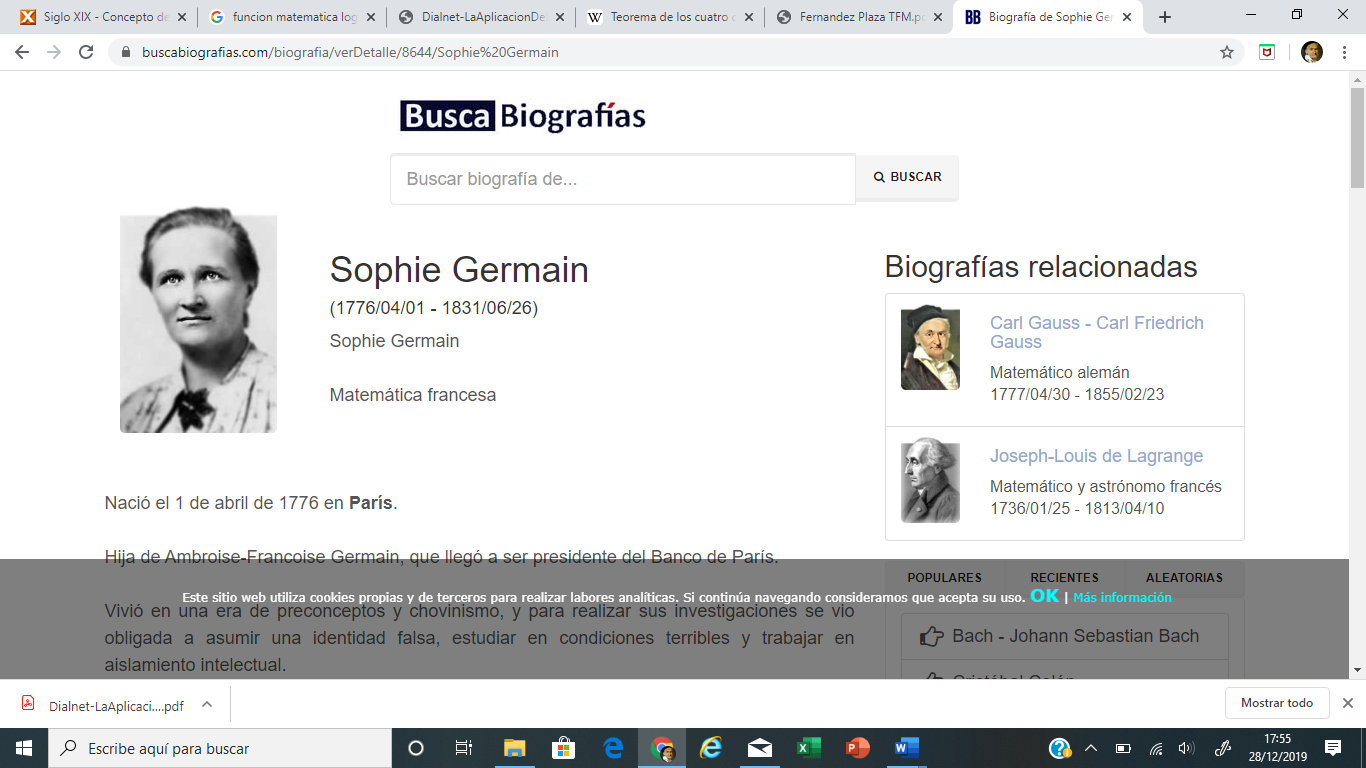
**INNOVACIÓN EDUCATIVA - SIGLO XIX**

# Números enteros, primos y congruencias

Antes de leer la biografía de Sophie Germain, conviene entender el contexto histórico de principios del siglo XIX, en este documento:

<https://www.conevyt.org.mx/colaboracion/colabora/objetivos/libros_pdf/sso2_u8lecc2.pdf>

**1.1 Introducción**: Durante la historia no debemos perder de vista la gran influencia que tenía la sociedad en el desarrollo de los diferentes descubrimientos. En la sociedad francesa del siglo XIX el acceso a la universidad no estaba permitido a mujeres, por eso es más impresionante la historia de Sophie Germain, una de los dos protagonistas de esta actividad, Sophie Germain, nacida en el seno de una familia burguesa francesa a finales del siglo XVIII, convencida de que su familia sólo pensaba en el dinero y la política, se refugió en la lectura comenzando con las obras de la biblioteca de su padre.

 Su interés por las matemáticas surgió después de leer la [Historia de las Matemáticas](http://gallica.bnf.fr/ark:/12148/bpt6k1076512) de [Jean-Baptiste Montucla](https://es.wikipedia.org/wiki/Jean-%C3%89tienne_Montucla). En particular le impresionó la leyenda de la muerte de [Arquímedes](https://es.wikipedia.org/wiki/Arqu%C3%ADmedes), por los soldados romanos, mientras él estaba absorto en un problema de geometría. Quedó tan conmovida por el fuerte efecto de la matemática, capaz de hacer olvidar la guerra, que decidió dedicarse a su estudio.

Leía todo lo que caía en sus manos con un ardor que preocupaba a su familia. Sus padres para que no pudiera estudiar a escondidas de noche, decidieron dejarla sin luz, sin calefacción y sin sus ropas. Sophie parecía dócil, pero sólo en las apariencias, de noche, mientras su familia dormía, se envolvía en mantas y estudiaba a la luz de una vela que previamente había ocultado. Un día la encontraron dormida sobre su escritorio, con la tinta congelada, delante de una hoja llena de cálculos. Su tenacidad venció la resistencia de sus padres que, aunque no comprendían su dedicación a las matemáticas terminaron por dejarla libre para estudiar. Comenzó por el [tratado de aritmética](http://gallica.bnf.fr/ark:/12148/bpt6k201342q/f2.table) de [Étienne Bezout](https://es.wikipedia.org/wiki/%C3%89tienne_B%C3%A9zout) y el de [cálculo diferencial](http://gallica.bnf.fr/ark:/12148/bpt6k5403309n) de [A. J. Cousin](https://fr.wikipedia.org/wiki/Jacques_Antoine_Joseph_Cousin) para seguir, después de aprender latín sin ninguna ayuda, con las obras de [Isaac Newton](https://es.wikipedia.org/wiki/Isaac_Newton) y [Leonhard Euler](https://es.wikipedia.org/wiki/Leonhard_Euler).

Como las mujeres no eran admitidas en la Escuela Politécnica (no admitió mujeres hasta 1792), consiguió hacerse con apuntes de algunos cursos, entre ellos, el de [Análisis](http://gallica.bnf.fr/ark:/12148/bpt6k86263h) de [Lagrange](https://es.wikipedia.org/wiki/Joseph-Louis_de_Lagrange). Al final del período lectivo los estudiantes podían presentar sus investigaciones a los profesores, Sophie presentó un trabajo firmándolo como Antoine-Auguste Le Blanc, un antiguo alumno de la escuela. El trabajo impresionó a Joseph Louis Lagrange por su originalidad y quiso conocer a su autor. Al saber su verdadera identidad, la felicitó personalmente y le predijo éxito como analista, animándola de esta forma a seguir estudiando (en España el acceso de la mujer en igualdad de condiciones a la universidad llego mucho más tarde, toda la información en este link. <http://www.rtve.es/noticias/dia-internacional-mujer/universidad/>).

En 1798, [Adrien-Marie Legendre](https://es.wikipedia.org/wiki/Adrien-Marie_Legendre) había publicado *[Essai sur la théorie des nombres](http://gallica.bnf.fr/ark:/12148/bpt6k62826k/f37" \t "_blank)* y en 1801, apareció el libro de [Karl Friedrich Gauss](https://es.wikipedia.org/wiki/Carl_Friedrich_Gauss) (1777-1855) *[Disquisitiones Arithmeticae](https://es.wikipedia.org/wiki/Disquisitiones_arithmeticae" \t "_blank)*. Sophie, impresionada por estas obras, se dedicó al estudio de la teoría de números. Entre 1804 y 1809 escribió a Gauss una decena de cartas mostrándole sus investigaciones. Temerosa del ridículo que en aquella época suponía una mujer erudita, las primeras cartas estaban firmadas con el seudónimo*Le Blanc.* Pero esta correspondencia fue irregular, Gauss estaba tan ocupado en su propia investigación que sólo le contestaba cuando el trabajo de Sophie estaba relacionado con sus propios teoremas.

Con motivo de la conquista de Prusia por Napoleón, en la [campaña de Jena](https://es.wikipedia.org/wiki/Guerras_Napole%C3%B3nicas#La_Cuarta_Coalici.C3.B3n) (1806), temió por la vida de Gauss y se puso en contacto con un militar amigo de su familia, el general Pernetti, para pedirle que velara por su seguridad. El militar le comunicó que había contactado con Gauss y que éste agradecía su mediación, pero que afirmaba no conocer a Sophie Germain. En la siguiente carta que le escribió tuvo que revelarle la verdad: ella era M. *Le Blanc*. Gauss sorprendido al conocer su identidad, elogia su talento y su genio. En la última carta que, en esta época, escribió a Gauss, le comentaba un resultado muy importante sobre teoría de números, el teorema que hoy lleva su nombre, pero él no respondió a esa carta.

El hecho de que Gauss ya no contestaba a sus cartas, propició que Sophie abandonara la teoría de números y comenzara sus investigaciones en física-matemática. Tuvo que presentar tres memorias sucesivas en 1811, 1813 y 1815 hasta conseguir, el 8 de enero de 1816, el *Prix Extraordinaire* de la Academia de Ciencias. Se reunió mucha gente para ver a la famosa mujer matemática, pero Sophie no asistió a la ceremonia de entrega. *Aunque años antes se había considerado una novata entre gigantes, en ese momento no sentía ninguna admiración por muchos de sus colegas.* [6]

A partir de entonces consiguió el respeto y el reconocimiento por parte de la comunidad científica, debido, sobre todo, a su amistad con [Jean-Baptiste Joseph Fourier](https://es.wikipedia.org/wiki/Jean-Baptiste_Joseph_Fourier) (1768-1830) que, después de ser elegido Secretario Permanente de la Academia de Ciencias, le permitió asistir a sesiones, siendo la primera mujer, no esposa de académico, que lo hizo. También continuó sus investigaciones con Legendre sobre teoría de números con el que trabajaba en un plano de igualdad, y reanudó la correspondencia con Gauss sobre este tema.

El 27 de junio de 1831 murió en París a consecuencia de un cáncer de pecho a los 55 años. A pesar de su extensa correspondencia, Gauss y Sophie nunca se conocieron personalmente. Gauss intentó que la [Universidad de Gotinga](https://es.wikipedia.org/wiki/Universidad_de_Gotinga) le otorgara el título de doctor *honoris causa;* pero a pesar de su gran influencia en esta universidad, su propuesta no tuvo éxito. No será éste un hecho para recordar a Sophie Germain, pero siempre la evocaremos por su obra, que perdurara siempre, y por su talento que fue excepcional, además de otras cualidades como su valor y su dedicación a la ciencia.

**Teoría de números – Sophie Germain**

En matemáticas lo que llamamos “**Teoría de números**” se refiere a la rama de matemáticas puras que estudia las operaciones y las propiedades de los números en general, y de los números enteros en particular. Para hablar de la parte de la obra de Sophie Germain, debemos recordar que un siglo antes **Pierre de Fermat** enunció el archiconocido “**Teorema de Fermat**”, que no es más que una generalización del teorema de Pitágoras, pero con exponentes mayores que dos y en el sentido contrario, esto es:

|  |  |
| --- | --- |
| **Teorema de Pitágoras para números naturales:** | **Teorema de Fermat** |
| Números naturales que cumplen que: | No existe ninguna terna de números naturales  , para |
| Son las conocidas ternas pitagóricas, como:  3, 4 y 5,  5, 12 y 13, etc, … | Al contrario que el teorema de Pitágoras, aquí se trata de demostrar que no hay. |

Este teorema fue conjeturado por Fermat en 1637, quitando a otro gran Matemático como Euler, que los probó para , ninguno de los grandes matemáticos de la época lo consiguió atacar.

Sophie Germain estableció el siguiente teorema:

Teorema de Sophie Germain: Si para p primo impar, existe un primo auxiliar tal que:

* No existen dos potencias de p modulo que difieran en 1
* No existe ningún número tal que p sea potencia de orden p [modulo](https://es.wikipedia.org/wiki/Aritm%C3%A9tica_modular) θ de él.

Entonces, cualquier solución del teorema de Fermat que se cumpla, deben ser divisibles por .

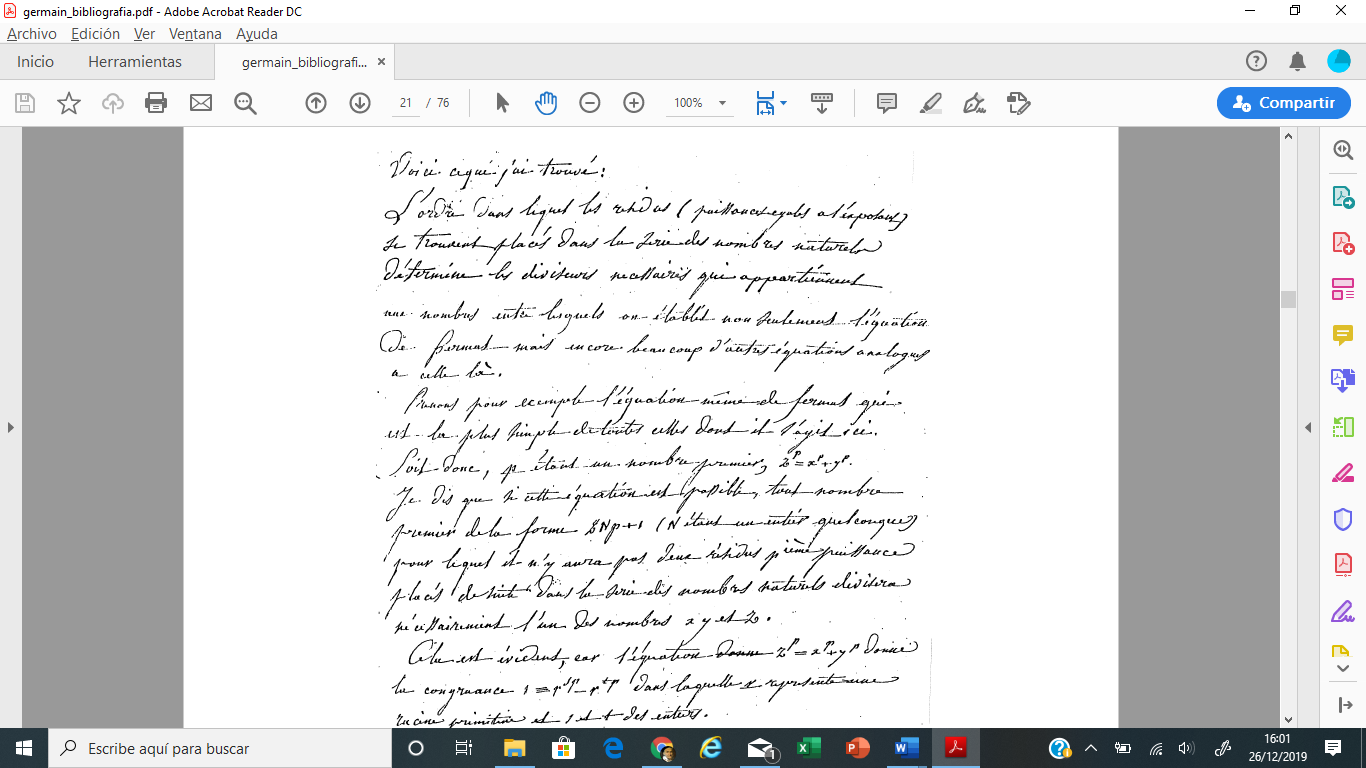
Esto fue un gran descubrimiento en su época, y tiene merito doble pensando en que Sophie era mujer y mucho conocimiento era difícilmente accesible para ella.

Por ejemplo: .

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Números(mod13) | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
| Cubo (mod13) | 1 | 8=8 | 27=1 | 64=12 | 125=8 | 216=8 | 343=5 | 512 | 729 | 1000 | 1331 | 1728 |
|  | 1 | 8 | 1 | 12 | 8 | 8 | 5 | 5 | 1 | 12 | 5 | 12 |

La primera condición se cumple porque los únicos cubos (mod13) son 1, 5, 8 y 12, que no son números consecutivos

La segunda condición se cumple porque ningún cubo es congruente con 3(mod13)

Entonces, por el teorema anterior, uno de ellos debe ser divisor de 9.

A continuación, vemos una carta de Sophie Germain a Gauss hablando de como está enfocando este problema de difícil resolución. Vayamos ahora a que es todo esto que arriba se llama congruencias, módulo residuos, y aquí enlazamos con el que ha sido quizás el más grande matemático de toda la historia, Gauss, y que quizás siguiera haciendo grandes descubrimientos porque Sophie Germain consiguió cierta protección para el en la invasión de Francia sobre Alemania.

Gauss fue un matemático muy prolífico, pero no era muy proclive a publicar, de toda su obra nos vamos a centrar en una obra que publico tan solo dos años después de publicar su tesis, aquí tenemos un resumen de todas sus contribuciones al mundo científico.

<https://fme.upc.edu/ca/arxius/butlleti-digital/gauss/060208_conferencia_mariano_santander.pdf>

**“El álgebra de las congruencias”** que es lo que utilizó Sophie Germain para demostrar parte de su teorema y muchos otros más. El libro en cuestión fue llamado “Disquisitiones Arithmeticae”.

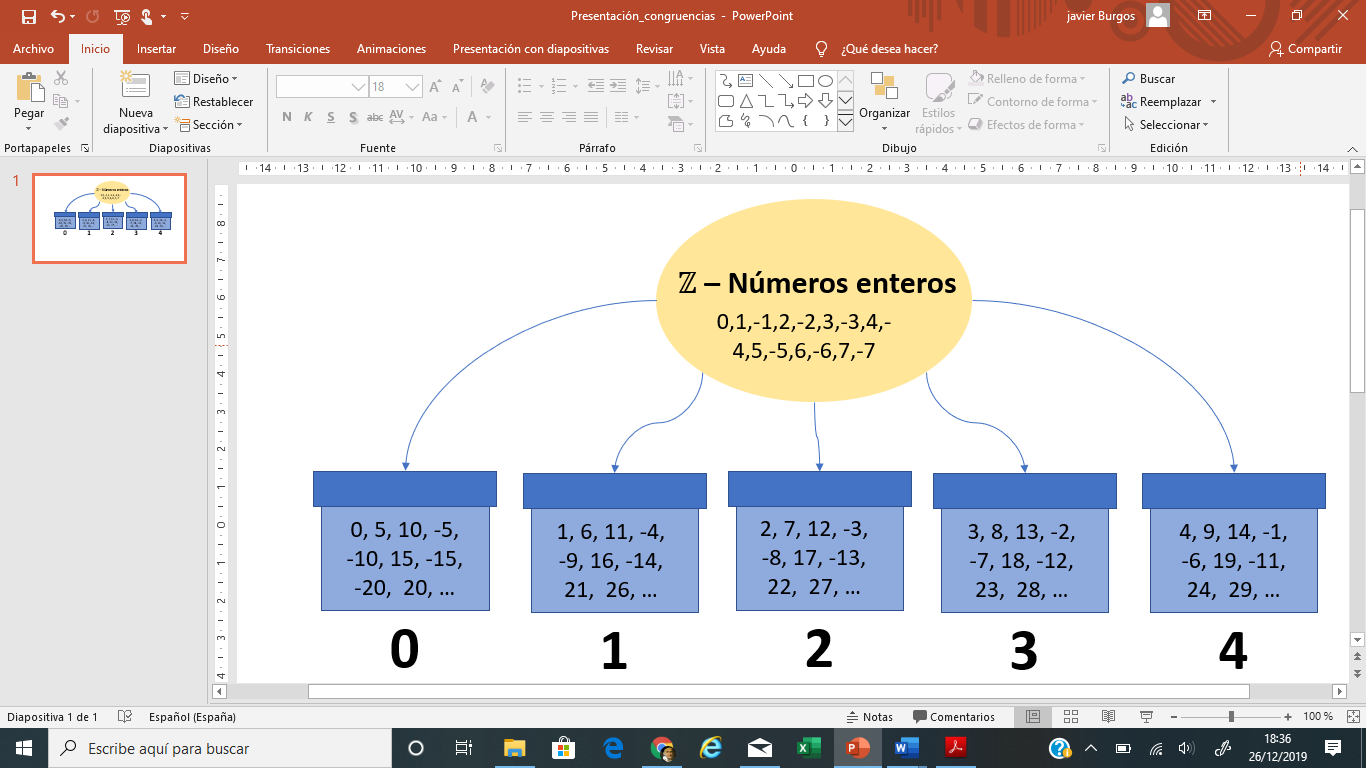
Antes de la publicación de esta obra, la teoría de números era esencialmente una colección de teoremas y conjeturas aislados unos de otros. Gauss reunió el trabajo de sus predecesores con su propio trabajo y lo compiló en un marco común, rellenó huecos, corrigió demostraciones faltas de rigor y extendió el tema del estudio de numerosas formas.

La estructura lógica de las Disquisitiones (enunciado de un [teorema](https://es.wikipedia.org/wiki/Teorema) seguido por su [demostración](https://es.wikipedia.org/wiki/Demostraci%C3%B3n_matem%C3%A1tica) y a su vez por [corolarios](https://es.wikipedia.org/wiki/Corolario)) estableció un formato estándar para textos posteriores. Aun reconociendo la importancia fundamental de las demostraciones lógicas, Gauss también ilustra muchos teoremas con ejemplos numéricos.

Las Disquisitiones fueron el punto de partida para el trabajo de otros matemáticos europeos del siglo XIX tales como [Kummer](https://es.wikipedia.org/wiki/Ernst_Kummer), [Dirichlet](https://es.wikipedia.org/wiki/Dirichlet) y [Dedekind](https://es.wikipedia.org/wiki/Richard_Dedekind). Muchas de las anotaciones de Gauss son efectivamente anuncios de futuras investigaciones suyas, algunas de las cuales permanecieron sin publicar. Debieron resultar particularmente crípticas a ojos de sus contemporáneos, aunque actualmente se pueden entender como el inicio de las teorías de [funciones L](https://es.wikipedia.org/wiki/Funci%C3%B3n_L) y [multiplicación compleja](https://es.wikipedia.org/wiki/Multiplicaci%C3%B3n_compleja), en particular.

Veamos ahora que es eso de lo que hablaba Sophie Germain en su teorema, que significa congruente o residuo. Primero tenemos que fijar un número antes de hablar de ello, por ejemplo para entenderlo, fijemos el número 5 (es muy diferente si este número es primo o no). Al dividir cualquier número entero entre 5, nos podemos encontrar 5 posibles restos, 0, 1, 2, 3, 4, …..

Vamos a identificar todos los números enteros con los restos al dividirlos por 5, de tal forma que diremos que dos números son congruentes módulo 5 si tienen el mismo resto al dividirlos por 5, así, podemos ver los infinitos números enteros agrupados en 5 cajas:

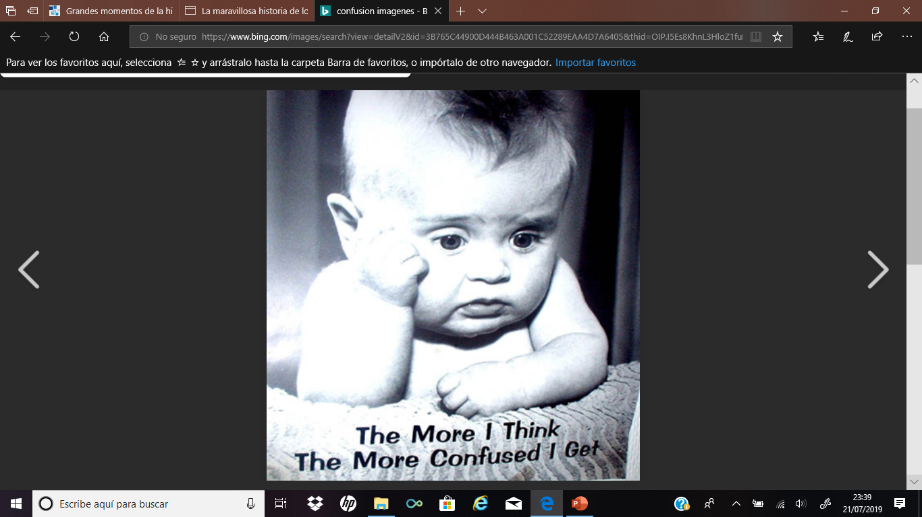


Cualquier número de cada caja diremos que es congruente módulo 5, así, 0, 5 y 10 son congruentes con 0 módulo 5, 6 y -14 son congruentes con 1 módulo 5 y lo escribiremos

Ahora tenemos todos los números enteros divididos en 4 cajas y podemos sumar, restar y multiplicar números entre esas cajas que siempre iremos a un número que está en una de las otras cajas, por ejemplo:

Si sumamos un elemento de la caja del 2 y de la caja del 3, nos resulta siempre un elemento de la caja del 0, por ejemplo:

De la misma forma, si multiplicamos un elemento de la caja del 2 y uno de la del 3, nos dará siempre un elemento de lo que llamamos caja del 1, por ejemplo:

Así, pues como no nos cambia nada, podemos utilizar los 5 números de arriba para hacer las operaciones que nada cambiará y nunca cambiaremos de caja, y de aquí en adelante en vez de decir el número de la caja, hablaremos de los identificadores de las cajas, y habremos entrado en un nuevo mundo para hacer operaciones, en el que se cumplen estas operaciones:

Este tipo de operaciones que a priori no tienen nada que ver con las operaciones que estamos acostumbrados a utilizar permiten demostraciones de lo más variadas a diferentes teoremas matemáticos de la historia.

Pero no nos olvidemos que no hemos hablado de la división, en este mundo que solo hay 5 números parece complicado dividir, porque nos debería dar un número de esos 5, lo cual lo complica todo mucho. Así, utilizaremos la definición de división que dio Euclides, más de 20 siglos atrás:

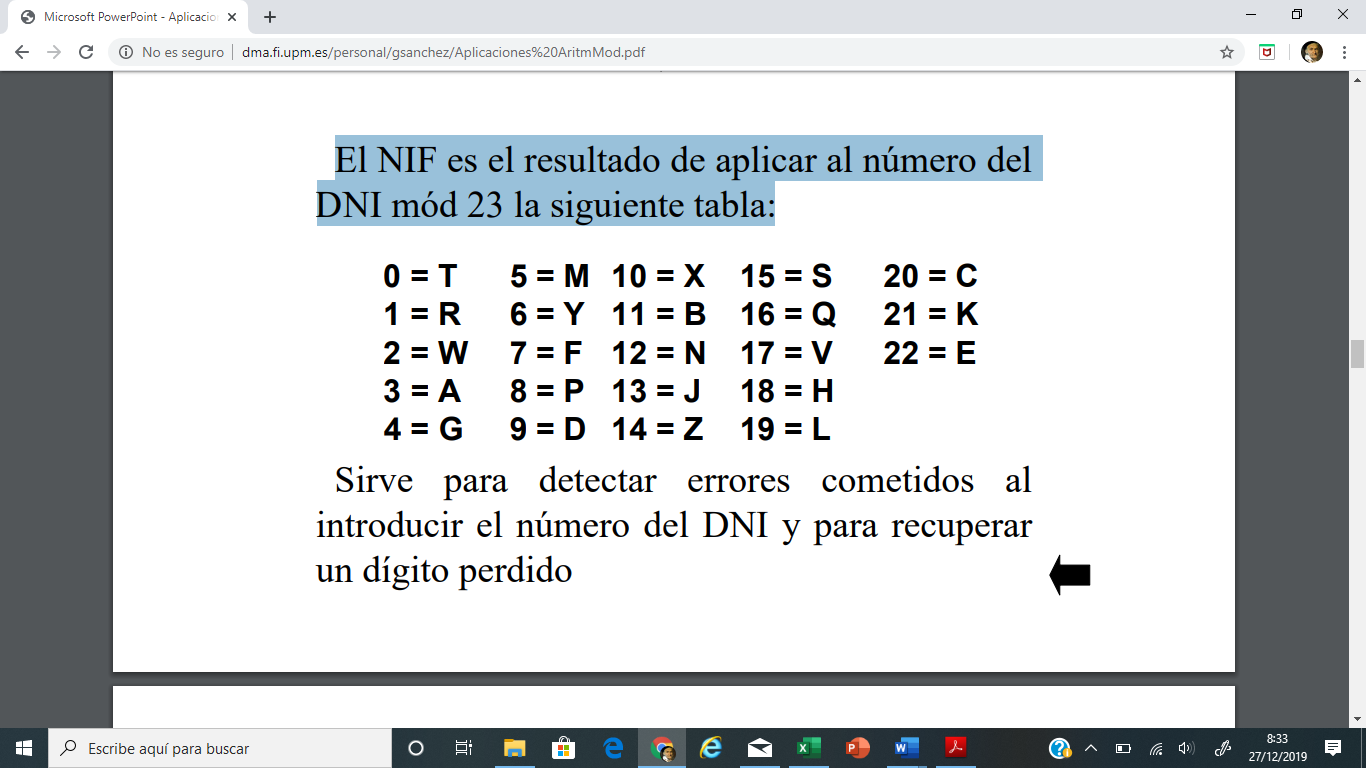
, si queremos que la división sea exacta, entonces así será aquel número x si:

, así pues:

Como observamos, todas las operaciones cambian en este mundo numérico en el que hay muy pocos números, solo 5 en el caso anterior.

Veamos a continuación algunas de las aplicaciones que tienen estos nuevos números:

* **Calculo de la letra del DNI:** La letra se calcula como el resultado de aplicar al número del DNI (mod 23) la siguiente tabla:



Sirve para detectar errores cometidos al introducir el número del DNI y para recuperar un dígito perdido

La elección del 23 no es aleatoria, pues recordemos que 23 es el número primo más grande menor que 28 (número de letras del abecedario), así que por posibles utilizaciones del futuro decidieron utilizar un número primo que tiene multitud de propiedades más que si no lo fuera.

* **ISBN de un libro**: El ISBN es un número de 10 cifras que identifica cualquier libro editado en el mundo Las dos primeras cifras corresponden al **país.** Las cuatro siguientes a la **editorial**. Las tres siguientes al **identificador del libro** dentro de la editorial. La décima se obtiene (X si se trata de 10). También sirve para detectar errores cometidos al introducir el número o para recuperar un dígito perdido en la transmisión.
* **Calcular restos en divisiones de potencias de números muy grandes sin necesidad de utilizar la calculadora, por ejemplo**: . Este es un número que tendrá más de 1000 cifras con lo cual la calculadora no es capaz de hacer esa operación, por supuesto, para nosotros sería una labor odiosa ponernos a calcular este tipo de operaciones. Como lo resolvemos entonces, pues muy sencillo, utilizando este nuevo tipo de números viendo como se comportan las potencias modulo 7 y las propiedades de las potencias.

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |  |  |
| 1(mod7) | 2(mod7) | 4(mod7) | 1(mod7) | 2(mod7) | 4(mod7) | 1(mod7) | 2(mod7) | 4(mod7) |

Vemos que se van repitiendo cada 3 veces, así, si divido 3541 entre 3 resulta que:

 Así, por tanto, **el resto de esa división es dos** y no hemos tenido que calcular el número de 1000 cifras ni hacer la división.

* **¿De dónde vienen los criterios de divisibilidad de los números más básicos que se aprenden en primaria?,** el del 2, del 3, del 5, del 9, del 11?. Por ejemplo, hablemos del criterio del 9.

La tabla que hemos hecho anteriormente se llaman restos potenciales de 2 módulo 7. Para cualquier número ver si es divisible por 9, parece claro que deberíamos utilizar congruencias módulo 9, pero sobre que, es aquí cuando nos acordamos de la descomposición polinómica de un número, así, por ejemplo, el número:

Pero que ganamos con esto, construyamos la misma tabla que en el ejercicio anterior:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  |  |  |  |  |  |  |
| 1(mod9) | 1(mod9) | 1(mod9) | 1(mod9) | 1(mod9) | 1(mod9) | 1(mod9) |

Si desarrollamos el número y tomamos congruencias módulo 9:

Así pues, la suma de las cifras de un número si las divido por 9, me da el mismo resto que si divido el número por 9, por lo tanto, para que sea divisible por 9, bastará conque la suma de sus cifras sea divisible por 9.

**ACTIVIDADES A REALIZAR:**

* **Preparar una exposición de 15 minutos para hacerla en clase que hable de:**
  + Contexto histórico y geográfico en Europa al inicio del siglo XIX.
  + Vida de Sophie Germain
    - Breve resumen de su vida.
  + Acceso de las mujeres en la universidad en España
  + ¿Qué es el teorema de Fermat?
  + ¿Quién fue Gauss?, ¿A qué se dedicó?
  + ¿Qué es el algebra de congruencias?
  + Cálculo de la cifra del DNI
  + Criterio de divisibilidad del 11 (no del 9)
  + Calcula la suma de las cifras de la suma de las cifras de la suma de las cifras de
  + Que es el teorema de los cuatro cuadrados <https://es.wikipedia.org/wiki/Teorema_de_los_cuatro_cuadrados>
  + Dudas y preguntas
* **Preparar un documento resumen de la exposición entregable.**

**En la exposición se valorará:**

* Será necesario que expongan todos los miembros del grupo
* La exposición en clase es totalmente libre y los recursos a utilizar son totalmente libres.
* Claridad en la exposición
* Científico y riguroso
* Original e impactante, ameno y entretenido (puede incluir atrezo y decorado)
* Improvisación