Carl Friedrich GAUSS

1777 - 1855

VIII Seminario de Matemática Discreta

GAUSS, una mirada discreta

Gregorio Hernández, UPM

20-04-2006

SUMARIO

- Un pizarrín   “Ligget se”
- Disquisitiones arithmeticae
- Teoría Geométrica de Números
- Teoría Analítica de Números
- Empaquetamiento de esferas

Ligget se!

1777 Brunswick. Nacimiento de Gauss

1780 Contar antes de leer

1786 Katherinen Vokschule.

$1 + 2 + 3 + \ldots + 99 + 100 = ?$

$1 + 100 = 2 + 99 = \ldots = 50 + 51 = 101$

$? = 50 \cdot 101 = 5050$

Martin Bartels

1788 Gymnasium Catharineum

1791 Duque de Brunswick. Collegium Carolinum

1795 Universidad de Gotinga

1796 Heptadecágono regular

Diario de notas

"Principia quibus innititur sectio circuli, ac divisibilitas eiusdem geometrica in septemdecim partes, ... Mart. 30 Brunsv."

Ligget se!

1798 Vuelta a Brunswick.

1799 Tesis doctoral. Universidad de Helmstedt

“Demonstratio nova theorematis omnem functionem algebraicam rationalem integram unius variabilis in factores reales primi vei secundi gradus posse”

(Nuevas demostraciones: 1815, 1816, 1849)

1801 *Disquisitiones arithmeticae*

Órbita de Ceres

1807 Profesor en Gotinga

Director del Observatorio Astronómico

Disquisitiones arithmeticae

Elaborado durante 1795-98, en Gotinga
Hasta el siglo XIX la Teoría de Números, resultados aislados

- establece la notación
- sistematiza y extiende la teoría existente
- clasifica los problemas y métodos a estudiar
- introduce nuevos métodos

* congruencias
* números algebraicos
* teoría de formas, base del análisis diofántico

Disquisitiones arithmeticae

1. Números congruentes en general
2. Congruencias de primer grado
3. Residuos de potencias
4. Congruencias de segundo grado
5. Formas y ecuaciones indeterminadas de segundo grado
6. Aplicaciones de las nociones anteriores
7. Ecuaciones de las secciones de un círculo.

Disquisitiones arithmeticae

1. Números congruentes en general

Si m divide la diferencia $a - b$, se dice que a y b son congruentes según m

$$a \equiv b \ (\text{mód } m)$$

–9 y 16 son congruentes módulo 5

–7 es un residuo de 15 según el módulo 11, pero no según el módulo 3

Propiedades

- Todos los residuos de a según m son $a+km$
- Dados los enteros $a, a+1, a+2, \ldots, a+m-1$ y otro A, sólo uno de los primeros es congruente con A módulo m
- Suma y producto de congruencias
- Reglas de divisibilidad por 9 y por 11

Disquisitiones arithmeticae

2. Congruencias de primer grado

- Si p es primo, $a<p$, no existe $b<p$ tal que $ab \equiv 0 \ (mod\ p)$
- Unicidad de la descomposición en factores primos
- Número de divisores de un número
- mcd, mcm
- Si $ak \equiv bk \ (mod\ m)\ y\ mcd(m,k)=e$ entonces $a \equiv b \ (mod\ m/e)$
- Resolución de $ax+b \equiv c \ (mod\ m)$

Aplicaciones

Función φA, números positivos menores que A y primos con A

Si $A=a^m b^n c^p...$ $\varphi A= A\frac{a-1}{a}\frac{b-1}{b}\frac{c-1}{c}\cdots$

Disquisitiones arithmeticae

2. Congruencias de primer grado

Aplicaciones

La congruencia de grado *m* $Ax^m+Bx^{m-1}+ \ldots +Mx+N\equiv 0 \pmod{p}$ cuyo módulo *p* es primo y no divide a A, no puede resolverse de más de *m* maneras distintas (o no puede tener más de *m* raíces no congruentes con relación a *p*)

Demostrado por Lagrange en 1768 y en casos particulares por Euler

Disquisitiones arithmeticae

3. Residuos de potencias

Estudia los restos de potencias a, a^2, a^3, ... módulo p primo con a

Si p es primo, a no es múltiplo de p entonces

$$a^{p-1} \equiv 1 \pmod{p}$$

Teorema enunciado por Fermat y demostrado por Euler y Lambert.
Gauss lo demuestra a partir del estudio de la ecuación en congruencias $x^n \equiv a \pmod{m}$ donde a y m primos entre sí

El producto de todos los números menores que un primo dado, aumentado en una unidad es siempre divisible por dicho número

Teorema de Wilson
Gauss lo generaliza para un A cualquiera

Disquisitiones arithmeticae

4. Congruencias de segundo grado

Si m y r son primos entre sí y existe x tal que $x^2 \equiv r \ (mod\ m)$, entonces r es residuo cuadrático de m, en caso contrario r es no-residuo cuadrático de m

Según el módulo 13 los residuos son 0, 1, 4, 9, 3, 12, 10, y los no-residuos 2, 5, 6, 7, 8, 11

Según el módulo 15 los residuos son 0, 1, 4, 9, 1, 10, 6, 4 y los no-residuos 2, 3, 5, 7, 8, 11, 12, 13, 14

Los residuos módulo m se obtienen como restos de dividir por m a los cuadrados de 1, 2, 3, ..., $m/2$

Disquisitiones arithmeticae

4. Congruencias de segundo grado

- Si el módulo es primo p, hay $(p-1)/2$ residuos y la misma cantidad de no residuos.
- -1 es residuo de todos los primos de la forma $4k+1$ y es no-residuo de los primos de la forma $4k+3$
- 2 es residuo de los primos de la forma $8k+1$ y $8k+7$ y es no-residuo de los demás primos impares
- -2 es residuo de los primos de la forma $8k+1$ y $8k+3$ y es no-residuo de los demás primos impares
- Obtiene la regla para 3, -3, 5, -5, 7, -7
- Cualquier número no cuadrado es no-residuo de un primo

Disquisitiones arithmeticae

4. Congruencias de segundo grado

Ley de reciprocidad cuadrática. Theorema aureum

"Si p es primo de la forma $4n+1$, $+p$ será un residuo o un no-residuo de todo primo que, tomado positivamente, sea un residuo o un no residuo de p. Si p es de la forma $4n+3$, $-p$ tiene la misma propiedad"

Existe reciprocidad entre el par de congruencias

$x^2 \equiv q \pmod{p}$

$x^2 \equiv p \pmod{q}$

ambas son posibles o bien ambas son imposibles, a no ser que tanto p como q sean de la forma $4n+3$, en cuyo caso una de las congruencias es posible y la otra no.

Demostración por inducción. Otras 4 a lo largo de su vida (y 2 inéditas)

Disquisitiones arithmeticae

4. Congruencias de segundo grado

Algo de historia

Búsqueda de primos de la forma x^2+y^2, x^2+2y^2, x^2+3y^2

Fermat

Un primo impar p es de la forma $x^2+y^2 \Leftrightarrow p=4n+1$

Un primo p es de la forma $x^2+2y^2 \Leftrightarrow p=8n+1$ o $8n+3$

Un primo p es de la forma $x^2+3y^2 \Leftrightarrow p=3n+1$

Euler

Conjetura la ley de reciprocidad cuadrática y prueba algunos casos

Símbolo de Legendre o símbolo de carácter cuadrático

$$\left(\frac{p}{q}\right) = \begin{cases} 1 & \text{si } p \text{ es un cuadrado } mod\ q \\ -1 & \text{si } p \text{ } no \text{ es un cuadrado } mod\ q \end{cases}$$

Disquisitiones arithmeticae

4. Congruencias de segundo grado

Ley de reciprocidad cuadrática

Si p y q son primos impares $$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Legendre la demuestra suponiendo que en una progresión aritmética $an+b$ con mcd$(a,b)=1$ hay infinitos primos. (1785-1798)

El teorema favorito de Gauss.
Teorema clave en Teoría de Números (196 demostraciones)

Disquisitiones arithmeticae

Generalización a reciprocidad cúbica, bicuadrática, ...

Euler observa sin probarlo que:
p es un primo de la forma $x^2+27y^2 \Leftrightarrow p=3n+1$ y 2 es un cubo *mod p*
p es un primo de la forma $x^2+64y^2 \Leftrightarrow p=4n+1$ y 2 es cuarta pot. *mod p*

Gauss demuestra estos resultados, 1808-17
La ley de reciprocidad bicuadrática aparece en ensayos de 1828, 1832, y necesita los enteros de Gauss $a+bi$, con a,b enteros

La ley de reciprocidad cúbica fue encontrada por Jacobi y Eisenstein. Requiere el estudio de los "enteros" $a+b\rho$, con a,b enteros y ρ una raíz cúbica de la unidad

Disquisitiones arithmeticae

Enteros de Gauss Z[i] 1832

En Z[i] hay descomposición única salvo unidades {1, –1, i, –i}

Extensión del teorema de Fermat

Si p es primo en Z[i] y k no es divisible por p entonces

$$k^{a^2+b^2-1} \equiv 1 (\mathrm{mod}\, p)$$

Disquisitiones arithmeticae

Símbolo bicuadrático

Si p es primo en Z[i], α no divisible por p entonces

$$\left(\frac{\alpha}{p}\right) \equiv \alpha^{\frac{N(p)-1}{4}} \pmod{p}$$

Ley de reciprocidad para residuos bicuadráticos

Si α, β son enteros de Gauss primos entre sí y $\alpha \equiv \beta \equiv 1 (\mathrm{mod}(1+i)^3)$

$$\left(\frac{\alpha}{\beta}\right)_4 = (-1)^{\frac{N(\alpha)-1}{4}\frac{N(\beta)-1}{4}} \left(\frac{\beta}{\alpha}\right)_4$$

Los caracteres bicuadráticos son iguales si $\alpha \equiv 1 (\mathrm{mod}\ 4)$ ó $\beta \equiv 1 (\mathrm{mod}\ 4)$

Los caracteres bicuadráticos son opuestos si $\alpha \equiv \beta \equiv 1 (\mathrm{mod}\ 3+2i)$

Disquisitiones arithmeticae

5. Formas y ecuaciones indeterminadas de segundo grado

Forma cuadrática binaria $ax^2+2bxy+cy^2$

Un número entero M está representado por la forma si M=$ax^2+2bxy+cy^2$

Problema directo: Determinar todos los enteros que pueden representarse por una forma dada $ax^2+2bxy+cy^2$

Problema inverso: Dados M, a,b,c encontrar los valores x e y que representan a M

Disquisitiones arithmeticae

5. Formas y ecuaciones indeterminadas de segundo grado

Forma cuadrática binaria $ax^2+2bxy+cy^2$

Lagrange

Formas equivalentes si representan el mismo número

Se obtienen por un cambio lineal

$x=\alpha x'+\beta y'$, $y=\gamma x'+\delta y'$, con $\alpha\delta-\beta\gamma=1$

Discriminante D $= b^2 - ac$ (Gauss lo llamó determinante)

Para un discriminante dado D existe un nº finito de formas tal que cada forma con ese discriminante es equivalente a una de ellas

Disquisitiones arithmeticae

5. Formas y ecuaciones indeterminadas de segundo grado

Forma cuadrática binaria $ax^2+2bxy+cy^2$

Gauss sistematiza y extiende la equivalencia de formas

Si F = $ax^2+2bxy+cy^2$ se transforma en F' = $a'x'^2+2b'x'y'+c'y'^2$
por un cambio lineal
$x=\alpha x'+\beta y'$, $y=\gamma x'+\delta y'$,
entonces $b'^2-a'c' = (b^2-ac)(\alpha\delta-\beta\gamma)$
Por tanto, si $(\alpha\delta-\beta\gamma)^2 = 1$, los discriminantes de F y F' son iguales y la transformación llevará F' a F

Si $\alpha\delta-\beta\gamma = 1$ F y F' son propiamente equivalentes
Si $\alpha\delta-\beta\gamma = -1$ F y F' son impropiamente equivalentes

Disquisitiones arithmeticae

5. Formas y ecuaciones indeterminadas de segundo grado

Forma cuadrática binaria $ax^2+2bxy+cy^2$

Gauss sistematiza y extiende la equivalencia de formas

Si F es equivalente a F', cualquier M representable por F lo será por F' y de tantas maneras por una como por otra.

- Demuestra cómo encontrar todas las transformaciones de F en F'
- Encuentra todas las representaciones de M por la forma F, siempre que los valores x,y sean primos entre sí.
- Dos formas con el mismo discriminante pueden no ser equivalentes.
- Las formas con un D dado se pueden dividir en clases equivalentes.
- El nº de clases es finito.
- Proporciona criterios para la elección del representante más simple
- $a=1$, $b=0$, $c=-D$ forma principal, su clase es la clase principal.

Disquisitiones arithmeticae

5. Formas y ecuaciones indeterminadas de segundo grado

Si *bb* – *ac* es un cuadrado

$12 = 3x^2 + 4xy - 7y^2$

descompone en factores (x –y)(3x+7y), analiza casos y ....

Dos soluciones x=2, y=0; x= –2, y=0

Si *bb* – *ac* no es un cuadrado

Si F es una forma primitiva (*a*,*b*,*c* primos entre sí) con discriminante D y *p* primo divide a D, entonces los M representados por F son o bien todos residuos cuadráticos de *p* o bien todos no residuos

Disquisitiones arithmeticae

5. Formas y ecuaciones indeterminadas de segundo grado

Si $bb - ac$ no es un cuadrado

$585 = 42x^2 + 62xy + 21y^2$ $\qquad$ $bb - ac = 79$

585 es sólo divisible por el cuadrado 9 $\qquad$ $585 = 9 \cdot 65$

Las soluciones primas entre sí se obtienen de $65 = 42x'^2 + 62x'y' + 21y'^2$

Los valores de $\sqrt{79}$ (mod 65) son $\pm 12, \pm 27$

Una representación de 65 correspondiente a 12 es $x' = 2,\ y' = -1$

todas las rep. correspondientes a 12 son $x' = 2t - 41u,\ \ y' = -t + 53u$

y las representaciones de 585 son $x = 6t - 123u,\ \ y = -3t + 159u$

De modo análogo se obtienen el resto de representaciones de 585

$x = 6t - 123u,\ \ y = -3t + 159u$ $\qquad$ $x = 66t - 597u,\ \ y = -69t + 633u$

$x = 3t - 114u,\ \ y = t + 157u$ $\qquad$ $x = 83t - 746u,\ \ y = -87t + 789u$

donde $tt - 79uu = 1$

Disquisitiones arithmeticae

5. Formas y ecuaciones indeterminadas de segundo grado

Si $bb - ac$ es negativo

Estudia las representaciones con x,y primos entre sí

Todo primo de la forma $4n+1$ se descompone en suma de dos cuadrados de forma única

Todo primo de la forma $8n+1$ ó 8n+3 puede ser representado en la forma x^2+2y^2 de una única manera

Disquisitiones arithmeticae

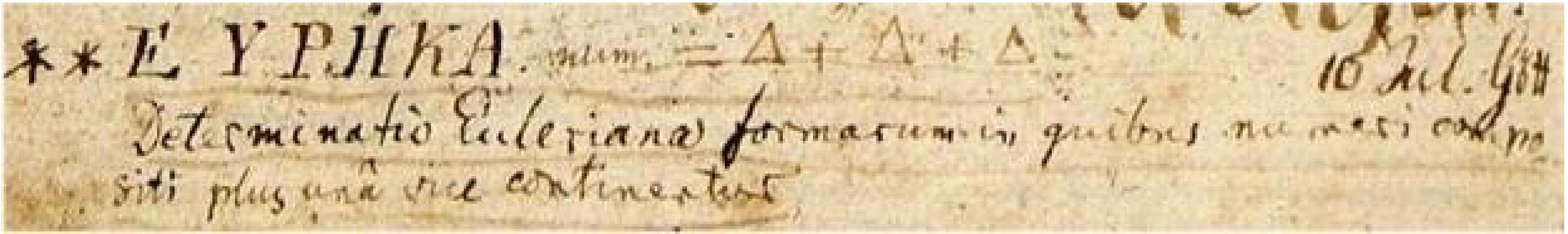
5. Formas y ecuaciones indeterminadas de segundo grado

Formas cuadráticas ternarias

$ax^2+2bxy+cy^2+2dxz+2eyz+fz^2$

Todo entero positivo se puede descomponer en suma de tres números triangulares. (1,3,6,10,15,...)

Anotación en el diario el 16 de julio de 1796



Todo entero positivo se puede descomponer en suma de cuatro cuadrados. (Lagrange)

Disquisitiones arithmeticae

6. Aplicaciones de las nociones anteriores

Solución de la congruencia $xx \equiv A$
Solución de la ecuación $m\,xx + nyy = A$

Métodos para distinguir compuestos de primos y para determinar sus factores

Disquisitiones arithmeticae

7. De las ecuaciones que definen las secciones de un círculo

Estudio de la congruencia $x^n \equiv 1 \pmod{p}$

Construcción de polígonos regulares con regla y compás

Artículo 366.

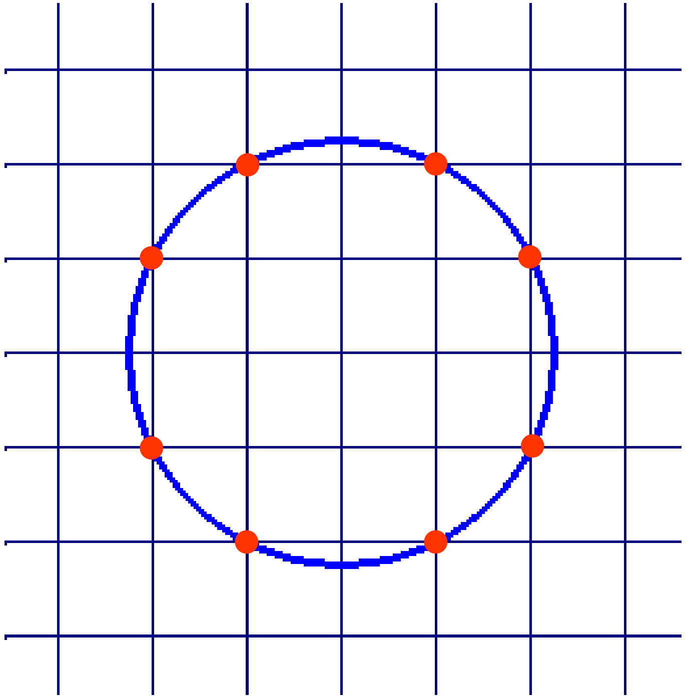
[Para poder seccionar geométricamente el círculo en N partes iguales]... se requiere que N no contenga ningún factor primo impar que no sea de la forma $2^m + 1$, ni tampoco ningún factor primo de la forma $2^m + 1$ más de una vez.

De esta forma, se encuentran los 38 valores de N menores que 300: 2, 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, 32, 34, 40, 48, 51, 60, 64, 68, 80, 85, 96, 102, 120, 128, 136, 160, 170, 192, 204, 240, 255, 256, 257, 272.

TEORÍA GEOMÉTRICA DE NÚMEROS

Puntos reticulares en la circunferencia $x^2+y^2=n$ $r_2(n)$

Nº de representaciones de n como suma de dos cuadrados



$x^2+y^2=5$ $r_2(5)=8$

$2^2+1^2=5$ $(-2)^2+1^2=5$

$2^2+(-1)^2=5$ $(-2)^2+(-1)^2=5$

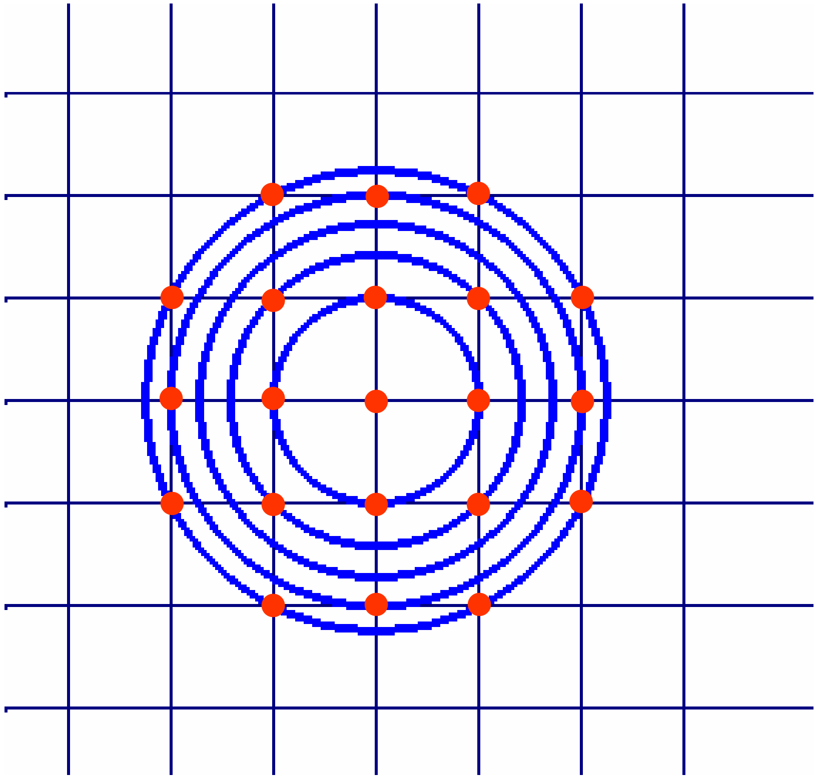
$1^2+2^2=5$ $(-1)^2+2^2=5$

$1^2+(-2)^2=5$ $(-1)^2+(-2)^2=5$

TEORÍA GEOMÉTRICA DE NÚMEROS

Puntos reticulares en la circunferencia $x^2+y^2=n$ $\quad$ $r_2(n)$

Gauss's Circle Problem $\qquad$ Estimar $\displaystyle \frac{1}{N}\sum_{n=0}^{N} r_2(n)$

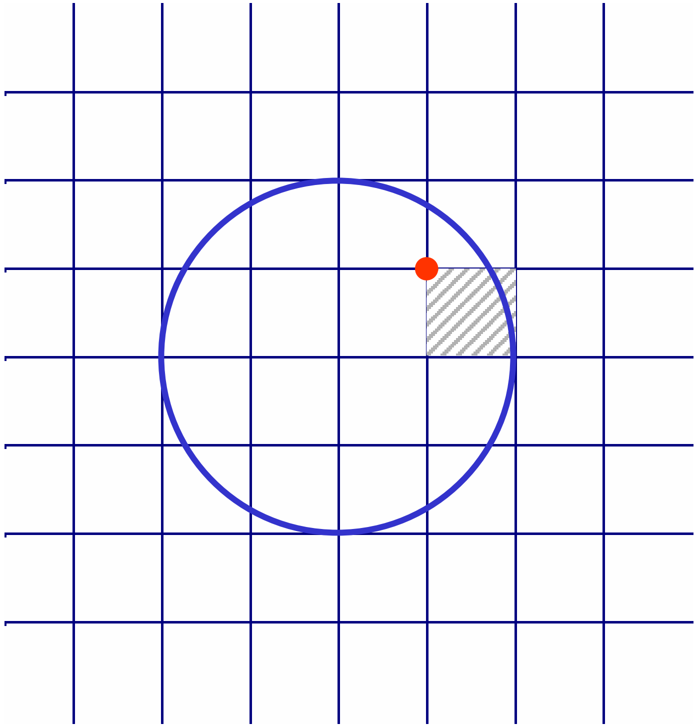


n	0	1	2	3	4	5	6 ....
$r_2(n)$	1	4	4	0	4	8	0 ....

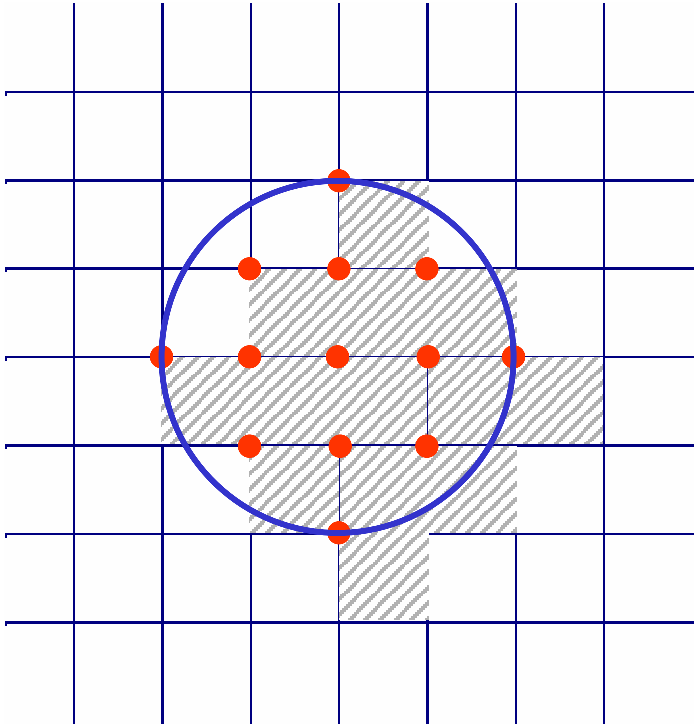
TEORÍA GEOMÉTRICA DE NÚMEROS

Gauss's Circle Problem

Estimar $\frac{1}{N}\sum_{n=0}^{N} r_2(n)$



Un punto reticular en C(4)



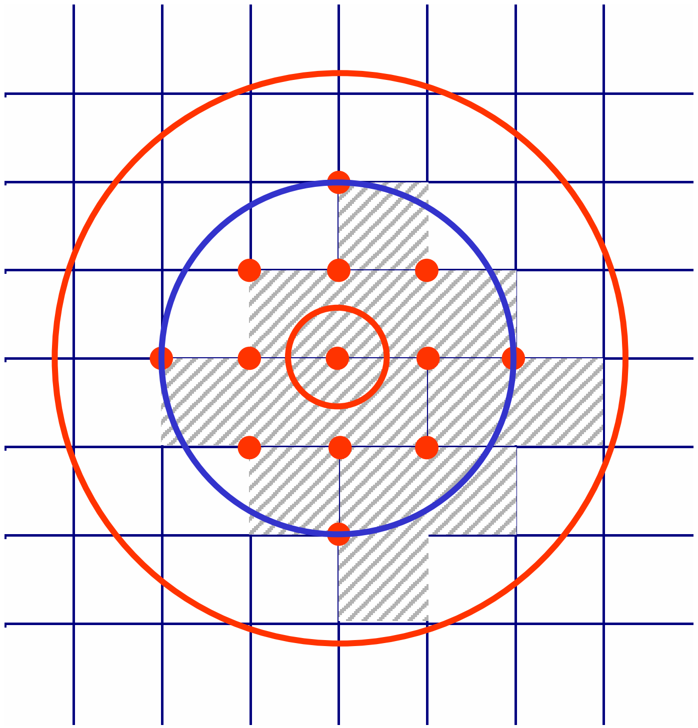
Zona rayada P(4)

Área (P(N)) = nº puntos reticulares en C(N)

TEORÍA GEOMÉTRICA DE NÚMEROS

Gauss's Circle Problem

Estimar $\frac{1}{N}\sum_{n=0}^{N} r_2(n)$



Área (P(N)) = $\sum_{n=0}^{N} r_2(n)$

Un punto en el borde de P(N) dista de C(N) a lo más $\sqrt{2}$ unidades

P(N) $\subset$ Disco de radio $\sqrt{N} + \sqrt{2}$

P(N) $\supset$ Disco de radio $\sqrt{N} - \sqrt{2}$

TEORÍA GEOMÉTRICA DE NÚMEROS

Gauss's Circle Problem

Estimar $\frac{1}{N}\sum_{n=0}^{N} r_2(n)$

$$\pi\left(\sqrt{N}-\sqrt{2}\right)^2 < \acute{A}rea(P(N)) < \pi\left(\sqrt{N}+\sqrt{2}\right)^2$$

$$\pi\left(N-2\sqrt{2}\sqrt{N}+2\right) < \sum_{n=0}^{N} r_2(n) < \pi\left(N+2\sqrt{2}\sqrt{N}+2\right)$$

$$-\pi 2\sqrt{2}\sqrt{N} < \sum_{n=0}^{N} r_2(n) - (N+2)\pi < \pi 2\sqrt{2}\sqrt{N}$$

$$\left|\frac{1}{N}\sum_{n=0}^{N} r_2(n) - \frac{(N+2)\pi}{N}\right| < \frac{\pi 2\sqrt{2}}{\sqrt{N}}$$

$$\lim_{N\to\infty}\frac{1}{N}\sum_{n=0}^{N} r_2(n) = \lim_{N\to\infty}\frac{(N+2)\pi}{N} = \pi$$

Teorema

$$\lim_{N\to\infty}\frac{1}{N}\sum_{n=0}^{N} r_2(n) = \pi$$

TEORÍA ANALÍTICA DE NÚMEROS

Estimación de $\pi(x)$, número de primos que no exceden x

Estudia todos los primos hasta 3000000 y conjetura que

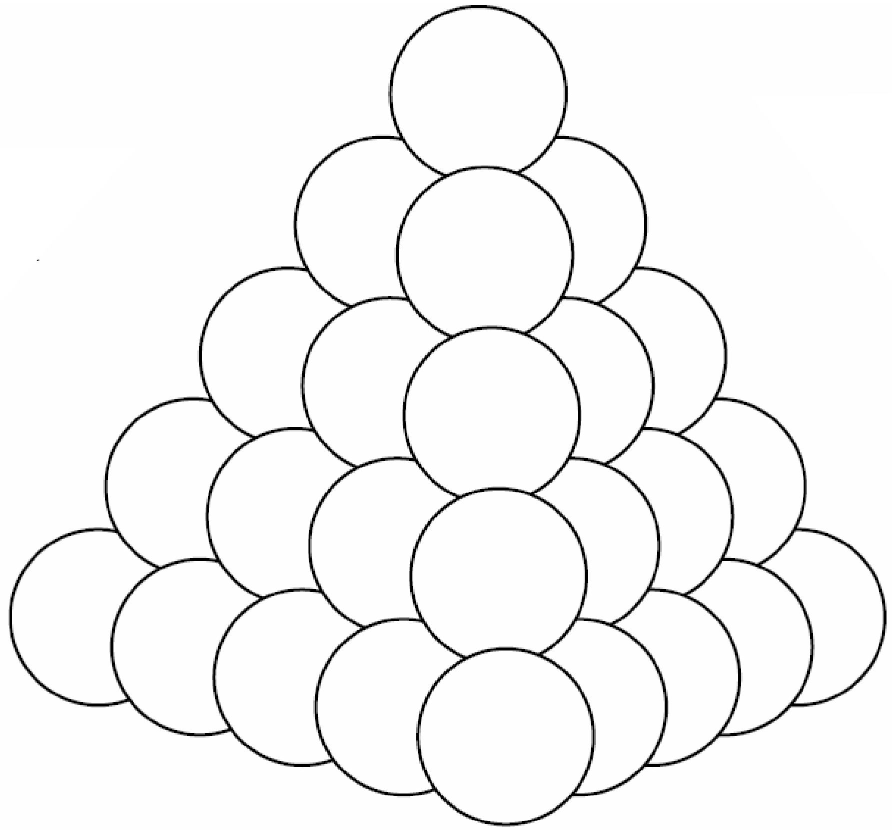
números primos menores que $a(=\infty)\dfrac{a}{la}$

Teorema de los números primos

$$\lim_{x\to\infty}\frac{\pi(x)}{\dfrac{x}{\ln(x)}}=1$$

1896, Hadamard, de la Valleé Poussin
1948, Selberg, Erdös

EMPAQUETAMIENTO DE ESFERAS



¿Se pueden apilar las naranjas de mejor forma que la tradicional forma de pirámide de las fruterías?

SPHERE PACKING PROBLEM

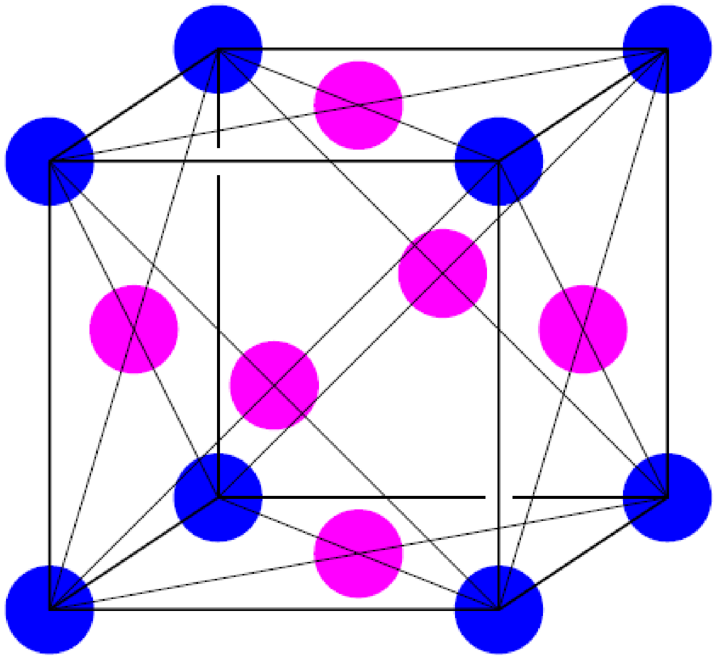
¿Cuál es el empaquetamiento óptimo?

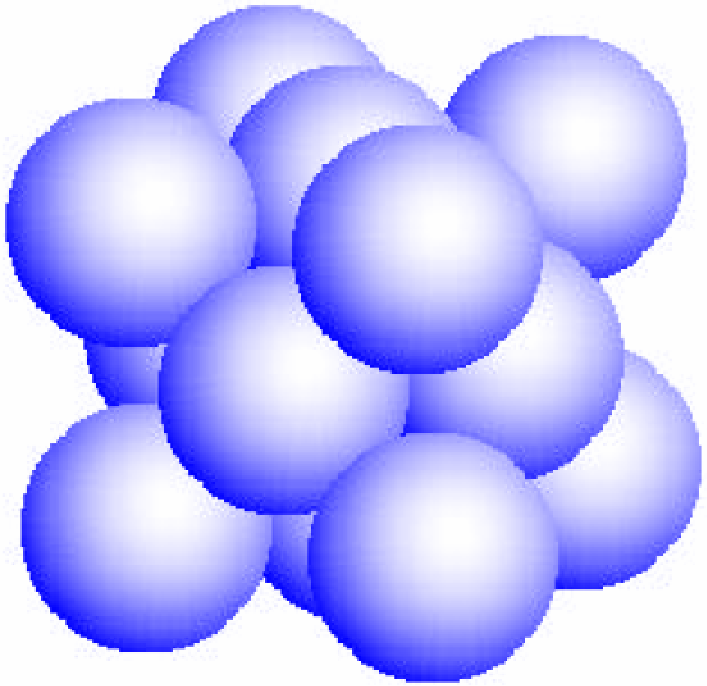
Determinar la densidad máxima de un empaquetamiento de bolas iguales

EMPAQUETAMIENTO DE ESFERAS

Conjetura de Kepler

Ningún empaquetamiento de bolas iguales en R^3 tiene mayor densidad que el empaquetamiento fcc (face-centered-cubic)



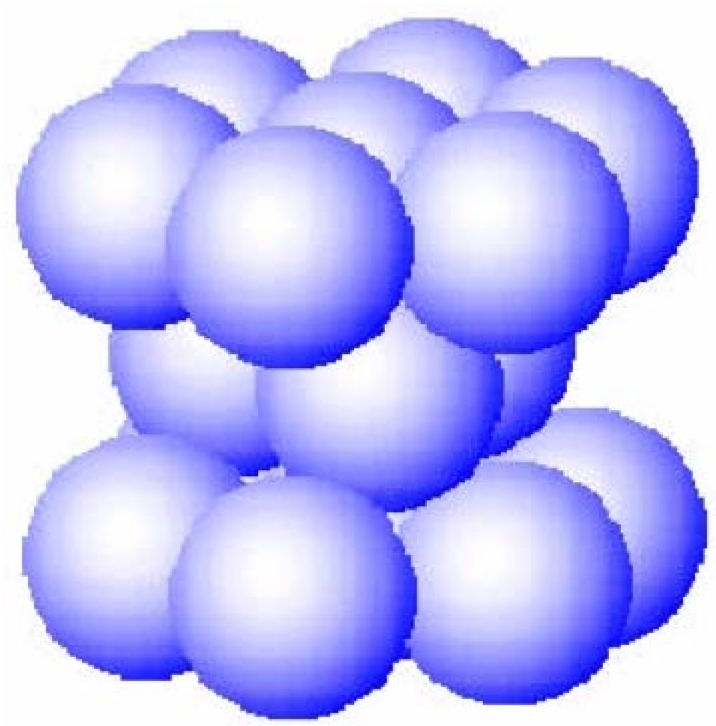


Densidad $\dfrac{\pi}{\sqrt{18}} \approx 0.74$

EMPAQUETAMIENTO DE ESFERAS

Conjetura de Kepler

Ningún empaquetamiento de bolas iguales en R^3 tiene mayor densidad que el empaquetamiento fcc (face-centered-cubic)



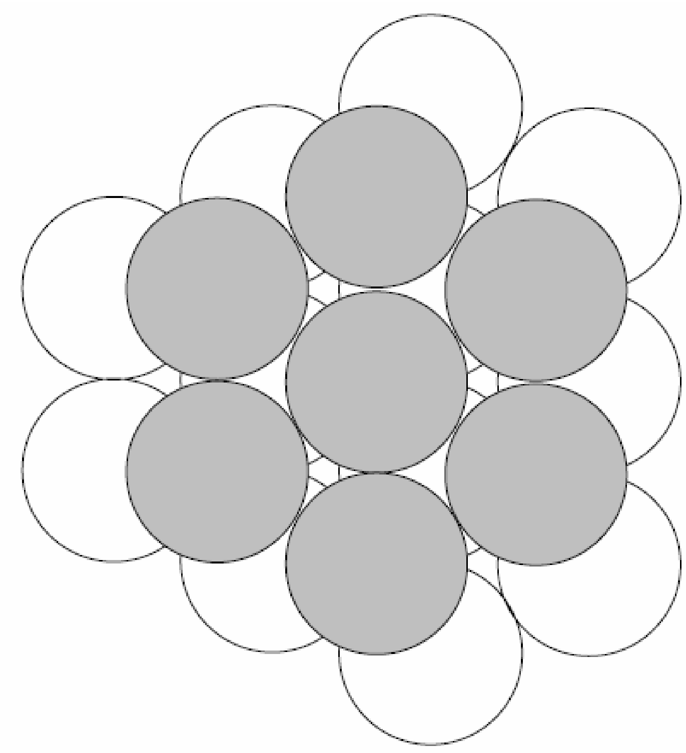
Empaquetamiento hc (hexagonal-close)

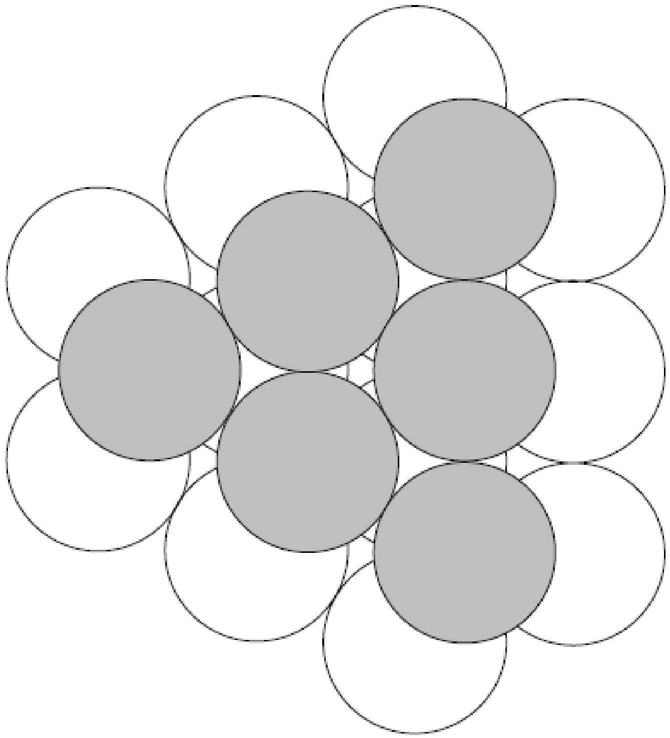
Densidad $\frac{\pi}{\sqrt{18}} \approx 0.74$

EMPAQUETAMIENTO DE ESFERAS

Conjetura de Kepler

Ningún empaquetamiento de bolas iguales en R^3 tiene mayor densidad que el empaquetamiento fcc (face-centered-cubic)

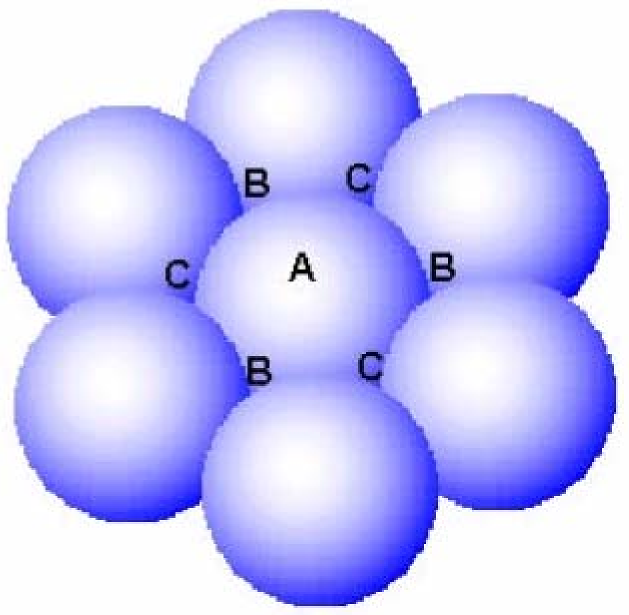




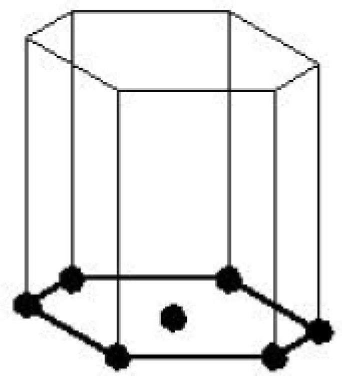
EMPAQUETAMIENTO DE ESFERAS

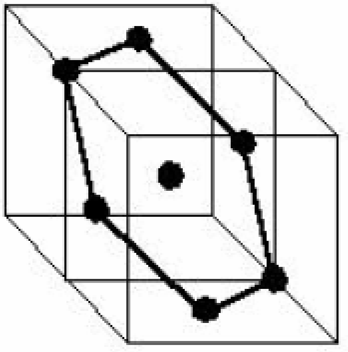
Conjetura de Kepler

Ningún empaquetamiento de bolas iguales en R^3 tiene mayor densidad que el empaquetamiento fcc (face-centered-cubic)



Empaquetamiento hc ABABAB...
Empaquetamiento fcc ABCABC...





EMPAQUETAMIENTO DE ESFERAS (Versión reticular)

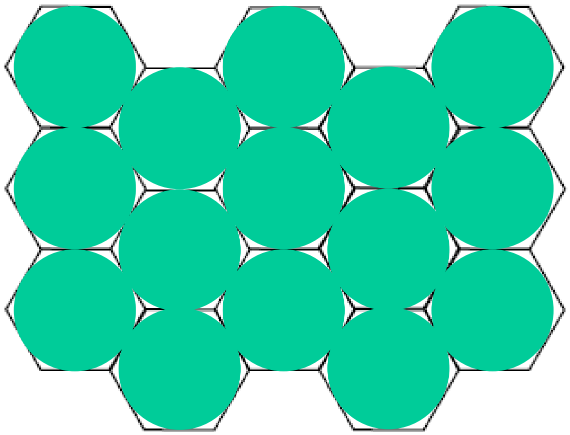
Lattice Packing Problem

Empaquetamiento *reticular*, si es invariante por cualquier traslación que lleve una bola a otra.

Ningún empaquetamiento reticular de bolas iguales en R^3 tiene mayor densidad que el empaquetamiento fcc (face-centered-cubic)

En el plano, empaquetamiento hexagonal

Densidad $\frac{\pi}{\sqrt{12}} \approx 0.90$



Gauss, 1831

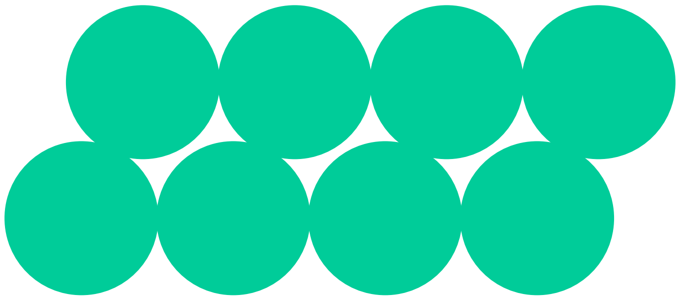
Resultado sobre formas cuadráticas ternarias

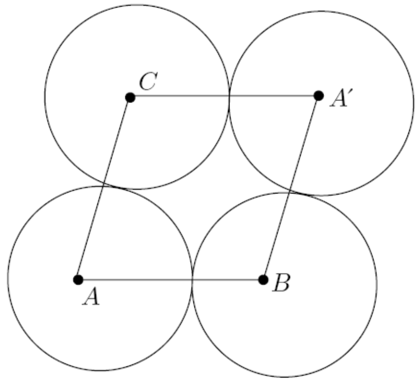
EMPAQUETAMIENTO DE ESFERAS (Versión reticular)

Lattice Packing Problem

Ningún empaquetamiento reticular de bolas iguales en R^3 tiene mayor densidad que el empaquetamiento fcc (face-centered-cubic)

Gauss, 1831





La bola en la siguiente capa, D, en el hueco entre ABC
luego ABD equilátero

Mirando desde ABD, en las capas se repite el diseño ABD, las bolas en los huecos de la capa anterior $\Rightarrow$ fcc

REFERENCIAS

Referencias

Gauss

En la red

http://platea.pntic.mec.es/aperez4/html/sigloxix/CarLFriedrichGauss.htm
http://www.geocities.com/grandesmatematicos/cap14.html
http://www-groups.dcs.st-and.ac.uk/%7Ehistory/Biographies/Gauss.html

En papel

"Gauss: Titan of Science". G. Waldo Dunnington, MAA, 2004
"Prince of Mathematics: Carl Friedrich Gauss". M. B. W. Tent, A. K. Peters, 2006

Teoría de Números

"Number Theory". G. Andrews, Dover, 1971

Conjetura de Kepler

T. C. Hales http://www.math.pitt.edu/~thales/

Carl Friedrich Gauss

1777 - 1855