Divisibilidad De Numeros Combinatorios. El Teorema De Lucas.

ROBERTO J. MIATELLO - ISABEL VIGGIANI ROCHA

El objeto de la presente nota es analizar el problema de divisibilidad de un número combinatorio $\binom{n}{k}$ por un número primo p. La respuesta de esta pregunta no trivial resulta ser muy elegante y su demostración elemental. Este resultado, debido al matemático francés Edouard Lucas, apareció por primera vez en un texto de Teoría de Números de éste autor. La demostración que daremos es debida a Fine (American Math. Monhly 1947). Antes de abordar el resultado general consideraremos el caso en que $p = 2$, y daremos una prueba independiente en este caso.

En primer lugar recordamos el resultado básico de expansión m-ádica de un número natural.
Fijamos $m \in \mathbb{N}$, $m > 1$.

Teorema. Sea $x \in \mathbb{N} \cup \{0\}$. Entonces existen $a_0, a_1, \ldots, a_r$ únicos, $0 \le a_i < m$, tales que

$$x = \sum_{i=0}^{t} a_i . m^i$$

Prueba. Por el algoritmo de división

$x = m q + r \quad 0 \le r < m \quad$ q y r únicos. Si $x = 0$ el resultado es obvio. Supongamos $x \neq 0$.

Como $m > 1$ es $q < x$, luego, por hipótesis inductiva, $q = \sum_{i=0}^{t} a'_i m^i$ $(0 \le a'_i < m)$ donde a'_i $\forall$ $i = 1,\dots, t$, está unívocamente determinado por q. Luego

$$x = \sum_{i=0}^{t} a'_i m^{i+1} + r$$

y tomando $a_0 = r$, $a_i = a'_{i-1}$, si $i = 1,\dots,t-1$.
La unicidad de los a_i's sigue de la de los a'_i's.

La expansión del teorema anterior se llama *expansión m-ádica de x.* Si $m = 10$ se obtiene la expansión decimal usual. Si $m = 2$ se llama expansión diádica o binaria.

Definición. Si p es primo y $x \in \mathbb{Q}-\{0\}$ se define $v_p(x) = i(p)$, donde $x = \prod_{j=1}^{r} P_j^{i(p_j)}$ con $i(p_j) \in \mathbb{Z}$ (p_1, $p_2,\dots,p_r$ son primos distintos).

Se llama a $v_p(x)$ la valuación p-ádica de p en x. En el caso en que $p = 2$, escribiremos $v_2(x) = v(x)$.

Se tiene así, si $x \in \mathbb{Z}-\{0\}$, que $v_p(x) > 0$ si y sólo si x es divisible por p.

Lema 1. Dados $x, y \in Q - \{0\}$ se tiene

$$v_p(xy) = v_p(x) + v_p(y).$$

Prueba. Ejercicio.

Lema 2. Si $r \ge s$, $v\left(\binom{p^r}{p^s}\right) = r-s$.

Prueba. Si $r = s$ la afirmación es obvia. Ahora si $j < p^r$ entonces

$$\binom{p^r}{j} = \frac{p^r(p^r-1)\,(p^r-2)\ldots(p^r-j+1)}{1.2.\ \ldots\ (j-1).j}\ .$$

Es claro que $v_p\left(\frac{p^r-i}{i}\right) = 0$, si $1 \le i \le (j-1)$.

Luego $\quad v\binom{p^r}{j} = v\left(\frac{p^r}{j}\right)$. Así, si $j = p^s$,

$$v\binom{p^r}{p^s} = v(p^{r-s}) = r-s.$$

Lema 3. Sea $n = \sum_{i=1}^{n} 2^{k_i}$, $k_1<k_2<\ldots<k_r$.

Entonces $v(n!) = \sum_{1}^{r} v(2^{k_i}!)$.

Prueba.

$$n! = \prod_{i_1=1}^{2^{k_1}} (2^{k_r} +\ldots+ 2^{k_2} + i_1) \prod_{i_r=1}^{2^{k_1}} (2^{k_r} +\ldots+ 2^{k_3} + i_2)\ldots$$

$$\prod_{i_{r-1}=1}^{2^{k_{r-1}}} (2^{k_r} + i_{r-1}) \prod_{i_r=1}^{2^{k_r}} i_r$$

Luego

$$v(n!) = \sum_{j=1}^{r} \sum_{i_j=1}^{2^{k_j}} v(2^{k_r}+\ldots+ 2^{k_{j+1}} + i_j)$$

$$= \sum_{j=1}^{r} \sum_{i_j=1}^{2^{k_j}} v(i_j) = \sum_{j=1}^{r} v(2^{k_j}!). \blacksquare$$

Pasamos a responder la pregunta de cuándo $\binom{n}{k}$ es par, esto es, bajo qué condiciones $v\binom{n}{k} > 0$. En primer lugar, es instructivo escribir el triángulo de Tartaglia para $1 \leq n \leq 10$. Recordemos la identidad $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$ si $0 \leq k < n$.

1

1 1

1 2 1

1 3 3 1

1 4 6 4 1

1 5 10 10 5 1

1 6 15 20 15 6 1

1 7 21 35 35 21 7 1

1 8 28 56 70 56 28 8 1

1 9 36 84 126 126 84 36 9 1

11 10 45 120 210 252 210 120 45 10 1

o sea el esquema de paridad de $\binom{n}{k}$ es, si $1 \leq k \leq n \leq 10$, i

i i

i p i

i i i i

i p p p i

i i p p i i

i p i p i p i

i i i i i i i i

i p p p p p p p i

i i p p p p p p i i

i p i p p p p p i p i

Teorema A. Si $n = \sum_{i=0}^{r} a_i 2^i$, $k = \sum_{i=0}^{r_0} b_j 2^j$, $\binom{n}{k}$ es impar si y sólo si $a_i \geq b_i$, $\forall i$.

Corolario. (i) Si $n = 2^s$ entonces $\binom{n}{k}$ es par $\forall k$, $0 < k < n$.

(ii) Si $n = 2^s - 1 = 1 + 2 + \ldots + 2^{s-1}$, $\binom{n}{k}$ es impar $\forall$ k, $0 \leq k \leq n$.

Prueba (del Teorema A).

Escribamos $n = \sum_{1}^{r} 2^{k_i}$, $k = \sum_{1}^{s} 2^{h_i}$

$$n-k = \sum_{1}^{t} 2^{\ell_i}$$

donde $k_1 < \ldots < k_r$, $h_1 < \ldots < h_s$, $\ell_1 < \ldots < \ell_t$.

Es fácil ver que la condición $a_i \geq b_i$, $\forall i$, es equivalente a que los conjuntos $\{h_1, \ldots, h_s\}$ y $\{\ell_1, \ldots, \ell_t\}$ sean disjuntos.

Supongamos por lo tanto que este es el caso. Luego, por el Lema 3 tenemos

$$v\binom{n}{k} = v(n!) - v(k!) - v((n-k)!)$$

$$= \sum_{i=1}^{r} v(2^{k_i}!) - \sum_{i=1}^{s} v(2^{h_i}!) - \sum_{i=1}^{t} v(2^{\ell_i}!)$$

$$= 0$$

es decir $\binom{n}{k}$ es impar.

Supongamos por el contrario ahora que existen u, v tales que $h_v = \ell_v = m$. Entonces $k = \sum_{\hat{u}} 2^{k_i} + 2^m, n-k = \sum_{\hat{v}} 2^{\ell_j} + 2^m$ ($\hat{j}$ significa que se omite el índice j).

$$(*)\ v(k!) + v((n-k)!) = \sum_{\hat{u}} v(2^{h_i}!) + \sum v(2^{\ell_j}!) + 2\,v(2^m!)$$

Ahora bien, por el Lema 2,

$$1 = v\binom{2^{m+1}}{2^m} = v(2^{m+1}!) - 2v(2^m!)$$

Reemplazando en (*) obtenemos

$$\sum_{\hat{u}} v(2^{h_i}!) + v(2^{m+1}!) + \sum_{\hat{v}} v(2^{\ell_j}!) - 1$$

$$= v\left(\left(\sum_{\hat{u}} 2^{h_i}\right)!\right) + v(2^{m+1}!) + v\left(\left(\sum_{\hat{v}} 2^{\ell_j}\right)!\right) - 1.$$

Ahora bien, si $b = \sum_{\hat{u}} 2^{h_i} + 2^{m+1} = k+2^m$ es $n-b =$

$n-k-2^m = \sum_{\hat{v}} 2^{\ell_j}$, luego (*) es igual a $v(b!) - v\binom{b}{2^{m+1}} +$

$v((n-b)!) - 1.$

Por lo tanto

$$v\binom{n}{k} = v(n!) - v(k!) - v((n-k)!)$$
$$= v\binom{n}{b} + v\binom{b}{2^{m+1}} + 1 > 0$$

luego $\binom{n}{k}$ es par. La demostración del teorema está completa.

Consideramos a seguir el caso de p un primo arbitrario.

Teorema B. (Lucas, 1890). Sea p primo $n = \sum_{i=0}^{r} a_i p^i$, $k = \sum_{j=0}^{r} b_j\, p^j$ $0 \le a_i, b_j \le p\ \forall_{i,j}$. Entonces

$$\binom{n}{k} \equiv \binom{a_0}{b_0}\binom{a_1}{b_1} \cdots \binom{a_r}{b_r} \mod p.$$

Se usa acá la convención $\binom{m}{n} = 0$ si $m < n$.

Corolario. (ver Teorema A).
Si $p = 2$, $\binom{n}{k} \equiv 0 \mod 2$ si y sólo si existe j $(0 \le j \le r)$ con $a_j = 0$, $b_j = 1$.

Prueba. (del Teorema B)
Escribamos el polinomio

$$\sum_{k=0}^{n} \binom{n}{k} x^k = (1+x)^n$$

$$= (1+x)^{(\sum_{i=0}^{r} a_i p^i)}$$

$$= \prod_{i=0}^{r} ((1+x)^{p^i})^{a_i}$$

$$\equiv \prod_{i=0}^{r} (1+x^{p^i})^{a_i} \qquad \text{mod } p.$$

$$= \prod_{i=0}^{r} \left(\sum_{c_i=0}^{a_i} \binom{a_i}{c_i} x^{c_i p^i} \right)$$

Para obtener el coeficiente de x^k en el miembro derecho debemos considerar las posibles expresiones $k = \sum_{j=0}^{r} c_j p^j$ con $0 \le c_j \le a_j < p$. Ahora bien, tal expresión de k es única y se tiene $c_j = b_j$, $\forall\ j = 0,1,\ldots,r$. El coeficiente correspondiente es $\binom{a_0}{b_0}\binom{a_1}{b_1},\ldots,\binom{a_r}{b_r}$, por lo tanto, igualando coeficientes se obtiene el Teorema B.

Para concluir proponemos algunos ejercicios al lector.

Ejercicio 1. Pruebe que $\binom{n}{k} \equiv 0$ mod p, $\forall k$ con $0 < k < n$ si y sólo si $n = p^r$ para algún r.

Ejercicio 2. Pruebe que $\binom{p^r}{k}$ no es divisible por p^2, $\forall k\ 0 < k < n$. (Una pregunta más difícil es hallar todos los valores de k con $0 < k < n$ tales que p^2 no divide a $\binom{p^r}{k}$).

Ejercicio 3. Pruebe que $n = \sum_{i=0}^{r} a_i p^i$, $(a_r > 0)$ satisface $\binom{n}{k} \not\equiv 0 \bmod p$, $\forall k$ $0 < k < n$, si y sólo si $a_i = p-1$, $\forall_i$, $0 \le i < r$.

Ejercicio 4. (i) Concluya del Ejercicio 3 que si $p = 2$, $\binom{n}{k}$ es impar $\forall k$ si y sólo si $n = 2^k-1$.

(ii) Dé ejemplos, si $p > 2$, de $n \neq p^r-1$ tales que $\binom{n}{k} \not\equiv 0 \bmod p$ $\forall$ k, $0 < k < n$.

FAMAF, Universidad Nacional de Córdoba.
Fac. de Ciencias Exactas y Tecnología,
Universidad Nacional de Tucumán.