Teorema Fundamental de la Aritmética y Residuos

Entrenamiento #2 para 3ª etapa
12-18 de marzo de 2016
Por: Lulú

Resumen

En este documento podrás encontrar la información necesaria para poder resolver problemas básicos de teoría de números (sí, reciclé esta parte del documento de nuevo). Esta vez quizá tengamos que recurrir un poco al álgebra. Ligeramente más que en combinatoria, pero menos que en geometría.

Además del material necesario para resolver problemas básicos de teoría de números, podrás encontrar ejercicios (situaciones rápidas y sencillas para que apliques y comprendas mejor los conceptos) y una lista de problemas (sí, también volví a reciclar esta parte). Aquí aprenderás cómo se conforman los números y cómo determinar si es divisible por otro o no, además de los criterios de divisibilidad.

1. Un pequeño preámbulo

Probablemente te preguntes "¿qué es el Teorema Fundamental de la Aritmética?, ¿qué dice?, ¿para qué sirve?, ¿qué es eso de la Teoría de Números?" No te espantes. Se trata de una de mis partes favoritas de las matemáticas. La Teoría de Números es la rama que estudia las propiedades de los numeritos (no de cuerpos y uniones de puntos, ni de los conjuntos y estructuras). Ya después aprenderás que hay muchos tipos de números: felices, azules, perfectos, etc.

Lamentablemente esos podrás aprenderlos después durante la marcha. Aquí sólo nos competerá un par: números primos y números compuestos. Y no, no hablo de los números que son hijos de nuestros tíos, me refiero a otra cosa. Por lo tanto, empezaremos con unas pequeñas definiciones.

Número primo es el tipo de número que sólo es divisible de manera entera entre sí mismo y uno. Por ejemplo: 2, 3, 5, 7, 11, 13. Nótese que el número 1 no es primo porque uno de los requisitos es que el número tenga exactamente dos divisores; y el 1 sólo tiene uno.

Número compuesto es el tipo de número que se obtiene de multiplicar dos o más primos (aunque éstos puedan ser iguales). Por ejemplo: $6 = 2 \times 3$, $10 = 2 \times 5$, $420 = 2 \times 2 \times 3 \times 5 \times 7$.

2. El Teorema Fundamental

El famoso y renombrado Teorema Fundamental de la Aritmética dice que "todo número natural tiene una representación única como producto de potencias de primos". Eso en cristiano quiere decir que cualquier número puede escribir como un primo por otro primo por otro primo (y así cuantas veces sea necesario, incluso con números iguales) y que ese número es el único que se puede escribir de esa forma particular. Además, cada número tiene una sola forma de ser representado.

Sí, ya sé. Vamos por ejemplos. El 12 es $12 = 2^2 \cdot 3$. Si hacemos el producto $2^2 \cdot 3$, jamás obtendremos un número distinto a 12; y, por otra parte, jamás encontraremos una representación diferente para el 12. Por eso la representación es única para cada número, y el número es único para cada representación. Qué romántico, ¿no? Siendo así, podemos generalizarlo para cualquier n. De modo que, ya en lenguaje matemático, el Teorema Fundamental dice:

$$n = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_k^{\alpha_k}$$

Aquí k es la cantidad de factores primos distintos que conforman a n. En el ejemplo del 12, $k = 2$, $p_1 = 2$, $\alpha_1 = 2$, $p_2 = p_k = 3$ y $\alpha_2 = \alpha_k = 1$. Ahora, con el mismo 12, ¿qué pasa si lo dividimos entre 2?. Tendríamos $\frac{12}{2} = \frac{2^2 \times 3}{2}$. Con ello, podemos eliminar un dos de arriba y uno de abajo. Nos queda un entero: $2 \times 3 = 6$. Por lo tanto 12 es divisible entre 2. Si lo hiciéramos entre 3 o entre $4 = 2^2$ también se podría, o entre $6 = 2 \times 3$. Pero si dividimos entre 5, no podemos eliminar un 5 de arriba con uno de abajo, entonces 12 no es divisible entre 5.

Queda claro entonces que un número no puede ser dividido entre otro que no forma parte de su composición en primos, ¿no? Porque no se puede eliminar reducir la fracción. Pero también hay otras restricciones en la divisibilidad. ¿Qué pasa si dividimos entre $8 = 2^3$. Podremos eliminar sólo dos de los factores de abajo, pero nos sobraría uno:

$$\frac{12}{8} = \frac{\cancel{2 \cdot 2} \cdot 3}{\cancel{2 \cdot 2} \cdot 2}$$

De modo que volvemos al ejemplo del 5. Ya no tenemos primos que podamos eliminar, y como 2 no divide a 3, entonces 8 no divide a 12. ¿Cómo saber si un número a no es divisible entre otro número b? Te pondré una lista de condiciones en base a lo que hemos visto:

1. Si b es mayor, el resultado será menor que 1, por lo que nunca obtendremos un natural, ni siquiera entero.
2. Si b tiene factores primos que no se encuentran en la representación de a.
3. Si alguno de los primos de b tiene un exponente mayor al del mismo primo en la composición de a.

Basta con que se cumpla una sola para saber que un número no será divisible entre otro. Por ello no debe cumplirse ninguna para que el número sí sea divisible.

Basándonos en el Teorema Fundamental de la Aritmética, ¿qué pasa con los cuadrados perfectos, los cubos perfectos? Te dejo pensando un poco sobre

$$n^a = (p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \cdots p_k^{\alpha_k})^a$$

3. A caminar entre residuos

Y no, no me refiero a residuos tóxicos ni nada. Nadie saldrá de aquí con tres ojos, ni superpoderes. Esto tiene que ver con lo que queda en una división. Si lo hacemos como nos enseñaron en la primera, con la casita y toda la cosa, sabremos que un número es divisible entre otro si el residuo es cero. Pero si no es cero, entonces no es divisible. Intenta dividir 35 y 100 entre 5 y verás que no dejan residuo, pero divide al 99 o al 83 y, como no son divisibles entre 5, la división tendrá un residuo.

Siguiendo la lógica de la casita, el número de adentro se llama **dividendo**, el de afuera **divisor**, el resultado **cociente** y lo que sobre el **residuo**. Llamemos n al dividendo, m al divisor, q al cociente y r al residuo. Para cualquier número n y cualquier divisor q, existe forma de expresar a n de la siguiente manera:

$$n = mq + r$$

Si $r = 0$, entonces n es divisible entre m y el resultado será q. Pero si no, igual es una forma chida de expresar a los numeritos, ¿no? De ese modo, por ejemplo, podemos decir que $100 = 9 \cdot 11 + 1$, o que $123 = 10 \cdot 12 + 3$. Esta última es más o menos la manera en que funciona nuestro sistema decimal (véase La notación desarrollada).

Este tipo de expresiones son útiles porque nos permite saber al instante si n es divisible entre m (a quien llamaremos módulo) o no, o qué tanto le sobró para ser divisible. Las operaciones entre residuos se manejan igual que siempre, pero hay que saber interpretarlas. Por ejemplo: que pasa si hacemos operaciones con dos números a y b tales que $a = mq_1 + r_1$ y $b = mq_2 + r_2$. Tendríamos:

1. Si sumamos: $a + b = m(q_1 + q_2) + (r_1 + r_2)$

2. Si restamos: $a - b = m(q_1 + q_2) + (r_1 - r_2)$

3. Si multiplicamos: $ab = m^2 q_1 q_2 + m q_1 r_2 + m q_2 r_1 + r_1 r_2 = m(m q_1 q_2 + q_1 r_2 + q_2 r_1) + r_1 r_2$

En cualquier caso, sigue habiendo algún múltiplo de m y un residuo. Es como si las operaciones se hicieran con los residuos. Entonces, para saber si $a + b$ es divisible entre el módulo basta ver si la suma de sus residuos lo es; si se quiere que $a - b$ sea divisible entre el módulo, entonces basta ver si $r_1 = r_2$. Del mismo modo, cuando se multiplican el residuo es el producto de los residuos.

3.1. La notación desarrollada

Se llama así a cuando expresamos un número de la forma:

$$a_n \cdot 10^n + a_{n-1} 10^{n-1} + \cdots + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$$

Por ejemplo, el 1235 es $1 \cdot 1000 + 2 \cdot 100 + 3 \cdot 10 + 5$. Y así es en verdad como funciona nuestro sistema decimal.

4. Ejercicios

1. a) ¿Es $2^9 \cdot 3$ divisible por 2?
   b) ¿Es $2^9 \cdot 3$ divisible por 5?
   c) ¿Es $2^9 \cdot 3$ divisible por 8?
   d) ¿Es $2^9 \cdot 3$ divisible por 9?
   e) ¿Es $2^9 \cdot 3$ divisible por 6?

2. Determina todos los primos entre 1 y 80

3. Encuentra la descomposición canónica de 6916

4. ¿Cuántas cifras tiene el número $2^{2009} \times 5^{2013}$?

5. El producto de tres enteros mayores que 1 y distintos entre sí es 100. ¿Cuáles son los tres enteros?

6. Explica por qué si pA es divisible por q, siendo q y p coprimos, entonces A también debe ser divisible entre q.

7. ¿Es cierto que si un número es divisible por 4 y 3, entonces es divisible por 12?

8. ¿Es cierto que si un número natural es divisible por 4 y 6, entonces en divisible por 24?

9. El número A no es divisible por 3. ¿Es posible que $2A$ sea divisible por 3?

10. Encuentra el máximo común divisor y el mínimo común múltiplo de A y B, siendo $A = 2^8 \cdot 5^3 \cdot 7$ y $B = 2^5 \cdot 3 \cdot 5^7$.

5. Agregados culturales

1. Para denotar que un a es divisible por b, se usa la simbología $b|a$.

2. Es bien sabido que cuando un número multiplicado por un impar mantiene su paridad.

3. Un número multiplicado por un par se hace par.

4. El criterio de divisibilidad del 7 es horrible y dice que un número es divisible entre 7 si el número que resulta de borrar el último dígito y restarlo dos veces también es divisible entre 7.
5. Un par de números son coprimos si ninguno los primos que componen a uno se encuentra en la composición del otro.
6. A los números que son coprimos, también se les llama primos relativos.
7. A la descomposición en primos de un número también se le conoce como descomposición canónica.
8. El cero se considera múltiplo de todos.
9. Existen muchas formas de representar una multiplicación: $a * b$, ab, $(a)(b)$, $a \cdot b$ y la más importante y conocida $a \times b$.
10. Las vacas, al igual que los humanos (bueno, las humanas), tienen un embarazo de 9 meses.

6. Lista de problemas

Ahora sí, siendo un poquitín más abstracto, intenta resolver los problemas utilizando las distintas herramientas que se te explicaron en el papel. Para dudas tienes mi facebook, mi número de teléfono y a algún entrenador frente a ti.

1. Prueba que el producto de dos números consecutivos siempre es par.
2. Prueba que el producto de tres números consecutivos siempre es divisible entre 6.
3. Muestra que el producto de cuatro números consecutivos siempre es divisible entre 24.
4. Encontrar un número entero positivo a tal que

$$a + 2a + 3a + 4a + 5a + 6a + 7a + 8a + 9a$$

sea un número con todas sus cifras iguales

5. Encuentra la suma de todos los dígitos del número $10^{99} - 99$.
6. ¿Para qué valores enteros de n la expresión

$$\frac{18}{n+4}$$

es un entero?

7. Si m y n son enteros tales que $2m - n = 3$, prueba que $m - 2n$ es múltiplo de 3.
8. Prueba que todo primo de la forma $3k + 1$ también se puede expresar de la forma $6k + 1$.
9. Demuestra que el mínimo común múltiplo de una pareja se hace eligiendo el mayor de los exponentes para cada primo existente en la composición.
10. Demuestra que el resultado de multiplicar el mcm con el MCD de una pareja de números A y B es AB.
11. Demuestra los criterios de divisibilidad:
    a) Un número es divisible entre 2 si su última cifra es par.
    b) Un número es divisible entre 3 si la suma de sus cifras es múltiplo de 3-
    c) Un número es divisible entre 4 si sus últimas dos cifras forman un número divisible entre 4.

d) Un número es divisible entre 5 si su última cifra es 5 ó 0.

e) Un número es divisible entre 6 si cumple los criterios del 3 y del 2.

f) Un número es divisible entre 8 si sus últimas tres cifras forman un número divisible entre 8.

g) Un número es divisible entre 9 si sus cifras suman un múltiplo de 9.

h) Un número es divisible entre 10 si su último dígito es 0.

i) Un número es divisible entre 11 si la diferencia generada entre la suma de las cifras en posición impar y la suma de las cifras en posición par es múltiplo de 11.

7. Problemas más jarcors

1. ¿Cuál es el criterio de divisibilidad para 2^n? Demuéstralo.

2. Demuestra que el máximo común divisor de una pareja se hace eligiendo el menor de los exponentes para cada primo existente en la composición.

3. ¿Cuántos divisores positivos tiene un número n?

4. En un pasillo oscuro y estrecho quieres prender la luz. Tanteas la pared y encuentras un botón que oprimes por instinto. Todos los focos a lo largo del pasillo se encienden como una fila de soldados. La luz es demasiada y vuelves a oprimir el botón, pero sólo se apagan los que tienen una posición par. Sigue habiendo mucha luz y presionas el botón de nuevo, pero notas que se altera el estado de los que se encuentran en una posición divisible entre tres. Y así continuas ajustando la iluminación del pasillo en el que te encuentras. Si hay n focos y presionaste el botón n veces, ¿qué focos se quedarán prendidos?