Introducción al curso

Alan Reyes-Figueroa

Teoría de Números

(Aula 01) 05.julio.2022

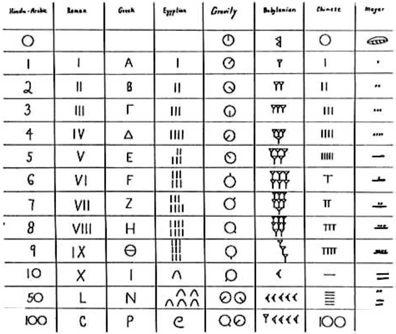
Motivación

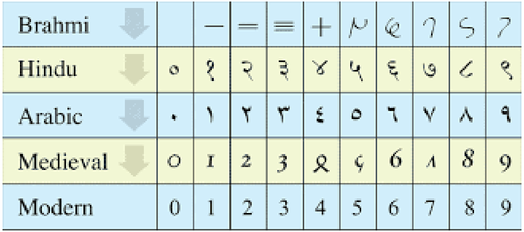
La teoría de números es el estudio de los número naturales $\mathbb{N}$ y sus propiedades, y por extensión de los números enteros $\mathbb{Z}$ o los racionales $\mathbb{Q}$. Es una de las ramas más antiguas de la matemática.

En este curso haremos un desarrollo de la teoría de números “clásica”, y haremos una breve introducción a la teoría algebraicas de números, y a la teoría analítica de números. Conviene conocer muy bien

- fundamentos (inducción, relaciones de orden y equivalencia)
- técnicas discretas (combinaciones, permutaciones, recurrencias)
- álgebra lineal,
- cálculo, un poco de análisis real,
- elementos de grupos y de anillos,
- programación.

Números y más. Culturas como Sumeria, los babilonios, los egipcios, las civilizaciones del Valle del Indus, China, las culturas en Mesoamérica, entre otros, seguramente fueron los primeros en desarrollar un estudio de los números (naturales).



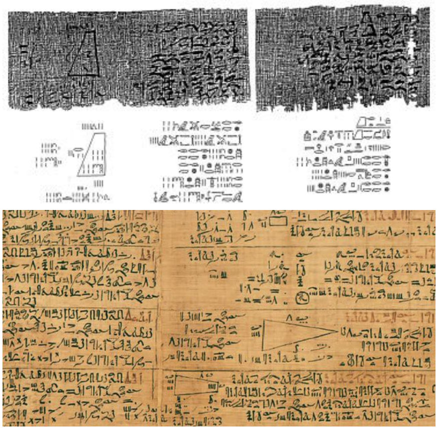


UVG UNIVERSIDAD DEL VALLE DE GUATEMALA

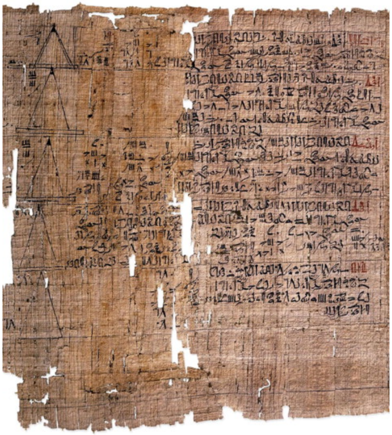
Un poco de historia

(Arriba): Tablillas cerámicas. (Abajo): Tabla Plimpton 322.

Un poco de historia

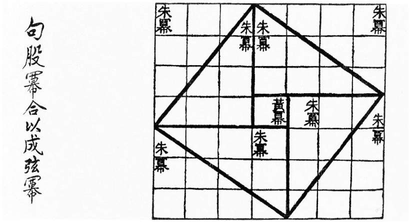


(Arriba): Papiro de Moscú. (Abajo): Detalle del Papiro de Rhynd.

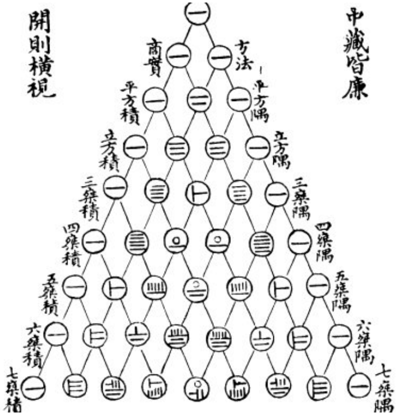


Papiro de Rhynd.

Un poco de historia

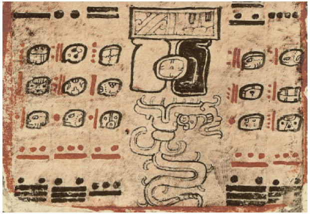


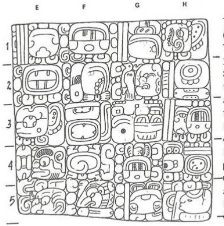
Zhoubi Suanjing es uno de los más antiguos escritos chinos sobre matemáticas. “Zhou” se refiere a la dinastía Zhou (*circa* 1050-250 B.C.



Jia Xian, siglo XI a.D.

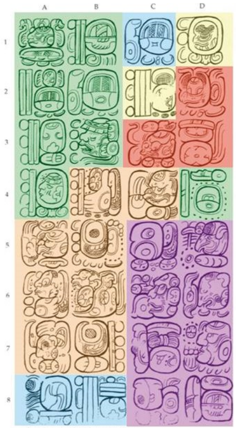
Un poco de historia





The Initial Series on Yaxchilan Lintel 29 (not shown) records the birth date of Yaxun Bahlam IV on 9.13.17.12.10 8 Ok 13 Yax. Lintel 30 records the associated 819 (2.4.19) Day Station beginning with the Distance Number 17 K'ins, 1 Winal, and 1 Tun at E1-F1 that counts backward from 9.13.17.12.10 to 1 Ben 1 Ch'en (E2-F2), (9.13.16.10.13). The standard components of the event are present at E3-F5, including the proto-Cholan positional verb root, *wa'*, 'standing upright' at E3. The direction *elk'in*, 'east' and the color *chak*, 'red' appear at F3 and E4a. *K'awiil* appears at E5. (Drawing by Graham, 1976).

(Arriba): Detalle Códice Dresden. (Abajo): Yaxchilán Lintel 30.



Cuenta Larga: 12.10.1.13.2 9 *Ik'* 5 te' *Mol*

Serie sumplementaria

Número de distancia entre la Cuenta Larga y la fecha de 819 dias: 1.16.17

Fecha del calendario de 819 dias: 12.9.19.14.5 1 *Chikchan* 17 *Ch'en*

Frase verbal asociada al calendario de 819 dias

Frase verbal asociada a la fecha de la Cuenta Larga de la inscripción

UNIVERSIDAD DEL VALLE DE GUATEMALA

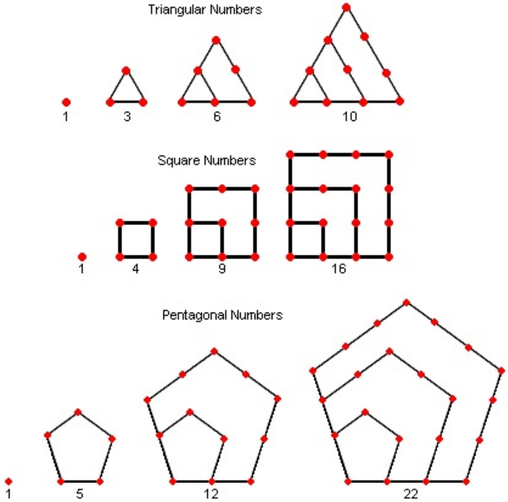
Un poco de historia

Teoría de números en Grecia. Los griegos, a distinción de las otras culturas, fueron los primeros en innovar y explicar el comportameinto del mundo.
A ellos debemos

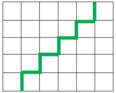
- El esquema deductivo, usado hoy en matemática.
- El método axiomático.
- Las primeras obras documentadas/organizadas sobre matemática.

- La aritmética y la geometría estaban ligadas.
- Los griegos eran místicos. Gustaban de números con propiedades especiales.
- Simpleza, relaciones simples entre cantidades.

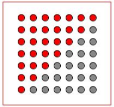
Un poco de historia



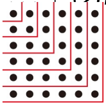
$$1 + 2 + 3 + \ldots + n = \frac{n(n+1)}{2}.$$



$$\frac{(n-1)n}{2} + \frac{n(n+1)}{2} = n^2.$$



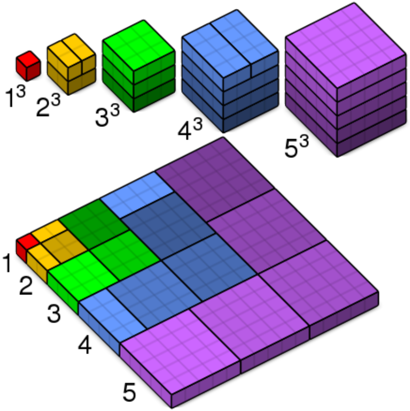
$$1 + 3 + 5 + \ldots + (2n-1) = n^2.$$



Un poco de historia

O propiedades como el Teorema de NICÓMANO (*circa* 100 a.D.)

$$1^3 + 2^3 + 3^3 + \ldots + n^3 = (1 + 2 + 3 + \ldots + n)^2 = \left(\frac{n(n+1)}{2}\right)^2.$$



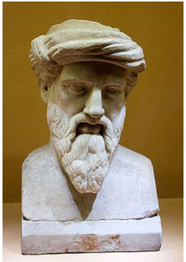
UVG UNIVERSIDAD DEL VALLE DE GUATEMALA

Un poco de historia

La Escuela Pitagórica.

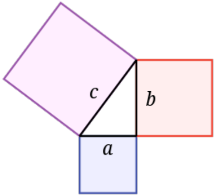
Pitágoras de Samos (*circa* 600 B.C.). Considerado el primer matemático. Fue estudiante de Tales de Mileto, y de Anaximandro. Contribuyó de manera significativa en el avance de la matemática helénica, la geometría y la aritmética, derivadas particularmente de las relaciones numéricas, y aplicadas por ejemplo a la teoría de pesos y medidas, a la teoría de la música o a la astronomía.

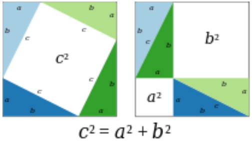
Viajó a oriente, donde se instruye en ritos sagrados, los cultos mistéricos, así como las matemáticas cultivadas por los egipcios, babilonios, caldeos.

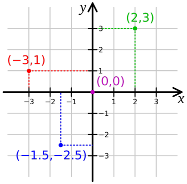


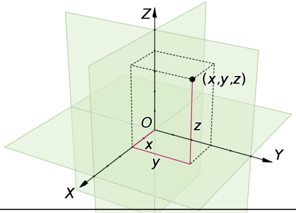
Un poco de historia

Hoy es conocido por el Teorema de Pitágoras. Descubierto y re-descubierto muchas veces y muchos años antes por otros en Asia.



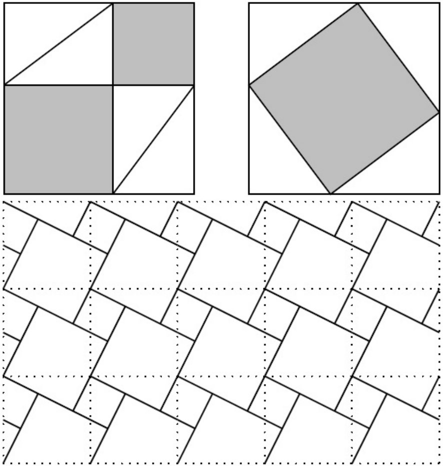




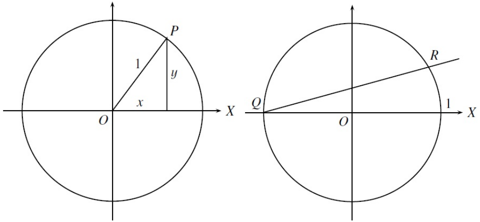


UVG UNIVERSIDAD DEL VALLE DE GUATEMALA

Un poco de historia



Ternas pitagóricas: $(a, b, c) \in \mathbb{N}^3$ con $a^2 + b^2 = c^2$. Parametrizaciones



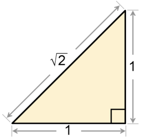
Hallar ternas pitagórica equivale a hallar puntos racionales sobre el círculo:

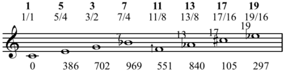
$$\left(\frac{a}{c}\right)^2 + \left(\frac{b}{c}\right)^2 = 1.$$

La Escuela Pitagórica. Movimiento filosófico-religioso siglo VI B.C. Formada por astrólogos, músicos, matemáticos y filósofos, cuya creencia más destacada era que el mundo era explicable en números.

- Contribuciones a la medicina, astronomía, música, ...
- Explicar el mundo en proporciones "divinas": proporciones racionales simples $\frac{a}{b}$.
- HÍPASO de Metaponto: descubre números irracionales.
- Ternas pitagóricas: (a, b, c) soluciones de $a^2 + b^2 = c^2$.

HÍPASO





UVG UNIVERSIDAD DEL VALLE DE GUATEMALA

Un poco de historia

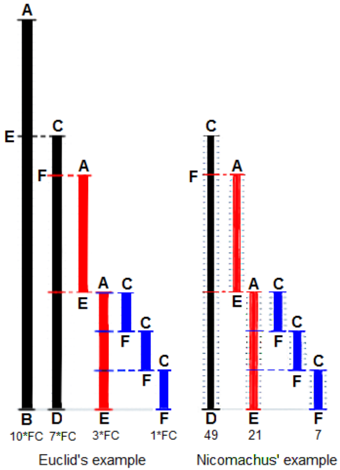
EUCLIDES (*circa* Siglo IV B.C.) Los Elementos, libros VI a IX. Dedicados a la aritmética.

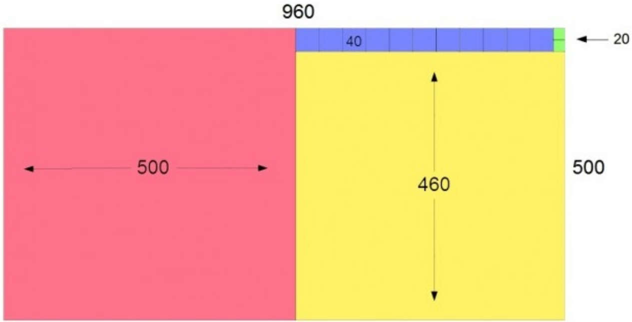
- Números primos.
- Libro IX, Proposición 20: "Los números primos son más que cualquier multitud asignada de números primos".
  En lenguaje moderno: El conjunto de números primos es infinito.
- Números perfectos: n es perfecto si sus divisores $< n$ suman n.
- Libro IX, Proposición 36: Si $M = 1 + 2 + 4 + \ldots + 2^{n-1}$ es primo, entonces $M\,2^{n-1}$ es perfecto.

Un poco de historia

- Relación entre la aritmética y la geometría.
- El algoritmo de Euclides: forma eficiente de hallar el máximo divisor común de dos números *a* y *b*.
  En lenguaje moderno: El conjunto de números primos es infinito.
- Números perfectos.
- Libro IX, Proposición 36: Si $M = 1 + 2 + 4 + 8 + \ldots + 2^{n-1}$ es primo, entonces $M\,2^{n-1}$ es perfecto.

Un poco de historia





Varias formas de visualizar el algoritmo de Euclides.

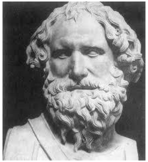
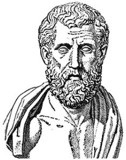
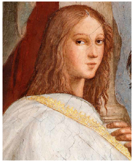
UVG UNIVERSIDAD DEL VALLE DE GUATEMALA

Un poco de historia

Nueva generación de matemáticos griegos:

- Apolonio de Perga. (*circa* 200 b.C.) Cónicas.
- Ptolomeo (*circa* 150 a.D.) el *Almagesto*.
- Diofanto de Alejandría (*circa* 300 a.D.).
- Pappus de Alejandría (*circa* 250 a.D.). Trabajos en geometría.
- Teón de Alejandría (*circa* 360-370 a.D.). Comentarios a varias obras.
- Hypathia de Alejandría (*circa* 400 a.D.). Trabaja más en temas como cónicas, astronomía, geometría y óptica. Comentarios a la *Arithmetica* de Diofanto.



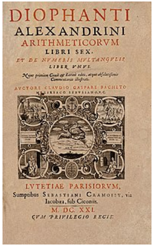
DIOFANTO de Alejandría (*circa* siglo III b.C.) .

- Publica la *Arithmeticorvm*, un tratado de 13 libros de los cuales sólo se conocen 6.
- Epitafio en forma de problema. Transeúnte, esta es la tumba de Diofanto: los números pueden mostrar, ¡oh maravilla! la duración de su vida. Su niñez ocupó la sexta parte de su vida; después, durante la doceava parte, de vello se cubrieron sus mejillas. Pasó aún una séptima parte de su vida antes de tomar esposa y, cinco años después, tuvo un precioso niño que, una vez alcanzada la mitad de la edad de la vida de su padre, pereció de una muerte desgraciada. Su padre tuvo que sobrevivirle, llorándole, durante cuatro años. De todo esto se deduce su edad.

$$\frac{x}{6} + \frac{x}{12} + \frac{x}{7} + 5 + \frac{x}{2} + 4 = x.$$

- Ecuaciones diofantinas: ecuaciones con soluciones enteras o racionales.

DIOFANTO



DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX.
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.

LVTETIAE PARISIORVM,
M. DC. XXI.
CVM PRIVILEGIO REGIS.

UNIVERSIDAD DEL VALLE DE GUATEMALA

Un poco de historia

Entre las ecuaciones diofánticas más populares de esa época estaban:

- $ax + by = c$, con $a, b, c \in \mathbb{Z}$.
- $a^2 + b^2 = c^2$.

<u>Ecuación de Pell</u>: (Pell siglo XVII a.D.). Diofanto estudió las ecuaciones de la forma

$$x^2 - Ny^2 = 1, \quad \text{con } N \text{ entero no cuadrado.}$$

Relación con aproximación de números. Por ejemplo, las soluciones racionales de la ecuación $x^2 - 2y^2 = 0$, corresponden a soluciones racionales de $\frac{x^2}{y^2} = 2$, o equivalentemente $\frac{x}{y} = \sqrt{2}$.

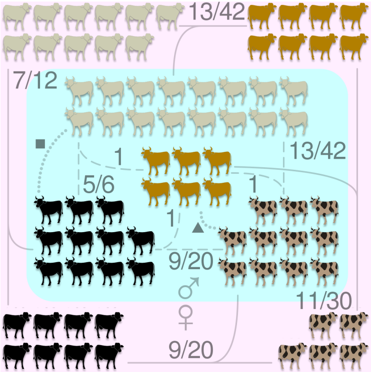
Las soluciones de la ecuación $x^2 - 2y^2 = 1$, corresponden a aproximaciones racionales de $\sqrt{2}$: $(3, 2)$, $(17, 12)$, $(99, 70)$, ...

$$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{\ddots}}}}$$

$$\frac{3}{2} = 1.5, \quad \frac{17}{12} \approx 1.41666, \quad \frac{99}{70} \approx 1.414285, \ldots \to \sqrt{2} \approx 1.414213562373$$

Un poco de historia

ARQUÍMEDES (*circa* 250 B.C.) Problema del ganado (*cattle problem*). Relacionado con las soluciones de la ecuación de Pell $u^2 - 6,097,766\, v^2 = 1$.



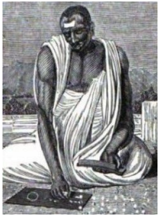
UVG UNIVERSIDAD DEL VALLE DE GUATEMALA

Un poco de historia

Teoría de números en Asia: Posterior a los griegos, el desarrollo de la matemática en general se mueve a Asia (Persia, Arabia, China, India).

- Desarrollo del álgebra.
- Sistemas de numeración decimal.

En la teoría de números tenemos los trabajos de BRAHMAGUPTA (*circa* 600 a.D.) y de BHÂSKARA (*circa* siglo XII a.D.).



Un poco de historia

Brahmagupta

- India redescubre la ecuación de Pell.
- BRAHMAGUPTA hace avances en la solución de la eq. de Pell.
- Compone soluciones de dos ecuaciones de Pell

$$x^2 - Ny^2 = k_1 \quad \text{y} \quad x^2 - Ny^2 = k_2$$

  para producir soluciones de $x^2 - Ny^2 = k_1 k_2$.

Bhâskara:

- Bhâskara extiende el método de Brahmagupta.
- Produce soluciones para todas las ecuaciones de la forma $x^2 - Ny^2 = 1$, para cualquier $N \geq 1$ no cuadrado.
- Ilustra el caso $N = 61$, cuya menor solución es extremadamente grande.

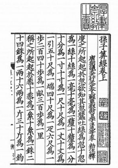
Un poco de historia

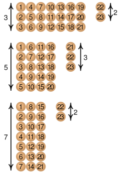
China: Dinastía HAN (*circa* 200 b.C. y 200 a.D.).

- Uso del algoritmo de Euclides para simplificar fracciones con el m.d.c.
- Solución de ecuaciones de la forma $ax - by = c$, por ejemplo $1461x = 118y - 4$
- Conocimiento de ternas pitagóricas.
- Congruencias, por ejemplo, $1461 \equiv -4 \pmod{118}$.

SUN TZI SUANJING ó SUN TZU SUAN CHING (*circa* 400-600 a.D.)

- Publica tratado “Matemáticas clásicas del Maestro Sun”. Compendio de matemática. Uno de los 10 *cánones computacionales* de la dinastía TANG.
- Teorema Chino del residuo.





Un poco de historia

- Âryabhat ó Âryabhat I publica la *Âryabhatîya* en 499.
- Qin Jiushao publica *Mathematical Treatise* en 1247.

Europa en la edad media: Oscuridad total.

- Leonardo de Pisa alias Fibonacci (*circa* 1200 a.D.) Estudio de secuencias numéricas. Publica el *Liber abaci* en 1202.
- Levi ben Gershon o Gersónides (*circa* siglo XIV). Encuentra fórmulas para el número de combinaciones y permutaciones. Pruebas rudimentarias por inducción. Triángulo de Pascal.

Un poco de historia

- Levi Ben Gershon da expresiones para $\binom{n}{k} = \frac{n!}{k!(n-k)!}$. Propiedades del tipo $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.
- Cerca de establecer la inducción matemática, si no de inventarla. Para mostrar $P(n), \forall n$ se demuestra $P(1)$, y para n arbitrario, se prueba $P(n) \Rightarrow P(n+1)$.
- Blaise Pascal (1623-1662) publica su *Traité du triangle arithmétique* en 1654. Establece que $(a+b)^n$ es una función generadora del número de combinaciones.

$$
\begin{array}{c}
1 \\
1 \quad 1 \\
1 \quad 2 \quad 1 \\
1 \quad 3 \quad 3 \quad 1 \\
1 \quad 4 \quad 6 \quad 4 \quad 1 \\
1 \quad 5 \quad 10 \quad 10 \quad 5 \quad 1 \\
1 \quad 6 \quad 15 \quad 20 \quad 15 \quad 6 \quad 1 \\
1 \quad 7 \quad 21 \quad 35 \quad 35 \quad 21 \quad 7 \quad 1
\end{array}
$$

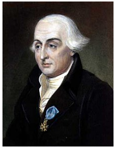
$$
\begin{array}{c}
a + b \\
a^2 + 2ab + b^2 \\
a^3 + 3a^2b + 3ab^2 + b^3 \\
a^4 + 4a^3b + 6a^2b^2 + 4ab^3 + b^4 \\
a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5 \\
a^6 + 6a^5b + 15a^4b^2 + 20a^3b^3 + 15a^2b^4 + 6ab^5 + b^6 \\
a^7 + 7a^6b + 21a^5b^2 + 35a^4b^3 + 35a^3b^4 + 21a^2b^5 + 7ab^6 + b^7
\end{array}
$$

Un poco de historia

<u>Renacimiento de la teoría de números</u>: Siglos XVII a XIX, donde la teoría de los números toma su lugar, tal como la conocemos hoy.

- Pierre de Fermat (1601-1655)
- Blaise Pascal (1623-1662)
- Leonhard Euler (1707-1783)
- J. L. Lagrange (1736-1813)
- A. M. Legendre (1752-1833)
- Karl F. Gauss (1777-1855)





Un poco de historia

- FERMAT. Abogado. No publicó muchos de sus trabajos.
- Co-fundador de la geometría analítica.
- Interés en curvas, geometría, óptica. Se interesa por las obras de Diofanto.
- Un primo p de la forma $4m+1$ es suma de dos cuadrados. Un primo de la forma $4m+3$ no.
- Pequeño teorema de Fermat $n^{p-1} \equiv 1 \pmod{p}$.
- Teorema del binomio, Teorema del multinomio.
- Famoso por el "último" teorema de Fermat: no hay soluciones no-triviales para $a^n + b^n = c^n$, $n > 2$.
- Trabajos en curvas cúbicas. Su trabajo da inicio a las funciones elípticas, y a lo que hoy conocemos como puntos racionales sobre curvas, y curvas elípticas.

Un poco de historia

- EULER. Se interesa en la teoría de números a partir de los trabjos de Fermat.
- Interes en primos. Primos de Mersenne ($2^n - 1$), primos de Fermat ($2^{2^n} + 1$). Primos de Goldbach.
- Suma de los inversos de los primos:

$$\prod_p \left(1 - \tfrac{1}{p}\right)^{-1} = \sum_p \tfrac{1}{p}.$$

- Función totiente $\varphi(n)$ que cuenta el número de primos relativos a n.
- Números perfectos.
- Conjetura la ley de reciprocidad cuadrática.
- Último teorema de Fermat para el caso $n = 3$.

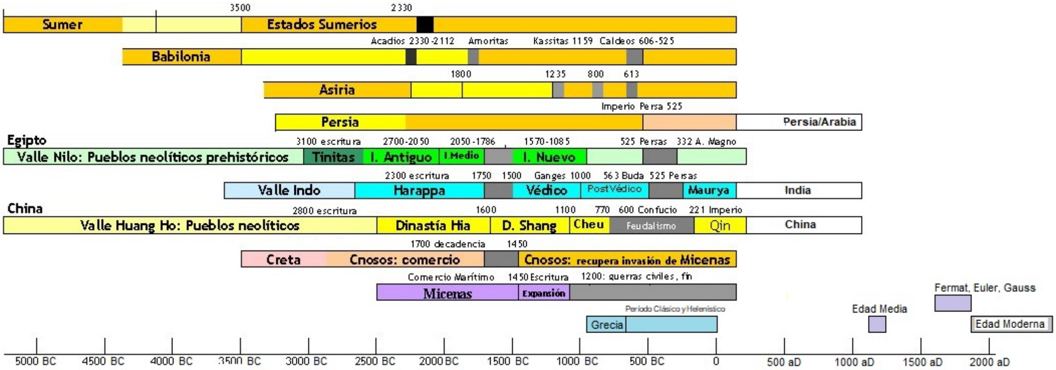
Un poco de historia

- LAGRANGE. Fracciones continuas.
- Extiende los trabajos de Fermat en congruencias.
- Sumas de 4 cuadrados $n = a^2 + b^2 + c^2 + d^2$.

- LEGENDRE Demostración del último teorema de Fermat para el caso $n = 5$
- Ley de reciprocidad cuadrática, símbolo de Legendre.
- Pionero en la distribución de números primos. Aplica análisis a la teoría de números. Conjetura en 1798 el teorema de los números primos.

- GAUSS Congruencias con notación algebraica. Reciprocidad cuadrática. Distribución de primos.
- Último teorema de Fermat para $n = 4$. Enteros gaussianos.

Un poco de historia



Línea de tiempo de las principales contribuciones en teoría de números. (Ver al final del libro de Burton, otra línea de tiempo más detallada.)

Teorema (Principio de buen orden)

Cada conjunto no vacío S de enteros no negativos contiene un elemento mínimo; es decir, hay un entero a en S tal que $a < b$, para todo $b \in S$. $\square$

Teorema (Propiedad Arquimedeana)

Si a y b son números enteros positivos, entonces existe un entero positivo n tal que $na \geq b$.

Prueba: Suponga que el enunciado del teorema no es verdadero, de modo que para algunos a y b, $na < b$ para todo entero positivo n.

Entonces el conjunto

$$S = \{b - na : n \text{ es un entero positivo}\}$$

consta enteramente de números enteros positivos.

Por el principio de buen orden, S posee un elemento mínimo, digamos, $b - ma$.

Observe que $b - (m + 1)a$ también se está en S, ya que S contiene todos los enteros de esta forma. Además, tenemos que

$$b - (m + 1)a = (b - ma) - a < b - ma$$

contrario a la elección de $b - ma$ como el menor número entero en S. Esta contradicción surge del supuesto inicial que la propiedad Arquimedeana no es válida. Por tanto, esto prueba el teorema. $\square$

Teorema (Primer principio de inducción finita)

Sea S un conjunto de enteros positivos con las siguientes propiedades:

1. *El número entero 1 pertenece a S.*
2. *Siempre que un entero k esté en S, el siguiente entero $k+1$ también está en S.*

Entonces, S es el conjunto de todos los enteros positivos $\mathbb{Z}^+$.

Prueba: Sea T el conjunto de todos los enteros positivos que no están en S, y suponga que T no es vacío.

Por el principio del buen orden, T posee un elemento mínimo, que denotamos por a. Como $1 \in S$, ciertamente $a > 1$, por lo que $0 < a - 1 < a$.

La elección de a como menor entero positivo en T implica que $a-1 \notin T \;\Rightarrow\; a-1 \in S$. Por hipótesis, $a-1 \in S \;\Rightarrow\; a = (a-1)+1 \in S$, lo que contradice el hecho de que $a \in T$.

Portanto, $T = \varnothing$ y $S = \mathbb{Z}^+$. $\square$