La importancia de ser primo

Maratón matemático

Fernando Chamizo Lorente

Universidad Autónoma de Madrid
http://www.uam.es/fernando.chamizo

22 de febrero de 2007

Índice

Definición básica

Definición

Un número primo es aquel que sólo es divisible por él mismo y por la unidad.

Definición básica

Definición

Un número primo es aquel que sólo es divisible por él mismo y por la unidad.

Nota: Desde el siglo XIX se excluye el 1 de los primos por convenio.

Definición básica

Definición

Un número primo es aquel que sólo es divisible por él mismo y por la unidad.

Nota: Desde el siglo XIX se excluye el 1 de los primos por convenio.

Son los números malos para hacer repartos.

Definición básica

Definición

Un número primo es aquel que sólo es divisible por él mismo y por la unidad.

Nota: Desde el siglo XIX se excluye el 1 de los primos por convenio.

Son los números malos para hacer repartos.

Propiedad fundamental:
Los primos son los bloques con los que están compuestos el resto de los números naturales.

Algunas propiedades

Pequeño teorema de Fermat

Si p es primo, entonces p divide a $n^p - n$ para cualquier n.

Algunas propiedades

Pequeño teorema de Fermat

Si p es primo, entonces p divide a $n^p - n$ para cualquier n.

$$n = 2 \qquad p = 3 \qquad 3 | 2^3 - 2$$

Algunas propiedades

Pequeño teorema de Fermat

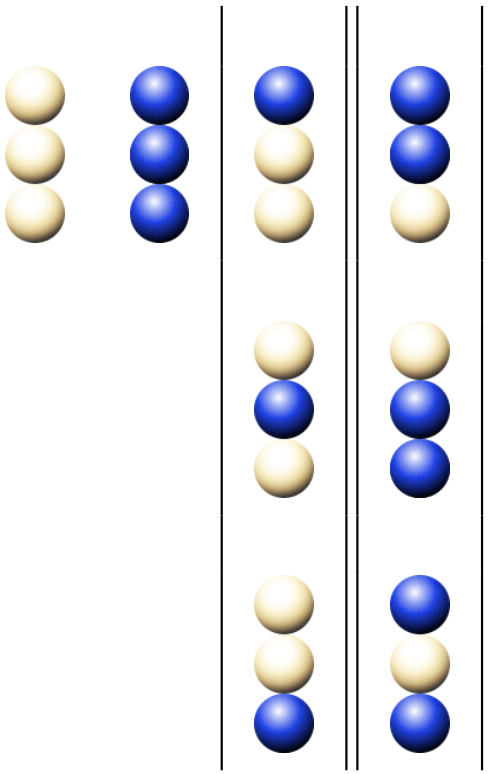
Si p es primo, entonces p divide a $n^p - n$ para cualquier n.

$$n = 2 \text{ (colores)} \quad p = 3 \text{ (cuentas)}$$

Algunas propiedades

Pequeño teorema de Fermat

Si p es primo, entonces p divide a $n^p - n$ para cualquier n.



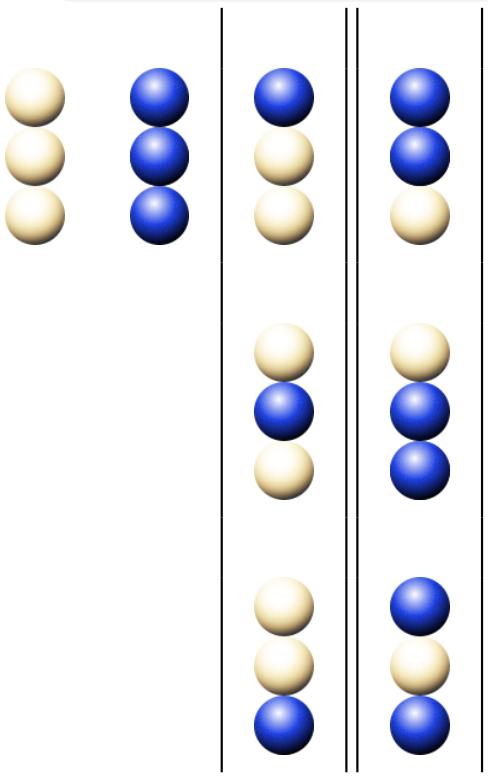
$n = 2$ (colores) $p = 3$ (cuentas)

- n. de tiras $= 2 \times 2 \times 2 = n^p$

Algunas propiedades

Pequeño teorema de Fermat

Si p es primo, entonces p divide a $n^p - n$ para cualquier n.



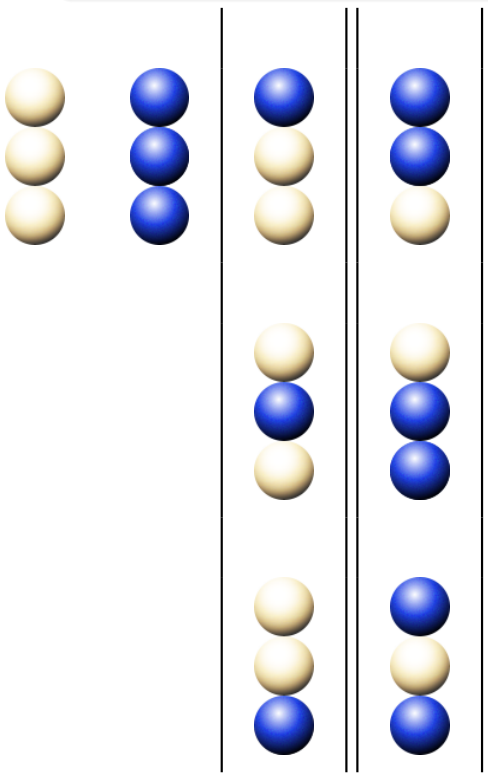
$n = 2$ (colores) $p = 3$ (cuentas)

- n. de tiras $= 2 \times 2 \times 2 = n^p$
- n. de collares $= \frac{2\times2\times2-2}{3} + 2 = \frac{n^p-n}{p} + n$

Algunas propiedades

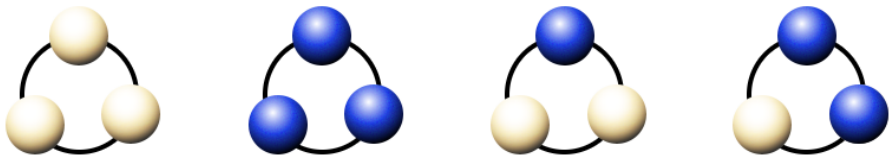
Pequeño teorema de Fermat

Si p es primo, entonces p divide a $n^p - n$ para cualquier n.



$n = 2$ (colores) $p = 3$ (cuentas)

- n. de tiras $= 2 \times 2 \times 2 = n^p$
- n. de collares $= \frac{2\times2\times2-2}{3} + 2 = \frac{n^p-n}{p} + n$



Algunas propiedades

- Se cumple la igualdad $\prod (1 - \frac{1}{p^2}) = \frac{6}{\pi^2}$.

Algunas propiedades

- Se cumple la igualdad $\prod (1 - \frac{1}{p^2}) = \frac{6}{\pi^2}$.
- Un número n es primo si y sólo si divide a $(n-1)! + 1$.

Algunas propiedades

- Se cumple la igualdad $\prod (1 - \frac{1}{p^2}) = \frac{6}{\pi^2}$.
- Un número n es primo si y sólo si divide a $(n-1)! + 1$.
- Los números primos de la forma $20n + 1$ y $20n + 9$ son exactamente los que se pueden representar como $a^2 + 5b^2$.
  (Ej. $61 = 20 \cdot 3 + 1 = 4^2 + 5 \cdot 3^2$, $389 = 20 \cdot 19 + 9 = 12^2 + 5 \cdot 7^2$)

Algunas propiedades

- Se cumple la igualdad $\prod (1 - \frac{1}{p^2}) = \frac{6}{\pi^2}$.
- Un número n es primo si y sólo si divide a $(n-1)! + 1$.
- Los números primos de la forma $20n + 1$ y $20n + 9$ son exactamente los que se pueden representar como $a^2 + 5b^2$.
  (Ej. $61 = 20 \cdot 3 + 1 = 4^2 + 5 \cdot 3^2$, $389 = 20 \cdot 19 + 9 = 12^2 + 5 \cdot 7^2$)
- Si el desarrollo decimal de $1/n$ tiene periodo máximo $(= n - 1)$ entonces n es primo.

Algunas propiedades

- Se cumple la igualdad $\prod (1 - \frac{1}{p^2}) = \frac{6}{\pi^2}$.
- Un número n es primo si y sólo si divide a $(n-1)! + 1$.
- Los números primos de la forma $20n + 1$ y $20n + 9$ son exactamente los que se pueden representar como $a^2 + 5b^2$.
  (Ej. $61 = 20 \cdot 3 + 1 = 4^2 + 5 \cdot 3^2$, $389 = 20 \cdot 19 + 9 = 12^2 + 5 \cdot 7^2$)
- Si el desarrollo decimal de $1/n$ tiene periodo máximo $(= n - 1)$ entonces n es primo.

$$\frac{1}{7} = 0'\overline{142857}\ldots \qquad \frac{1}{17} = 0'\overline{0588235294117647}\ldots$$

Algunas propiedades

- Se cumple la igualdad $\prod (1 - \frac{1}{p^2}) = \frac{6}{\pi^2}$.
- Un número n es primo si y sólo si divide a $(n-1)! + 1$.
- Los números primos de la forma $20n + 1$ y $20n + 9$ son exactamente los que se pueden representar como $a^2 + 5b^2$.
  (Ej. $61 = 20 \cdot 3 + 1 = 4^2 + 5 \cdot 3^2$, $389 = 20 \cdot 19 + 9 = 12^2 + 5 \cdot 7^2$)
- Si el desarrollo decimal de $1/n$ tiene periodo máximo $(= n - 1)$ entonces n es primo.

$$\frac{1}{7} = 0'\overline{142857}\ldots \qquad \frac{1}{17} = 0'\overline{0588235294117647}\ldots$$

Algunas propiedades

- Se cumple la igualdad $\prod (1 - \frac{1}{p^2}) = \frac{6}{\pi^2}$.
- Un número n es primo si y sólo si divide a $(n-1)! + 1$.
- Los números primos de la forma $20n + 1$ y $20n + 9$ son exactamente los que se pueden representar como $a^2 + 5b^2$.
  (Ej. $61 = 20 \cdot 3 + 1 = 4^2 + 5 \cdot 3^2$, $389 = 20 \cdot 19 + 9 = 12^2 + 5 \cdot 7^2$)
- Si el desarrollo decimal de $1/n$ tiene periodo máximo $(= n - 1)$ entonces n es primo.

$$\frac{1}{7} = 0'\overline{142857}\ldots \qquad \begin{matrix} 857 \\ \hline 999 \end{matrix}$$

$$\frac{1}{17} = 0'\overline{0588235294117647}\ldots \qquad \begin{matrix} 94117647 \\ \hline 99999999 \end{matrix}$$

Criptografía RSA

La criptografia se basa en funciones trampa: operaciones fáciles de hacer y muy difíciles de deshacer sin datos especiales.

Criptografía RSA

La criptografia se basa en funciones trampa: operaciones fáciles de hacer y muy difíciles de deshacer sin datos especiales.

Criptografía RSA

La criptografia se basa en funciones trampa: operaciones fáciles de hacer y muy difíciles de deshacer sin datos especiales.

p, q primos de cientos de cifras, $n = p \cdot q$, $m = (p-1) \cdot (q-1)$, c = arbitrario sin factores comunes con m.

Criptografía RSA

La criptografia se basa en funciones trampa: operaciones fáciles de hacer y muy difíciles de deshacer sin datos especiales.

p, q primos de cientos de cifras, $n = p \cdot q$, $m = (p-1) \cdot (q-1)$, c = arbitrario sin factores comunes con m.

Cosas fáciles y difíciles

- Dados p y q hallar n y m
- Dados n hallar p y q o hallar m
- Dado m resolver $cx = 1 +$ mult. de m
- Dado n resolver $cx = 1 +$ mult. de m

Criptografía RSA

La criptografia se basa en funciones trampa: operaciones fáciles de hacer y muy difíciles de deshacer sin datos especiales.

p, q primos de cientos de cifras, $n = p \cdot q$, $m = (p-1) \cdot (q-1)$, c = arbitrario sin factores comunes con m.

Cosas fáciles y difíciles

- F Dados p y q hallar n y m
- Dados n hallar p y q o hallar m
- Dado m resolver $cx = 1 +$ mult. de m
- Dado n resolver $cx = 1 +$ mult. de m

Criptografía RSA

La criptografia se basa en funciones trampa: operaciones fáciles de hacer y muy difíciles de deshacer sin datos especiales.

p, q primos de cientos de cifras, $n = p \cdot q$, $m = (p-1) \cdot (q-1)$, c = arbitrario sin factores comunes con m.

Cosas fáciles y difíciles

- F Dados p y q hallar n y m
- D Dados n hallar p y q o hallar m
- Dado m resolver $cx = 1 +$ mult. de m
- Dado n resolver $cx = 1 +$ mult. de m

Criptografía RSA

La criptografia se basa en funciones trampa: operaciones fáciles de hacer y muy difíciles de deshacer sin datos especiales.

p, q primos de cientos de cifras, $n = p \cdot q$, $m = (p-1) \cdot (q-1)$, c = arbitrario sin factores comunes con m.

Cosas fáciles y difíciles

- F Dados p y q hallar n y m
- D Dados n hallar p y q o hallar m
- F Dado m resolver $cx = 1 +$ mult. de m
- Dado n resolver $cx = 1 +$ mult. de m

Criptografía RSA

La criptografia se basa en funciones trampa: operaciones fáciles de hacer y muy difíciles de deshacer sin datos especiales.

p, q primos de cientos de cifras, $n = p \cdot q$, $m = (p-1) \cdot (q-1)$, c = arbitrario sin factores comunes con m.

Cosas fáciles y difíciles

- F Dados p y q hallar n y m
- D Dados n hallar p y q o hallar m
- F Dado m resolver $cx = 1 +$ mult. de m
- D Dado n resolver $cx = 1 +$ mult. de m

Criptografía RSA

$n = pq, \quad m = (p-1)(q-1)$

$c \longrightarrow$ cerrojo, $\quad d \longrightarrow$ llave, $\quad cd = 1 + km$

$M =$Mensaje, $\quad M < n$ sin factores comunes

Criptografía RSA

$n = pq, \quad m = (p-1)(q-1)$

$c \longrightarrow$ cerrojo, $\quad d \longrightarrow$ llave, $\quad cd = 1 + km$

$M =$Mensaje, $\quad M < n$ sin factores comunes

Codif. (pública): resto de $M^c \div n$

Desc. (privada): resto de $(M^c)^d \div n$

Criptografía RSA

$n = pq, \quad m = (p-1)(q-1)$

$c \longrightarrow$ cerrojo, $\quad d \longrightarrow$ llave, $\quad cd = 1 + km$

$M =$Mensaje, $\quad M < n$ sin factores comunes

Codif. (pública): resto de $M^c \div n$

Desc. (privada): resto de $(M^c)^d \div n$

$n = 5 \cdot 7,\ m = 24,\ c = d = 5$

$2^5 \mapsto 32$

$32^5 \mapsto (-3)^5 = 35 \cdot 7 + 2 \mapsto 2$

Criptografía RSA

$n = pq, \quad m = (p-1)(q-1)$

$c \longrightarrow$ cerrojo, $\quad d \longrightarrow$ llave, $\quad cd = 1 + km$

$M =$Mensaje, $\quad M < n$ sin factores comunes

Codif. (pública): resto de $M^c \div n$

Desc. (privada): resto de $(M^c)^d \div n$

$n = 5 \cdot 7,\ m = 24,\ c = d = 5$

$2^5 \mapsto 32$

$32^5 \mapsto (-3)^5 = 35 \cdot 7 + 2 \mapsto 2$

¿Por qué funciona?

$$M^{cd} = M^{1+km} = nM\frac{M^{km}-1}{n} + M = \text{múltiplo de } n + M$$

Criptografía RSA

$n = pq, \quad m = (p-1)(q-1)$

$c \longrightarrow$ cerrojo, $\quad d \longrightarrow$ llave, $\quad cd = 1 + km$

$M =$Mensaje, $\quad M < n$ sin factores comunes

Codif. (pública): resto de $M^c \div n$

Desc. (privada): resto de $(M^c)^d \div n$

$n = 5 \cdot 7,\ m = 24,\ c = d = 5$

$2^5 \mapsto 32$

$32^5 \mapsto (-3)^5 = 35 \cdot 7 + 2 \mapsto 2$

¿Por qué funciona?

$$M^{cd} = M^{1+km} = nM\frac{M^{km}-1}{n} + M = \text{múltiplo de } n + M$$

Distribución de los primos

¿Están los números primos distribuidos “al azar”?

Distribución de los primos

¿Están los números primos distribuidos "al azar"?

$$\prod (1 - \frac{1}{p^2}) = \frac{6}{\pi^2}$$

Distribución de los primos

¿Están los números primos distribuidos "al azar"?

Gauss 1849

La densidad de los primos de tamaño x parece ser $1/\log x$.

Distribución de los primos

¿Están los números primos distribuidos "al azar"?

Gauss 1849

La densidad de los primos de tamaño x parece ser $1/\log x$.

$$\text{n. de primos menores que } x \approx \int_2^x \frac{dt}{\log t}$$

Distribución de los primos

¿Están los números primos distribuidos "al azar"?

Gauss 1849

La densidad de los primos de tamaño x parece ser $1/\log x$.

$$\text{n. de primos menores que } x \approx \int_2^x \frac{dt}{\log t}$$

Unter	gibt es Primzahlen	Integral $\int \frac{dn}{\log n}$	Abweich.
500000	41556	41606,4	+ 50,4
1000000	78501	79627,5	+126,5
1500000	114112	114263,1	+151,1
2000000	148883	149054,8	+171,8
2500000	183016	183245,0	+229,0
3000000	216745	216970,6	+225,6

Distribución de los primos

¿Están los números primos distribuidos "al azar"?

Gauss 1849

La densidad de los primos de tamaño x parece ser $1/\log x$.

$$\text{n. de primos menores que } x \approx \int_2^x \frac{dt}{\log t}$$

Teorema de los números primos. **Hadamard** y **de la Vallée Poussin** 1896

El error relativo en la aproximación anterior tiende a cero. Es decir, el cociente de ambas cantidades se aproxima arbitrariamente a 1 cuando x crece.

Distribución de los primos

Riemann

Los primos están relacionados con los números (complejos) para los que se anula la suma

$$\frac{1}{1^s} - \frac{1}{2^s} + \frac{1}{3^s} - \frac{1}{4^s} + \frac{1}{5^s} - \frac{1}{6^s} + \cdots$$

Distribución de los primos

Riemann

Los primos están relacionados con los números (complejos) para los que se anula la suma

$$\frac{1}{1^s} - \frac{1}{2^s} + \frac{1}{3^s} - \frac{1}{4^s} + \frac{1}{5^s} - \frac{1}{6^s} + \dots$$

$$\rho_1 = 1/2 + i14'134725\dots$$
$$\rho_2 = 1/2 + i21'022040\dots$$
$$\dots \quad \dots \quad \text{(calculados } 10^{13} \text{ de ellos)}$$

Distribución de los primos

Riemann

Los primos están relacionados con los números (complejos) para los que se anula la suma

$$\frac{1}{1^s} - \frac{1}{2^s} + \frac{1}{3^s} - \frac{1}{4^s} + \frac{1}{5^s} - \frac{1}{6^s} + \dots$$

$\rho_1 = 1/2 + i14'134725\dots$
$\rho_2 = 1/2 + i21'022040\dots$
$\dots \quad \dots$ (calculados 10^{13} de ellos)

Hipótesis de Riemann 1859

Todos tienen parte real igual a $1/2$.

Distribución de los primos

Riemann

Los primos están relacionados con los números (complejos) para los que se anula la suma

$$\frac{1}{1^s} - \frac{1}{2^s} + \frac{1}{3^s} - \frac{1}{4^s} + \frac{1}{5^s} - \frac{1}{6^s} + \dots$$

$\rho_1 = 1/2 + i14'134725\dots$
$\rho_2 = 1/2 + i21'022040\dots$
$\dots \quad \dots$ (calculados 10^{13} de ellos)

Hipótesis de Riemann 1859

Todos tienen parte real igual a $1/2$.

El error absoluto en la aproximación es mínimo si y sólo si se cumple la hipótesis de Riemann.

Algunas conjeturas

Nos gustaría saber si...

1. ¿Es cierta la hipótesis de Riemann?
2. ¿Es todo número par mayor que 2 suma de dos primos?
3. ¿Hay infinitos primos gemelos (con diferencia dos)?
4. ¿Hay infinitos primos de la forma $n^2 + 1$?
5. ¿Entre dos cuadrados hay siempre un primo?
6. ...

Algunas conjeturas

Nos gustaría saber si...

1. ¿Es cierta la hipótesis de Riemann?
2. ¿Es todo número par mayor que 2 suma de dos primos?
3. ¿Hay infinitos primos gemelos (con diferencia dos)?
4. ¿Hay infinitos primos de la forma $n^2 + 1$?
5. ¿Entre dos cuadrados hay siempre un primo?
6. ...

Hay muchos resultados parciales, pero en ninguno de estos problemas se conoce una línea de ataque esperanzadora.