# Presentación del curso, Teoría de Números

Prof. Jhon Fredy Tavera Bucurú

2025

2025

Problemas Abiertos en Teoría de Números

Aplicaciones de la Teoría de Números

Comentarios sobre la formalidad

2025

- **Cuadrado perfecto:**

$$2025 = 45^2$$

- **Suma de dos cuadrados:**

$$2025 = 27^2 + 36^2$$

- **Suma de tres cuadrados:**

$$2025 = 5^2 + 20^2 + 40^2$$

- **Suma de cubos consecutivos:**

$$1^3 + 2^3 + \cdots + 9^3 = 2025$$

- **Partición curiosa:** Al separar 2025 en "20" y "25", se obtiene que

$$20 + 25 = 45 \quad (\sqrt{2025})$$

- **Suma de números impares:** Dado que cualquier cuadrado perfecto es la suma de los primeros números impares,

$$2025 = 1 + 3 + \cdots + 89 \quad \text{(45 términos)}$$

- **Factorización:**

$$2025 = 3^4 \cdot 5^2$$

- **Número Harshad:** La suma de sus dígitos es $2 + 0 + 2 + 5 = 9$ y 2025 es divisible por 9.

# Problemas Abiertos en Teoría de Números

# Conjetura de Collatz

- También conocida como el problema $3x + 1$. Formulada en 1937 por Lothar Collatz.
- Propone que tomando cualquier número natural, si es par se divide por 2, y si es impar se multiplica por 3 y se le suma 1, eventualmente se llega al número 1.

# Conjetura de Collatz

- También conocida como el problema $3x + 1$. Formulada en 1937 por Lothar Collatz.
- Propone que tomando cualquier número natural, si es par se divide por 2, y si es impar se multiplica por 3 y se le suma 1, eventualmente se llega al número 1.
- 27, 82, 41, 124, 62, 31, 94, 47, 142, 71, 214, 107, 322, 161, 484, 242, 121, 364, 182, 91, 274, 137, 412, 206, 103, 310, 155, 466, 233, 700, 350, 175, 526, 263, 790, 395, 1186, 593, 1780, 890, 445, 1336, 668, 334, 167, 502, 251, 754, 377, 1132, 566, 283, 850, 425, 1276, 638, 319, 958, 479, 1438, 719, 2158, 1079, 3238, 1619, 4858, 2429, 7288, 3644, 1822, 911, 2734, 1367, 4102, 2051, 6154, 3077, 9232, 4616, 2308, 1154, 577, 1732, 866, 433, 1300, 650, 325, 976, 488, 244, 122, 61, 184, 92, 46, 23, 70, 35, 106, 53, 160, 80, 40, 20, 10, 5, 16, 8, 4, 2, 1
- Ha sido probada para todos los números enteros hasta $2.95 \times 10^{20}$, pero no hay prueba general.

# Conjetura de Goldbach

- Propuesta por Christian Goldbach en 1742.
- Afirma que todo número par mayor que 2 puede ser expresado como la suma de dos números primos.

# Conjetura de Goldbach

- Propuesta por Christian Goldbach en 1742.
- Afirma que todo número par mayor que 2 puede ser expresado como la suma de dos números primos.
- Ejemplo: $28 = 11 + 17$
- T. Oliveira e Silva realizó una búsqueda computacional distribuida que ha verificado la conjetura para $n \leq 4 \times 10^{18}$ (y se ha verificado dos veces hasta $4 \times 10^{17}$ a partir de 2013). pero aún no se ha demostrado para todos los números.

# Conjetura de los Primos Gemelos

- Propone que hay infinitos pares de números primos que tienen una diferencia de 2.

# Conjetura de los Primos Gemelos

- Propone que hay infinitos pares de números primos que tienen una diferencia de 2.
- Ejemplo: (3, 5), (11, 13)
- Formulada por Alphonse de Polignac en 1846.
- En 2013, Yitang Zhang demostró que hay infinitos pares de primos que difieren por menos de 70 millones.
- Desde entonces, este límite ha sido reducido significativamente, pero la conjetura original aún no está probada.

# Conjetura de Beal

- Propuesta por Andrew Beal en 1993.
- Afirmaba que para $A^x + B^y = C^z$, donde $A, B, C$ son enteros positivos y $x, y, z$ son enteros mayores que 2, $A, B, C$ deben tener un factor primo en común.

[1] Más información sobre el premio: https://www.ams.org/prizes-awards/paview.cgi?parent_id=41

# Conjetura de Beal

- Propuesta por Andrew Beal en 1993.
- Afirmaba que para $A^x + B^y = C^z$, donde $A, B, C$ son enteros positivos y $x, y, z$ son enteros mayores que 2, $A, B, C$ deben tener un factor primo en común.
- Por ejemplo $3^3 + 6^3 = 3^5$ tiene sus bases con un factor común 3, y la solución $7^6 + 7^7 = 98^3$ tiene las bases con un factor común 7

[1] Más información sobre el premio: https://www.ams.org/prizes-awards/paview.cgi?parent_id=41

# Conjetura de Beal

- Propuesta por Andrew Beal en 1993.
- Afirmaba que para $A^x + B^y = C^z$, donde $A, B, C$ son enteros positivos y $x, y, z$ son enteros mayores que 2, $A, B, C$ deben tener un factor primo en común.
- Por ejemplo $3^3 + 6^3 = 3^5$ tiene sus bases con un factor común 3, y la solución $7^6 + 7^7 = 98^3$ tiene las bases con un factor común 7
- Hay un premio de un millón de dólares ofrecido por Beal para una prueba o contraejemplo de esta conjetura. [1].

[1]Más información sobre el premio:
https://www.ams.org/prizes-awards/paview.cgi?parent_id=41

# Conjetura de los Números Perfectos Impares

- Un número perfecto es un número entero positivo que es igual a la suma de sus divisores propios positivos.
- Ejemplo: $6 = 1 + 2 + 3$.

# Conjetura de los Números Perfectos Impares

- Un número perfecto es un número entero positivo que es igual a la suma de sus divisores propios positivos.
- Ejemplo: $6 = 1 + 2 + 3$.
- Todos los números perfectos conocidos son pares.
- La conjetura propone que no existen números perfectos impares.
- Ha sido verificada para números muy grandes, pero aún no hay prueba general.

# Aplicaciones de la Teoría de Números

# Criptografia: Sistema RSA

- El sistema RSA es uno de los algoritmos de criptografía más utilizados.
- Es empleado por muchos sitios web conocidos para asegurar la comunicación.

# Criptografia: Sistema RSA

- El sistema RSA es uno de los algoritmos de criptografía más utilizados.
- Es empleado por muchos sitios web conocidos para asegurar la comunicación.
- Ejemplos de sitios web que utilizan RSA:
  - **Google:** Utiliza RSA para la seguridad en Gmail y otros servicios.
  - **Amazon:** Emplea RSA para proteger las transacciones en su plataforma de comercio electrónico.
  - **Facebook:** Utiliza RSA para asegurar la transmisión de datos entre usuarios y servidores.
  - **Bancos en línea:** La mayoría de las plataformas de banca en línea utilizan RSA para asegurar las transacciones financieras.

# Criptografia: Sistema RSA

- El sistema RSA es uno de los algoritmos de criptografía más utilizados.
- Es empleado por muchos sitios web conocidos para asegurar la comunicación.
- Ejemplos de sitios web que utilizan RSA:
  - **Google:** Utiliza RSA para la seguridad en Gmail y otros servicios.
  - **Amazon:** Emplea RSA para proteger las transacciones en su plataforma de comercio electrónico.
  - **Facebook:** Utiliza RSA para asegurar la transmisión de datos entre usuarios y servidores.
  - **Bancos en línea:** La mayoría de las plataformas de banca en línea utilizan RSA para asegurar las transacciones financieras.
- La seguridad del RSA depende de la dificultad de factorizar el número $n$ en sus factores primos.

# Generación de Números Pseudoaleatorios: BBS

- Los números pseudoaleatorios son cruciales para simulaciones, criptografía y algoritmos.

# Generación de Números Pseudoaleatorios: BBS

- Los números pseudoaleatorios son cruciales para simulaciones, criptografía y algoritmos.
- Ejemplo: El generador de números pseudoaleatorios basado en la teoría de números conocido como "BBS" (Blum-Blum-Shub).
- **Blum-Blum-Shub:**
  - Genera números pseudoaleatorios seguros.
  - Fórmula: $x_{n+1} = (x_n^2) \mod M$, donde $M = p \times q$ y $p$ y $q$ son números primos.

# Generación de Números Pseudoaleatorios: BBS

- Los números pseudoaleatorios son cruciales para simulaciones, criptografía y algoritmos.
- Ejemplo: El generador de números pseudoaleatorios basado en la teoría de números conocido como "BBS" (Blum-Blum-Shub).
- **Blum-Blum-Shub:**
  - Genera números pseudoaleatorios seguros.
  - Fórmula: $x_{n+1} = (x_n^2) \mod M$, donde $M = p \times q$ y $p$ y $q$ son números primos.
- Propiedades deseadas:
  - Uniformidad
  - Independencia
  - Periodo largo

# Codificación y Corrección de Errores: Red-Solomon

- La teoría de números también se utiliza en la codificación y corrección de errores.

# Codificación y Corrección de Errores: Red-Solomon

- La teoría de números también se utiliza en la codificación y corrección de errores.
- **Códigos de Reed-Solomon:**
  - Utilizados en CDs, DVDs y códigos QR.
  - Basados en polinomios sobre cuerpos finitos (números primos).
  - Permiten la detección y corrección de múltiples errores en datos.

# Codificación y Corrección de Errores: Red-Solomon

- La teoría de números también se utiliza en la codificación y corrección de errores.
- **Códigos de Reed-Solomon:**
  - Utilizados en CDs, DVDs y códigos QR.
  - Basados en polinomios sobre cuerpos finitos (números primos).
  - Permiten la detección y corrección de múltiples errores en datos.
- **Código de Hamming:**
  - Utilizado en comunicaciones digitales y almacenamiento de datos.
  - Permite la corrección de errores de un solo bit y la detección de errores de dos bits.

# Comentarios sobre la formalidad

# Conjetura Números de Fermat primos

- Los números de Fermat se definen como $F_n = 2^{2^n} + 1$.
- Fermat conjeturó que todos estos números son primos.

# Conjetura Números de Fermat primos

- Los números de Fermat se definen como $F_n = 2^{2^n} + 1$.
- Fermat conjeturó que todos estos números son primos.
- Los primeros cuatro números de Fermat son primos:
  - $F_0 = 3$
  - $F_1 = 5$
  - $F_2 = 17$
  - $F_3 = 257$
  - $F_4 = 65537$

# Conjetura Números de Fermat primos

- Los números de Fermat se definen como $F_n = 2^{2^n} + 1$.
- Fermat conjeturó que todos estos números son primos.
- Los primeros cuatro números de Fermat son primos:
  - $F_0 = 3$
  - $F_1 = 5$
  - $F_2 = 17$
  - $F_3 = 257$
  - $F_4 = 65537$
- Sin embargo, el quinto número de Fermat:

$$F_5 = 2^{2^5} + 1 = 4294967297$$

- No es primo, ya que:

$$4294967297 = 641 \times 6700417$$

# Números de Fermat: Problemas Abiertos y Últimos Descubrimientos

- Es un problema abierto si hay infinitos primos de Fermat.

# Números de Fermat: Problemas Abiertos y Últimos Descubrimientos

- Es un problema abierto si hay infinitos primos de Fermat.
- El último número de Fermat parcialmente factorizado es $F_{223380}$:
  - El 4 de julio de 2024, Ryan Propper y Serge Batalov descubrieron que
    $$56073 \cdot 2^{223382} + 1$$
    divide a $F_{223380}$.

# Números de Fermat: Problemas Abiertos y Últimos Descubrimientos

- Es un problema abierto si hay infinitos primos de Fermat.
- El último número de Fermat parcialmente factorizado es $F_{223380}$:
  - El 4 de julio de 2024, Ryan Propper y Serge Batalov descubrieron que
    $$56073 \cdot 2^{223382} + 1$$
    divide a $F_{223380}$.
- Otro descubrimiento reciente:
  - El 24 de mayo de 2024, Gary Gostin encontró que
    $$322072887044529 \cdot 2^{253} + 1$$
    divide a $F_{251}$, haciendo que $F_{251}$ sea el quinto número de Fermat más grande con múltiples factores conocidos.

# Aplicaciones de los Números de Fermat

- Los números de Fermat tienen aplicaciones importantes en varios campos de las matemáticas y la informática.

# Aplicaciones de los Números de Fermat

- Los números de Fermat tienen aplicaciones importantes en varios campos de las matemáticas y la informática.
- **Construcción de Polígonos:**
  - Pierre Wantzel demostro en 1837, el teorema conocido como Gauss-Wantzel.
  - Un polígono regular de $n$ lados se puede construir con regla y compás si y solo si $n$ es una potencia de 2 o 2 multiplicada por un producto de distintos números de Fermat primos.
  - Ejemplo: un polígono de 17 lados se puede construir porque 17 es un número de Fermat primo ($F_2$).

# Aplicaciones de los Números de Fermat

- Los números de Fermat tienen aplicaciones importantes en varios campos de las matemáticas y la informática.
- **Construcción de Polígonos:**
  - Pierre Wantzel demostro en 1837, el teorema conocido como Gauss-Wantzel.
  - Un polígono regular de $n$ lados se puede construir con regla y compás si y solo si $n$ es una potencia de 2 o 2 multiplicada por un producto de distintos números de Fermat primos.
  - Ejemplo: un polígono de 17 lados se puede construir porque 17 es un número de Fermat primo ($F_2$).
- **Generación de Números Pseudoaleatorios:**

# Conjetura del Polinomio generador de primos $n^2 + n + 41$

- Euler descubrió que el polinomio $n^2 + n + 41$ genera números primos.

# Conjetura del Polinomio generador de primos $n^2 + n + 41$

- Euler descubrió que el polinomio $n^2 + n + 41$ genera números primos.
- Ejemplos:
  - $n = 0 \rightarrow 41$
  - $n = 1 \rightarrow 43$
  - $n = 2 \rightarrow 47$
  - $n = 3 \rightarrow 53$

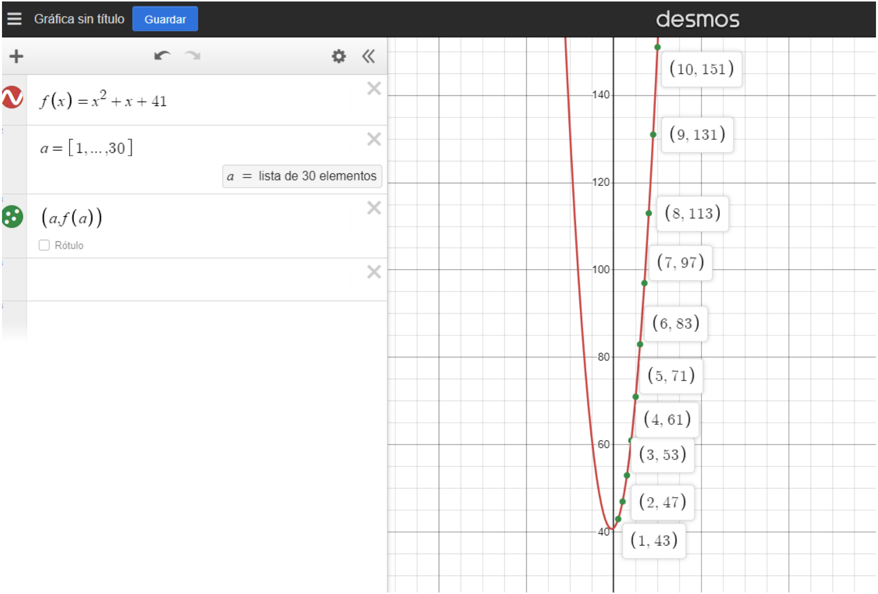


Figure: Gráfica de la función $n^2 + n + 41$

- Sin embargo, para $n = 40$:

$$40^2 + 40 + 41 = 1681$$

- $1681 = 41^2$, que no es primo.

# Conjetura $n^{17} + 9$ y $(n+1)^{17} + 9$ primos relativos

- Consideremos las expresiones $n^{17} + 9$ y $(n+1)^{17} + 9$.

# Conjetura $n^{17}+9$ y $(n+1)^{17}+9$ primos relativos

- Consideremos las expresiones $n^{17}+9$ y $(n+1)^{17}+9$.
- Ejemplos:
  - $n=1$: 10 y 131081 .
  - $n=2$: 131081 y 129140172 .
  - $n=3$: 129140172 y 17179869193.
  - $n=4$: 17179869193 y 762939453134.

# Conjetura $n^{17}+9$ y $(n+1)^{17}+9$ primos relativos

- Consideremos las expresiones $n^{17}+9$ y $(n+1)^{17}+9$.
- Ejemplos:
  - $n=1$: 10 y 131081 .
  - $n=2$: 131081 y 129140172 .
  - $n=3$: 129140172 y 17179869193.
  - $n=4$: 17179869193 y 762939453134.
- Para los primeros valores de $n$, el Máximo Común Divisor parece ser 1.

```
import math
n=3
print(math.gcd(n**17+9, (n+1)**17+9))
```

# Conjetura $n^{17} + 9$ y $(n+1)^{17} + 9$ primos relativos

- Consideremos las expresiones $n^{17} + 9$ y $(n+1)^{17} + 9$.
- Ejemplos:
  - $n = 1$: 10 y 131081 .
  - $n = 2$: 131081 y 129140172 .
  - $n = 3$: 129140172 y 17179869193.
  - $n = 4$: 17179869193 y 762939453134.
- Para los primeros valores de $n$, el Máximo Común Divisor parece ser 1.

```
import math
n=3
print(math.gcd(n**17+9, (n+1)**17+9))
```

- pero no es verdad!

## conjetura, dados primos $p, q$ existe $n \in \mathbb{N}$, talque q divide a $n^p - p$

- Se puede probar que dado cualquier primo $p$, existe siempre un primo $q$ talque $q$ no divide ninguno de los números $n^p - p$ donde $n$ es cualquier número natural.
- La demostración no explicita cual es el primo $q$.