# MATEMÁTICA Y LITERATURA, PROPUESTAS PARA EL AULA

Natalia Ferre
Facultad de Ciencias Exactas, U.N.L.P.
nataliaferre@fibertel.com.ar
**Nivel educativo:** terciario - universitario
**Palabras clave**: interdisciplinariedad - integración – demostración – número primo

## Resumen

El presente trabajo es una propuesta para el aula dirigido a alumnos de 1er año de un curso de álgebra de nivel universitario para carreras de licenciatura o profesorado.
La propuesta pedagógica es vincular distintas disciplinas con la matemática, de modo de mirar desde otro lado y de manera integrada los conceptos matemáticos que se han ido trabajando. Se supone conocido el concepto de divisibilidad, números primos, el Teorema algoritmo de la división, el Teorema fundamental de la aritmética, congruencia módulo p y Teorema de Fermat.
Se presentará el libro “El Tío Petros y la conjetura de Goldbach” de Apóstolos Dioxadis, y una serie de actividades para realizar luego de su lectura, con una propuesta metodológica de trabajo en grupos, con intervención del docente como guía y al final de cada bloque habrá una puesta en común con explicaciones en el pizarrón de los conceptos que han ido apareciendo.
Se trabajará fundamentalmente en las demostraciones, qué significa demostrar una proposición universal y una existencial, y qué significa demostrar su falsedad, qué son las conjeturas. Por otro lado se verán relaciones entre los números primos, con dos herramientas para analizar primalidad. Se enunciará también el Teorema de Gödel y su incidencia en el quehacer matemático. Finalmente se dará una aplicación, es decir, luego de haber trabajado en todos los aspectos de números primos, se muestra la criptografía de clave pública como una aplicación directa de esta teoría.

## Fundamentos

El presente trabajo es una propuesta para motivar el estudio de la matemática desde un planteo literario. Un enfoque distinto que puede estimular y desestructurar la clase de matemática generando un mayor interés.
Por otro lado se pretende generar un proceso integrador de distintos temas ya vistos, que de sentido y unidad. Se trata también de que la enseñanza de la matemática provoque investigación y descubrimiento.
Menciona Claudi Alsina a la creatividad como un fin educativo, que muchas veces se les pide a los alumnos en la resolución de problemas.
El va mas allá mencionando la creatividad que debe tener el profesorado en su actuación docente.
Dice Alsina: “El desarrollo de la ciencia tiende a una especialización cada vez más fina, y por eso puede resultar muy creativo el unir resultados de varias ramas del saber y en particular llevar a cabo labores interdisciplinarias donde la matemática pueda aparecer realmente aplicada y motivada”. (Alsina, 2000).
El enfoque de conectar las matemáticas con otras disciplinas puede resultar sumamente provechoso. Así, y de acuerdo con Irene Zapico y su grupo de investigación las conexiones existentes entre estas asignaturas se hallan no solo en sus orígenes sino también en su desarrollo y consecuencias. “El verdadero conocimiento es integrador y no reconoce propietarios”. (Zapico y otros, 2002).
El libro “ El Tío Petros y la Conjetura de Goldbach” es una novela escrita por Apostolos Dioxadis, que narra la historia de un joven que quiere ser matemático y es desalentado por su

tío, también matemático pero retirado de sus estudios, que le da para resolver la Conjetura de Goldbach, sin decirle que se trata de un problema no resuelto. Disponer de una novela en la que aparecen tantos contenidos matemáticos es una maravillosa estrategia para abordar diferentes temas desde una perspectiva distinta. El tema central son los números primos y los teoremas y conjeturas acerca de ellos, pero también la interpretación de los teoremas y conjeturas y su significado.
La guía de actividades propuesta para el aula es sólo una muestra de las numerosas que se pueden extraer y generar y son de diferentes características.

- Actividades de fijación para reafirmar y validar conceptos y definiciones que se han ido tratando en el aula.
- Actividades de opinión personal acerca de la matemática, del trabajo de un matemático, debates que a veces están ausentes y que aportan a conocer el trabajo de investigación.
- Actividades de ejercitación: resolución de ejercicios que refuerzan definiciones y conceptos.
- Actividades de aplicación. Aquí se plantean situaciones nuevas o diferentes que requieren un proceso de reflexión acerca de las estrategias a seguir. En la aplicación los estudiantes llegan a entender los propósitos y usos del conocimiento que se está estudiando.

**Actividad**

Lee el libro “El tío Petros y la conjetura de Goldbach” de Apóstolos Dioxadis.

**I. Introducción**

1) En la página 12, cuando el protagonista va a la conferencia en homenaje al nacimiento de Leonhard Euler queda maravillado , a pesar de no entender demasiado acerca del significado de algunas cosas, dice ”…*Los nombres mágicos, nunca oídos, se sucedían interminablemente, cautivándome con su sublime musicalidad: el problema del continuo, el aleph, Gottiod Frege, razonamiento inductivo, el programa de Hilbert, verificabilidad y no verificabilidad, pruebas de consistencia, pruebas de completitud, conjunto de conjuntos, la máquina de Von Neumann, la paradoja de Russell, el álgebra de Boole…*”
”…*los axiomas de Peano para la aritmética, el teorema de los números primos, los sistemas abiertos y cerrados, más axiomas, Euclides, Euler, Cantor, Zenon, Gödel…”*
Lee las biografías que figuran al final del libro, de los matemáticos citados y haz una lista cronológica de ellos.
Los axiomas de Peano son 5. Investiga acerca de ellos, escríbelos y discutan en el grupo si hay más conjuntos que satisfagan los 2 últimos.
2) En la página 14 Petros habla acerca del significado de la matemática, explica brevemente. Explica que son las matemáticas para vos. En la página 15 y en la pagina 25 se menciona cómo debe ser un matemático, ¿Estás de acuerdo con ese punto de vista? da tu opinión.
3) En la página 16 Petros plantea un problema a su sobrino que involucra los números primos. Da una definición de número primo. Encuentra 5 números primos mayores que 50.
4) En la página 17 se menciona que la prueba de la infinitud de los números primos la demostró por primera vez Euclides con el método de reducción al absurdo. Explica el método con tus palabras. Demuestra que el cuadrado de todo entero par es par, utilizando ese método.
Luego Petros enuncia el problema de demostrar que todo par mayor a dos puede escribirse como suma de dos primos y da algunos ejemplos. Escribe el 16, 18, 20, 22 y 24 de esa forma.
5) “*Después de innumerables divisiones había creado una tabla de los primeros cien números primos (una versión primitiva y casera de la criba de Eratóstenes)*” (pagina 18). Investiga acerca de la criba de Eratóstenes. Describe el método y ejemplifica.

6) Cuando el protagonista cree haber demostrado el problema que le dio Petros, éste le envía un telegrama diciendo: "*Lo único que has demostrado es que todo número par puede expresarse como la suma de un primo y un impar, lo cual es obvio. Stop*." (pagina 19). Lo que sigue es la demostración de esa afirmación. Justifica cada paso.

Sea n un número par, entonces n=2k, con k $\in$ ……..y k>1

Existe un número p primo tal que p < n y p$\neq$2, ya que………………………….

Entonces n = p t + r , t y r únicos y r < p porque………………………………..

Entonces n = p + (t-1)p + r porque ……………………………………………

caso 1) t par , entonces (t-1) es impar y r es par porque…………………………
entonces (t-1)p + r es impar porque……………………………………….
entonces n es suma de un primo y un impar.

caso 2) t impar , entonces (t-1) es par y r es impar porque………………………
entonces (t-1)p + r es impar porque……………………………………….
entonces n es suma de un primo y un impar.

También puede simplificarse mucho la prueba si pensamos que para todo par mayor que 2, el 3 es menor que él y primo. ¿Puedes formalizar esta demostración?

7) El problema que Petros da a su sobrino es la Conjetura de Goldbach. ¿Por qué se llama conjetura? En la pagina 17 se mostraron varios casos en los que la proposición es verdadera, ¿Por qué no es suficiente? ¿Por qué el protagonista busca casos donde la conjetura falle? ¿Hubiera sido suficiente encontrar un caso en el que no fuera cierta para afirmar que es verdadera o que es falsa?

Lee los siguientes enunciados y discute su valor de verdad justificando tu respuesta con la demostración:

a. " **Todo** número par es múltiplo de 4"
b. " **Todo** múltiplo de 6 es múltiplo de 3"
c. " **Algunos** números son primos"
d. " **Existen** números pares e impares a la vez"

8) En la página 22 se menciona que la conjetura está en una carta enviada a Euler en 1742 que en realidad dice "*Todo entero puede expresarse como la suma de tres números primos*". Lo que se conoce como la conjetura de Goldbach es un corolario o una consecuencia de esta afirmación. ¿Puedes explicar porqué?

9) En la página 27 se comenta acerca del trabajo de los matemáticos, discutan en grupos y escriban cómo imaginan este trabajo.

**II. La historia de Petros Papachristos:**

1) " *A los 11 años, tras aprender que todo entero positivo puede expresarse como suma de cuatro cuadrados, Petros sorprendía a los buenos de los jesuitas proporcionándoles la composición de cualquier número que le sugirieran después de escasos segundos de reflexión* " (pagina 1)
Esta expresión no es única, ¿puedes encontrar 5 números con dos expresiones diferentes?
Escribe el 325 y el 171 como suma de 4 cuadrados.

2) “ *Y qué me dices de la distribución de los números primos? - preguntó Caratheodory - ¿Se te ocurre una forma de calcular cuántos primos existen menores que un número dado n?*
*- No - respondió Petros -, pero conforme n tiende a infinito, la cantidad de primos se aproxima a n dividido por su logaritmo neperiano*.” (página 3)
El enunciado que se menciona es el teorema de los números primos. En las páginas 12 y 13 se vuelve a mencionar el Teorema, busca quién lo enunció y quien lo demostró. Ejemplifica con n = 50 y n = 100.
Con respecto a esta distribución en la página 12 se menciona que: “*… es sumamente fácil demostrar que para cualquier entero dado k, es posible encontrar una sucesión de k enteros que no contiene un solo número primo*”. Lee la demostración que figura al pie, transcríbela completando las justificaciones y da ejemplos.
3) “*El sol aún no había salido cuando se sentó al escritorio, tomó su gruesa estilográfica y escribió en una hoja de papel blanca y nueva:*
*ENUNCIADO: Todo entero par mayor que 2 es igual a la suma de dos primos.*
*PRUEBA: Supongamos que el enunciado anterior es falso. Luego, existe un entero n tal que 2n no puede expresarse como la suma de dos números primos; por ejemplo, para todo primo p< 2n, 2n - p está compuesto...”* (página 11)
¿Cuál es el método de demostración que va a utilizar? ¿Porqué dice que suponer falso el enunciado implica suponer que para todo primo primo p, p<2n 2n-p está compuesto? ¿Qué pasaría si no estuviera compuesto?
4) En la página 13 se menciona la segunda conjetura de Goldbach. Enúnciala y da 5 ejemplos de impares mayores que 50.
5) “*Como muchos matemáticos que trabajan durante largos períodos con problemas aritméticos básicos, Petros había adquirido la cualidad denominada de amistad con los enteros, esto es, un conocimiento profundo de la idiosincrasia y las peculiaridades de miles de números específicos. He aquí algunos ejemplos: un amigo de los enteros identificará de inmediato como primos los números 199, 457 o 1009. De manera automática asociará el 220 con el 284, puesto que están ligados por una relación atípica (la suma de los divisores enteros de cada uno es igual a la del otro). Leerá con naturalidad el 256 como 2 a la octava potencia que como bien sabe está seguido por un número de gran interés histórico, dado que el 257 puede expresarse como* $2^{2^3}+1$, *y una hipótesis sostenía que todos los números de la forma* $2^{2^n}+1$, *eran primos*” (página 35)
Encuentra el primo siguiente a 1009 usando la Criba de Eratóstenes. ¿Qué ocurrió con la hipótesis que aparece en el relato? ¿Pudo demostrarse?
6) En las páginas 38 y 39 Petros se encuentra con Alain Turig y conversan acerca del teorema de Gödel. Anteriormente, en la pagina 29 también se menciona la posición de Euclides acerca de la posibilidad de demostrar las proposiciones verdaderas. Relee estas páginas y discutan en el grupo sus opiniones. Expliquen brevemente las conclusiones.
En la página 44 Turig envía un telegrama a Petros: “… *He demostrado la imposibilidad de demostrar la solubilidad de un problema a priori. Stop.*”
¿Pueden explicar el significado de esas palabras? ¿Qué relación tiene esto con el problema que Petros estaba estudiando?

**III. De vuelta a Estados Unidos:**

1) En la página 13 Petros dice a su sobrino: “*– Ahora demuestra que los ceros complejos de la función de Riemann tienen una parte real igual a ½. Me eché a reír y el me imitó.*
*- ¡No! ¡Otra vez, no, Tío Petros!- exclamé* “
¿Cómo se llama el enunciado que Petros le pide que demuestre? ¿Es un teorema o una conjetura aún?

2) En la página 22 se menciona lo que se conoce como el último teorema de Fermat. Escribe el enunciado. Averigua quién demostró este teorema y cuando lo hizo.

**IV. Algunos ejercicios:**

1) Demostrar que para todo p primo, p>5, $p^2-1$ es múltiplo de 24.
2) a) Si se suman 3 números naturales consecutivos el resultado ¿es siempre un múltiplo de 3?
   b) Si se suman 5 números naturales consecutivos el resultado ¿es siempre un múltiplo de 5?
   c) ¿Será cierto que si se suman k números naturales consecutivos el resultado es siempre un múltiplo de k?
3) Encontrar todos los números naturales n tales que $n$ y $n^2+8$ sean ambos primos.
4) Demostrar que para todo número primo p distinto de 2 y 5, existe un número cuyas cifras son todas 9 tal que p lo divide.
5) Uno de los temas importantes que aparecen en el texto es la dificultad de averiguar si un número es primo o no. Se ha trabajado con la Criba de Eratóstenes, pero para números muy grandes sigue siendo muy trabajoso.
   Mersenne escribió una vez a Fermat preguntándole si $100895598169$ era un número primo. Fermat respondió inmediatamente que es el producto de $898423$ por $112303$, ambos primos.
   Al día de hoy no se sabe a ciencia cierta cómo factorizó ese número tan grande en tan poco tiempo. Lo que sí se conoce es un método de factorización ideado por Fermat, aunque no sabemos si fue el que usó para este caso.

**El método de factorización de Fermat**

La cuestión es factorizar un cierto número $n$. Si $n$ es igual a la diferencia de dos cuadrados, digamos $n=x^2-y^2$, entonces $n$ puede factorizarse de forma muy sencilla: $n=(x+y)(x-y)$.

Como $x^2$ debe ser mayor que $n$ se tiene que $x$ debe ser mayor que $\sqrt{n}$. Dado un número entero positivo $n$ que queremos factorizar tomamos un entero positivo $x$ mayor que $\sqrt{n}$. Calculamos $x^2$ y le restamos $n$. Si obtenemos un cuadrado hemos terminado. Si no es así tomamos $x+1$, calculamos $(x+1)^2$, restamos $n$ y si hemos obtenido un cuadrado se acaba. Procedemos de la misma forma hasta encontrar un cuadrado.

Ejemplos:

- Vamos a factorizar el número $13837$. Su raíz cuadrada está entre $117$y $118$. Tomamos $x=118$. Pero $118^2-13837=87$, que no es un cuadrado. Tomamos ahora $x=119$. Ahora $119^2-13837=324=18^2$. Por tanto despejando $n=13837$ de esta expresión tenemos su factorización:

$$13837=119^2-18^2=(119+18)(119-18)=137\cdot 101$$

- Vamos ahora con un número más grande, el que utilizó **Fermat** para probar la efectividad de su método: $2027651281$. Su raíz cuadrada está entre $45029$ y $45030$. Comenzamos con $x=45030$. Veamos qué resultados obtenemos:

$45030^2 - 2027651281 = 49619$, que no es un cuadrado.
$45031^2 - 2027651281 = 139680$, que no es un cuadrado.
$45032^2 - 2027651281 = 229743$, que no es un cuadrado.
$45033^2 - 2027651281 = 319808$, que no es un cuadrado.
$45034^2 - 2027651281 = 409875$, que no es un cuadrado.
$45035^2 - 2027651281 = 499944$, que no es un cuadrado.
$45036^2 - 2027651281 = 590015$, que no es un cuadrado.
$45037^2 - 2027651281 = 680088$, que no es un cuadrado.
$45038^2 - 2027651281 = 770163$, que no es un cuadrado.
$45039^2 - 2027651281 = 860240$, que no es un cuadrado.
$45040^2 - 2027651281 = 950319$, que no es un cuadrado.
$45041^2 - 2027651281 = 1040400 = 1020^2$.

Por tanto ya tenemos la factorización:
$2027651281 = 45041^2 - 1020^2 = (45041 + 1020)(45041 - 1020) = 44021 \cdot 46061$
Como podemos ver el método está muy bien si la diferencia entre los factores del número no es muy grande pero no es demasiado eficiente si los dos factores están muy alejados el uno del otro, ya que en ese caso la cantidad de cálculos que deberíamos realizar sería enorme. De todas formas el método es interesante ya que hasta en nuestros tiempos ha servido como motivación para la búsqueda de nuevos métodos de factorización.

- Elijan un número de 10 cifras y utilicen la factorización de Fermat para investigar si es compuesto o no.

7) Tenemos cuatro números primos que se escriben de la siguiente manera: **AA , BAB , BACD , AAAC**. Cada letra representa una cifra del 0 al 9. A letras distintas corresponden cifras distintas y a letras iguales corresponden letras iguales. ¿Cuáles son estos números primos?

**V. Una aplicación importante: Criptografía: Cifrado de clave pública II. Cifrado RSA**

El algoritmo fue descripto en 1977 por Ron Rivest, Adi Shamir y Len Adleman *(la sigla RSA es Rivest Shamir Adleman)* en el MIT.El cifrado RSA es un algoritmo de cifrado de clave pública (o asimétrico) por bloques, que como todos los cifrados de clave pública tiene dos claves: una pública, que se distribuye a los usuarios que quiera el propietario de ella, y otra privada, la cual es guardada en secreto por su propietario. Así cuando se envía un mensaje, el emisor usa la clave pública de cifrado del receptor para cifrar el mensaje y una vez que dicho mensaje llega al receptor, éste se ocupa de descifrarlo usando su clave oculta. Los mensajes enviados usando el algoritmo RSA se representan mediante números y el funcionamiento se basa en el producto de dos números primos grandes (mayores que $10^{100}$) elegidos al azar para conformar la clave de descifrado. Emplea expresiones exponenciales en aritmética modular. La seguridad de este algoritmo radica en que no hay maneras rápidas conocidas de factorizar un número grande en sus factores primos utilizando computadoras tradicionales.

**Cifrado de mensajes:**

Bob quiere enviar a Alicia un mensaje secreto que solo ella pueda leer. Alicia envía a Bob una caja con una cerradura abierta, de la que solo Alicia tiene la llave. Bob recibe la caja, escribe el mensaje, lo pone en la caja y la cierra con su cerradura (ahora Bob no puede leer el mensaje).

Bob envía la caja a Alicia y ella la abre con su llave. En este ejemplo, la caja con la cerradura es la clave pública de Alicia, y la llave de la cerradura es su clave privada.

1. Cada usuario elige $n = p \cdot q$
2. Los valores p y q NO se hacen públicos
3. Cada usuario calcula $\varphi(n) = (p-1)(q-1)$
4. Cada usuario elige una clave pública e de forma que $1 < e < \varphi(n)$ y que cumpla con la condición: mcd $[e, \varphi(n)] = 1$
5. Cada usuario calcula la clave privada d , tal que $e.d \equiv 1 \bmod \varphi(n)$
6. Se hace público el grupo n y la clave e
7. Se guarda en secreto la clave d

Cifra: $c \equiv m^e \pmod n$

Ejemplo: Supongamos que Bob desea enviar un mensaje M a Alicia. Él cambia M en un número m<n, usando un protocolo reversible conocido como padding scheme. Bob ahora tiene m, y conoce n y e, mientras Alicia fue avisada. Él entonces calcula el texto cifrado c correspondiente a m. Bob transmite c a Alicia.

$c \equiv m^e \pmod n$ donde e y n son la clave pública de Alicia ( la caja abierta)

Alicia para descifrar tiene su clave privada d (llave) tal que $d.e \equiv 1 \pmod{\varphi(n)}$, entonces calcula: $c^d = (m^e)^d = m^{1+k\varphi(n)} = m\,.m^{k\varphi(n)} \equiv m \pmod n$, ya que por el Teorema de Euler Fermat

si a y n son coprimos $(a^{\varphi(n)}) \equiv 1 \pmod n$, donde $\varphi(n)$ es la función de Euler que a cada n le asigna el número de coprimos menores que él.

Por lo tanto recupera m.

Supongamos que Bob quiere enviar a Alicia el mensaje: YES (es lo que hemos llamado M), Bob conoce (n, e) = (46927, 39423) dado por Alicia. Utiliza un protocolo reversible como puede ser, tomando un alfabeto de 26 letras (comenzando en 0 y sin ñ), se escribe el número 24418 (haciendo corresponder la Y con 24, la E con 4, la S con 19) en base 26, entonces $24418 = 24.26^2 + 4.\ 26 + 18 \equiv 16346 \pmod{46927}$, notemos que este valor de n es el dado por Alicia. Este número obtenido es el que hemos llamado m.

Ahora calcula $16346^{39423} \equiv 21166 \pmod{46927}$, ahora lo escribe en base 26,

$21166 = 1.26^3 + 5.\ 26^2 + 8.\ 26 + 2$ = BFIC (haciendo corresponder el 1 con B, el 5 con F, el 8 con I y el 2 con C), este es el mensaje c que recibe Alicia.

Al recibirlo Alicia escribe BFIC en base 26 y obtiene el 21166 y como conoce d, su llave, calcula $21166^{26767} \equiv 16346 \pmod{46927}$, lo escribe en base 26 y recupera YES.

Seguridad: La factorización de números grandes por lo general proponen métodos teniendo 663 bits de longitud usando métodos distribuidos avanzados. Las claves RSA son normalmente entre 1024-2048 bits de longitud. Algunos expertos creen que las claves de 1024 bits podrían comenzar a ser débiles en poco tiempo; con claves de 4096 bits podrían ser rotas en un futuro. Por lo tanto, si n es suficientemente grande el algoritmo RSA es seguro

Generación de claves: Buscando números primos grandes p y q por el test de aleatoriedad y realizando tests probabilísticos de primalidad los cuales eliminan virtualmente todos los no-primos (eficientemente).Los números p y q no deberían ser suficientemente cercanos para que la factorización de Fermat para n sea exitosa. Además, si cualquier p-1 o q-1 tiene sólo factores primos pequeños, n puede ser factorizado rápidamente, con lo que estos valores de p o q deben ser descartados.

**Ejercicio:** Cada grupo de trabajo elija una clave pública y reserve su clave secreta. Hagan una lista con las claves públicas de cada grupo, envíen un mensaje a todos los grupos y decodifiquen los mensajes que reciban de cada uno de ellos.

**Conclusión:** En este proyecto se intenta lograr un enfoque desestructurado de la clase de matemática, integrar conocimientos y dar una aplicación. Este último aspecto es de suma importancia como estímulo al estudio de distintos temas, que a veces pueden aparecer a los alumnos como vacíos de significado y con un interés meramente teórico.

**Referencias Bibliográficas**


- Alsina, Claudi. (2000). La Matemática de la Liberación. *La Matemática hermosa… y otras conferencias*. Pág. 17 y 18. Red Olímpica.
- Alsina, Claudi. (2000). Creatividad y musas matemáticas. *La Matemática hermosa… y otras conferencias*. Pág. 63, 70 y 75. Red Olímpica.
- Gentile, Enzo. (1976). Capítulo III. Anillo de enteros racionales. *Notas de Algebra*. Pág. 105 a 195. Eudeba.
- Sessa, Carmen. (2005). Formulación y validación de conjeturas sobre los números y las operaciones. *Iniciación al estudio didáctico del Algebra*. Pág. 109, 113, 114 y 115. Libros del Zorzal.
- Stewart, Ian. (2005). La importancia de ser primos. *De aquí al infinito. Las matemáticas de hoy*. Pag 24 a 31, Biblioteca de bolsillo.
- Zapico, Irene y Tajeyan, Silvia. (2008). *Curso Matemática en la Literatura.* Material del curso realizado a través de la plataforma del aula virtual de SOAREM.
- Zapico, Irene y otros. (2002). Acerca de la Integración de áreas. *Integración por áreas para el mejoramiento de la enseñanza de la Geometría.* UIDI, ISP "Dr. J. V. González.