Números Primos

Alan Reyes-Figueroa
Teoría de Números

(Aula 06) 21.julio.2022

Ejemplo: Hallar la factoración en primos de 7777.

Teorema Fundamental de la Aritmética

Ejemplo: Hallar la factoración en primos de 7777.

Sabemos que $7 \mid 7777$, pues $7777 = 7 \cdot 1111$.

Teorema Fundamental de la Aritmética

Ejemplo: Hallar la factoración en primos de 7777.

Sabemos que $7 \mid 7777$, pues $7777 = 7 \cdot 1111$. Además, sabemos que $11 \mid 1111$, ya que $1111 = 11 \cdot 101$. Finalmente, 101 es primo:

$$\begin{array}{r|c} 7777 & 7 \\ 1111 & 11 \\ 101 & 101 \\ 1 & \end{array}$$

Teorema Fundamental de la Aritmética

Ejemplo: Hallar la factoración en primos de 7777.

Sabemos que $7 \mid 7777$, pues $7777 = 7 \cdot 1111$. Además, sabemos que $11 \mid 1111$, ya que $1111 = 11 \cdot 101$. Finalmente, 101 es primo:

$$\begin{array}{r|c} 7777 & 7 \\ 1111 & 11 \\ 101 & 101 \\ 1 & \end{array}$$

Entonces $7777 = 7 \cdot 11 \cdot 101$.

Teorema Fundamental de la Aritmética

Ejemplo: Hallar la factoración en primos de 7777.

Sabemos que $7 \mid 7777$, pues $7777 = 7 \cdot 1111$. Además, sabemos que $11 \mid 1111$, ya que $1111 = 11 \cdot 101$. Finalmente, 101 es primo:

$$\begin{array}{r|c} 7777 & 7 \\ 1111 & 11 \\ 101 & 101 \\ 1 & \end{array}$$

Entonces $7777 = 7 \cdot 11 \cdot 101$.

Ejemplo: La factoración en primos de 360 es:

Ejemplo: Hallar la factoración en primos de 7777.

Sabemos que $7 \mid 7777$, pues $7777 = 7 \cdot 1111$. Además, sabemos que $11 \mid 1111$, ya que $1111 = 11 \cdot 101$. Finalmente, 101 es primo:

$$\begin{array}{r|c} 7777 & 7 \\ 1111 & 11 \\ 101 & 101 \\ 1 & \end{array}$$

Entonces $7777 = 7 \cdot 11 \cdot 101$.

Ejemplo: La factoración en primos de 360 es: $360 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5$.

Teorema Fundamental de la Aritmética

Ejemplo: Hallar la factoración en primos de 7777.

Sabemos que $7 \mid 7777$, pues $7777 = 7 \cdot 1111$. Además, sabemos que $11 \mid 1111$, ya que $1111 = 11 \cdot 101$. Finalmente, 101 es primo:

$$\begin{array}{r|c} 7777 & 7 \\ 1111 & 11 \\ 101 & 101 \\ 1 & \end{array}$$

Entonces $7777 = 7 \cdot 11 \cdot 101$.

Ejemplo: La factoración en primos de 360 es: $360 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5$.

Ejemplo: ¿Cuál es la factoración en primos de 2021?

Corolario (Forma Canónica)

Todo entero positivo $n > 1$ *puede representarse de manera única en la forma*

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r},$$

donde para cada $i = 1, 2, \ldots, r$*, cada* k_i *es un entero positivo y y los* p_i *son todos primos, con* $p_1 < p_2 \ldots < p_r$*.* $\square$

Corolario (Forma Canónica)

Todo entero positivo $n > 1$ puede representarse de manera única en la forma

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r},$$

donde para cada $i = 1, 2, \ldots, r$, cada k_i es un entero positivo y y los p_i son todos primos, con $p_1 < p_2 \ldots < p_r$. $\square$

Comentario: Cunado sea conveniente, el corolario puede extenderse a una expresión de la forma

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}, \qquad \text{donde } k_i \geq 0, \text{ y } p_1 < p_2 \ldots < p_r$$

UNIVERSIDAD DEL VALLE DE GUATEMALA

Corolario (Forma Canónica)

Todo entero positivo $n > 1$ puede representarse de manera única en la forma

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r},$$

donde para cada $i = 1, 2, \ldots, r$, cada k_i es un entero positivo y y los p_i son todos primos, con $p_1 < p_2 \ldots < p_r$. $\square$

Comentario: Cunado sea conveniente, el corolario puede extenderse a una expresión de la forma

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}, \qquad \text{donde } k_i \geq 0, \text{ y } p_1 < p_2 \ldots < p_r$$

Ejemplo: $360 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 = 2^3 \cdot 3^2 \cdot 5.$

Corolario (Forma Canónica)

Todo entero positivo $n > 1$ puede representarse de manera única en la forma

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r},$$

donde para cada $i = 1, 2, \ldots, r$, cada k_i es un entero positivo y y los p_i son todos primos, con $p_1 < p_2 \ldots < p_r$. $\square$

<u>Comentario</u>: Cunado sea conveniente, el corolario puede extenderse a una expresión de la forma

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}, \qquad \text{donde } k_i \geq 0, \text{ y } p_1 < p_2 \ldots < p_r$$

Ejemplo: $360 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 = 2^3 \cdot 3^2 \cdot 5$.

Ejemplo: $24 = 2^3 \cdot 3$, y $63 = 3^2 \cdot 7$. Podemos escribir estos números en la base común

$$24 = 2^3 \cdot 3 \cdot 7^0 \qquad \text{y} \qquad 63 = 2^0 \cdot 3^2 \cdot 7.$$

Propiedad

Sea $n \in \mathbb{Z}^+$ un entero positivo con factoración en primos $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$. Si d es un divisor positivo de n, entonces d es de la forma

$$d = p_1^{t_1} p_2^{t_2} \cdots p_r^{t_r}, \qquad \textit{con } 0 \leq t_j \leq k_j, \; \textit{para todo } j = 1, 2, \ldots, r.$$

Propiedad

Sea $n \in \mathbb{Z}^+$ un entero positivo con factoración en primos $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$. Si d es un divisor positivo de n, entonces d es de la forma

$$d = p_1^{t_1} p_2^{t_2} \cdots p_r^{t_r}, \qquad \text{con } 0 \leq t_j \leq k_j, \text{ para todo } j = 1, 2, \ldots, r.$$

Prueba: Sea $d = q_1^{u_1} q_2^{u_2} \cdots q_m^{u_m}$ la factoración en primos de d, con $s_i \geq 0$.

Propiedad

Sea $n \in \mathbb{Z}^+$ un entero positivo con factoración en primos $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$. Si d es un divisor positivo de n, entonces d es de la forma

$$d = p_1^{t_1} p_2^{t_2} \cdots p_r^{t_r}, \qquad \text{con } 0 \leq t_j \leq k_j, \ \text{para todo } j = 1, 2, \ldots, r.$$

<u>Prueba</u>: Sea $d = q_1^{u_1} q_2^{u_2} \cdots q_m^{u_m}$ la factoración en primos de d, con $s_i \geq 0$. Para cada $i = 1, \ldots, m$, $q_i \mid n \;\Rightarrow q_i = p_j$, para algún j.

Propiedad

Sea $n \in \mathbb{Z}^+$ un entero positivo con factoración en primos $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$. Si d es un divisor positivo de n, entonces d es de la forma

$$d = p_1^{t_1} p_2^{t_2} \cdots p_r^{t_r}, \qquad \text{con } 0 \leq t_j \leq k_j, \ \text{para todo } j = 1, 2, \ldots, r.$$

Prueba: Sea $d = q_1^{u_1} q_2^{u_2} \cdots q_m^{u_m}$ la factoración en primos de d, con $s_i \geq 0$. Para cada $i = 1, \ldots, m$, $q_i \mid n \Rightarrow q_i = p_j$, para algún j. De ahí que $d = p_1^{s_1} p_2^{s_2} \cdots p_r^{s_r}$. Además, como $p_j^{\alpha} \mid p_j^{\beta} \Leftrightarrow \alpha \leq \beta$, se tiene el resultado. $\square$

Teorema Fundamental de la Aritmética

Propiedad

Sea $n \in \mathbb{Z}^+$ un entero positivo con factoración en primos $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$. Si d es un divisor positivo de n, entonces d es de la forma

$$d = p_1^{t_1} p_2^{t_2} \cdots p_r^{t_r}, \qquad \text{con } 0 \leq t_j \leq k_j, \text{ para todo } j = 1, 2, \ldots, r.$$

Prueba: Sea $d = q_1^{u_1} q_2^{u_2} \cdots q_m^{u_m}$ la factoración en primos de d, con $s_i \geq 0$. Para cada $i = 1, \ldots, m$, $q_i \mid n \;\Rightarrow q_i = p_j$, para algún j. De ahí que $d = p_1^{s_1} p_2^{s_2} \cdots p_r^{s_r}$. Además, como $p_j^{\alpha} \mid p_j^{\beta} \;\Leftrightarrow\; \alpha \leq \beta$, se tiene el resultado. $\square$

Corolario

Sea n entero positivo, con factorización en primos $n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}$, donde $k_j \geq 1$. Entonces, el número de divisores positivos de n es

$$d(n) = (k_1 + 1)(k_2 + 1) \cdots (k_r + 1). \;\square$$

Corolario

Sean $a, b \in \mathbb{Z}^+$*, con factoraciones*

$$a = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} \qquad y \qquad b = p_1^{\ell_1} p_2^{\ell_2} \cdots p_r^{\ell_r},$$

sobre una base común de primos $p_1 < p_2 < \ldots < p_r$*, y con exponentes* $k_j, \ell_j \geq 0$ *para* $j = 1, 2, \ldots, r$*. Entonces*

- $(a, b) = p_1^{\min\{k_1,\ell_1\}} p_2^{\min\{k_2,\ell_2\}} \cdots p_r^{\min\{k_r,\ell_r\}}$.
- $[a, b] = p_1^{\max\{k_1,\ell_1\}} p_2^{\max\{k_2,\ell_2\}} \cdots p_r^{\max\{k_r,\ell_r\}}$. $\square$

Corolario

Sean $a, b \in \mathbb{Z}^+$, con factoraciones

$$a = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r} \qquad y \qquad b = p_1^{\ell_1} p_2^{\ell_2} \cdots p_r^{\ell_r},$$

sobre una base común de primos $p_1 < p_2 < \ldots < p_r$, y con exponentes $k_j, \ell_j \geq 0$ para $j = 1, 2, \ldots, r$. Entonces

- $(a, b) = p_1^{\min\{k_1,\ell_1\}} p_2^{\min\{k_2,\ell_2\}} \cdots p_r^{\min\{k_r,\ell_r\}}$.
- $[a, b] = p_1^{\max\{k_1,\ell_1\}} p_2^{\max\{k_2,\ell_2\}} \cdots p_r^{\max\{k_r,\ell_r\}}$. $\square$

A partir de estas expresiones se pueden mostrar muchas de las propiedades que involucran al (a, b) o al $[a, b]$.

Más Propiedades

Teorema (Irracionalidad de $\sqrt{2}$, Hípaso)
El número $\sqrt{2}$ es irracional.

Teorema (Irracionalidad de $\sqrt{2}$, Hípaso)
El número $\sqrt{2}$ es irracional.

Prueba: Supongamos que $\sqrt{2} \in \mathbb{Q}$, es racional.

Más Propiedades

Teorema (Irracionalidad de $\sqrt{2}$, Hípaso)

El número $\sqrt{2}$ es irracional.

Prueba: Supongamos que $\sqrt{2} \in \mathbb{Q}$, es racional. Entonces $\sqrt{2} = \frac{a}{b}$, para algunos $a, b \in \mathbb{Z}^+$.

Más Propiedades

Teorema (Irracionalidad de $\sqrt{2}$, Hípaso)

El número $\sqrt{2}$ es irracional.

Prueba: Supongamos que $\sqrt{2} \in \mathbb{Q}$, es racional. Entonces $\sqrt{2} = \frac{a}{b}$, para algunos $a, b \in \mathbb{Z}^+$. Más aún, podemos suponer que $(a, b) = 1$.

Más Propiedades

Teorema (Irracionalidad de $\sqrt{2}$, Hípaso)

El número $\sqrt{2}$ es irracional.

Prueba: Supongamos que $\sqrt{2} \in \mathbb{Q}$, es racional. Entonces $\sqrt{2} = \frac{a}{b}$, para algunos $a, b \in \mathbb{Z}^+$. Más aún, podemos suponer que $(a, b) = 1$. Elevando al cuadrado esta relación y limpiando denominadores, obtenemos $a^2 = 2b^2$.

Más Propiedades

Teorema (Irracionalidad de $\sqrt{2}$, Hípaso)

El número $\sqrt{2}$ es irracional.

Prueba: Supongamos que $\sqrt{2} \in \mathbb{Q}$, es racional. Entonces $\sqrt{2} = \frac{a}{b}$, para algunos $a, b \in \mathbb{Z}^+$. Más aún, podemos suponer que $(a, b) = 1$. Elevando al cuadrado esta relación y limpiando denominadores, obtenemos $a^2 = 2b^2$. En particular $b \mid 2b^2 = a^2$.

Teorema (Irracionalidad de $\sqrt{2}$, Hípaso)

El número $\sqrt{2}$ es irracional.

Prueba: Supongamos que $\sqrt{2} \in \mathbb{Q}$, es racional. Entonces $\sqrt{2} = \frac{a}{b}$, para algunos $a, b \in \mathbb{Z}^+$. Más aún, podemos suponer que $(a, b) = 1$. Elevando al cuadrado esta relación y limpiando denominadores, obtenemos $a^2 = 2b^2$. En particular $b \mid 2b^2 = a^2$.

Si $b > 1$, por el Teorema fundamental de la Aritmética, existe un primo p tal que $p \mid b$.

Más Propiedades

Teorema (Irracionalidad de $\sqrt{2}$, Hípaso)

El número $\sqrt{2}$ es irracional.

Prueba: Supongamos que $\sqrt{2} \in \mathbb{Q}$, es racional. Entonces $\sqrt{2} = \frac{a}{b}$, para algunos $a, b \in \mathbb{Z}^+$. Más aún, podemos suponer que $(a, b) = 1$. Elevando al cuadrado esta relación y limpiando denominadores, obtenemos $a^2 = 2b^2$. En particular $b \mid 2b^2 = a^2$.

Si $b > 1$, por el Teorema fundamental de la Aritmética, existe un primo p tal que $p \mid b$. De ello se deduce que $p \mid a^2$ y, en consecuencia, que $p \mid a$.

Más Propiedades

Teorema (Irracionalidad de $\sqrt{2}$, Hípaso)

El número $\sqrt{2}$ es irracional.

<u>Prueba</u>: Supongamos que $\sqrt{2} \in \mathbb{Q}$, es racional. Entonces $\sqrt{2} = \frac{a}{b}$, para algunos $a, b \in \mathbb{Z}^+$. Más aún, podemos suponer que $(a, b) = 1$. Elevando al cuadrado esta relación y limpiando denominadores, obtenemos $a^2 = 2b^2$. En particular $b \mid 2b^2 = a^2$.

Si $b > 1$, por el Teorema fundamental de la Aritmética, existe un primo p tal que $p \mid b$. De ello se deduce que $p \mid a^2$ y, en consecuencia, que $p \mid a$. De ahí que $(a, b) \geq p > 1$, una contradicción.

Teorema (Irracionalidad de $\sqrt{2}$, HÍPASO)

El número $\sqrt{2}$ es irracional.

Prueba: Supongamos que $\sqrt{2} \in \mathbb{Q}$, es racional. Entonces $\sqrt{2} = \frac{a}{b}$, para algunos $a, b \in \mathbb{Z}^+$. Más aún, podemos suponer que $(a, b) = 1$. Elevando al cuadrado esta relación y limpiando denominadores, obtenemos $a^2 = 2b^2$. En particular $b \mid 2b^2 = a^2$.

Si $b > 1$, por el Teorema fundamental de la Aritmética, existe un primo p tal que $p \mid b$. De ello se deduce que $p \mid a^2$ y, en consecuencia, que $p \mid a$. De ahí que $(a, b) \geq p > 1$, una contradicción. Entonces $b = 1$.

Más Propiedades

Teorema (Irracionalidad de $\sqrt{2}$, Hípaso)

El número $\sqrt{2}$ es irracional.

Prueba: Supongamos que $\sqrt{2} \in \mathbb{Q}$, es racional. Entonces $\sqrt{2} = \frac{a}{b}$, para algunos $a, b \in \mathbb{Z}^+$. Más aún, podemos suponer que $(a, b) = 1$. Elevando al cuadrado esta relación y limpiando denominadores, obtenemos $a^2 = 2b^2$. En particular $b \mid 2b^2 = a^2$.

Si $b > 1$, por el Teorema fundamental de la Aritmética, existe un primo p tal que $p \mid b$. De ello se deduce que $p \mid a^2$ y, en consecuencia, que $p \mid a$. De ahí que $(a, b) \geq p > 1$, una contradicción. Entonces $b = 1$. Pero si esto sucede, entonces $2 = a^2$, de modo que $\sqrt{2} = a$ es un entero, lo cual es imposible

Teorema (Irracionalidad de $\sqrt{2}$, Hípaso)

El número $\sqrt{2}$ es irracional.

Prueba: Supongamos que $\sqrt{2} \in \mathbb{Q}$, es racional. Entonces $\sqrt{2} = \frac{a}{b}$, para algunos $a, b \in \mathbb{Z}^+$. Más aún, podemos suponer que $(a, b) = 1$. Elevando al cuadrado esta relación y limpiando denominadores, obtenemos $a^2 = 2b^2$. En particular $b \mid 2b^2 = a^2$.

Si $b > 1$, por el Teorema fundamental de la Aritmética, existe un primo p tal que $p \mid b$. De ello se deduce que $p \mid a^2$ y, en consecuencia, que $p \mid a$. De ahí que $(a, b) \geq p > 1$, una contradicción. Entonces $b = 1$. Pero si esto sucede, entonces $2 = a^2$, de modo que $\sqrt{2} = a$ es un entero, lo cual es imposible (asumimos que el lector está dispuesto a admitir que $1 < \sqrt{2} < 2$ y no existe ningún número entero entre 1 y 2).

Teorema (Irracionalidad de $\sqrt{2}$, Hípaso)

El número $\sqrt{2}$ es irracional.

Prueba: Supongamos que $\sqrt{2} \in \mathbb{Q}$, es racional. Entonces $\sqrt{2} = \frac{a}{b}$, para algunos $a, b \in \mathbb{Z}^+$. Más aún, podemos suponer que $(a, b) = 1$. Elevando al cuadrado esta relación y limpiando denominadores, obtenemos $a^2 = 2b^2$. En particular $b \mid 2b^2 = a^2$.

Si $b > 1$, por el Teorema fundamental de la Aritmética, existe un primo p tal que $p \mid b$. De ello se deduce que $p \mid a^2$ y, en consecuencia, que $p \mid a$. De ahí que $(a, b) \geq p > 1$, una contradicción. Entonces $b = 1$. Pero si esto sucede, entonces $2 = a^2$, de modo que $\sqrt{2} = a$ es un entero, lo cual es imposible (asumimos que el lector está dispuesto a admitir que $1 < \sqrt{2} < 2$ y no existe ningún número entero entre 1 y 2).
Así, el supuesto inicial $\sqrt{2} \in \mathbb{Q}$ es insostenible, por lo que $\sqrt{2} \notin \mathbb{Q}$, debe ser un irracional. $\square$

Cribas

Pregunta: Dado $n > 1$, ¿cómo podemos determinar si es primo o no?

Cribas

Pregunta: Dado $n > 1$, ¿cómo podemos determinar si es primo o no?
El enfoque obvio consiste en dividir sucesivamente el número n por cada de los números $1, 2, \ldots, n-1$

Cribas

Pregunta: Dado $n > 1$, ¿cómo podemos determinar si es primo o no?
El enfoque obvio consiste en dividir sucesivamente el número n por cada de los números $1, 2, \ldots, n-1$ si ninguno de ellos (excepto 1) sirve como divisor, entonces n debe ser primo.

Cribas

Pregunta: Dado $n > 1$, ¿cómo podemos determinar si es primo o no?
El enfoque obvio consiste en dividir sucesivamente el número n por cada de los números $1, 2, \ldots, n-1$ si ninguno de ellos (excepto 1) sirve como divisor, entonces n debe ser primo. Sin embargo, en la práctica este método no es eficiente.

Pregunta: Dado $n > 1$, ¿cómo podemos determinar si es primo o no?
El enfoque obvio consiste en dividir sucesivamente el número n por cada de los números $1, 2, \ldots, n-1$ si ninguno de ellos (excepto 1) sirve como divisor, entonces n debe ser primo. Sin embargo, en la práctica este método no es eficiente.

Existe una propiedad de los números compuestos que permite reducir los cálculos, pero el proceso sigue siendo engorroso.

Cribas

Pregunta: Dado $n > 1$, ¿cómo podemos determinar si es primo o no?
El enfoque obvio consiste en dividir sucesivamente el número n por cada de los números $1, 2, \ldots, n-1$ si ninguno de ellos (excepto 1) sirve como divisor, entonces n debe ser primo. Sin embargo, en la práctica este método no es eficiente.

Existe una propiedad de los números compuestos que permite reducir los cálculos, pero el proceso sigue siendo engorroso. Si $n > 1$ es compuesto, entonces puede escribirse como $n = ab$, con $1 < a, b < n$.

Cribas

Pregunta: Dado $n > 1$, ¿cómo podemos determinar si es primo o no? El enfoque obvio consiste en dividir sucesivamente el número n por cada de los números $1, 2, \ldots, n-1$ si ninguno de ellos (excepto 1) sirve como divisor, entonces n debe ser primo. Sin embargo, en la práctica este método no es eficiente.

Existe una propiedad de los números compuestos que permite reducir los cálculos, pero el proceso sigue siendo engorroso. Si $n > 1$ es compuesto, entonces puede escribirse como $n = ab$, con $1 < a, b < n$. Suponiendo que $a \leq b$, obtenemos $a^2 \leq ab = n$, de modo que $a \leq \sqrt{n}$.

Cribas

Pregunta: Dado $n > 1$, ¿cómo podemos determinar si es primo o no?
El enfoque obvio consiste en dividir sucesivamente el número n por cada de los números $1, 2, \ldots, n-1$ si ninguno de ellos (excepto 1) sirve como divisor, entonces n debe ser primo. Sin embargo, en la práctica este método no es eficiente.

Existe una propiedad de los números compuestos que permite reducir los cálculos, pero el proceso sigue siendo engorroso. Si $n > 1$ es compuesto, entonces puede escribirse como $n = ab$, con $1 < a, b < n$. Suponiendo que $a \leq b$, obtenemos $a^2 \leq ab = n$, de modo que $a \leq \sqrt{n}$. Como $a > 1$, el Teorema Fundamental de la Aritmética asegura que a tiene al menos un factor primo p.

UNIVERSIDAD DEL VALLE DE GUATEMALA

Cribas

Pregunta: Dado $n > 1$, ¿cómo podemos determinar si es primo o no? El enfoque obvio consiste en dividir sucesivamente el número n por cada de los números $1, 2, \ldots, n-1$ si ninguno de ellos (excepto 1) sirve como divisor, entonces n debe ser primo. Sin embargo, en la práctica este método no es eficiente.

Existe una propiedad de los números compuestos que permite reducir los cálculos, pero el proceso sigue siendo engorroso. Si $n > 1$ es compuesto, entonces puede escribirse como $n = ab$, con $1 < a, b < n$. Suponiendo que $a \leq b$, obtenemos $a^2 \leq ab = n$, de modo que $a \leq \sqrt{n}$. Como $a > 1$, el Teorema Fundamental de la Aritmética asegura que a tiene al menos un factor primo p. Entonces $p \leq a\sqrt{n}$.

Cribas

Pregunta: Dado $n > 1$, ¿cómo podemos determinar si es primo o no?
El enfoque obvio consiste en dividir sucesivamente el número n por cada de los números $1, 2, \ldots, n-1$ si ninguno de ellos (excepto 1) sirve como divisor, entonces n debe ser primo. Sin embargo, en la práctica este método no es eficiente.

Existe una propiedad de los números compuestos que permite reducir los cálculos, pero el proceso sigue siendo engorroso. Si $n > 1$ es compuesto, entonces puede escribirse como $n = ab$, con $1 < a, b < n$. Suponiendo que $a \leq b$, obtenemos $a^2 \leq ab = n$, de modo que $a \leq \sqrt{n}$. Como $a > 1$, el Teorema Fundamental de la Aritmética asegura que a tiene al menos un factor primo p. Entonces $p \leq a\sqrt{n}$. Además, como $p \mid a$ y $a \mid n \;\Rightarrow\; p \mid n$.

Cribas

Pregunta: Dado $n > 1$, ¿cómo podemos determinar si es primo o no?
El enfoque obvio consiste en dividir sucesivamente el número n por cada de los números $1, 2, \ldots, n-1$ si ninguno de ellos (excepto 1) sirve como divisor, entonces n debe ser primo. Sin embargo, en la práctica este método no es eficiente.

Existe una propiedad de los números compuestos que permite reducir los cálculos, pero el proceso sigue siendo engorroso. Si $n > 1$ es compuesto, entonces puede escribirse como $n = ab$, con $1 < a, b < n$. Suponiendo que $a \leq b$, obtenemos $a^2 \leq ab = n$, de modo que $a \leq \sqrt{n}$. Como $a > 1$, el Teorema Fundamental de la Aritmética asegura que a tiene al menos un factor primo p. Entonces $p \leq a\sqrt{n}$. Además, como $p \mid a$ y $a \mid n \;\Rightarrow\; p \mid n$. El punto es simplemente este: **un número compuesto n siempre poseerá un divisor primo p que satisface $p \leq \sqrt{n}$.**

Ejemplo: ¿Son 517 y 521 primos?

Ejemplo: ¿Son 517 y 521 primos?

Veamos. La raíz de 517 es $\sqrt{517} \approx 22.737\ldots$. Basta con buscar factores primos por $1 < p \leq 22$, que son $2, 3, 5, 7, 11, 13, 17$ y 19.

Cribas

Ejemplo: ¿Son 517 y 521 primos?

Veamos. La raíz de 517 es $\sqrt{517} \approx 22.737\ldots$. Basta con buscar factores primos por $1 < p \leq 22$, que son $2, 3, 5, 7, 11, 13, 17$ y 19.
Es inmediato que los primos $2, 3, 5$ y 7 no dividen a 517. ¿Por qué?

Ejemplo: ¿Son 517 y 521 primos?

Veamos. La raíz de 517 es $\sqrt{517} \approx 22.737\ldots$. Basta con buscar factores primos por $1 < p \leq 22$, que son $2, 3, 5, 7, 11, 13, 17$ y 19.
Es inmediato que los primos $2, 3, 5$ y 7 no dividen a 517. ¿Por qué? Pero $11 \mid 517$, ya que $17 = 11 \cdot 47$. Portanto 517 es compuesto.

Ejemplo: ¿Son 517 y 521 primos?

Veamos. La raíz de 517 es $\sqrt{517} \approx 22.737\ldots$. Basta con buscar factores primos por $1 < p \leq 22$, que son $2, 3, 5, 7, 11, 13, 17$ y 19.
Es inmediato que los primos $2, 3, 5$ y 7 no dividen a 517. ¿Por qué? Pero $11 \mid 517$, ya que $17 = 11 \cdot 47$. Portanto 517 es compuesto.

Para el segundo ejemplo, de nuevo $\sqrt{521} \approx 22.825\ldots$, y debemos buscar factore sprimos por $1 < p <\leq 22$. De nuevo, estos factores son $2, 3, 5, 7, 11, 13, 17$ y 19.

Ejemplo: ¿Son 517 y 521 primos?

Veamos. La raíz de 517 es $\sqrt{517} \approx 22.737...$. Basta con buscar factores primos por $1 < p \leq 22$, que son $2, 3, 5, 7, 11, 13, 17$ y 19.
Es inmediato que los primos $2, 3, 5$ y 7 no dividen a 517. ¿Por qué? Pero $11 \mid 517$, ya que $17 = 11 \cdot 47$. Portanto 517 es compuesto.

Para el segundo ejemplo, de nuevo $\sqrt{521} \approx 22.825...$, y debemos buscar factore sprimos por $1 < p <\leq 22$. De nuevo, estos factores son $2, 3, 5, 7, 11, 13, 17$ y 19.
Es inmediato que los primos $2, 3, 5, 7$ y 11 no dividen a 521.

Ejemplo: ¿Son 517 y 521 primos?

Veamos. La raíz de 517 es $\sqrt{517} \approx 22.737\ldots$. Basta con buscar factores primos por $1 < p \leq 22$, que son $2, 3, 5, 7, 11, 13, 17$ y 19.
Es inmediato que los primos $2, 3, 5$ y 7 no dividen a 517. ¿Por qué? Pero $11 \mid 517$, ya que $17 = 11 \cdot 47$. Portanto 517 es compuesto.

Para el segundo ejemplo, de nuevo $\sqrt{521} \approx 22.825\ldots$, y debemos buscar factore sprimos por $1 < p << 22$. De nuevo, estos factores son $2, 3, 5, 7, 11, 13, 17$ y 19.
Es inmediato que los primos $2, 3, 5, 7$ y 11 no dividen a 521. Ahora, los restantes $13, 17$ y 19 tampoco lo dividen.

Ejemplo: ¿Son 517 y 521 primos?

Veamos. La raíz de 517 es $\sqrt{517} \approx 22.737\ldots$. Basta con buscar factores primos por $1 < p \leq 22$, que son $2, 3, 5, 7, 11, 13, 17$ y 19.
Es inmediato que los primos $2, 3, 5$ y 7 no dividen a 517. ¿Por qué? Pero $11 \mid 517$, ya que $17 = 11 \cdot 47$. Portanto 517 es compuesto.

Para el segundo ejemplo, de nuevo $\sqrt{521} \approx 22.825\ldots$, y debemos buscar factore sprimos por $1 < p <\leq 22$. De nuevo, estos factores son $2, 3, 5, 7, 11, 13, 17$ y 19.
Es inmediato que los primos $2, 3, 5, 7$ y 11 no dividen a 521. Ahora, los restantes $13, 17$ y 19 tampoco lo dividen.
Entonces, $n = 521$ no posee factores primos entre 1 y $\sqrt{n}$. Portanto, 521 es primo.

Cribas

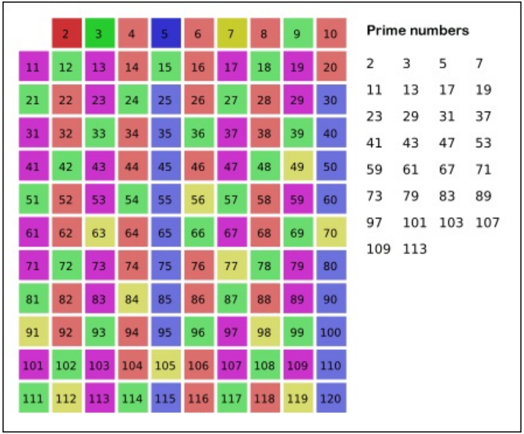
Otras cribas: Dado n, son algoritmos o procedimientos que usualmente producen la lista de todos los primos $\leq n$ (otros no producen la lista si no sólo cuentan la cantidad de primos).

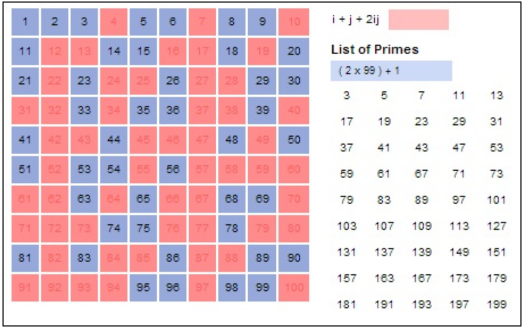
Cribas

Otras cribas: Dado n, son algoritmos o procedimientos que usualmente producen la lista de todos los primos $\leq n$ (otros no producen la lista si no sólo cuentan la cantidad de primos).

Existen muchas cribas:

- Eratóstenes (*circa* 200 b.C.)
- Legendre (1752-1833) Esta cuenta el número de primos $\leq n$.
- Sundaram (1934)
- *Wheel sieves* (años 80's)
- Atkin y Bernstein (2003).





Cribas: (a) Criba de Eratóstenes, (b) Criba de Sundaram.

Teorema (Euclides (*circa* 300 b.C.))

Hay un número infinito de números primos.

Teorema (Euclides (*circa* 300 b.C.))
Hay un número infinito de números primos.

Prueba: La prueba de Euclides es por contradicción.

Teorema (Euclides (*circa* 300 b.C.))

Hay un número infinito de números primos.

<u>Prueba</u>: La prueba de Euclides es por contradicción. Suponga que $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, \ldots, p_n$ es la lista de todos los primos en orden ascendente, y supongamos que hay un último primo, llamado p_n.

Teorema (Euclides (*circa* 300 b.C.))

Hay un número infinito de números primos.

Prueba: La prueba de Euclides es por contradicción. Suponga que $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, \ldots, p_n$ es la lista de todos los primos en orden ascendente, y supongamos que hay un último primo, llamado p_n. Consideremos el entero positivo

$$N = p_1 p_2 p_3 \cdots p_n + 1.$$

Teorema (Euclides (*circa* 300 b.C.))

Hay un número infinito de números primos.

Prueba: La prueba de Euclides es por contradicción. Suponga que $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, \ldots, p_n$ es la lista de todos los primos en orden ascendente, y supongamos que hay un último primo, llamado p_n. Consideremos el entero positivo

$$N = p_1 p_2 p_3 \cdots p_n + 1.$$

Claramente, $N > p_j$, para todo primo p_j en la lista anterior.

Teorema (Euclides (*circa* 300 b.C.))

Hay un número infinito de números primos.

Prueba: La prueba de Euclides es por contradicción. Suponga que $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, \ldots, p_n$ es la lista de todos los primos en orden ascendente, y supongamos que hay un último primo, llamado p_n. Consideremos el entero positivo

$$N = p_1 p_2 p_3 \cdots p_n + 1.$$

Claramente, $N > p_j$, para todo primo p_j en la lista anterior. Como $N > 1$, por el Teorema Fundamental de la Aritmética, existe un número primo p tal que $p \mid N$.

Teorema (Euclides (*circa* 300 b.C.))

Hay un número infinito de números primos.

<u>Prueba</u>: La prueba de Euclides es por contradicción. Suponga que $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, \ldots, p_n$ es la lista de todos los primos en orden ascendente, y supongamos que hay un último primo, llamado p_n. Consideremos el entero positivo

$$N = p_1 p_2 p_3 \cdots p_n + 1.$$

Claramente, $N > p_j$, para todo primo p_j en la lista anterior. Como $N > 1$, por el Teorema Fundamental de la Aritmética, existe un número primo p tal que $p \mid N$. Pero $p_1, p_2, \ldots, p_n$ son los únicos números primos, entonces que p debe ser igual a uno de $p_1, p_2, \ldots, p_n$.

Teorema (Euclides (*circa* 300 b.C.))

Hay un número infinito de números primos.

Prueba: La prueba de Euclides es por contradicción. Suponga que $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, \ldots, p_n$ es la lista de todos los primos en orden ascendente, y supongamos que hay un último primo, llamado p_n. Consideremos el entero positivo

$$N = p_1 p_2 p_3 \cdots p_n + 1.$$

Claramente, $N > p_j$, para todo primo p_j en la lista anterior. Como $N > 1$, por el Teorema Fundamental de la Aritmética, existe un número primo p tal que $p \mid N$. Pero $p_1, p_2, \ldots, p_n$ son los únicos números primos, entonces que p debe ser igual a uno de $p_1, p_2, \ldots, p_n$. Combinando las relaciones de divisibilidad $p \mid p_1 p_2 \cdots p_n$ y $p \mid N$, entonces $p \mid N - p_1 p_2 \cdots p_n = 1$.

Teorema (Euclides (*circa* 300 b.C.))

Hay un número infinito de números primos.

<u>Prueba</u>: La prueba de Euclides es por contradicción. Suponga que $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, \ldots, p_n$ es la lista de todos los primos en orden ascendente, y supongamos que hay un último primo, llamado p_n. Consideremos el entero positivo

$$N = p_1 p_2 p_3 \cdots p_n + 1.$$

Claramente, $N > p_j$, para todo primo p_j en la lista anterior. Como $N > 1$, por el Teorema Fundamental de la Aritmética, existe un número primo p tal que $p \mid N$. Pero $p_1, p_2, \ldots, p_n$ son los únicos números primos, entonces que p debe ser igual a uno de $p_1, p_2, \ldots, p_n$. Combinando las relaciones de divisibilidad $p \mid p_1 p_2 \cdots p_n$ y $p \mid N$, entonces $p \mid N - p_1 p_2 \cdots p_n = 1$. Pero el único divisor positivo de 1 es 1 mismo, lo que implica que $p = 1$, un absurdo, pues 1 no es primo.

Teorema (Euclides (*circa* 300 b.C.))

Hay un número infinito de números primos.

<u>Prueba</u>: La prueba de Euclides es por contradicción. Suponga que $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, \ldots, p_n$ es la lista de todos los primos en orden ascendente, y supongamos que hay un último primo, llamado p_n. Consideremos el entero positivo

$$N = p_1 p_2 p_3 \cdots p_n + 1.$$

Claramente, $N > p_j$, para todo primo p_j en la lista anterior. Como $N > 1$, por el Teorema Fundamental de la Aritmética, existe un número primo p tal que $p \mid N$. Pero $p_1, p_2, \ldots, p_n$ son los únicos números primos, entonces que p debe ser igual a uno de $p_1, p_2, \ldots, p_n$. Combinando las relaciones de divisibilidad $p \mid p_1 p_2 \cdots p_n$ y $p \mid N$, entonces $p \mid N - p_1 p_2 \cdots p_n = 1$. Pero el único divisor positivo de 1 es 1 mismo, lo que implica que $p = 1$, un absurdo, pues 1 no es primo. Portanto, N debe ser primo, y ninguna lista finita de primos es completa, de donde el número de primos es infinito. $\square$

Primos

Otra prueba: HERMITE (Siglo XIX).
Sea $n \in \mathbb{Z}^+$ arbitrario.

Otra prueba: Hermite (Siglo XIX).

Sea $n \in \mathbb{Z}^+$ arbitrario. Tome $x = n! + 1 > 1$. Por el Teorema Fundamental de la Aritmética, x tiene algún factor primo $p \mid x$.

Primos

Otra prueba: Hermite (Siglo XIX).

Sea $n \in \mathbb{Z}^+$ arbitrario. Tome $x = n! + 1 > 1$. Por el Teorema Fundamental de la Aritmética, x tiene algún factor primo $p \mid x$. Luego $p \neq 1, 2, 3, \ldots, n$, pues de lo contrario $p \mid 1$.

Otra prueba: HERMITE (Siglo XIX).

Sea $n \in \mathbb{Z}^+$ arbitrario. Tome $x = n! + 1 > 1$. Por el Teorema Fundamental de la Aritmética, x tiene algún factor primo $p \mid x$. Luego $p \neq 1, 2, 3, \ldots, n$, pues de lo contrario $p \mid 1$. Luego, $p > n$. $\square$

Primos

Otra prueba: Hermite (Siglo XIX).
Sea $n \in \mathbb{Z}^+$ arbitrario. Tome $x = n! + 1 > 1$. Por el Teorema Fundamental de la Aritmética, x tiene algún factor primo $p \mid x$. Luego $p \neq 1, 2, 3, \ldots, n$, pues de lo contrario $p \mid 1$. Luego, $p > n$. $\square$

Otra prueba: Saidak (2006).
Defina $N_1 = 2$, $N_2 = N_1(N_1 + 1) = 2 \cdot 3$, $N_3 = N_2(N_2 + 1) = 2 \cdot 3 \cdot 7$, y en general $N_{k+1} = N_k(N_k + 1)$, para $k \geq 1$.

Primos

Otra prueba: Hermite (Siglo XIX).

Sea $n \in \mathbb{Z}^+$ arbitrario. Tome $x = n! + 1 > 1$. Por el Teorema Fundamental de la Aritmética, x tiene algún factor primo $p \mid x$. Luego $p \neq 1, 2, 3, \ldots, n$, pues de lo contrario $p \mid 1$. Luego, $p > n$. $\square$

Otra prueba: Saidak (2006).

Defina $N_1 = 2$, $N_2 = N_1(N_1 + 1) = 2 \cdot 3$, $N_3 = N_2(N_2 + 1) = 2 \cdot 3 \cdot 7$, y en general $N_{k+1} = N_k(N_k + 1)$, para $k \geq 1$. En este caso, se muestra que N_k tiene al menos k factores primos distintos. $\square$

Primos

Otra prueba: Hermite (Siglo XIX).
Sea $n \in \mathbb{Z}^+$ arbitrario. Tome $x = n! + 1 > 1$. Por el Teorema Fundamental de la Aritmética, x tiene algún factor primo $p \mid x$. Luego $p \neq 1, 2, 3, \ldots, n$, pues de lo contrario $p \mid 1$. Luego, $p > n$. $\square$

Otra prueba: Saidak (2006).
Defina $N_1 = 2$, $N_2 = N_1(N_1 + 1) = 2 \cdot 3$, $N_3 = N_2(N_2 + 1) = 2 \cdot 3 \cdot 7$, y en general $N_{k+1} = N_k(N_k + 1)$, para $k \geq 1$. En este caso, se muestra que N_k tiene al menos k factores primos distintos. $\square$

Otra prueba: Euler (Siglo XVIII).
La suma $\displaystyle\sum_p \frac{1}{p}$ diverge.

Primos

Sea p_n el n-ésimo primo: $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, ...

Primos

Sea p_n el n-ésimo primo: $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, ...

La prueba de EUCLIDES muestra que la expresión $p_1 p_2 \cdots p_n + 1$ es divisible por al menos un número primo. Sí hay son varios de estos divisores primos, entonces $p_n + 1$ no puede exceder al menor de estos,

Primos

Sea p_n el n-ésimo primo: $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, ...

La prueba de Euclides muestra que la expresión $p_1 p_2 \cdots p_n + 1$ es divisible por al menos un número primo. Sí hay son varios de estos divisores primos, entonces $p_n + 1$ no puede exceder al menor de estos, por lo que $p_n + 1 \leq p_1 p_2 \cdots p_n + 1$, para $n > 1$.

Primos

Sea p_n el n-ésimo primo: $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, ...

La prueba de Euclides muestra que la expresión $p_1 p_2 \cdots p_n + 1$ es divisible por al menos un número primo. Sí hay son varios de estos divisores primos, entonces $p_n + 1$ no puede exceder al menor de estos, por lo que $p_n + 1 \leq p_1 p_2 \cdots p_n + 1$, para $n > 1$. Otra forma de decir lo mismo es que

$$p_n \leq p_1 p_2 \cdots p_{n-1} + 1, \qquad \text{para } n \geq 2.$$

Primos

Sea p_n el n-ésimo primo: $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, ...

La prueba de EUCLIDES muestra que la expresión $p_1 p_2 \cdots p_n + 1$ es divisible por al menos un número primo. Sí hay son varios de estos divisores primos, entonces $p_n + 1$ no puede exceder al menor de estos, por lo que $p_n + 1 \leq p_1 p_2 \cdots p_n + 1$, para $n > 1$. Otra forma de decir lo mismo es que

$$p_n \leq p_1 p_2 \cdots p_{n-1} + 1, \qquad \text{para } n \geq 2.$$

Con una ligera modificación de este razonamiento, esta desigualdad se puede mejorar como

$$p_n \leq p_1 p_2 \cdots p_{n-1} - 1, \qquad \text{para } n \geq 3.$$

Primos

Sea p_n el n-ésimo primo: $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, ...

La prueba de EUCLIDES muestra que la expresión $p_1 p_2 \cdots p_n + 1$ es divisible por al menos un número primo. Sí hay son varios de estos divisores primos, entonces $p_n + 1$ no puede exceder al menor de estos, por lo que $p_n + 1 \leq p_1 p_2 \cdots p_n + 1$, para $n > 1$. Otra forma de decir lo mismo es que

$$p_n \leq p_1 p_2 \cdots p_{n-1} + 1, \qquad \text{para } n \geq 2.$$

Con una ligera modificación de este razonamiento, esta desigualdad se puede mejorar como

$$p_n \leq p_1 p_2 \cdots p_{n-1} - 1, \qquad \text{para } n \geq 3.$$

Por ejemplo, cuando $n = 5$, esta desigualdad nos dice que $11 = p_5 < 2 \cdot 3 \cdot 5 \cdot 7 - 1 = 209$.

Primos

La estimación es bastante exagerada.

Primos

La estimación es bastante exagerada. Una limitación un poco más cercana en el tamaño p_n viene dada por la *desigualdad de* BONSE, que establece que

$$p_n^2 < p_1 p_2 \cdots p_{n-1}, \qquad \text{para } n \geq 5.$$

Primos

La estimación es bastante exagerada. Una limitación un poco más cercana en el tamaño p_n viene dada por la *desigualdad de* BONSE, que establece que

$$p_n^2 < p_1 p_2 \cdots p_{n-1}, \qquad \text{para } n \geq 5.$$

Esta desigualdad produce $p_5^2 < 210$, ó $p_5 \leq 14$.

Primos

La estimación es bastante exagerada. Una limitación un poco más cercana en el tamaño p_n viene dada por la *desigualdad de* BONSE, que establece que

$$p_n^2 < p_1 p_2 \cdots p_{n-1}, \qquad \text{para } n \geq 5.$$

Esta desigualdad produce $p_5^2 < 210$, ó $p_5 \leq 14$. Una mejor estimación del tamaño del primo p_n proviene de la desigualdad

$$p_{2n} \leq p_2 p_3 \cdots p_n - 2, \qquad \text{para } n \geq 3.$$

La estimación es bastante exagerada. Una limitación un poco más cercana en el tamaño p_n viene dada por la *desigualdad de* BONSE, que establece que

$$p_n^2 < p_1 p_2 \cdots p_{n-1}, \qquad \text{para } n \geq 5.$$

Esta desigualdad produce $p_5^2 < 210$, ó $p_5 \leq 14$. Una mejor estimación del tamaño del primo p_n proviene de la desigualdad

$$p_{2n} \leq p_2 p_3 \cdots p_n - 2, \qquad \text{para } n \geq 3.$$

Aquí obtenemos $p_5 < p_6 \leq p_2 p_3 - 2 = 3 \cdot 5 - 2 = 13$, de modo que $p_5 \leq 12$.

Primos

La estimación es bastante exagerada. Una limitación un poco más cercana en el tamaño p_n viene dada por la *desigualdad de* BONSE, que establece que

$$p_n^2 < p_1 p_2 \cdots p_{n-1}, \qquad \text{para } n \geq 5.$$

Esta desigualdad produce $p_5^2 < 210$, ó $p_5 \leq 14$. Una mejor estimación del tamaño del primo p_n proviene de la desigualdad

$$p_{2n} \leq p_2 p_3 \cdots p_n - 2, \qquad \text{para } n \geq 3.$$

Aquí obtenemos $p_5 < p_6 \leq p_2 p_3 - 2 = 3 \cdot 5 - 2 = 13$, de modo que $p_5 \leq 12$.

Para aproximar p_n a partir de estas fórmulas, es necesario conocer los valores de $p_1, p_2, \ldots, ..., p_{n-1}$.

Primos

La estimación es bastante exagerada. Una limitación un poco más cercana en el tamaño p_n viene dada por la *desigualdad de* BONSE, que establece que

$$p_n^2 < p_1 p_2 \cdots p_{n-1}, \qquad \text{para } n \geq 5.$$

Esta desigualdad produce $p_5^2 < 210$, ó $p_5 \leq 14$. Una mejor estimación del tamaño del primo p_n proviene de la desigualdad

$$p_{2n} \leq p_2 p_3 \cdots p_n - 2, \qquad \text{para } n \geq 3.$$

Aquí obtenemos $p_5 < p_6 \leq p_2 p_3 - 2 = 3 \cdot 5 - 2 = 13$, de modo que $p_5 \leq 12$.

Para aproximar p_n a partir de estas fórmulas, es necesario conocer los valores de $p_1, p_2, \ldots, ..., p_{n-1}$. Para una cota en la que los números primos anteriores no intervienen, tenemos el siguiente teorema

Teorema

Si p_n es el n-ésimo número primo, entonces $p_n \leq 2^{2^{n-1}}$.

Teorema

Si p_n es el n-ésimo número primo, entonces $p_n \leq 2^{2^{n-1}}$.

Prueba: Por inducción sobre n.

Teorema

Si p_n es el n-ésimo número primo, entonces $p_n \leq 2^{2^{n-1}}$.

Prueba: Por inducción sobre n. Para $n = 1$, $p_1 = 2 \leq 2^{2^0}$.

Teorema

Si p_n es el n-ésimo número primo, entonces $p_n \leq 2^{2^{n-1}}$.

Prueba: Por inducción sobre n. Para $n = 1$, $p_1 = 2 \leq 2^{2^0}$. Asuminos como hipótesis de inducción, que $n > 1$ y que el el resultado es válido para todos los enteros hasta n.

Teorema

Si p_n es el n-ésimo número primo, entonces $p_n \leq 2^{2^{n-1}}$.

Prueba: Por inducción sobre n. Para $n = 1$, $p_1 = 2 \leq 2^{2^0}$. Asuminos como hipótesis de inducción, que $n > 1$ y que el el resultado es válido para todos los enteros hasta n. Luego

$$p_{n+1} \leq p_1 p_2 \cdots p_n + 1 \leq 2 \cdot 2^2 \cdot 2^4 \cdots 2^{2^{n-1}} + 1 = 2^{1+2+4+\ldots 2^{n-1}} + 1 = 2^{2^{n-1}} + 1.$$

Teorema

Si p_n es el n-ésimo número primo, entonces $p_n \leq 2^{2^{n-1}}$.

<u>Prueba</u>: Por inducción sobre n. Para $n = 1$, $p_1 = 2 \leq 2^{2^0}$. Asuminos como hipótesis de inducción, que $n > 1$ y que el el resultado es válido para todos los enteros hasta n. Luego

$$p_{n+1} \leq p_1 p_2 \cdots p_n + 1 \leq 2 \cdot 2^2 \cdot 2^4 \cdots 2^{2^{n-1}} + 1 = 2^{1+2+4+\ldots 2^{n-1}} + 1 = 2^{2^{n-1}} + 1.$$

Como $1 \leq 2^{2^{n-1}}$, para todo n, entonces

$$p_{n+1} \leq 2^{2^{n-1}} + 1 \leq 2^{2^{n-1}} + 2^{2^{n-1}} = 2^{2^n}. \quad \square$$

Teorema

Si p_n es el n-ésimo número primo, entonces $p_n \leq 2^{2^{n-1}}$.

Prueba: Por inducción sobre n. Para $n = 1$, $p_1 = 2 \leq 2^{2^0}$. Asuminos como hipótesis de inducción, que $n > 1$ y que el el resultado es válido para todos los enteros hasta n. Luego

$$p_{n+1} \leq p_1 p_2 \cdots p_n + 1 \leq 2 \cdot 2^2 \cdot 2^4 \cdots 2^{2^{n-1}} + 1 = 2^{1+2+4+\ldots 2^{n-1}} + 1 = 2^{2^{n-1}} + 1.$$

Como $1 \leq 2^{2^{n-1}}$, para todo n, entonces

$$p_{n+1} \leq 2^{2^{n-1}} + 1 \leq 2^{2^{n-1}} + 2^{2^{n-1}} = 2^{2^n}. \quad \square$$

Corolario

Para $n \geq 1$, hay al menos $n + 1$ primos menores que 2^{2^n}.

Teorema

Si p_n es el n-ésimo número primo, entonces $p_n \leq 2^{2^{n-1}}$.

Prueba: Por inducción sobre n. Para $n = 1$, $p_1 = 2 \leq 2^{2^0}$. Asuminos como hipótesis de inducción, que $n > 1$ y que el el resultado es válido para todos los enteros hasta n. Luego

$$p_{n+1} \leq p_1 p_2 \cdots p_n + 1 \leq 2 \cdot 2^2 \cdot 2^4 \cdots 2^{2^{n-1}} + 1 = 2^{1+2+4+\ldots 2^{n-1}} + 1 = 2^{2^{n-1}} + 1.$$

Como $1 \leq 2^{2^{n-1}}$, para todo n, entonces

$$p_{n+1} \leq 2^{2^{n-1}} + 1 \leq 2^{2^{n-1}} + 2^{2^{n-1}} = 2^{2^n}. \quad \square$$

Corolario

Para $n \geq 1$, hay al menos $n+1$ primos menores que 2^{2^n}.

Prueba: Del teorema, $p_1, p_2, \ldots, p_{n+1}$ son todos menores que 2^{2^n}.

Primos

Hay estimativas mejores. En 1845, J. BERTRAND conjeturó que los números primos están bien distribuidos en el sentido de que entre n y $2n$, $n \geq 2$ hay al menos un primo. (Verificado por Bertrand hasta $n < 3 \times 10^6$, probado por TCHEBYSHEFF en 1852).

Primos

Hay estimativas mejores. En 1845, J. Bertrand conjeturó que los números primos están bien distribuidos en el sentido de que entre n y $2n$, $n \geq 2$ hay al menos un primo. (Verificado por Bertrand hasta $n < 3 \times 10^6$, probado por Tchebysheff en 1852).

Con el postulado de Bertrand, se demuestra que $p_n < 2^n$, para $n \geq 2$; y, como consecuencia directa, que $p_{n+1} < 2p_n$, $n \geq 2$.

Primos

Hay estimativas mejores. En 1845, J. Bertrand conjeturó que los números primos están bien distribuidos en el sentido de que entre n y $2n$, $n \geq 2$ hay al menos un primo. (Verificado por Bertrand hasta $n < 3 \times 10^6$, probado por Tchebysheff en 1852).

Con el postulado de Bertrand, se demuestra que $p_n < 2^n$, para $n \geq 2$; y, como consecuencia directa, que $p_{n+1} < 2p_n$, $n \geq 2$. En particular, $11 = p_5 < 2 \cdot p_4 = 14$.

Primos

Hay estimativas mejores. En 1845, J. BERTRAND conjeturó que los números primos están bien distribuidos en el sentido de que entre n y $2n$, $n \geq 2$ hay al menos un primo. (Verificado por Bertrand hasta $n < 3 \times 10^6$, probado por TCHEBYSHEFF en 1852).

Con el postulado de Bertrand, se demuestra que $p_n < 2^n$, para $n \geq 2$; y, como consecuencia directa, que $p_{n+1} < 2p_n$, $n \geq 2$. En particular, $11 = p_5 < 2 \cdot p_4 = 14$.

Primos

La fascinación por los números primos ha llevado a estudiar tipos particulares de primos:

- primos *gemelos*, de la forma $p, p+2$.
- primos de Fermat, de la forma $F_n = 2^{2^n} + 1$.
- primos de Mersenne, de la forma $M_n = 2^n - 1$.
- primos de Sophie Germain, primo p tal que $2p+1$ también es primo.
- primos de Fibonacci, si son parte de la secuencia $F_{n+1} = F_n + F_{n-1}$, $F_1 = 1$, $F_2 = 2$.
- primos de Lucas, son parte de la secuencia de Lucas $L_{n+1} = L_n + L_{n-1}$, $L_1 = 2$, $L_2 = 1$.
- primos de Ramanujan.

Primos

Primos de Fermat: $2^{2^n}+1$.

$$2^{2^0}+1=3,\quad 2^{2^1}+1=5,\quad 2^{2^2}+1=17,\quad 2^{2^3}+1=257,\quad 2^{2^4}+1=65537,$$
$$2^{2^5}+1=4294967297=641\cdot 6700417,\ \ldots$$

Primos

Primos de Fermat: $2^{2^n}+1$.

$$2^{2^0}+1=3,\quad 2^{2^1}+1=5,\quad 2^{2^2}+1=17,\quad 2^{2^3}+1=257,\quad 2^{2^4}+1=65537,$$
$$2^{2^5}+1=4294967297=641\cdot 6700417,\ \ldots$$

Primos de Mersenne: 2^n-1.

$$2^2-1=3,\quad 2^3-1=7,\quad 2^5-1=31,\quad 2^7-1=127,\quad 2^{11}-1=2047$$

Primos de Fermat: $2^{2^n}+1$.

$$2^{2^0}+1=3,\quad 2^{2^1}+1=5,\quad 2^{2^2}+1=17,\quad 2^{2^3}+1=257,\quad 2^{2^4}+1=65537,$$
$$2^{2^5}+1=4294967297=641\cdot 6700417,\ \ldots$$

Primos de Mersenne: 2^n-1.

$$2^2-1=3,\quad 2^3-1=7,\quad 2^5-1=31,\quad 2^7-1=127,\quad 2^{11}-1=2047=23\cdot 89,\ \ldots$$

Primos

Primos de $\textsc{Fermat}$: $2^{2^n}+1$.

$$2^{2^0}+1=3, \quad 2^{2^1}+1=5, \quad 2^{2^2}+1=17, \quad 2^{2^3}+1=257, \quad 2^{2^4}+1=65537,$$
$$2^{2^5}+1=4294967297=641\cdot 6700417, \ \ldots$$

Primos de $\textsc{Mersenne}$: 2^n-1.

$$2^2-1=3, \quad 2^3-1=7, \quad 2^5-1=31, \quad 2^7-1=127, \quad 2^{11}-1=2047=23\cdot 89, \ \ldots$$

Conjeturas como estas, han llevado por muchos años a la búsque de números primos cada vez mayores, (por ejemplo los proyectos *GIMPS* o *PrimeGrid*).

Primos

Primos de Fermat: $2^{2^n}+1$.

$$2^{2^0}+1=3,\quad 2^{2^1}+1=5,\quad 2^{2^2}+1=17,\quad 2^{2^3}+1=257,\quad 2^{2^4}+1=65537,$$
$$2^{2^5}+1=4294967297=641\cdot 6700417,\ \ldots$$

Primos de Mersenne: 2^n-1.

$$2^2-1=3,\quad 2^3-1=7,\quad 2^5-1=31,\quad 2^7-1=127,\quad 2^{11}-1=2047=23\cdot 89,\ \ldots$$

Conjeturas como estas, han llevado por muchos años a la búsque de números primos cada vez mayores, (por ejemplo los proyectos *GIMPS* o *PrimeGrid*).

Al día de hoy, el mayor primo conocido es

Número	Expansión decimal	Dígitos	Año	Descubridor
$M_{82589933}$	14889444...17902591	24,862,048	2018 (of 12.2020)	GIMPS, Patrick Laroche

UNIVERSIDAD DEL VALLE DE GUATEMALA

Conjeturas y Problemas acerca de primos:
Los *Problemas de Landau* son cuatro problemas básicos conocidos sobre números primos, que E. Landau catalogó como "inabarcables en el estado actual de la ciencia" durante el 5° ICM, en 1912.

Primos

Conjeturas y Problemas acerca de primos:
Los *Problemas de Landau* son cuatro problemas básicos conocidos sobre números primos, que E. LANDAU catalogó como "inabarcables en el estado actual de la ciencia" durante el 5° ICM, en 1912.

Los cuatro problemas son los siguientes:

- La **conjetura de** GOLDBACH, que establece que todos los números pares mayores que 2 se pueden expresar como la suma de dos números primos.

UNIVERSIDAD DEL VALLE DE GUATEMALA

Primos

Conjeturas y Problemas acerca de primos:
Los *Problemas de Landau* son cuatro problemas básicos conocidos sobre números primos, que E. LANDAU catalogó como "inabarcables en el estado actual de la ciencia" durante el 5° ICM, en 1912.

Los cuatro problemas son los siguientes:

- La **conjetura de** GOLDBACH, que establece que todos los números pares mayores que 2 se pueden expresar como la suma de dos números primos.
- La **conjetura de los primos gemelos**, que establece que hay infinitos números primos p tales que $p + 2$ también es primo.

Primos

Conjeturas y Problemas acerca de primos:
Los *Problemas de Landau* son cuatro problemas básicos conocidos sobre números primos, que E. LANDAU catalogó como "inabarcables en el estado actual de la ciencia" durante el 5° ICM, en 1912.

Los cuatro problemas son los siguientes:

- La **conjetura de** GOLDBACH, que establece que todos los números pares mayores que 2 se pueden expresar como la suma de dos números primos.
- La **conjetura de los primos gemelos**, que establece que hay infinitos números primos p tales que $p+2$ también es primo.
- La **conjetura de** LEGENDRE, que establece que siempre existe un número primo entre dos cuadrados perfectos.

Conjeturas y Problemas acerca de primos:
Los *Problemas de Landau* son cuatro problemas básicos conocidos sobre números primos, que E. LANDAU catalogó como "inabarcables en el estado actual de la ciencia" durante el 5° ICM, en 1912.

Los cuatro problemas son los siguientes:

- La **conjetura de** GOLDBACH, que establece que todos los números pares mayores que 2 se pueden expresar como la suma de dos números primos.
- La **conjetura de los primos gemelos**, que establece que hay infinitos números primos p tales que $p + 2$ también es primo.
- La **conjetura de** LEGENDRE, que establece que siempre existe un número primo entre dos cuadrados perfectos.
- La conjetura de que hay infinitos números primos p tales que $p - 1$ es un cuadrado perfecto. Dicho de otra forma, hay infinitos primos de la forma $n^2 + 1$.

Hasta la fecha, ninguno de estos problemas ha sido resuelto.

Primos

Fórmulas que producen primos:
No se conoce una fórmula simple para generar primos.

Fórmulas que producen primos:
No se conoce una fórmula simple para generar primos. Una de estas fórmulas es

$$p_n = \left\lfloor 1 - \frac{1}{\log 2} \log \Big(-\frac{1}{2} + \sum_{d|P_{n-1}} \frac{\mu(d)}{2^d - 1} \Big) \right\rfloor,$$

donde $P_{n-1} = p_1 p_2 \cdots p_{n-1}$.

Fórmulas que producen primos:
No se conoce una fórmula simple para generar primos. Una de estas fórmulas es

$$p_n = \left\lfloor 1 - \frac{1}{\log 2} \log\left(-\frac{1}{2} + \sum_{d \mid P_{n-1}} \frac{\mu(d)}{2^d - 1} \right) \right\rfloor,$$

donde $P_{n-1} = p_1 p_2 \cdots p_{n-1}$.

Otra fórmula

$$p_n = \lfloor 10^{2^n} c \rfloor - 10^{2^{n-1}} \lfloor 10^{2^{n-1}} c \rfloor,$$

donde $c = \sum_{n \geq 1} \frac{p_n}{10^{2^n}} = 0.0203000500000007\ldots$

Fórmulas que producen primos:
No se conoce una fórmula simple para generar primos. Una de estas fórmulas es

$$p_n = \left\lfloor 1 - \frac{1}{\log 2} \log \left(-\frac{1}{2} + \sum_{d \mid P_{n-1}} \frac{\mu(d)}{2^d - 1} \right) \right\rfloor,$$

donde $P_{n-1} = p_1 p_2 \cdots p_{n-1}$.

Otra fórmula

$$p_n = \lfloor 10^{2^n} c \rfloor - 10^{2^{n-1}} \lfloor 10^{2^{n-1}} c \rfloor,$$

donde $c = \sum_{n \geq 1} \frac{p_n}{10^{2^n}} = 0.0203000500000007\ldots$

Un resultado de Mills establece lo siguiente: Existe una constante $A \in \mathbb{R}$ tal que $\lfloor A^{3^n} \rfloor$ es primo, para todo $n \geq 1$.

Primos

Otro ejemplo famoso es el polinomio $x^2 + x + 41$ (Euler, 1774).

Primos

Otro ejemplo famoso es el polinomio $x^2 + x + 41$ (EULER, 1774). Produce primos para $x = 1, 2, \ldots, 39$.

Primos

Otro ejemplo famoso es el polinomio $x^2 + x + 41$ (Euler, 1774). Produce primos para $x = 1, 2, \ldots, 39$.

Distribución de los números primos:

- El **Teorema de los Números Primos**: Generar fórmulas para contar o para estimar $\pi(x)$, el número de primos $2 \leq p \leq x$.

Primos

Otro ejemplo famoso es el polinomio $x^2 + x + 41$ (Euler, 1774). Produce primos para $x = 1, 2, \ldots, 39$.

Distribución de los números primos:

- El **Teorema de los Números Primos**: Generar fórmulas para contar o para estimar $\pi(x)$, el número de primos $2 \leq p \leq x$.
- Se sabe que existen infinitos primos de la forma $4n + 1$, y que existen infinitos primos de la forma $4n + 3$.

Primos

Otro ejemplo famoso es el polinomio $x^2 + x + 41$ (Euler, 1774). Produce primos para $x = 1, 2, \ldots, 39$.

Distribución de los números primos:

- El **Teorema de los Números Primos**: Generar fórmulas para contar o para estimar $\pi(x)$, el número de primos $2 \leq p \leq x$.
- Se sabe que existen infinitos primos de la forma $4n + 1$, y que existen infinitos primos de la forma $4n + 3$. ¿Existe la misma proporcion de ellos? ¿Hay más de un tipo que del otro?

Primos

Otro ejemplo famoso es el polinomio $x^2 + x + 41$ (EULER, 1774). Produce primos para $x = 1, 2, \dots, 39$.

Distribución de los números primos:

- El **Teorema de los Números Primos**: Generar fórmulas para contar o para estimar $\pi(x)$, el número de primos $2 \leq p \leq x$.
- Se sabe que existen infinitos primos de la forma $4n + 1$, y que existen infinitos primos de la forma $4n + 3$. ¿Existe la misma proporcion de ellos? ¿Hay más de un tipo que del otro?
- El **Teorema de Dirichlet**: Dados $a, d \in \mathbb{N}$, con $(a, d) = 1$. ¿Existen infinitos primos de la forma $dn + a$, $n \in \mathbb{N}$.

Primos

Otro ejemplo famoso es el polinomio $x^2 + x + 41$ (Euler, 1774). Produce primos para $x = 1, 2, \ldots, 39$.

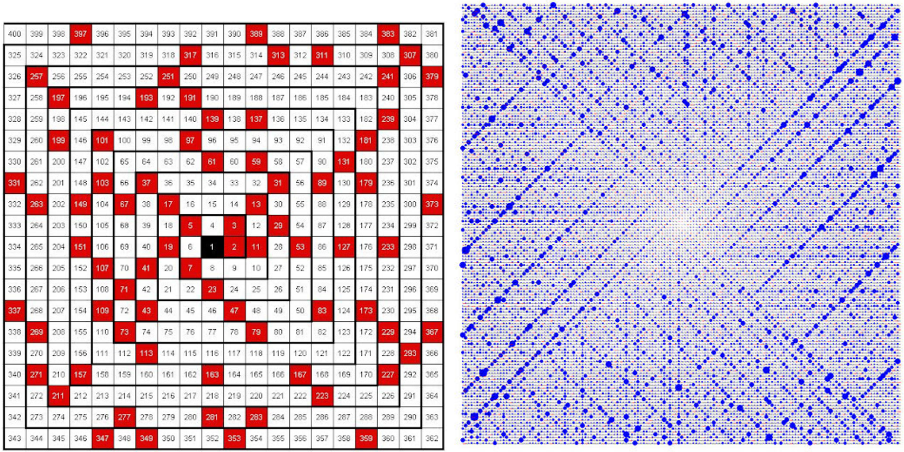
Distribución de los números primos:

- El **Teorema de los Números Primos**: Generar fórmulas para contar o para estimar $\pi(x)$, el número de primos $2 \leq p \leq x$.
- Se sabe que existen infinitos primos de la forma $4n + 1$, y que existen infinitos primos de la forma $4n + 3$. ¿Existe la misma proporcion de ellos? ¿Hay más de un tipo que del otro?
- El **Teorema de Dirichlet**: Dados $a, d \in \mathbb{N}$, con $(a, d) = 1$. ¿Existen infinitos primos de la forma $dn + a$, $n \in \mathbb{N}$.
- Estudiar la proporción de primos en secuencias de la forma $\{dn + a\}$, $n \in \mathbb{N}$.

Primos

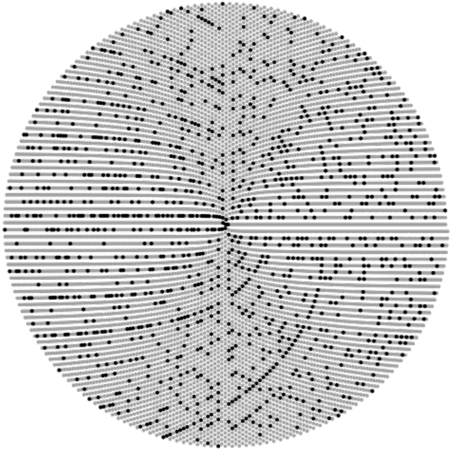
400	399	398	397	396	395	394	393	392	391	390	389	388	387	386	385	384	383	382	381
325	324	323	322	321	320	319	318	317	316	315	314	313	312	311	310	309	308	307	380
326	257	256	255	254	253	252	251	250	249	248	247	246	245	244	243	242	241	306	379
327	258	197	196	195	194	193	192	191	190	189	188	187	186	185	184	183	240	305	378
328	259	198	145	144	143	142	141	140	139	138	137	136	135	134	133	182	239	304	377
329	260	199	146	101	100	99	98	97	96	95	94	93	92	91	132	181	238	303	376
330	261	200	147	102	65	64	63	62	61	60	59	58	57	90	131	180	237	302	375
331	262	201	148	103	66	37	36	35	34	33	32	31	56	89	130	179	236	301	374
332	263	202	149	104	67	38	17	16	15	14	13	30	55	88	129	178	235	300	373
333	264	203	150	105	68	39	18	5	4	3	12	29	54	87	128	177	234	299	372
334	265	204	151	106	69	40	19	6	1	2	11	28	53	86	127	176	233	298	371
335	266	205	152	107	70	41	20	7	8	9	10	27	52	85	126	175	232	297	370
336	267	206	153	108	71	42	21	22	23	24	25	26	51	84	125	174	231	296	369
337	268	207	154	109	72	43	44	45	46	47	48	49	50	83	124	173	230	295	368
338	269	208	155	110	73	74	75	76	77	78	79	80	81	82	123	172	229	294	367
339	270	209	156	111	112	113	114	115	116	117	118	119	120	121	122	171	228	293	366
340	271	210	157	158	159	160	161	162	163	164	165	166	167	168	169	170	227	292	365
341	272	211	212	213	214	215	216	217	218	219	220	221	222	223	224	225	226	291	364
342	273	274	275	276	277	278	279	280	281	282	283	284	285	286	287	288	289	290	363
343	344	345	346	347	348	349	350	351	352	353	354	355	356	357	358	359	360	361	362

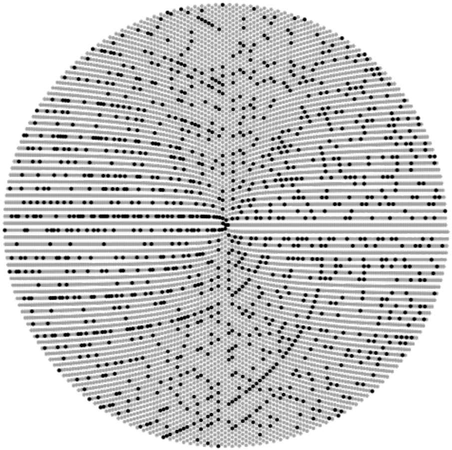
Primos

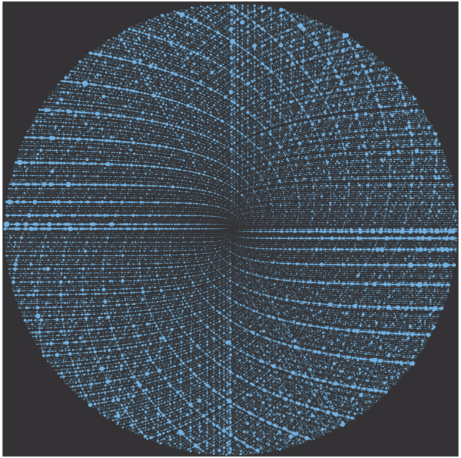


Espiral de ULAM. Ver `https://www.youtube.com/watch?v=iFuR97YcSLM`

Primos

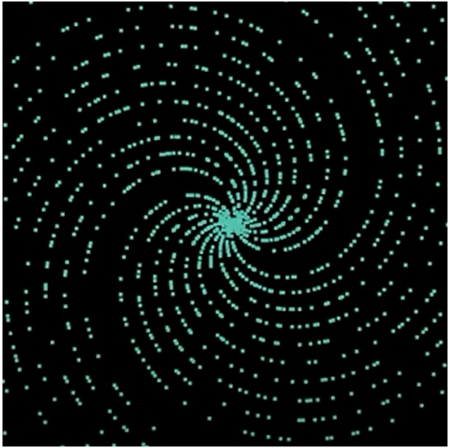


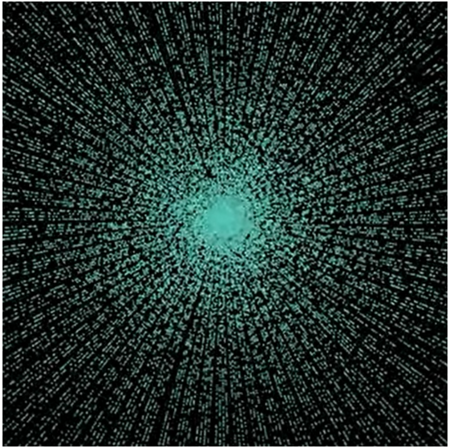




Espiral de SACKS.

Primos





Otros patrones de primos. Ver `https://www.youtube.com/watch?v=EK32jo7i5LQ`