UNIVERSIDAD PANAMERICANA Campus Bonaterra	**Escuela de Ingeniería**	Tarea 3. Divisibilidad 1
	Área: Matemáticas	Fecha:
	Materia: Matemáticas Discretas	Ciclo:1208
	Profesor: Dr. Adrián Cerda	CALIFICACIÓN
	Carrera:	
	Alumno(a):	

INSTRUCCIONES: Resuelve cada uno de los siguientes ejercicios. Cuida por favor el orden, la limpieza y la ortografía en cada uno de tus argumentos, asimismo pon especial cuidado en la sintaxis matemática de tu procedimiento.

Ejercicio 1. Calcule la factorización en potencias de números primos de cada uno de los siguientes números: $47, 637, 4141, 1007, 3738$ y 1050703.

Ejercicio 2. Encuentre el máximo común divisor de cada uno de los siguientes pares de números enteros: $60, 90$, $220, 1400$, $2091, 4807$ y $15, 15^9$.

Ejercicio 3. Encuentre el mínimo común múltiplo de cada uno de los pares de números enteros dados en el ejercicio anterior.

Ejercicio 4. Para cada par de enteros del ejercicio 2, verifique que $mcd(m,n) \cdot mcm(m,n) = mn$.

Ejercicio 5. Sean m y n y d números enteros. Demuestre que si se cumple que $d|m$ y $d|n$, entonces $d|(m-n)$.

Bonus 1. Muestre que el conjunto de los números primos es un conjunto infinito.

Bonus 2. Investiga cuál es la definición de un número primo de Mersenne y proporciona el ejemplo de 4 de dichos números. Por otro lado, considera números enteros de la forma $2^m - 1$ con m siendo un número compuesto, y prueba que para cada número compuesto m, el numero $2^m - 1$ también es un número compuesto.

UNIVERSIDAD PANAMERICANA Campus Bonaterra	**Escuela de Ingeniería**	Tarea 3. Divisibilidad 1
	Área: Matemáticas	Fecha:
	Materia: Matemáticas Discretas	Ciclo:1208
	Profesor: Dr. Adrián Cerda	CALIFICACIÓN
	Carrera:	
	Alumno(a):	

SOLUCIONARIO

Ejercicio 1. Calcule la factorización en potencias de números primos de cada uno de los siguientes números: $47, 637, 4141, 1007, 3738$ y 1050703.

SOLUCIÓN Iniciaremos este ejercicio proporcionando una tabla de con los primeros 27 números primos

2	3	5	7	11	13	17
19	23	29	31	37	41	43
47	53	59	61	67	71	73
79	83	89	97	101	103	

Recordemos: un número $p > 1$ es un número primo si, y solo si, los únicos factores de p son 1 y p.

Ahora, daremos la respuesta al ejercicio

$$47 = 47$$
$$637 = 7^2 \cdot 13,$$
$$4141 = 41 \cdot 101,$$
$$1007 = 19 \cdot 53,$$
$$3738 = 2 \cdot 3 \cdot 7 \cdot 89$$
$$1050703 = 101^2 \cdot 103.$$

Ejercicio 2. Encuentre el máximo común divisor de cada uno de los siguientes pares de números enteros: $60, 90$, $220, 1400$, $2091, 4807$ y $15, 15^9$.

SOLUCIÓN

$$\text{mcd}(60, 90) = \text{mcd}(2^2 \cdot 3 \cdot 5, 2 \cdot 3^2 \cdot 5) = 2^{min(2,1)} \cdot 3^{min(1,2)} \cdot 5^{min(1,1)} = 2^1 \cdot 3^1 \cdot 5^1 = 30$$
$$\text{mcd}(220, 1400) = \text{mcd}(2^2 \cdot 5 \cdot 11, 2^3 \cdot 5^2 \cdot 7) = 2^{min(2,3)} \cdot 5^{min(1,2)} \cdot 7^{min(0,1)} \cdot 11^{min(1,0)} = 2^2 \cdot 5^1 \cdot 7^0 \cdot 11^0 = 20$$
$$\text{mcd}(2091, 4807) = \text{mcd}(3 \cdot 17 \cdot 41, 11 \cdot 19 \cdot 23) = 3^{min(1,0)} \cdot 11^{min(0,1)} \cdot 17^{min(1,0)} \cdot 19^{min(0,1)} \cdot 23^{min(0,1)} \cdot 41^{min(1,0)} = 3^0 \cdot 11^0 \cdot 17^0 \cdot 19^0 \cdot 23^0 \cdot 41^0 = 1$$
$$\text{mcd}(15, 15^9) = \text{mcd}(3 \cdot 5, 3^9 \cdot 5^9) = 3^{min(1,9)} \cdot 5^{min(1,9)} = 3^1 \cdot 5^1 = 15.$$

Ejercicio 3. Encuentre el mínimo común múltiplo de cada uno de los pares de números enteros dados en el ejercicio anterior.

SOLUCIÓN

$$\text{mcm}(60, 90) = \text{mcm}(2^2 \cdot 3 \cdot 5, 2 \cdot 3^2 \cdot 5) = 2^{max(2,1)} \cdot 3^{max(1,2)} \cdot 5^{max(1,1)} = 2^2 \cdot 3^2 \cdot 5^1 = 180$$

$\text{mcm}(220, 1400) = \text{mcm}(2^2 \cdot 5 \cdot 11, 2^3 \cdot 5^2 \cdot 7) = 2^{max(2,3)} \cdot 5^{max(1,2)} \cdot 7^{max(0,1)} \cdot 11^{max(1,0)} = 2^3 \cdot 5^2 \cdot 7^1 \cdot 11^1 = 15\,400$

$\text{mcm}(2091, 4807) = \text{mcm}(3 \cdot 17 \cdot 41, 11 \cdot 19 \cdot 23) = 3^{max(1,0)} \cdot 11^{max(0,1)} \cdot 17^{max(1,0)} \cdot 19^{max(0,1)} \cdot 23^{max(0,1)} \cdot 41^{max(1,0)} = 3^1 \cdot 11^1 \cdot 17^1 \cdot 19^1 \cdot 23^1 \cdot 41^1 = 10\,051\,437$

$\text{mcm}(15, 15^9) = \text{mcm}(3 \cdot 5, 3^9 \cdot 5^9) = 3^{max(1,9)} \cdot 5^{max(1,9)} = 3^9 \cdot 5^9 = (3 \cdot 5)^9 = 15^9.$

Ejercicio 4. Para cada par de enteros del ejercicio 2, verifique que $mcd(m, n) \cdot mcm(m, n) = mn$.

SOLUCIÓN

Para 60 y 90, se cumple $60 \cdot 90 = 5400 = 30 \cdot 180 = \text{mcd}(60, 90) \cdot \text{mcm}(60, 90)$

Para 220 y 1400, se cumple $220 \cdot 1400 = 308\,000 = 20 \cdot 15\,400 = \text{mcd}(220, 1400) \cdot \text{mcm}(220, 1400)$

Para 2091 y 4807, se cumple $2091 \cdot 4807 = 10\,051\,437 = 1 \cdot 10\,051\,437 = \text{mcd}(2091, 4807) \cdot \text{mcm}(2091, 4807)$

Para 15 y 15^9, se cumple $15 \cdot 15^9 = 15^{10} = 15 \cdot 15^9 = \text{mcd}(15, 15^9) \cdot \text{mcm}(15, 15^9)$

Ejercicio 5. Sean m y n y d números enteros. Demuestre que si se cumple que $d|m$ y $d|n$, entonces $d|(m - n)$.

SOLUCIÓN Recordemos que a divide b si y solo si existe un entero c tal que $b = ac$, lo cual denotamos por $a|b$. Para demostrar la afirmación del ejercicio, notemos que por hipótesis existen enteros r y s tales que $m = dr$ y $n = ds$. De modo que al efectuar la resta $m - n$ obtenemos

$$m - n = dr - sd = d(r - s)$$

Es decir, existe un entero, precisamente $r - s$ tal que al multiplicarse por d se obtiene m-n, lo cual significa que $d|(m - n)$.

Bonus 1. Muestre que el conjunto de los números primos es un conjunto infinito.

SOLUCIÓN La demostración la realizaremos por contradicción, es decir, sabiendo a priori que el resultado es verdad, supondremos una barbaridad, es decir, lo contrario "el conjunto de los números primos es finito"y mediante una serie de argumentos válidos buscaremos un absurdo o contradicción.

Si el conjunto de los números primos es finito, entonces los podemos ordenar y enumerar como p_1 al primer número primo, p_2 al segundo número primo, etc. y p_N al último número primo. Esto es, suponemos que hay exactamente N números primos

$$p_1 < p_2 < \cdots < p_N$$

Luego, puesto que todos los p_k son números enteros positivos, su producto $\Pi_{k=1}^{N} p_k = p_1 \cdot p_2 \cdots p_N$ también será un número entero positivo y lo mismo sucederá con

$$P = \Pi_{k=1}^{N} p_k + 1$$

Ahora, por el Teorema fundamental de la Aritmética, sabemos que todo número entero positivo se puede descomponer de forma única como un producto de factores primos. Así que esta factorización también concierne a nuestro número P. Por lo tanto sea p uno de sus factores primos, se sigue que $p \neq p_k$ para todo $k = 1, ..., N$, ya que $p_k \nmid P$. De modo que este número primo p no pertenece a la lista dada incialmente

$$p \notin \{p_1, p_2, ..., p_N\}$$

En otras palabras, p_N no es el último numero primo, contrario a lo que habíamos supuesto. La deducción de este absurdo, garantiza que el conjunto de los números primos es un conjunto infinito.

Bonus 2. Investiga cuál es la definición de un número primo de Mersenne y proporciona el ejemplo de 4 de dichos números. Por otro lado, considera números enteros de la forma $2^m - 1$ con m siendo un número compuesto, y prueba que para cada número compuesto m, el número $2^m - 1$ también es un número compuesto.

SOLUCIÓN Un número primo de Mersenne se define como un número entero positivo $q > 1$ tal que q es primo y existe un primo p tal que $q = 2^p - 1$. En otras palabras, es un número primo de la forma $2^p - 1$ con p primo.

Los primeros 5 números primos de Mersenne son

$$3 = 2^2 - 1, 7 = 2^3 - 1, 31 = 2^5 - 1, 127 = 2^7 - 1, 8191 = 2^{13} - 1$$

Por otro lado, para la segunda parte del ejercicio, es necesario establecer la definición de número compuesto. Un número entero positivo c es llamado **compuesto**, si existe un entero b tal que $1 < b < c$ y tal que $b|c$.

En vista de la definición, debemos probar que si m es compuesto, entonces existen dos números enteros k y $1 < \ell < 2^m - 1$ tales que $2^m - 1 = \ell k$.

Ahora, como m es compuesto existen b_1 y k_1 tales que $1 < b_1 < m$ y $m = b_1 k_1$. Lo cual implica que

$$2^m - 1 = 2^{b_1 k_1} - 1 = (2^{b_1})^{k_1} - 1 = (2^{b_1})^{k_1} + (2^{b_1})^{k_1 - 1} - (2^{b_1})^{k_1 - 1} + \cdots + (2^{b_1})^{k_1 - (k_1 - 1)} - (2^{b_1})^{k_1 - (k_1 - 1)} - 1$$

$$= (2^{b_1} - 1)((2^{b_1})^{k_1 - 1} + (2^{b_1})^{k_1 - 2} + \cdots + (2^{b_1}) + 1)$$

pero esto significa que $2^{b_1} - 1$ es un factor de $2^m - 1$, es decir $2^{b_1} - 1 | 2^m - 1$. Así podemos tomar $\ell = 2^{b_1} - 1$ y $k = ((2^{b_1})^{k_1 - 1} + (2^{b_1})^{k_1 - 2} + \cdots + (2^{b_1}) + 1)$. Luego, finalizaremos nuestra prueba si probamos que $1 < \ell < 2^m - 1$.

En efecto, como $1 < b_1 < m$ se sigue que $2^1 < 2^{b_1} < 2^m$ y por lo tanto

$$2^1 - 1 < 2^{b_1} - 1 < 2^m - 1$$

es decir $1 < \ell < 2^m - 1$. Por lo tanto, $2^m - 1$ es un número entero positivo compuesto.