Números naturales, primos y parientes más lejanos

Fernando Chamizo Lorente

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

8 de noviembre 2007

Universidad de Murcia

Divide y te sorprenderás

Si $n \nmid m$ y $2,5 \nmid n$ entonces m/n es un decimal periódico puro

$$\frac{2}{3} = 0'66666\ldots \qquad \frac{24}{11} = 2'18181\ldots \qquad \frac{23}{21} = 1'0952309\ldots$$

Divide y te sorprenderás

Si $n \nmid m$ y $2,5 \nmid n$ entonces m/n es un decimal periódico puro

$$\frac{2}{3} = 0'66666\ldots \quad \frac{24}{11} = 2'18181\ldots \quad \frac{23}{21} = 1'0952309\ldots$$

Con el denominador 7 ocurre algo extraño:

$$\tfrac{1}{7} = 0'14285714\ldots \quad \tfrac{2}{7} = 0'28571428\ldots \quad \tfrac{3}{7} = 0'42857142\ldots$$

$$\tfrac{4}{7} = 0'57142857\ldots \quad \tfrac{5}{7} = 0'28571428\ldots \quad \tfrac{6}{7} = 0'85714285\ldots$$

¡El mismo periodo reordenado cíclicamente!

Dividiendo como en los viejos tiempos:

$$
\begin{array}{rrrrrrr|l}
\mathbf{1} & 0 & & & & & & 7 \\
\cline{8-8}
 & 3 & 0 & & & & & 0'142857 \\
 & & 2 & 0 & & & & \\
 & & & 6 & 0 & & & \\
 & & & & 4 & 0 & & \\
 & & & & & 5 & 0 & \\
 & & & & & & 1 &
\end{array}
$$

Dividiendo como en los viejos tiempos:

$$\begin{array}{llllllll} \mathbf{1} & 0 & & & & & \vert 7 & \\ & 3 & 0 & & & & \hline & \\ & & 2 & 0 & & & 0'142857 & \\ & & & 6 & 0 & & & \\ & & & & 4 & 0 & & \\ & & & & & 5 & 0 & \\ & & & & & & 1 & \end{array}$$

Los restos parciales sólo pueden ser 1,2,3,4,5,6 ¡Salen todos!
Al dividir $m/7$ siempre nos enganchamos a un punto de la cadena de restos.

Al dividir entre n hay $n-1$ posibles restos parciales.

Microteorema: La longitud del periodo de m/n es a lo más $n-1$.

Al dividir entre n hay $n-1$ posibles restos parciales.

Microteorema: La longitud del periodo de m/n es a lo más $n-1$.

Miniteorema: Cuando m varía, los periodos de m/n son permutaciones del de $1/n \Leftrightarrow$ La longitud del periodo es $n-1$.

Al dividir entre n hay $n-1$ posibles restos parciales.

Microteorema: La longitud del periodo de m/n es a lo más $n-1$.

Miniteorema: Cuando m varía, los periodos de m/n son permutaciones del de $1/n \Leftrightarrow$ La longitud del periodo es $n-1$.

¿Hay más ejemplos? Sí: 7, 17, 19, 23, 29, 47, 59, 61, 97, 109,...

$$\frac{1}{17} = 0'0588235294117647\ldots$$
$$\frac{2}{17} = 0'1176470588235294\ldots$$

(¿Qué tiene de especial la lista anterior?)

Euler 1758

Teorema: Sean a y n coprimos y $\phi(n) = n\prod_{p|n}(1-1/p)$, entonces $a^{\phi(n)}$ deja resto 1 al ser dividido por n.

Ejemplo: Si $3, 5 \nmid a$ entonces 15 divide a $a^8 - 1$.

k-ésimo resto parcial en $1/n$ = resto al dividir 10^k entre n.

Corolario: La longitud del periodo de $1/n$ es un divisor de $\phi(n)$.

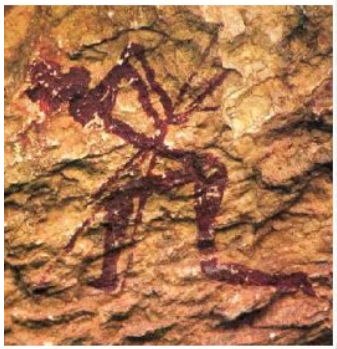
$n = p \Rightarrow \phi(n) = n - 1, \quad n = p_1 p_2 \Rightarrow \phi(n) = (p_1 - 1)(p_2 - 1) < n - 1$

Corolario: Si la longitud del periodo de $n - 1$ entonces n es primo. En particular los "números cíclicos" sólo aparecen para denominadores primos.

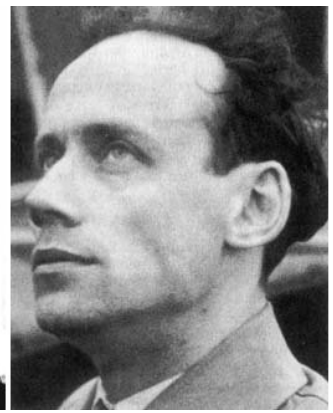
Epílogo histórico

Conjetura de Artin $\longleftrightarrow$ La probabilidad de que un primo tenga esta propiedad es $\prod (1 - 1/(p(p-1))) = 0'373955836\ldots$

Antigüedad		s. XVII		s. XVIII		s. XIX		s. XX
(?)	$\rightarrow$	Fermat	$\rightarrow$	Euler	$\rightarrow$	Gauss	$\rightarrow$	Artin
Divisiones		$p\|a^{p-1} - 1$		$n\|a^{\phi(n)} - 1$		$(\mathbb{Z}/n\mathbb{Z})^*$		Conjetura







Cuadrados en forma

Formas cuadráticas (binarias): $Q(x, y) = ax^2 + bxy + cy^2$, $a, b \in \mathbb{Z}$.

$$\text{Euler} \xrightarrow{\text{diag.}} Ax^2 + By^2 \xrightarrow{A\cdot} x^2 + Cy^2$$

Suponemos además que no hay factores comunes de los dos sumandos:

x, y coprimos, x, C coprimos.

Euler descubrió experimentalmente en 1748 que los primos en la descomposición de $x^2 + Cy^2$ no son arbitrarios.
Por ejemplo:

Forma	Factores primos
$x^2 + y^2$	$p = 2,\ p = 4n + 1$
$x^2 + 2y^2$	$p = 8n + 1,\ p = 8n + 3$

y resultados similares para el resto de las formas.

Euler descubrió experimentalmente en 1748 que los primos en la descomposición de $x^2 + Cy^2$ no son arbitrarios.
Por ejemplo:

Forma	Factores primos
$x^2 + y^2$	$p = 2,\ p = 4n + 1$
$x^2 + 2y^2$	$p = 8n + 1,\ p = 8n + 3$

y resultados similares para el resto de las formas.
Nos centraremos sólo en $x^2 + y^2$.
Ejemplos:

$$3^2 + 5^2 = 34 = 2 \cdot 17, \qquad 1^2 + 8^2 = 65 = 5 \cdot 13,$$
$$200^2 + 201^2 = 80401 = 37 \cdot 41 \cdot 53,$$
$$1000^2 + 2007^2 = 5028049 = 13 \cdot 29 \cdot 13337.$$

Teorema: Si $p|x^2 + y^2$ (x, y coprimos) entonces $p = 2$ o $p = 4n + 1$.

Corolario: Hay infinitos primos de la forma $4n + 1$.

Demostración: Si sólo existieran $p_1, p_2, \ldots, p_r$ entonces $(p_1 p_2 \ldots p_r)^2 + 2^2$ no tendría divisores primos. □

Corolario: $4k + 3$ no divide a $l^2 + 1$.

Demostración: $4k + 3$ tiene algún factor primo de la forma $4n + 3$. □

Con paciencia se pueden hacer cálculos que demuestren casos particulares. Por ejemplo $3 \nmid l^2 + 1$ porque si $l = 3m$, $l = 3m + 1$ ó $l = 3m + 2$ se llegaría a que 3 divide a $9m^2 + 1$, $3m(3m + 2) + 2$ ó $3m(3m + 4) + 5$, respectivamente y todos estos casos conducen a una contradicción.

Con paciencia se pueden hacer cálculos que demuestren casos particulares. Por ejemplo $3 \nmid l^2+1$ porque si $l=3m$, $l=3m+1$ ó $l=3m+2$ se llegaría a que 3 divide a $9m^2+1$, $3m(3m+2)+2$ ó $3m(3m+4)+5$, respectivamente y todos estos casos conducen a una contradicción.

¿Cómo se deduce el teorema en general?

Demostración del teorema: (recordando que $p|a^{p-1}-1$ si $p \nmid a$)

Si $2 \neq p|x^2+y^2$ se tiene

$$\begin{aligned} -y^2 = x^2 - l_1 p \quad &\Rightarrow \quad (-1)^{(p-1)/2} y^{p-1} = x^{p-1} + l_2 p \\ &\Rightarrow \quad (-1)^{(p-1)/2} - 1 = l_3 p \end{aligned}$$

y esto sólo puede ocurrir si $l_3 = 0$ y $(p-1)/2$ es par. □

Los primos crecen

Hay infinitos primos (Euclides c. 300 a.d.C.) pero ¿cómo crecen de rápido? ¿como los cuadrados? ¿como $n^{3/2}$? ¿como $10n$?

Euler 1744

$$\begin{aligned}
\sum_{2\nmid n} \frac{1}{n^s} &= \sum \frac{1}{n^s} - \sum \frac{1}{(2n)^s} = (1-\frac{1}{2^s}) \sum \frac{1}{n^s} \\
\sum_{2,3\nmid n} \frac{1}{n^s} &= (1-\frac{1}{3^s})(1-\frac{1}{2^s}) \sum \frac{1}{n^s} \\
\dots &= \dots\ \dots\ \dots\ \dots\ \dots \\
\frac{1}{1^s} &= \prod_p (1-\frac{1}{p^s}) \cdot \sum_n \frac{1}{n^s}
\end{aligned}$$

Identidad de Euler

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \left(1 - p^{-s}\right)^{-1}$$

Tomando $s \to 1^+$ y usando $\sum_{n=1}^{N} \frac{1}{n} \sim \int_1^N \frac{1}{x}\, dx = \log N \to \infty$ se obtiene

$$\infty = \prod_{p} \left(1 - p^{-1}\right)^{-1}$$

Una prueba ¡analítica! de la infinitud de los primos.

La identidad de Euler da más información: los primos no pueden crecer como n^2 ni como n^α con $\alpha > 1$; si fuera así se llegaría a una contradicción cuando $s \to 1^+$.

Con algunas trampitas podemos sospechar el verdadero orden de crecimiento de los primos.

Usando que $\log(1-x)^{-1} \sim x$ para x pequeño; cuando $s \approx 1$

$$\sum \frac{1}{p^s} \sim \log \prod_p \left(1-p^{-s}\right)^{-1} = \log \sum_{n=1}^{\infty} \frac{1}{n^s}$$

$$\overset{??}{\Rightarrow} \quad \sum_{p \leq N} \frac{1}{p} \sim \log \sum_{n \leq N} \frac{1}{n} \Rightarrow \sum_{p \leq N} \frac{1}{p} \sim \log\log N$$

(según Euler $\sum \frac{1}{p} = \log\log\infty$).

Esto sugiere que si $p_n \sim f(n)$ entonces $\int_1^N \frac{1}{f(n)}\, dn = \log\log N$.

Derivando se deduce $f(n) = n\log n$.

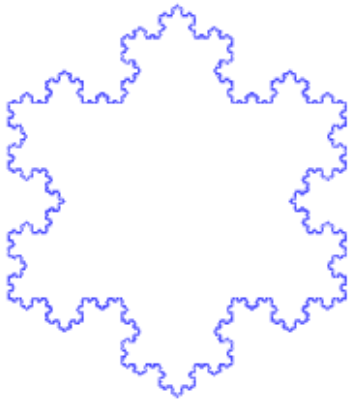
Epílogo histórico

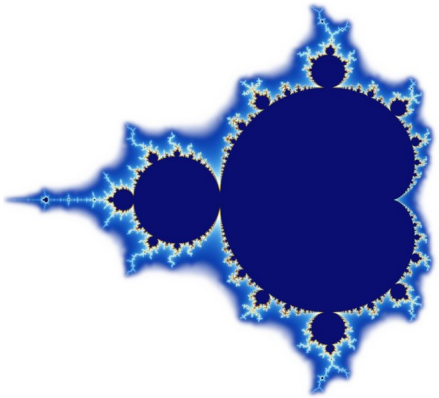
(1859) Riemann $\longrightarrow$	Esquema de la relación con la variable compleja
(1896) Hadamard y de la Vallée Poussin	$\longrightarrow \lim \frac{p_n}{n \log n} = 1$ (con variable compleja)
(1949) Erdős y Selberg	$\longrightarrow$ Prueba "elemental"

Gracias a la extensión del trabajo de Riemann sabemos que el error al aproximar el número de primos menores que N por cierta función se minimiza si y sólo si los ceros complejos de una extensión de $\sum 1/n^s$ están en fila india (en la recta $\Re z = 1/2$). Ésta es la **Hipótesis de Riemann**.

Un triángulo de dos

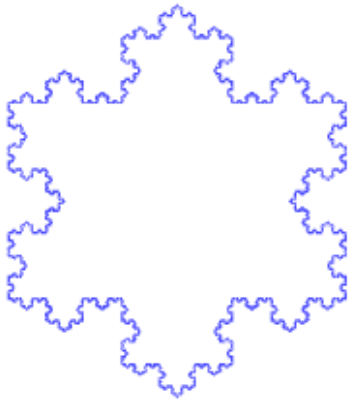
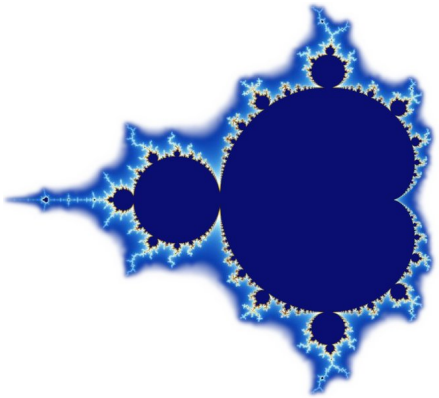
Los fractales son famosos en el mundo entero



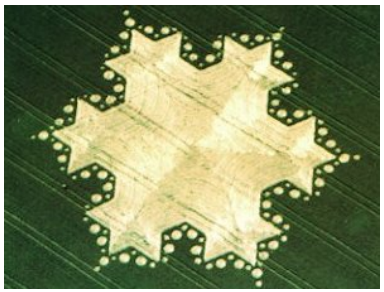


Un triángulo de dos

Los fractales son famosos en el mundo entero


e incluso fuera del mundo . . .



Uno de los primeros y más sencillos fractales es el triángulo de Sierpiński

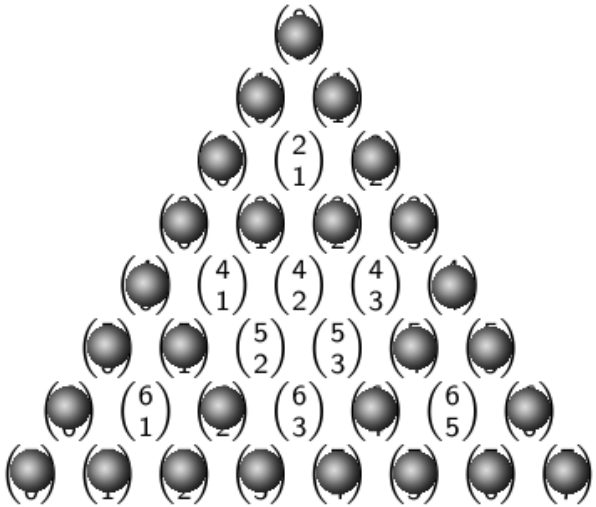
T_0 T_1 T_2 ... T_∞

T_{n+1} está formado por 3 copias semejantes a T_n.

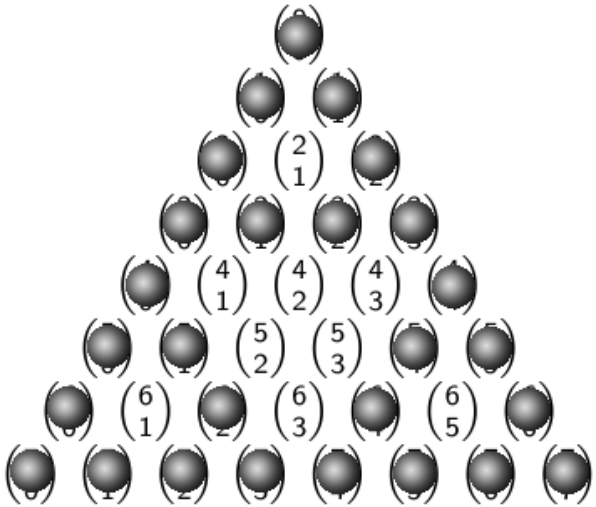
$$n = 8$$

$$\begin{array}{c}
\binom{0}{0} \\
\binom{1}{0}\ \binom{1}{1} \\
\binom{2}{0}\ \binom{2}{1}\ \binom{2}{2} \\
\binom{3}{0}\ \binom{3}{1}\ \binom{3}{2}\ \binom{3}{3} \\
\binom{4}{0}\ \binom{4}{1}\ \binom{4}{2}\ \binom{4}{3}\ \binom{4}{4} \\
\binom{5}{0}\ \binom{5}{1}\ \binom{5}{2}\ \binom{5}{3}\ \binom{5}{4}\ \binom{5}{5} \\
\binom{6}{0}\ \binom{6}{1}\ \binom{6}{2}\ \binom{6}{3}\ \binom{6}{4}\ \binom{6}{5}\ \binom{6}{6} \\
\binom{7}{0}\ \binom{7}{1}\ \binom{7}{2}\ \binom{7}{3}\ \binom{7}{4}\ \binom{7}{5}\ \binom{7}{6}\ \binom{7}{7}
\end{array}$$

$n = 8$

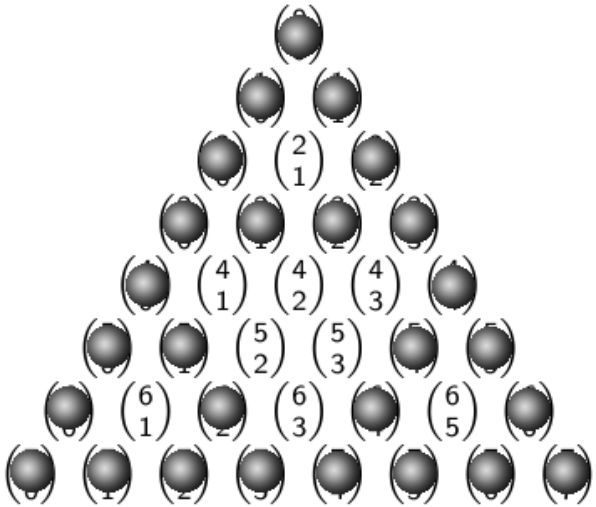

$\binom{2}{1}$
$\binom{4}{1}$ $\binom{4}{2}$ $\binom{4}{3}$
$\binom{5}{2}$ $\binom{5}{3}$
$\binom{6}{1}$ $\binom{6}{3}$ $\binom{6}{5}$

$n = 8$


$\binom{2}{1}$
$\binom{4}{1}$ $\binom{4}{2}$ $\binom{4}{3}$
$\binom{5}{2}$ $\binom{5}{3}$
$\binom{6}{1}$ $\binom{6}{3}$ $\binom{6}{5}$

$n = 16$

$n = 8$

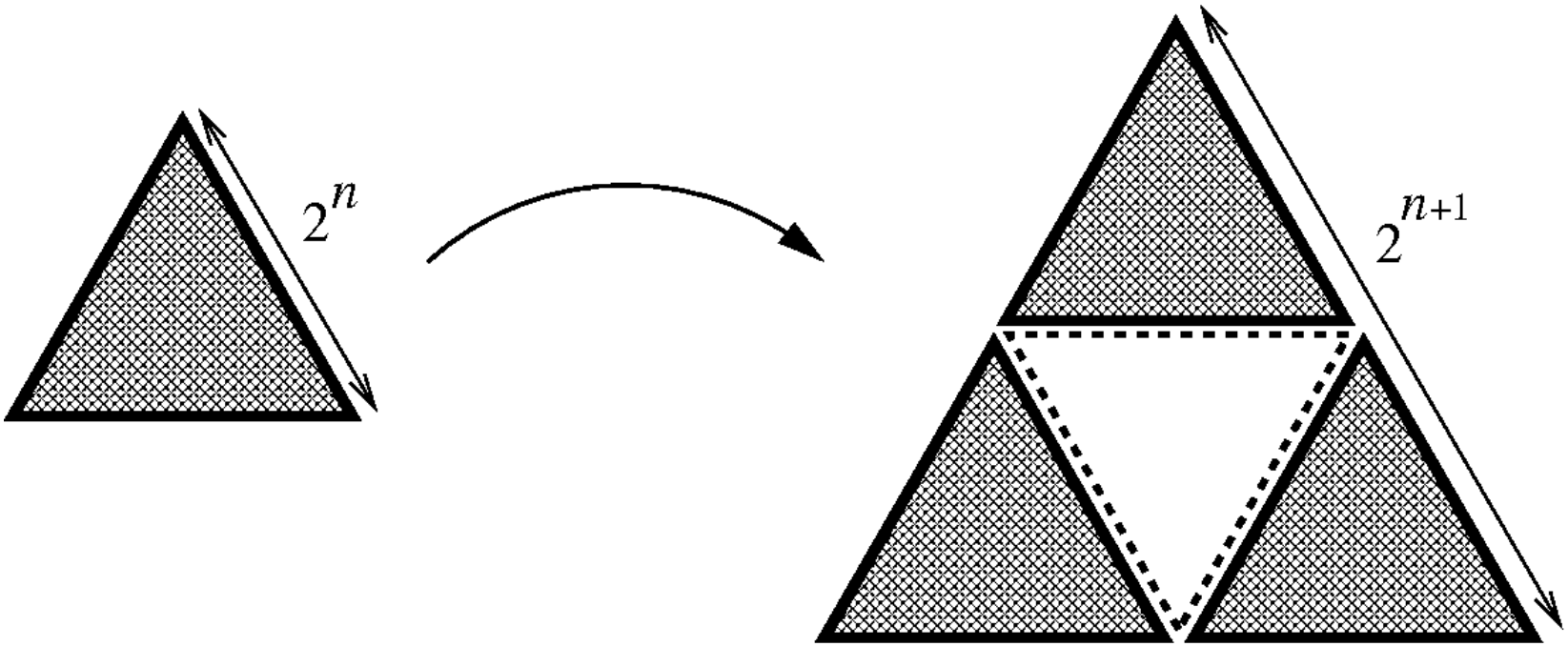


$n = 16$

Reglas de adición:

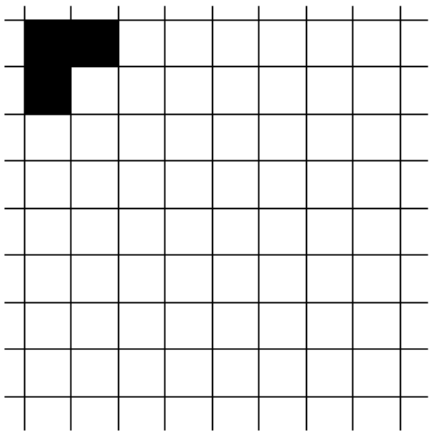
$P + P = P$ $P + I = I$ $I + P = I$ $I + I = P$

La prueba es por inducción (iteración): Al pegar tres bloques triangulares de lado 2^n y borde impar se obtiene un triángulo coherente con las leyes de adición.

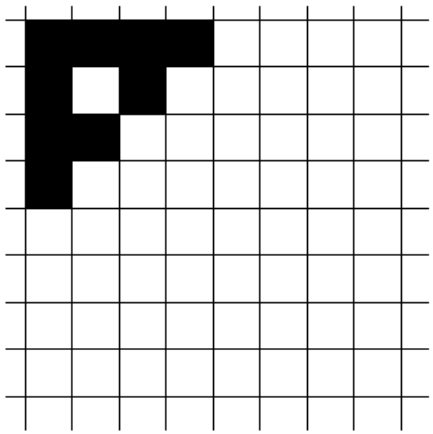


El triángulo discontinuo, claramente contiene sólo elementos pares.

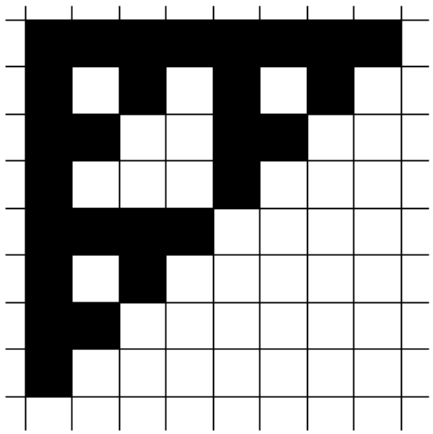
Cartesianizando el triángulo de Pascal: $\binom{n}{m} \longrightarrow (m, n-m)$.



$T_0 = \{(0,0),(1,0),(0,1)\},$



$T_1 = \{(0,0),(2,0),(0,2)\} + T_0,$



$T_2 = \{(0,0),(4,0),(0,4)\} + T_1$

En general $T_n = \{(0,0),(2^n,0),(0,2^n)\} + T_{n-1}$.
Esto es lo mismo que decir que cuando se escriben x e y en base dos, nunca aparece dos unos en el mismo lugar (al sumarlos no hay nunca llevadas).

Ejemplo: ¿Es $\binom{239}{169}$ par o impar?

$$\begin{matrix} n = 239 \\ m = 169 \end{matrix} \longrightarrow \begin{matrix} x = 169 \\ y = 70 \end{matrix} \longrightarrow \begin{array}{|c|c|c|c|c|c|c|c|} \hline 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ \hline 0 & 1 & 0 & 0 & 0 & 1 & 1 & 0 \\ \hline \end{array}$$

No hay llevadas al sumar $\Rightarrow$ es impar.

Corolario

$\binom{2^n-1}{k}$ es siempre impar, $\binom{2n}{n}$ es siempre par $(n > 0)$.

Justificaciones para el siglo XVIII ¿o el XXI?

L. Euler 1748

Por tanto, incluso si una proposición ya sea cierta o falsa parece que no redunda en ninguna utilidad para nosotros, todavía el método mismo por el cual se establece la certeza o falsedad usualmente abre el camino para que entendamos otras verdades más útiles. Por esta razón, creo firmemente que no he desperdiciado mi trabajo y mi esfuerzo en investigar estas propiedades que contienen notables propiedades sobre los divisores de los números. Esta teoría de los divisores no es de uso vano sino que alguna vez podría mostrar alguna utilidad no despreciable en análisis.