abordar la cantidad de números primos que existen. La *conjetura de Riemann* junto con la demostración de Euler de que la suma de los inversos de los primos es infinita nos acerca a una aproximación bastante real del cardinal de dicho conjunto.

3. Números Enteros, $\mathbb{Z}$

El edificio de las Matemáticas está construido sobre una serie de axiomas. Con ellos se consigue todo el entramado que hoy conocemos; con los axiomas se deducen proposiciones y definiciones, con éstos más proposiciones y más definiciones, y así hasta completar lo que conocemos del edificio.

A partir de los números naturales, construidos axiomáticamente de los postulados de Peano, se puede definir un nuevo conjunto que será el de los números enteros. Una de las propiedades interesantes de este conjunto será la resolución de aquellas ecuaciones que no podían resolverse dentro de los naturales.

Consideremos $\mathbb{N} \times \mathbb{N} : \{(a, b) : a, b \in \mathbb{N}\}$. Sobre este conjunto podemos considerar una relación $\mathcal{R}$:

$$(a, b)\mathcal{R}(c, d) \Leftrightarrow a + d = b + c$$

Proposición 3.1 *La relación antes definida es una relación de equivalencia.*

Demostración: La demostración es trivial y se deja para el lector.

A partir de aquí podemos formar las clases de equivalencia:

$$\overline{(a, b)} = \{(x, y) \in \mathbb{N} \times \mathbb{N} : (a, b)\mathcal{R}(x, y)\}$$

Definición 3.2 *Llamaremos conjunto de los* ***Números Enteros*** *y lo denotaremos como* $\mathbb{Z}$ *al conjunto resultante de las clases de equivalencia:*

$$\mathbb{Z} = \frac{\mathbb{N} \times \mathbb{N}}{\mathcal{R}}$$

Para escribir un número entero no vamos a utilizar el conjunto de clases, sino que lo haremos dependiendo de cualquier elemento de ella. Dado $\overline{(a, b)} \in \mathbb{Z}$:

- Si $a > b$ entonces escribiremos $m = \overline{(a, b)}$ siendo $m = a - b$.
- Si $a = b$ entonces escribiremos $0 = \overline{(a, b)}$
- Si $a < b$ entonces escribiremos $-m = \overline{(a, b)}$ siendo $m = b - a$.

Esta forma de denotar a los elementos de $\mathbb{Z}$ no depende del representante elegido. El lector puede comprobarlo sin excesiva complicación.

A los números que se escriben con el signo *"menos"* se les llama números negativos.

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$$

Los negativos a la izquierda, después el cero, y los positivos a la derecha. Esta manera de escribirlos no es casual, en secciones posteriores introduciremos un orden en $\mathbb{Z}$, que será el que especifique su disposición.

Comencemos, antes de nada, incluyendo dos operaciones necesarias en $\mathbb{Z}$: la adición y el producto de números enteros.

Consideremos la aplicación:

$$\begin{array}{rccc} f: & \mathbb{Z}\times\mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & (m,n) & \longmapsto & f(m,n) \end{array}$$

tal que si $m = \overline{(a,b)}$ y $n = \overline{(c,d)}$, entonces:

$$f(m,n) = \overline{(a+c, b+d)}$$

Es obvio que tenemos que comprobar que f está bien definida; es decir, si dados dos pares de elementos que pertenezcan a las mismas clases, sus imágenes coinciden.

Proposición 3.3 *La función f se encuentra bien definida.*

Demostración: En efecto, sean $m = \overline{(a,b)}$ y $m' = \overline{(a',b')}$ dos elementos de $\mathbb{Z}$, con $m = m'$; y sean además $n = \overline{(c,d)}$, y $n' = \overline{(c',d')}$, también con $n = n'$.

Entonces

$$m + n = \overline{(a,b)} + \overline{(c,d)} = \overline{(a+c, b+d)}$$
$$m' + n' = \overline{(a',b')} + \overline{(c',d')} = \overline{(a'+c', b'+d')}$$

Como $a + b' = b + a'$ y $c + d' = d + c'$, es fácil ver que

$$a + c + b' + d' = a + b' + c + d' = b + a' + d + c' = b + d + a' + c'$$

con lo que

$$\overline{(a+c, b+d)} = \overline{(a'+c', b'+d')}$$

y con ello

$$m + n = m' + n'$$

$\otimes$

A partir de este momento podemos cambiar la notación de f y escribir el signo $+$, que es como comúnmente se conoce a la adición.

$$\begin{array}{rccc} +: & \mathbb{Z}\times\mathbb{Z} & \longrightarrow & \mathbb{Z} \\ & (m,n) & \longmapsto & +(m,n) = f(m,n) = m+n \end{array}$$

Proposición 3.4 *La operación $+$, es una ley de composición interna que dota a $\mathbb{Z}$ de una estructura de grupo abeliano.*

Recordemos que para alcanzar la estructura de grupo, un conjunto debe tener una operación interna que verifique las propiedades asociativa, existencia de elemento neutro y existencia de elemento opuesto. Si deseamos que además el grupo sea abeliano o conmutativo, dicha operación también tiene que cumplir la propiedad conmutativa.

Las demostraciones de cada una de estas propiedades son bastante elementales.

Comencemos con la asociativa. Sean m, n, p tres números enteros: $m = \overline{(a,b)}$, $n = \overline{(c,d)}$ y $p = \overline{(e,f)}$.

Ya que la asociativa es una propiedad que sí se verifica para los números naturales, se tiene:

$$\begin{aligned}(m+n)+p &= (\overline{(a,b)} + \overline{(c,d)}) + \overline{(e,f)} = \overline{(a+c,b+d)} + \overline{(e,f)} = \\ &= \overline{((a+c)+e,(b+d)+f)} = \overline{(a+(c+e),b+(d+f))} = \\ &= \overline{(a,b)} + \overline{(c+e,d+f)} = \overline{(a,b)} + (\overline{(c,d)} + \overline{(e,f)}) = \\ &= m + (n+p)\end{aligned}$$

El elemento neutro de los enteros será el 0. En efecto:

$$\begin{aligned}m + 0 &= \overline{(a,b)} + \overline{(c,c)} = \overline{(a+c,b+c)} = \\ &= \overline{(c+a,c+b)} = \overline{(c,c)} + \overline{(a,b)} = \\ &= 0 + m\end{aligned}$$

Y por otra parte, como $(a,b)\mathcal{R}(a+c,b+c)$, se tiene

$$m + 0 = \overline{(a,b)} + \overline{(c,c)} = \overline{(a+c,b+c)} = m$$

El elemento opuesto de un número m será $-m$. Consideremos $m = \overline{(a,b)}$, entonces $-m = \overline{(b,a)}$

Se tiene:

$$m + (-m) = \overline{(a,b)} + \overline{(b,a)} = \overline{(a+b,b+a)} = 0$$

También:

$$(-m) + m = \overline{(b,a)} + \overline{(a,b)} = \overline{(b+a,a+b)} = 0$$

Queda por último demostrar la propiedad conmutativa, pero ésta se deja para el lector.

En definitiva: $(\mathbb{Z}, +)$ tiene estructura de grupo abeliano.

$\otimes$

Además podemos definir otra ley de composición interna que llamaremos producto por estar relacionada con el producto de números naturales.