4.2 Números primos grandes

MATE 3041

Profa. Milena R. Salcedo Villanueva

Números primos grandes

"Existe una cantidad infinita de números primos"[1]

[1]Resultado aprobado por Euclides alrededor del año 300 a. C.Uninorte 2006

Estudio de los números primos

Nunca podríamos estudiar toda la cantidad infinita de número primos de manera directa. Así que históricamente, se han investigado las propiedades de los más pequeños y conocidos, y luego se intentó refutar o probar las propiedades.

Enseguida se muestra una manera de clasificar los números naturales dividiéndoles en subconjuntos

- Conjunto A: todos los números de la forma $4k$
- Conjunto B: todos los números de la forma $4k+1$
- Conjunto C: todos los números de la forma $4k+2$
- Conjunto D: todos los números de la forma $4k+3$

En cada caso, k es un número entero no negativo, excepto para el conjunto A, k no puede ser cero.

Analizando subconjuntos de números Naturales

Hagamos una lista de los 8 primeros elementos de cada uno de los conjuntos infinitos A,B,C y D

Solución:

$$A = \{4,8,12,16,20,24,28,32, \dots\}$$
$$B = \{1,5,9,13,17,21,25,29, \dots\}$$
$$C = \{2,6,10,14,18,22,26,30, \dots\}$$
$$D = \{3,7,11,15,19,23,27,31, \dots\}$$

Analizando subconjuntos de números Naturales

Identifique todos los números primos, de los 8 elementos listados anteriormente en cada conjunto.

Solución:

$B = \{5,13,17,29\}$

$C = \{2\}$

$D = \{3,7,11,19,23,31\}$

Pierre Fermat probó que todos los número **primos** de la forma $4k+1$ se pueden expresar como la suma de dos cuadrados.

Al expresar los número primos encontrado en el ejemplo anterior en el conjunto de números de la forma $4k+1$, vemos la aplicación de lo probado por Fermat.

$5 = 1^2 + 2^2$
$13 = 2^2 + 3^2$
$17 = 1^2 + 4^2$
$29 = 2^2 + 5^2$

Busqueda de números más grandes

En la actualidad la identificación de números primos más y más grandes y la factorización de números compuestos grandes en sus componentes primos son de gran importancia práctica, porque constituyen la base de los sistemas de criptografía modernos o códigos secretos.

No se ha encontrado una formula que genere de modo consistente números primos, mucho menos “ Todos los números primos”

El intento más útil fue realizado Marin Mersenne (1588-1648)

Números de Mersenne y Primos de Mersenne

Para $n = 1,2,3,\ldots,$ los números de Mersenne son generados por la fórmula

$$M_n = 2^n - 1$$

- Si n es compuesto, entonces M_n es compuesto.
- Si n es primo, entonces M_n puede ser primo o compuesto.

Los valores primos de M_n se conocen como primos de Mersenne.

El mayor primo descubierto es primo de Mersenne y fue descubierto por GIMPS (El Sistema de Gran búsqueda de números primos de Mersenne por internet) el 25 de enero 2013. Este número tiene $17{,}425{,}170$ cifras y se obtiene reemplazando $n = 57{,}885{,}161$

Obtención de números de Mersenne

Obtenga los números de Mersenne M_n para $n = 2,3,4,5,6$ y verifique lo discutido anteriormente.

4.3 Temas selectos de teoría de números

MATE 3041

Profa. Milena R. Salcedo Villanueva

Divisores propios

Los **divisores propios** de un número natural incluye todos los divisors del número con excepción del número mismo.

Ejemplo:

Los **divisores propios** de 8 son: $\{1,2,4\}$

Los **divisores propios** de 28 son: $\{1,2,4,7,14\}$

Números Perfectos

Se dice que un número natural es perfecto si es igual a la suma de sus divisores propios.

El perfecto más pequeño es el 6: $6 = 1 + 2 + 3$

El siguiente es el 28: $28 = 1 + 2 + 4 + 7 + 14$.

Los siguiente dos son : 496 y $8{,}128$, el quinto perfecto es $33{,}550{,}336$. En la actualidad se han encontrado 48 números perfectos, el último encontrado tiene $34{,}850{,}340$ cifras, cuando n= $57, 885, 161$ Curtis Cooper,Kurowski, et al. (GIMPS)

De acuerdo al patrón de los números perfectos encontrados se puede dar la conjetura de que todos los números perfectos pares terminan en los dígitos 6 u 8

Euclides descubrió la fórmula para obtener números perfectos pares:

$$2^{n-1}(2^n - 1)$$

Números Deficientes

Un número natural es deficiente si es mayor que la suma de sus divisores propios. Por ejemplo, 8 es deficiente

Ejercicio:

Determine si los números $48, 10$ son deficientes

Números abundantes

Un número natural es abundante si es menor que la suma de sus divisores propios.

Ejercicio:

Determine si los números $12, , 45,$ son deficientes

Números amigables

Los naturales a y b son amigables o amigos, si la suma de los divisores propios de a es igual a b y la suma de los divisores propios de b es igual a a.

Los pitagóricos descubrieron el par números amigables mas pequeños, 220 y 284, luego Fermat 1636 descubrió el siguiente par, $17{,}296$ y $18{,}416$

Conjetura de Golbach

Todos los números pares mayores que 2 se pueden escribir como la suma de dos primos.

Ejemplo:

$$8 = 5 + 3$$
$$10 = 5 + 5$$
$$9 = 2 + 7$$

Los matemáticos han intentado demostrar la conjetura, pero no han tenido existo, sin embargo se ha verificado (abril 4 2013) para números hasta 4×10^8

Primos Gemelos

Los números primos que tienen una diferencia igual a 2 unidades se conocen como **primos gemelos**. Algunos pares de primos gemelos son:

- $3\ y\ 5$
- $5\ y\ 7$
- $11\ y\ 13, etc$

Para probar la infinitud de números primos se usan los números de la forma

$$p_1 \cdot p_2 \cdot p_3 \cdot (\ldots) \cdot p_n + 1$$

Donde todas las p son primos, parecería los numeros resultantes de aplicar esa forma son primos.

Verifica si siempre se obtiene números primos

$p_1 + 1 = 2 + 1 = 3$

$p_1 \cdot p_2 + 1 = 2 \cdot 3 + 1 = 7$

$p_1 \cdot p_2 \cdot p_3 + 1 = 2 \cdot 3 \cdot 5 + 1 = 31$

$p_1 \cdot p_2 \cdot p_3 \cdot p_4 + 1 = 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$

$p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot p_5 + 1 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311$

$p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot p_5 \cdot p_6 + 1 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 =?$

Último teorema de Fermat

Para cualquier número natural $n \geq 3$, no existen tripletas (a, b, c), que satisfagan la ecuación $a^n + b^n = c^n$

Ejercicio:

Para probar la infinitud de números primos se usan los números de la forma

$$p_1 \cdot p_2 \cdot p_3 \cdot (\ldots) \cdot p_n + 1$$

Donde todas las p son primos, parecería los numeros resultantes de aplicar esa forma son primos.

Verifica si siempre se obtiene números primos

$p_1 + 1 = 2 + 1 = 3$

$p_1 \cdot p_2 + 1 = 2 \cdot 3 + 1 = 7$

$p_1 \cdot p_2 \cdot p_3 + 1 = 2 \cdot 3 \cdot 5 + 1 = 31$

$p_1 \cdot p_2 \cdot p_3 \cdot p_4 + 1 = 2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$

$p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot p_5 + 1 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311$

$p_1 \cdot p_2 \cdot p_3 \cdot p_4 \cdot p_5 + 1 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 =?$

4.4 Máximo Común Divisor (MCD) y Mínimo Común Múltiplo (MCM)

MATE 3041

Profa. Milena R. Salcedo Villanueva

Mínimo Común Múltiplo

El máximo común divisor de un grupo de números naturales es el número natural más pequeño que es múltiplo de todos los números del grupo.

Ejemplo:

Halla el MCM de $24, 36$ y 48

$$\begin{array}{ccc|c} 24 & 36 & 48 & 2 \\ 12 & 18 & 24 & 2 \\ 6 & 9 & 12 & 2 \\ 3 & 9 & 6 & 2 \\ 3 & 9 & 3 & 3 \\ 1 & 3 & 1 & 3 \\ & 1 & & \end{array}$$

El MCM de $24, 36$ y $48 = 2^4 \times 3^2 = 144$

Maximo Común Divisor

El máximo común divisor de un grupo de números naturales es el número más grande que es factor (o divisor) de todos los números del grupo.

Ejemplo:

Halla el MCD de 60 y 140

$$\begin{array}{r|l} 60 & 2 \\ 30 & 2 \\ 15 & 3 \\ 5 & 5 \\ 1 & \end{array} \qquad\qquad \begin{array}{r|l} 140 & 2 \\ 70 & 2 \\ 35 & 5 \\ 7 & 7 \\ 1 & \end{array}$$

El MCD de 60 y $140 = 2 \times 2 \times 5 = 20$

Máximo Común Divisor

Otra forma de encontrar el MCD

Halla el MCD de 60 y 140

$$\begin{array}{cc|c} 60 & 140 & 2 \\ 30 & 70 & 2 \\ 15 & 35 & 5 \\ 3 & 7 & \end{array}$$

El MCD de 60 y $140 = 2 \times 2 \times 5 = 20$

Algoritmo Euclidiano para obtener el MCD

1. Divida el número mayor entre el número menor, se ignora el cociente pero se anota el residuo.
2. Divida el divisor anterior entre el residuo obtenido en el paso 1. Una vez más se anota el residuo.
3. Continue dividiendo los residuos sucesivos tantas veces como sea necesario para obtener un residuo igual a cero.
4. El último divisor positivo de este proceso es el MCD de los números iniciales.

Hallemos el MCD de los 60 y 140 usando el algoritmo Euclidiano:

$$\begin{array}{r|l} 60 & \overline{140} \\ - & 120 \\ \hline & \ \ 20 \end{array}$$

$$\begin{array}{r|l} & \ \ 3 \\ \hline 20 & 60 \\ - & 60 \\ \hline & \ \ 0 \end{array}$$

Entonces el MCD de 60 y $140 = 20$

Nota importante

El máximo común divisor (MCD) se conoce también como máximo factor común (MFC)

Ejercicios

Calcular el MCD de los siguientes números:

$a.$ $540\ y\ 1200$

$b.$ $52, 39\ y\ 78$

$c.$ $138, 184, 437$