Teoría de números naturales

Matemáticas - Grado 6

2020

1. Introducción: criptografía como aplicación de la teoría de números

Una aplicación muy importante de las matemáticas en el día de hoy se encuentra en la protección y transmisión de la información a través de cualquier cualquier red informática. El acceso a un correo electrónico, el retiro de dinero de un cajero automático, una conversación textual por la red WhatsApp son ejemplos de transmisión de información sobre los cuales debemos tener garantía que ella no es compartida o vulnerada por personas o entidades que violen nuestra privacidad. Hasta donde es públicamente conocido (o al menos eso nos hacen creer), la protección de información reposa en una rama tecnológica llamada *criptografía*. Ella, se ocupa de técnicas de codificación o de cifrado de los mensajes que suceden entre un ente emisor y un ente receptor en procura de garantizar que la información no quede expuesta a un ente externo. La mayoría de esas técnicas de codificación aprovechan las matemáticas a través de las relaciones que se encuentra entre grupos de números y reglas muy particulares que suceden entre ellos. Estas relaciones que se dan entre esos números es el campo de acción de la rama matemática llamada *Teoría de Números*.
Para explicar rápidamente como interactúan estas ramas, se mencionara el sistema de criptografía mas popular conocido como sistema RSA. Necesitas enviar mensajes entre tu y un amigo sin que sean descubiertos por personas ajenas; para ello luego de editar el mensaje lo depositas en una caja de seguridad que usa dos llaves. Una llave es "privada" -solamente tu la usas para escribir y enviar mensajes- y la otra es "pública" que compartes con tu amigo -solamente para que él pueda leer los mensajes-. El papel de la criptografía aquí es de codificar el mensaje (por ejemplo convertirlo de letras a números) y generar el par de llaves. Las llaves son "creadas" con la Teoría de números usando una particular relación llamada el *Pequeño teorema de Fermat*. Tal teorema dice que, si se eleva un número con un exponente (o sea formar una potencia) que sea número primo y a ese resultado se le resta el mismo número, lo que queda es divisible por el número primo elegido [5]. El par de números que allí aparecen son las claves que crean las llaves privada y pública. Con ayuda de la informática y cómputos de divisiones y potencias se cifran los mensajes brindando seguridad al mensaje dado entre emisor y receptor [3, 2].
El anterior uso permite mostrar la aplicación de la teoría de números y así mencionar los objetivos de la clase:

- Reconocer los múltiplos y divisores de un número.
- Descomponer un número en factores primos.
- Hallar el mínimo común múltiplo (m.c.m.) de varios números.
- Calcular y proponer soluciones a problemas que usen la teoría de números naturales.

A continuación se desarrolla el tema iniciando con un repaso de múltiplos y divisores, descomponer un número en factores primos, cómputo del m.c.m. de un conjunto de números y por último una actividad aplicada.

2. Teoría de números

2.1. Múltiplos y divisores

Los *múltiplos* de un número natural son números que resultan de multiplicar ese número por otros números, en otras palabras las tablas de multiplicar son ejemplos de los múltiplos de un número natural. Así, los diez primeros múltiplos de 8 son: 0, 8, 16, 24, 32, 40, 48, 56, 64 y 72.
Los *divisores* de un número natural son los números que le pueden dividir y cuyo residuo o resto es cero, esto es aquellos números que dejan una división exacta. De lo anterior se deduce que un número tiene una cantidad finita de divisores. También que el 0 tiene infinito número de divisores, ya que todos los números son divisores de 0. A cambio, el 1 tiene solamente un divisor: el mismo [4].

Ejemplo 1. Resolver:

1) Buscar todos los divisores de 21.
2) Buscar todos los divisores de 67.
3) De la siguiente lista {33, 9, 88, 68, 6, 89, 53, 73, 77, 42} ¿cuáles son múltiplos de 7?

1) Cuando se trata de buscar divisores de un número la herramienta básica para hallarlos es mediante divisiones sucesivas del número entre 1 y el mismo. Es decir, aquí dividir 21 entre números del 1 al 21. Resolviendo algunas de ellas

2	1	1													
0	1	2	1		2	1	3		2	1	5				
	0					0	7			1	4				
2	1	7		2	1	1	0		2	1	2	1			
	0	3			1	2				0	1				

Observando las divisiones exactas, los cuatro divisores de 21 son: 1, 3, 7 y 21. A los números naturales que tienen más de 2 divisores se les llama *números compuestos*.

2) Por un procedimiento similar al anterior ejemplo 1) 67 posee dos divisores: 1 y el mismo. A los números naturales que cumplen estos 2 requisitos se les llama *números primos* y son de uso fundamental e intensivo en criptografía.

3) Asumiendo que Ud. ya conoce la tabla del 7 al derecho y al revés! O simplemente sumando de 7 en 7 se tiene que aquellos números múltiplos de 7 son {77, 42}.

La teoría de números ofrece algunas reglas elementales para saber fácilmente si un número es divisible por otro, sin recurrir a la división:

- Números pares son divisores de 2.
- Un número es divisor de 3 si al sumar todas las cifras tiene por resultado un múltiplo de 3.
- Un número es divisor de 5 si la última cifra es 5 o 0.
- Un número es divisor de 10 si la última cifra es 0.

2.2. Descomposición de número natural en factores primos

Descomponer un número natural en factores primos es encontrar un conjunto de números primos[1] que por medio de una multiplicación permite obtener el número natural. Así, 21 tiene por factores primos {3,7}, por tanto 3×7=21. El procedimiento para factorizar un número es el siguiente [4]:

- Dividir el número dado por el menor número primo posible, de modo que su división sea exacta. El cociente que haya resultado se pone debajo del número y el divisor a la derecha de una línea vertical.
- Continuar dividiendo ese cociente por el mismo número primo.
- Cuando la división no es exacta, se toma el siguiente número primo con el que se pueda hacer la división.
- Repetir sucesivamente hasta que el cociente final sea 1.
- Finalmente, la descomposición del número se escribe como un producto de potencias de la columna derecha.

Ejemplo 2. Descomponer en sus factores primos: 1) el número 340. 2) el número 693.

1) Se dispone así,

340	2	→	porque $340 \div 2 = 170$
170	2	→	porque $170 \div 2 = 85$
85	5	→	porque $85 \div 5 = 17$
17	17	→	porque $17 \div 17 = 1$
1			

Luego, se escribe $340 = 2^2 \cdot 5 \cdot 17$

2) Se dispone así,

693	3	→	porque $693 \div 3 = 231$
231	3	→	porque $231 \div 3 = 77$
77	7	→	porque $77 \div 7 = 11$
11	11	→	porque $11 \div 11 = 1$
1			

Luego, se escribe $693 = 3^2 \cdot 7 \cdot 11$

2.3. Mínimo Común Múltiplo

El mínimo común múltiplo de un conjunto de números, es el número más pequeño que es múltiplo de todos esos números. Por ejemplo, obténgase los múltiplos de 12 y 20: de 12 son {12, 24, 36, 48, 60, 72, 84, 96, 108, 120, ...} y de 20 son {20, 40, 60, 80, 100, 120,...}. Ambos conjuntos coinciden con los números 60, 120, ..., y de ellos el más pequeño o mínimo es 60. Luego el mínimo común múltiplo de 12 y 20 es 60 y se escribe simbólicamente así $m.c.m(12,20) = 60$ [1].
Usualmente el *m.c.m.* no se evalúa como se indicó arriba, sino que se procede a descomponer en factores primos cada número y luego tomar el producto de los factores comunes y no comunes elevados a su mayor exponente.

Ejemplo 3.

1) Encontrar el *m.c.m.* de 15, 30 y 63.
2) En los engranajes (piñones) de la figura ¿cuántos dientes de cada rueda deben pasar para que vuelvan a coincidir los puntos rojos? ¿Cuántas vueltas habrá girado cada rueda?

[1] Puesto que el tema usa frecuentemente los números primos, aquí se mencionan los números primos menores a 50: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47

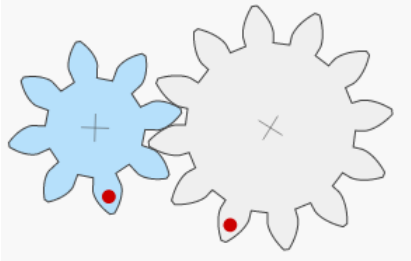
1) Descomponiendo cada número,

15	3	30	2	63	3
5	5	15	3	21	3
1		5	5	7	7
		1		1	

Así, $15 = 3 \cdot 5$, $30 = 2 \cdot 3 \cdot 5$, $63 = 3^2 \cdot 7$. Los factores no comunes (no repetidos) son 2 y 7; los factores comunes (repetidos) son 5 y 3, pero respecto a 3 se elige con exponente 2, o sea 3^2. Finalmente,

$$m.c.m(15,30,63) = 2 \cdot 3^2 \cdot 5 \cdot 7 = 630$$

2) La rueda mayor tiene 12 dientes y la menor 8; el mínimo número de dientes que deben avanzar para que vuelvan a coincidir es un múltiplo común a esos números, esto es, $m.c.m.(8,12)$. Como $8 = 2^3$ y $12 = 2^2 \cdot 3$, entonces $m.c.m.(8,12) = 2^3 \cdot 3 = 24$ dientes han de avanzar para que coincidan los puntos rojos.



La rueda mayor habrá girado $24 \div 12 = 2$ vueltas y la menor $24 \div 8 = 3$ vueltas.

3. Actividad Número 7

Resolver cada ejercicio en el cuaderno. A parte del procedimiento, también se tendra en cuenta el orden y la escritura para la revisión.

1. Dado el conjunto A={5, 6, 8, 10, 13, 15, 20, 24, 42} calcular los siguientes subconjuntos. a) Múltiplos de 4. b) Múltiplos de 7. c) Múltiplos de 11.

2. La Teoría de números ofrece una curiosa regla para contar el número de divisores de cualquier número sin necesidad de hacer divisiones. Para ello establece que, luego de descomponer el número en factores primos se toman los exponentes de cada factor y se aumentan en uno; el producto de esos exponentes aumentados es el número de divisores. Por ejemplo, ¿cuántos divisores tiene 9? Como $9 = 3^2$, al aumentar en uno el exponente, 2+1=3, luego tiene 3 divisores; en efecto son {1,3,9}. Verificar la validez o falsedad de la regla para el número 100 hallando todos los divisores y mostrando la cantidad de divisores desde esta curiosa regla.

3. En un velódromo parten simultáneamente 3 ciclistas de un mismo punto de largada. Uno de los ciclistas da una vuelta cada 30 segundos, otro cada 27 segundos y el tercero cada 24 segundos. ¿A los cuántos segundos cruzan los 3 ciclistas juntos, por primera vez por el punto de largada? ¿Cuántas vueltas ha dado el tercer ciclista en ese momento?

Nota: La sección referencias contiene fuentes de consulta bibliográficas si se tiene posibilidad de acceder a textos o navegación en la red. Estas aparecen en el contenido de este texto con paréntesis cuadrados [...].

Referencias

[1] Daniel López Avellaneda, *Calcular el mínimo común múltiplo*, https://matematicasies.com/Calcular-el-minimo-comun-multiplo-m-c-m, 2020, Consultado 13 jun 2020.

[2] Lázaro Escudero, *Los primos en la criptografía*, http://www.tierradelazaro.com/los-primos-en-la-criptografia, 2015, Consultado 13 jun 2020.

[3] Claudio Gutiérrez, *Teoría de números y criptografía*, Revista del Profesor de Matemáticas (1998), no. 6, 58–69.

[4] Jesús Ramos and Ludwig Ortiz, *Supermat 6*, Voluntad, 2000.

[5] Wikipedia, *Pequeño teorema de fermat*, https://es.wikipedia.org/wiki/Peque%C3%B1o_teorema_de_Fermat, 2020, Consultado 15 jun 2020.