Teoría de Números

Orlando Ochoa Castillo

25 de septiembre de 2011

1. Divisibilidad

La Teoría de Números es un tema muy importante en las Olimpiadas de Matemáticas, esta área estudia el comportamiento de los números enteros, observando distintas características de ellos.

Un tipo de números muy particulares son los llamados *Números primos* que son aquellos números naturales que tienen exactamente dos divisores positivos.

El primer teorema importante que induciremos es:

Teorema 1.1 (Teorema Fundamental de la Aritmética)**.** *Todo número entero positivo mayor a 1 se puede representar de forma única como producto de factores primos.*

Definición 1.2. *Decimos que* $\boldsymbol{a}$ *divide a* $\mathbf{b}$*, o bien, que* $\mathbf{b}$ *es divisible por* $\boldsymbol{a}$ *(se representa,* $a|b$*), si el resultado de dividir* b *entre* a *es entero, es decir, la división deja residuo 0.*

Normalmente decimos que si $a|b$, entonces a es un factor de b. Otra forma de decirlo es que $a|b$ significa que $b = am$, para algún entero m.

Proposición 1.3. *Las siguientes propiedades se cumplen:*

1. *Si* $a|b$*, entonces* $a|bc$ *para cualquier* c *entero.*
2. *Si* $a|b$ *y* $b|c$*, entonces* $a|c$*.*
3. *Si* $a|b$ *y* $a|c$*, entonces* $a|b+c$ *y* $a|b-c$*, más aún,* $a|bx+cy$ *para cualesquiera* x *y* y *enteros.*
4. *Si* $a|b$ *y* $b|a$*, entonces* $a = \pm b$*.*
5. *Si* $a|b$ *y* $0 < a, b$*, entonces* $a \leq b$*.*
6. *Si* $p|ab$ *y* p *es primo, entonces* $p|a$ *o* $p|b$*.*

Otros elementos importantes para el estudio de la Teoría de Números son los siguientes:

Definición 1.4 (Mínimo Común Múltiplo)**.** *El mínimo común múltiplo de dos o más números es el número natural más pequeño que es múltiplo de ellos, o bien, el número natural más pequeño que es divisible por todos los números. El mínimo común múltiplo de dos números* x *y* y *se representa como* $mcm(x, y)$.

Definición 1.5 (Máximo Común Divisor)**.** *El máximo común divisor de dos o más números es el número natural mayor que divide a dichos números, se representa como* $mcd(x, y)$.

Definición 1.6. *Dos números se dicen primos relativos o coprimos si su máximo común divisor es 1.*

Anteriormente mencionamos que un número natural puede ser expresado como producto de números primos, digamos $N = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$, entonces el número de divisores de N es $(1 - \alpha_1) \cdot (1 - \alpha_2) \cdot \ldots \cdot (1 - \alpha_k)$.

Ejercicio 1.1. *El conjunto de números primos es infinito.*

Ejercicio 1.2. *Demostrar el criterio de divisibilidad del 3.*

Ejercicio 1.3. *Demostrar que un entero de la forma* $6k + 5$ *es necesariamente de la forma* $3k - 1$.

Ejercicio 1.4. *Demostrar que sólo existe un primo* p *tal que* $2p + 1$ *es un cubo.*

Ejercicio 1.5. *Encuentra los dígitos* c *y* d *tales que hacen verdadera la expresión* $2^c 9^d = 2c9d$*, donde* $2c9d$ *representa un número de cuatro dígitos.*

Problema 1.1. *Juan juega a escribir números. Iniciando con dos enteros positivos cualesquiera* a_1 *y* a_2*, Juan escribe en la lista de números positivos* $a_1, a_2, \ldots$ *de manera que cada número* a_{n+1} *a partir del tercero satisface la siguiente relación con los dos anteriores:*

$$a_{n+1} = a_n a_{n-1} - k a_n + 450.$$

Donde el número k *es el número entero positivo favorito de Juan. Beto observa que en la lista que ha escrito Juan está el número 2009 (pero no es ninguno de los primeros tres números de la lista) ¿Cuál es el número favorito de Juan?*

2. Residuos

Dado cualquier número natural n, lo podemos dividir entre cualquier otro natural m, si n no es múltiplo de m, al realizar esta división *nos sobra* un número menor que m, a este número se le llama *residuo*. En otras palabras, podemos decir que cualquier entero n se puede representar de la forma $n = km + r$ para algún k y con $0 \leq r < m$, donde r es el llamado residuo.

Un uso útil de los residuos es que podemos hacer álgebra con ellos, esto es gracias al siguiente resultado:

Proposición 2.1. *Dados dos números naturales a y b, se cumple que:*

1. *La suma a y b tiene el mismo residuo cuando dividimos por n, que la suma de sus residuos.*
2. *El producto a y b tiene el mismo residuo, cuando lo dividimos por n, que el producto de sus residuos.*

Ejercicio 2.1. *Demuestra que $3|n^3 + 2n$ para cualquier número natural n.*

Ejercicio 2.2. *Demuestra que $x^3 + y^3 + z^3 = 2002$ no tiene soluciones enteras.*

Ejercicio 2.3. *Encuentra todos los números primos p que satisfacen que $2^p + p^2$ también es un número primo.*

3. Congruencias.

Congruencias es simplemente otro lenguaje para manejar el álgebra con los residuos. Decimos que a y b son congruentes módulo m; y lo expresamos como $a \equiv b \ (mod\, m)$, si a y b tienen el mismo residuo al dividirlos por m.

Una equivalencia interesante de esta nueva definición es la siguiente:

Proposición 3.1. *$a \equiv b \ (mod\, m)$ si y sólo si $m|a - b$.*

Algo muy útil de las congruencias es su facilidad para manipularlas, a continuación mencionaremos unas de las propiedades más importantes:

Proposición 3.2. *Dados a, b, c y d enteros, entonces:*

1. *Si $a \equiv b \ (mod\, m)$ y $b \equiv c \ (mod\, m)$, entonces $a \equiv c \ (mod\, m)$.*
2. *Si $a \equiv b \ (mod\, m)$ y $c \equiv d \ (mod\, m)$, entonces $a \pm c \equiv b \pm d \ (mod\, m)$.*
3. *Si $a \equiv b \ (mod\, m)$, entonces $ak \equiv bk \ (mod\, m)$ para cualquier entero k.*
4. *Si $a \equiv b \ (mod\, m)$ y $c \equiv d \ (mod\, m)$, entonces $ac \equiv bd \ (mod\, m)$.*
5. *Si $a \equiv b \ (mod\, m)$, entonces $a^n \equiv b^n \ (mod\, m)$ para cualquier natural n.*

La mayoría de los problemas que se resuelven utilizando técnicas de residuos se pueden resolver también con congruencias, como ejercicio de esto se pueden resolver los problemas de la sección anterior ahora con congruencias.

4. Examen Selectivo de Teoría de Números.

Problema 4.1. Demostrar que $p^2 - 1$ es divisible entre 24 si p es un primo mayor que 3.

Demostración. Sabemos que $p^2 - 1 = (p+1)(p-1)$. Como p primo y $p > 3$, entonces $p = 6k \pm 1$, para algún k. Entonces $p^2 - 1 = (6k \pm 1 + 1)(6k \pm 1 - 1)$. Supongamos que p es de la forma $6k + 1$, entonces

$$p^2 - 1 = (6k + 2)(6k) = 12k(3k + 1).$$

Si k es par, ya tenemos que $24|p^2 - 1$, si k es impar, $3k + 1$ es par y $24|p^2 - 1$. Por último hay que notar que si p es de la forma $6k - 1$ sucede lo mismo.

Problema 4.2. Encontrar todas las ternas de números enteros positivos (a, b, c) tales que cumplen

$$ab + bc = 44$$
$$ac + bc = 23.$$

Demostración. De la ecuación $ac + bc = 23$ obtenemos que $c(a + b) = 23$. Como 23 es un número primo, los factores deben ser 1 y 23. Como $a + b > 1$, entonces $c = 1$ y $a + b = 23$. Sustituyendo $b = 23 - a$ en la primera ecuación tenemos la ecuación $a^2 - 22a + 21 = 0$ y al resolverla obtenemos las soluciones $a = 1$ y $a = 21$. Por lo cual las posibles ternas son $(1, 22, 1)$ y $(21, 2, 1)$.

Problema 4.3. De los números positivos que pueden ser expresados como suma de 2005 enteros consecutivos, no necesariamente positivos, ¿cuál ocupa la posición 2005?

Demostración. Como 2005 es impar, entonces para cada n tenemos que:

$$2005n = (n - 1002) + (n - 1001) + \ldots + n + \ldots + (n + 1001) + (n + 1002).$$

Entonces, el número buscado es un múltiplo de 2005, así, el que ocupa la posición 2005 es 2005^2.

Problema 4.4. Demostrar que si n es múltiplo de 3, entonces $2^n - 1$ es divisible por 7.

Demostración. Si n es múltiplo de 3, entonces es de la forma $3k$. Notemos que los residuos de las potencias de 2 al dividir por 7 son $\{2, 4, 1\}$ y se van repitiendo en ese orden, empezando con 2^1, entonces, cada que el exponente es un múltiplo de 3, el residuo es 1 y por lo tanto $7|2^n - 1$.

Problema 4.5. Encontrar una lista de cinco primos distintos donde la diferencia entre cualesquiera dos términos consecutivos de la lista sea siempre seis. Demostrar que esta lista es única.

Demostración. Supongamos que los números primos son: p, $p+6$, $p+12$, $p+18$ y $p+24$. Al tomar las congruencias módulo 5 tenemos que estos números son congruentes a p, $p+1$, $p+2$, $p+3$ y $p+4$ respectivamente, pero entre cinco números consecutivos, como es este caso, siempre hay un múltiplo de 5, es decir, uno de estos primos es el 5, así que la única lista que cumple es 5, 11, 17, 23 y 29.

Problema 4.6. Demostrar que $6n^3+3$ no puede ser una sexta potencia de un entero para ningún n.

Demostración. Consideremos módulo 7 durante todo el problema. Sabemos que $k^3 \equiv \{0, \pm 1\}$, entonces $k^6 \equiv \{0, 1\}$ para cualquier entero k. Ahora bien, como $n^3 \equiv \{0, \pm 1\}$ solo resta checar las opciones posibles.

- Si $n^3 \equiv 0$, entonces $6n^3+3 \equiv 3$
- Si $n^3 \equiv 1$, entonces $6n^3+3 \equiv 2$
- Si $n^3 \equiv -1$, entonces $6n^3+3 \equiv 4$.

Como en ningún caso obtenemos que $6n^3+3$ se congruente a 0 o 1, no es puede ser igual a algún k^6.

Problema 4.7. Sadhi escribe en una lista números de cuatro dígitos con las siguientes propiedades:

1. Son múltiplos de 45.
2. Las cifras 58 se encuentran juntas en alguna parte del número.
3. 4 los divide.

El número favorito de Sadhi es la diferencia entre en el mayor y el menor de los números de la lista. ¿Cuál es el número favorito de Sadhi?

Demostración. Como los números son múltiplos de 45, deben ser múltiplos de 5 y de 9, es decir, al ser múltiplos de 5, el último dígito de los número solo puede ser 0 o 5, por lo que solo tenemos números de la forma $58a0$, $58a5$, $a580$ o $a585$, aunque la segunda y la última forma las podemos descartar pues el números deben ser divisibles por 4. Revisando la divisibilidad del 9, observamos que el único número que puede escribir es el 5580, por lo que el mayor y el menor número de la lista es el mismo, así, el número favorito de Sadhi es el 0.