1 El conjunto de los números enteros

El conjunto de los números enteros, que representamos como $\mathbb{Z}$, es el conjunto formado por los números $0, \pm 1, \pm 2, \pm 3, \ldots$. El conjunto $\mathbb{Z}$ goza de una serie de propiedades que podemos dividir en aritméticas, a partir de las operaciones de suma $(+)$ y producto $(\cdot)$, y de orden, a partir de la relación $\leq$.

Las propiedades aritméticas son las siguientes

P1.- $a + b$ y $a \cdot b$ son elementos de $\mathbb{Z}$.

P2.- $\forall a, b \in \mathbb{Z}$, $a + b = b + a$ y $a \cdot b = b \cdot a$.

P3.- $\forall a, b, c \in \mathbb{Z}$, $(a + b) + c = a + (b + c), (a \cdot b) \cdot c = a \cdot (b \cdot c)$.

P4.- $\exists\, 0, 1 \in \mathbb{Z}$ tal que $\forall a \in \mathbb{Z}$, $a + 0 = a$, $a \cdot 1 = a$.

P5.- $\forall a, b, c \in \mathbb{Z}$, $a \cdot (b + c) = a \cdot b + a \cdot c$.

P6.- $\forall a \in \mathbb{Z}\ \exists - a \in \mathbb{Z}$ único tal que $a + (-a) = 0$.

P7.- Si $a \neq 0$ y $a \cdot b = a \cdot c \Longrightarrow b = c$.

A partir de las mismas pueden deducirse otras muchas propiedades que nos son familiares, como la siguiente:

Ejemplo 1.- $x \cdot 0 = 0$ para todo $x \in \mathbb{Z}$.

$x \cdot (0 + 0) = x \cdot 0$, por la propiedad $P4$.
$x \cdot 0 + x \cdot 0 = x \cdot 0$, por la propiedad $P5$.
$-x \cdot 0 + (x \cdot 0 + x \cdot 0) = -x \cdot 0 + x \cdot 0 = 0$, por las propiedades $P4$ y $P6$.
$(-x \cdot 0 + x \cdot 0) + x \cdot 0 = 0 + x \cdot 0 = x \cdot 0 = 0$, por las propiedades $P2$, $P3$, $P4$ y $P6$. ∎

Las propiedades de orden son las siguientes

P8.- $a \leq a$ para todo $a \in \mathbb{Z}$.

P9.- Si $a \leq b$ y $b \leq a$, entonces $a = b$.

P10.- Si $a \leq b$ y $b \leq c$, entonces $a \leq c$.

P11.- Si $a \leq b$, entonces $a + x \leq b + x$ para todo $x \in \mathbb{Z}$.

P12.- Si $a \leq b$ y $0 \leq c$, entonces $a \cdot c \leq b \cdot c$.

Como en el caso de las propiedades aritméticas, se pueden deducir otras muchas propiedades conocidas.

Ejemplo 2.- Si $a \leq b$, entonces $-b \leq -a$.

$a \leq b \Longrightarrow a + (-a - b) \leq b + (-a - b)$, por la propiedad $P11$.
Aplicando las propiedades aritméticas $P2$, $P3$, $P4$ y $P6$ resulta $-b \leq -a$. ∎

Estas 12 propiedades no sólo las verifican los números enteros. También se cumplen para los números racionales y reales. ¿Qué es, entonces, lo que diferencia a los números enteros del resto de números? La diferencia radica en una propiedad que se conoce como *principio o axioma del buen orden.* Antes de enunciarlo, un par de definiciones

Definición 1 *Sea $X \subset \mathbb{Z}$ un subconjunto de números enteros. Decimos que $b \in \mathbb{Z}$ es una* **cota inferior** *de X si $b \leq x$ para todo $x \in X$. Entonces decimos que X es un conjunto acotado inferiormente.*

Algunos conjuntos no tienen cotas inferiores, como el conjunto de los enteros negativos ($\mathbb{Z}^-$). Otros conjuntos, como

$$\{-18, -27, -26, -15, -5, 5, 15, 24, 19, 6, 98, -23, 0, 7\}$$

sí tienen cotas inferiores. Por ejemplo -40 lo es. Sin embargo, vemos que -27 es *la mejor cota inferior*, ya que no se puede mejorar y, de hecho, pertenece al conjunto.

Definición 2 *Una cota inferior b de un conjunto X tal que $b \in X$ recibe el nombre de* **mínimo** *de X.*

Ahora estamos en condiciones de enunciar la propiedad más importante, que es la que distingue al conjunto de los números enteros.

P13.- **Principio del buen orden**. Todo subconjunto no vacío de $\mathbb{Z}$ acotado inferiormente tiene mínimo.

Ejemplo 3.- El conjunto de números racionales $\left\{ \frac{1}{n} \middle| \, n \in \mathbb{N} \right\}$ tiene cotas inferiores pero no tiene mínimo.

En efecto, basta darse cuenta que 0 es *la mejor cota inferior*, pero no está en el conjunto. Es decir, este conjunto no tiene mínimo. ■

Esto nos proporciona una justificación de la idea intuitiva de los números enteros como un conjunto de puntos regularmente espaciados en una recta que se extiende infinitamente en ambas direcciones. En particular, nos dice que no podemos acercarnos a un entero más y más sin llegar a él. El hecho de que haya huecos entre los enteros nos lleva a decir que $\mathbb{Z}$ es discreto y es esta propiedad la que da el nombre a la **Matemática Discreta**.

Lo relevante del principio del buen orden no es sólo el hecho de que distingue el conjunto $\mathbb{Z}$ de otros conjuntos de números, sino que resulta de gran utilidad desde el punto de vista matemático. Este principio es la base de distintas técnicas básicas, entre ellas la de la demostración por inducción.

1.1 El principio de inducción matemática

Teorema 1 *(Principio de inducción matemática) Sea $S \subseteq \mathbb{N}$ ($\mathbb{N}$ el conjunto de los enteros positivos, $\mathbb{N} = \mathbb{Z}^+ = \{1, 2, 3, \ldots\}$, llamado conjunto de los números naturales) tal que*

i) $1 \in S$,

ii) si $k \in S$, entonces $k + 1 \in S$.

Entonces $S = \mathbb{N}$.

La demostración se realiza por reducción al absurdo.

Supongamos que $S \neq \mathbb{N}$, entonces se cumple que $\mathbb{N} \setminus S \neq \emptyset$, es decir, hay elementos en $\mathbb{N}$ que no están en S. Puesto que $\mathbb{N} \setminus S$ es un conjunto de números naturales, está acotado inferiormente y, por el principio del buen orden, tiene mínimo. Llamemos a ese mínimo m_0 (notar que $m_0 \notin S$).

Es evidente que $m_0 \neq 1$, pues $1 \in S$ (por *i)*), por lo tanto $m_0 - 1 \geq 1$. Como, m_0 es el mínimo de $\mathbb{N} \setminus S$, entonces $m_0 - 1 \in S$ y, por *ii)*, $m_0 \in S$. Esto es absurdo, pues tenemos que $m_0 \in S$ y $m_0 \notin S$. En consecuencia, hemos partido de un supuesto falso, esto es suponer que $S \neq \mathbb{N}$. ■

La consecuencia inmediata del principo de inducción matemática deriva en una técnica para la demostración de proposiciones en las que aparece una variable n, que representa un número natural. De esta forma, si la proposición es cierta para $n = 1$ y si se supone cierta para un cierto k también lo es para $k + 1$, entonces la proposición es cierta para cualquier $n \geq 1$.

Ejemplo 4.- Probar por inducción que $1 + 2 + 3 + \cdots + n = \dfrac{n(n+1)}{2}$.

En primer lugar debemos verificar *la base de la inducción*, esto es, que la fórmula que debemos probar es cierta para $n = 1$, es decir, cuando sólo hay un sumando. Pero esto es obvio, pues

$$1 = \frac{1 \cdot (1+1)}{2} = 1.$$

Ahora tenemos que probar *el paso inductivo*, esto es, tenemos que ver que si la fórmula se cumple para $n = k$, también se cumple para $n = k + 1$. En este caso, suponemos cierto que

$$1 + 2 + \cdots + k = \frac{k(k+1)}{2}. \tag{1}$$

¿Se cumple entonces que $1+2+\cdots+k+(k+1)=\dfrac{(k+1)(k+1+1)}{2}$?

Teniendo en cuenta (1), resulta

$$1+2+\cdots+k+(k+1)=\frac{k(k+1)}{2}+(k+1).$$

Operando llegamos finalmente a

$$1+2+\cdots+k+(k+1)=\frac{(k+1)(k+2)}{2}.$$

Luego la fórmula también es cierta para $n=k+1$ y, por el principio de inducción matemática, es válida para cualquier $n\geq 1$. ∎

Es importante verificar los dos pasos de la inducción matemática. A veces, se tiende a prescindir del primer paso (la base de la inducción) y uno se centra sólo en el paso inductivo, que suele ser el más complicado. Esto puede llevar a errores, como en el siguiente ejemplo.

Ejemplo 5.- Probar que $1+2+\cdots+n=\dfrac{n^2+n+2}{2}$.

Si prescindimos de la base de la inducción y pasamos directamente al paso inductivo, probaremos que si la fórmula se verifica para un de terminado k, también se verifica para $k+1$. En este caso, partimos de

$$1+2+\cdots+k=\frac{k^2+k+2}{2} \tag{2}$$

y queremos probar que

$$1+2+\cdots+k+(k+1)=\frac{(k+1)^2+(k+1)+2}{2}.$$

Partiendo de (2) tenemos que

$$1+2+\cdots+k+(k+1)=\frac{k^2+k+2}{2}+(k+1)$$

y operando llegamos a

$$1+2+\cdots+k+(k+1)=\frac{(k+1)^2+(k+1)+2}{2}.$$

En resumen, el paso inductivo se cumple, pero no hemos verificado la base de la inducción. De hecho, no se cumple y la fórmula no es cierta cualquiera que sea el valor de n. ∎

La base de la inducción no tiene por qué ser necesariamente $n=1$, pudiendo ser cualquier entero n_0 tanto positivo como negativo. En este caso se tiene que si

i) La propiedad es cierta para $n=n_0$.

ii) Si la propiedad es cierta para $n=k$ también lo es para $n=k+1$.

Entonces la propiedad es cierta para $n\geq n_0$.

Ejemplo 6.- Demostrar por inducción que todo número mayor o igual que 8 puede escribirse como suma de treses y cincos.

En este caso la base de la inducción es $n=8$. Así, se tiene

$$8=5+3$$

y, por tanto, la propiedad es cierta para $n=8$.

Supongamos que la propiedad es cierta para un cierto $n = k$, es decir, k se puede poner como suma de treses y cincos. Esto quiere decir que existen a y b enteros mayores o iguales que 0 tales que

$$k = a \cdot 3 + b \cdot 5.$$

Siendo esto cierto, ¿se puede poner $k + 1$ como suma de treses y cincos? Distiguiremos dos casos, $b > 0$ y $b = 0$.

Si $b > 0$ en la descomposición de k tenemos por lo menos un 5 y podremos poner

$$k = a \cdot 3 + (b - 1) \cdot 5 + 5.$$

Por lo tanto

$$k + 1 = a \cdot 3 + (b - 1) \cdot 5 + 6 = (a + 2) \cdot 3 + (b - 1) \cdot 5.$$

Si $b = 0$, tenemos que k es múltiplo de 3, es decir $k = a \cdot 3$. Pero como $k \geq 8$, entonces $k = 9, 12, 15, 18, \ldots$, lo que quiere decir que $a \geq 3$. De esta forma podemos escribir

$$k = (a - 3) \cdot 3 + 9$$

y, en consecuencia

$$k + 1 = (a - 3) \cdot 3 + 10 = (a - 3) \cdot 3 + 2 \cdot 5.$$

Por tanto, si k cumple la propiedad también la cumple $k + 1$. Puesto que la base de la inducción está probada para $n = 8$, podemos concluir que todo número mayor o igual que 8 se puede expresar como suma de treses y cincos. ∎

1.2 El algoritmo de la división

Otra consecuencia relevante del principio del buen orden es el conocido algoritmo de la división.

Teorema 2 *(Algoritmo de la división) Dados dos enteros a y b, con $b > 0$, entonces existen $q, r \in \mathbb{Z}$ únicos tales que $a = q \cdot b + r$ con $0 \leq r < b$.*

Si aplicamos reiteradamente el algoritmo de la división llegamos a la representación de un número en una base de numeración $b \geq 2$. En efecto, podemos poner, para un entero $a > 0$

$$\begin{aligned} a &= q_0 \cdot b + r_0, \\ q_0 &= q_1 \cdot b + r_1, \\ &\vdots \\ q_{n-1} &= q_n \cdot b + r_n, \quad (q_n = 0). \end{aligned}$$

Notar que, debido a que $0 \leq q_{k+1} < q_k$, en algún momento tenemos que encontrar un n para el que $q_n = 0$. Mediante sustituciones reiteradas, se tiene

$$\begin{aligned} a &= q_0 \cdot b + r_0 = (q_1 \cdot b + r_1) \cdot b + r_0 = q_1 \cdot b + r_1 \cdot b + r_0, \\ a &= q_2 \cdot b^3 + r_2 \cdot b^2 + r_1 \cdot b + r_0, \\ &\vdots \\ a &= r_n \cdot b^n + r_{n-1} \cdot b^{n-1} + \cdots + r_2 \cdot b^2 + r_1 \cdot b + r_0. \end{aligned}$$

De esta forma pondremos $a = (r_n r_{n-1} \ldots r_2 r_1 r_0)_b$ y diremos que es la expresión de a en base b.

Ejemplo 7.- Expresar 4165 en base 7.

$$\begin{array}{rl|l} 4165 & & 7 \\ \hline r_0 \to 0 & 595 & 7 \\ \hline r_1 \to 0 & 85 & 7 \\ \hline r_2 \to 1 & 12 & 7 \\ \hline r_3 \to 5 & 1 & 7 \\ \hline r_4 \to 1 & 0 & \end{array}$$

Así, $4165 = (15100)_7 = 0 + 0 \cdot 7 + 1 \cdot 7^2 + 5 \cdot 7^3 + 1 \cdot 7^4$. ■

Ejemplo 8.- ¿Qué número es $(4165)_7$?

$(4165)_7 = 5 + 6 \cdot 7 + 1 \cdot 7^2 + 4 \cdot 7^3 = 1468$. ■

También pueden representarse fracciones en otras bases de numeración, así como números irracionales. Para ello basta tener en cuenta la notación posicional a la que estamos acostumbrados en base 10. En este sentido, si

$$\frac{1}{4} = 0.25$$

lo que queremos decir en realidad es que

$$\frac{1}{4} = 2 \cdot 10^{-1} + 5 \cdot 10^{-2}.$$

De esta forma, el punto no hace más que separar las potencias positivas de las potencias negativas de la base de numeración.

Consideremos una base de numeración b y una fracción $\frac{M}{N}$ de forma que $M < N$ y M y N sin divisores comunes, entonces

$$\frac{M}{N} = \frac{M \cdot b}{N \cdot b}.$$

Por el algoritmo de la división $M \cdot b = q_{-1} \cdot N + r_{-1}$, por lo que

$$\frac{M}{N} = \frac{q_{-1} \cdot N + r_{-1}}{N \cdot b} = q_{-1} \cdot b^{-1} + \frac{r_{-1}}{N \cdot b}.$$

Repitiendo el procedimiento con $\frac{r_{-1}}{N \cdot b}$ llegamos a

$$\frac{M}{N} = q_{-1} \cdot b^{-1} + q_{-2} \cdot b^{-2} + \frac{r_{-2}}{N \cdot b^2}.$$

El proceso se repite hasta que $r_{-k} = 0$ ó hasta que $r_{-k} = r_{-j}$ con $j < k$. En el primer caso, el número de cifras decimales es finito, mientras que en el segundo caso el número de cifras decimales es infinito, aunque éstas se repiten periódicamente.

Ejemplo 9.- Representar $\frac{1}{3}$ en base 2.

$$\begin{array}{rcl|l} r_0 = 1 & \xrightarrow{\times 2} & 2 & 3 \\ \hline & & 2 & 0 \quad \to q_{-1} \\ & \swarrow & & \\ \times 2 & & & \\ & \searrow & & \\ & & 4 & 3 \\ \hline & & 1 & 1 \quad \to q_{-2} \\ & & \downarrow & \end{array}$$

$r_{-2} = r_0 = 1 \Longrightarrow$ representación periódica infinita.

De esta forma, $\frac{1}{3} = 0.\,\widehat{01}_2$, donde $\frown$ indica que la secuencia 01 se repite infinitamente. ■

Para recuperar la fracción, a partir de su representación decimal en base b, podemos proceder de dos formas. La primera consiste en sumar las potencias negativas de b multiplicadas por el coeficiente correspondiente. Así,

$$\begin{aligned} 0.\,\widehat{01}_2 &= 0\cdot 2^{-1}+1\cdot 2^{-2}+0\cdot 2^{-3}+1\cdot 2^{-4}+0\cdot 2^{-5}+1\cdot 2^{-6}+\cdots = \\ &= 2^{-2}+2^{-4}+2^{-6}+\cdots = 2^{-2}\left(1+2^{-2}+2^{-4}+2^{-6}+\cdots\right) \end{aligned}$$

Para obtener la fracción, tenemos que sumar la serie

$$1+2^{-2}+2^{-4}+2^{-6}+\cdots$$

que es una progresión geométrica de razón 2^{-2} (cada sumando se obtiene multiplicando el anterior por la razón). Para sumar una progresión geométrica de razón r basta ver que

$$\begin{array}{r} S = 1+r+r^2+r^3+\cdots \\ rS = r+r^2+r^3+r^4+\cdots \\ \hline S-rS = 1 \end{array} \quad -$$

por tanto $S=\dfrac{1}{1-r}$ y en nuestro caso

$$1+2^{-2}+2^{-4}+2^{-6}+\cdots = \frac{1}{1-2^{-2}} = \frac{4}{3},$$

por lo que

$$0.\,\widehat{01}_2 = 2^{-2}\frac{4}{3} = \frac{1}{3}.$$

La otra forma de recuperar la fracción es darse cuenta que desplazar el punto decimal a la izquierda una posición equivale a multiplicar por b. Por tanto, si $F = 0.\,\widehat{01}_2$ entonces

$$2^2F = 1.\,\widehat{01}_2 \Longrightarrow 2^2F - F = 1_2 = 1 \Longrightarrow F = \frac{1}{3}.$$

1.3 Divisibilidad

Cuando el resto de una división es 0, decimos que los números a y b son divisibles. De esta manera llegamos al concepto de divisibilidad.

Definición 3 *Si $a, b \in \mathbb{Z}$ y $b \neq 0$, se dice que b divide a a, y se escribe $b|a$, si existe $c \in \mathbb{Z}$ tal que $a = b\cdot c$. Cuando esto ocurre, se dice que b es un divisor de a o bien que a es un múltiplo de b.*

Ejemplo 10.- Probar que n^2+3n es divisible por 2.

Basta ver que n^2+3n se puede factorizar y escribirse como

$$n^2+3n = n(n+3).$$

Si n es par, entonces el número resultante es divisible por 2. Si n es impar, entonces $n+3$ tiene que ser par y, por tanto, de nuevo el número resultante es divisible por 2. ∎

Ejemplo 11.- Probar que si $d|n$ y $c\left|\dfrac{n}{d}\right.$, entonces $c|n$ y $d\left|\dfrac{n}{c}\right.$.

Como $d|n$, entonces existe k tal que $n = k\cdot d$, por lo tanto $\dfrac{n}{d} = k$.

Por otra parte, como $c\left|\dfrac{n}{d}\right.$ se tiene que $k = \dfrac{n}{d} = c\cdot k'$. Por lo tanto

$$n = k\cdot d = k'\cdot d\cdot c \Longrightarrow c|n \quad \text{y} \quad \frac{n}{c} = k'\cdot d.$$

Por último, resulta que $d\left|\dfrac{n}{c}\right.$. ∎

A partir de la definición de divisibilidad, se pueden clasificar los números enteros positivos en dos clases. Los que llamaremos números primos, y el resto, que llamaremos compuestos.

Definición 4 *Un entero $p \geq 2$ se dice que es primo si sus únicos divisores son 1 y p.*

Es interesante resaltar que, como consecuencia del principio del buen orden, si un número es compuesto, entonces existe un primo que lo divide. Además, el número de primos es infinito.

A partir del concepto de divisibilidad llegamos a definir *el máximo común divisor* de dos enteros a y b, que denotaremos por m.c.d.(a, b).

Definición 5 *Dados dos enteros a y b, decimos que d es el máximo común divisor de a y b si cumple*

i) $d|a$ *y* $d|b$.

ii) Si $c|a$ *y* $c|b$, *entonces* $c|d$.

iii) $d \geq 1$.

Si m.c.d.$(a, b) = 1$ *diremos que los números son primos entre sí, o relativamente primos.*

El principio del buen orden garantiza la existencia y unicidad del máximo común divisor de dos números. Además podemos encontrar un algoritmo general que permite calcularlo. Este algoritmo se conoce como *Algoritmo de Euclides* y está basado en el algoritmo de la división y en la siguiente propiedad derivada de la divisibilidad.

Propiedad 1 *Si $a|b$ y $a|c$, entonces $a|(b \cdot x + c \cdot y)$, cualesquiera que sean x, y.*

Como $a|b$ entonces $b = k \cdot a$. Análogamente, $c = k' \cdot a$. Por lo tanto

$$b \cdot x + c \cdot y = k \cdot a \cdot x + k' \cdot a \cdot y = a \cdot (k \cdot x + k' \cdot y).$$

Es decir, $a|(b \cdot x + c \cdot y)$. ∎

Si queremos calcular $d =$ m.c.d.(a, b) y suponemos $0 < a < b$, mediante el algoritmo de la división obtenemos

$$a = q \cdot b + r \Longrightarrow r = a - q \cdot b.$$

Por la propiedad 1, resulta que $d|r$ y en consecuencia

$$\text{m.c.d.}(a, b) = \text{m.c.d.}(b, r).$$

Como quiera que $0 \leq r < b$, la repetición de este procedimiento nos conduce al máximo común divisor, que será el último resto distinto de 0. En la tabla 1 se reproduce el algoritmo de Euclides para el cálculo del m.c.d.$(1232, 344)$.

Además el algoritmo de Euclides nos proporciona una forma constructiva de obtener el máximo común divisor de dos números como una combinación lineal entera de éstos.

Teorema 3 *Sean a y b dos números enteros con $b > 0$ y sea $d =$ m.c.d.(a, b), entonces existen $m, n \in \mathbb{Z}$ tales que $d = m \cdot a + n \cdot b$.*

Apliquemos el algoritmo de Euclides

$$\begin{aligned}
a &= q_1 \cdot b + r_1 \\
b &= q_2 \cdot r_1 + r_2 \\
r_1 &= q_3 \cdot r_2 + r_3 \\
&\vdots \\
r_{n-2} &= q_n \cdot r_{n-1} + r_n r_{n-1} = q_{n+1} \cdot r_n
\end{aligned}$$

Entonces $r_n =$ m.c.d.(a, b) por ser el último resto distinto de 0. Procedamos ahora por un procedimiento de sustitución, marcha atrás, comenzando en la última división con resto.

$$\begin{aligned}
d = r_n &= r_{n-2} - q_n \cdot r_{n-1} = \\
&= r_{n-2} - q_n \cdot (r_{n-3} - q_{n-1} \cdot r_{n-2}) = r_{n-2} \cdot (1 + q_n \cdot q_{n-1}) - r_{n-3} \cdot q_n = \\
&= \cdots\cdots\cdots\cdots\cdots\cdots\cdots\cdots = m \cdot a + n \cdot b.
\end{aligned}$$

En la tabla 1 se muestra un ejemplo de cómo se realiza este proceso. ∎

$1232 \mid 344$ $200 \mid 3$		$8 = 7 \cdot 344 - 12 \cdot (1232 - 3 \cdot 344) = 43 \cdot 344 - 12 \cdot 1232$
$344 \mid 200$ $144 \mid 1$		$8 = 7 \cdot (344 - 200) - 5 \cdot 200 = 7 \cdot 344 - 12 \cdot \boxed{200}$ ($\boxed{200}$: $\uparrow$)
$200 \mid 144$ $56 \mid 1$		$8 = 2 \cdot 144 - 5 \cdot (200 - 144) = 7 \cdot \boxed{144} - 5 \cdot 200$ ($\boxed{144}$: $\uparrow$)
$144 \mid 56$ $32 \mid 2$		$8 = 2 \cdot (144 - 56 \cdot 2) - 56 = 2 \cdot 144 - 5 \cdot \boxed{56}$ ($\boxed{56}$: $\uparrow$)
$56 \mid 32$ $24 \mid 1$		$8 = 32 - (56 - 32) = 2 \cdot \boxed{32} - 56$ ($\boxed{32}$: $\uparrow$)
$32 \mid 24$ $8 \mid 1$		$8 = 32 - \boxed{24}$ ($\boxed{24}$: $\uparrow$)
$24 \mid \boxed{8}$ $0 \mid 3$	$\longrightarrow$	$8 =$ m.c.d.$(1232, 344)$ (último resto distinto de 0) ($\boxed{8}$: $\uparrow$)

Table 1: Cálculo del máximo común divisor de dos enteros a y b mediante el algoritmo de Euclides y esquema por el cual es posible expresar éste mediante una combinación entera de a y b.

Una aplicación del teorema anterior se puede ver en el siguiente ejemplo

Ejemplo 12.- Si $a|b \cdot c$ y m.c.d.$(a, b) = 1$ entonces $a|c$.

Por ser m.c.d.$(a, b) = 1$, existen $m, n \in \mathbb{Z}$ tales que $m \cdot a + n \cdot b = 1$. Multiplicando esta indentidad por c resulta

$$m \cdot c \cdot a + n \cdot b \cdot c = c. \tag{3}$$

Por otra parte, como $a|b \cdot c$, existe $k \in \mathbb{Z}$ tal que $b \cdot c = k \cdot a$ y sustituyendo en (3) se tiene

$$m \cdot c \cdot a + n \cdot k \cdot a = c$$

y por tanto $a|c$ ya que $c = a \cdot (m \cdot c + n \cdot k)$. ∎

Una consecuencia inmediata del ejemplo anterior es que $\sqrt{2}$ no es un número racional.

Ejemplo 13.- Probar que no existen a, b enteros positivos tales que $\sqrt{2} = \dfrac{a}{b}$ y m.c.d.$(a, b) = 1$.

Supongamos que $\sqrt{2} = \dfrac{a}{b}$ y m.c.d.$(a, b) = 1$. Elevando al cuadrado

$$2 \cdot b^2 = a^2.$$

Como m.c.d.$(a, b) = 1$ entonces m.c.d.$(a^2, b^2) = 1$ y, por el ejemplo 12, $2|a^2$. Por lo tanto $2|a$ y podemos poner $a = 2 \cdot k$. Así, $a^2 = 4 \cdot k^2$ y entonces

$$2 \cdot b^2 = 4 \cdot k^2 \Longrightarrow b^2 = 2 \cdot k^2.$$

Repitiendo el mismo argumento que antes resulta que $2|b$. Pero esto contradice el hecho de que m.c.d.$(a, b) = 1$. En consecuencia, la hipótesis de partida es falsa y $\sqrt{2}$ no es un número racional. ∎

1.4 Ecuaciones diofánticas

Una de las aplicaciones más interesantes del máximo común divisor es la resolución de las llamadas *ecuaciones diofánticas.*

Definición 6 *Una ecuación diofántica lineal de n incógnitas es una ecuación de la forma*

$$a_1x_1 + a_2x_2 + \cdot + a_nx_n = b,$$

donde $a_1, a_2, \ldots, a_n$ *y* b *son números enteros conocidos y* $x_1, x_2, \ldots, x_n$ *son números enteros a determinar.*

Si nos centramos en ecuaciones de dos incógnitas, trataremos de encontrar todas las soluciones enteras posibles de la ecuación

$$a \cdot x + b \cdot y = c, \tag{4}$$

donde a, b y c son enteros conocidos.

La primera observación que debemos hacer es que este tipo de ecuaciones tiene solución si y sólo si el máximo común divisor de a y b es un divisor de c. En efecto, sea m.c.d.$(a, b) = d$, entonces, por la propiedad 1, d divide a $a \cdot x + b \cdot y$. Por lo tanto para que la ecuación (4) tenga solución es necesario que $d|c$. Así pues, podemos suponer, sin pérdida de generalidad, que en la ecuación (4) se cumple m.c.d.$(a, b) = 1$. En caso contrario, basta dividir por el máximo común divisor. Ahora, por el teorema 3, existen m y n tales que $m \cdot a + n \cdot b = 1$. Multiplicando esta igualdad por c obtenemos una solución de la ecuación (4), esto es

$$x = c \cdot m, \qquad y = c \cdot n.$$

Para obtener todas las soluciones posibles de (4), consideramos la ecuación *homogénea*

$$a \cdot x + b \cdot y = 0, \tag{5}$$

cuyas soluciones enteras se obtienen de manera sencilla si despejamos una de las incógnitas. Así,

$$x = -\frac{b}{a}y.$$

Como m.c.d.$(a, b) = 1$, por el ejemplo 12, x es un número entero si a es un divisor de y. Por lo tanto, podemos poner $y = k \cdot a$ y las soluciones de (5) son de la forma

$$x = -k \cdot b, \qquad y = k \cdot a, \quad k \in \mathbb{Z}.$$

Es evidente que si a una solución de (4) le sumo una solución de (5) obtengo una solución de (4) (basta sumar las ecuaciones). En consecuencia, todas las posibles soluciones de (4) son de la forma

$$x = c \cdot m - k \cdot b, \qquad y = c \cdot n + k \cdot a, \quad k \in \mathbb{Z}.$$

Ejemplo 14.- Encontrar todas las soluciones enteras no negativas de la ecuación $7 \cdot x + 13 \cdot y = 147$.

En primer lugar, vemos que le ecuación se puede resolver por ser m.c.d.$(7, 13) = 1$.

Por el algoritmo de Euclides, encontramos que

$$1 = 2 \cdot 7 - 1 \cdot 13.$$

Multiplicando por 147, se obtiene

$$147 = 294 \cdot 7 - 147 \cdot 13.$$

Así, una solución es $x = 294$, $y = -147$. Sin embargo, para obtener el total de soluciones hay que añadir las soluciones de la ecuación homogenea

$$7 \cdot x + 13 \cdot y = 0,$$

que son de la forma $x = -13 \cdot k$, $y = 7 \cdot k$. Finalmente, se tiene que

$$x = 294 - 13 \cdot k, \qquad y = -147 + 7 \cdot k, \quad k \in \mathbb{Z}.$$

Como estamos interesados en las soluciones no negativas tiene que ser

$$294 - 13 \cdot k \geq 0 \Longrightarrow k \leq \frac{294}{13} = 22.615,$$
$$-147 + 7 \cdot k \geq 0 \Longrightarrow k \geq \frac{147}{7} = 21.$$

por lo tanto $21 \leq k \leq 22.615$. Puesto que $k \in \mathbb{Z}$, los únicos valores posibles de k que hacen que la solución sea no negativa son $k = 21$ y $k = 22$. En estos casos la solución es

$$k = 21, \qquad x = 21, \qquad y = 0.$$
$$k = 22, \qquad x = 8, \qquad y = 7.$$

■

Una vez visto cómo se resuelven las ecuaciones con dos incógnitas, no es difícil generalizar el procedimiento al caso general. Para ello, basta tener en cuenta que el concepto de máximo común divisor puede generalizarse a una colección arbitraria de enteros.

Definición 7 *El máximo común divisor de los enteros $a_1, a_2, \ldots, a_n$ ($d = m.c.d.(a_1, a_2, \ldots, a_n)$) es el mayor entero positivo que divide a todos y cada uno de los a_i. Si $d = 1$ diremos que los enteros son primos entre sí.*

Una observación importante es que si

$$d = \text{m.c.d.}(a_1, a_2, \ldots, a_n) \quad \text{y} \quad d' = \text{m.c.d.}(a_1, a_2, \ldots, a_{n-1}),$$

entonces $d = \text{m.c.d.}(d', a_n)$. Además, se puede ver que existen enteros $m_1, m_2, \ldots, m_n$ tales que

$$d = m_1 \cdot a_1 + m_2 \cdot a_2 + \cdots + m_n \cdot a_n.$$

Teniendo esto en cuenta, pueden resolverse ecuaciones diofánticas de n incógnitas.

Ejemplo 15.- Resolver la ecuación $6 \cdot x + 15 \cdot y + 10 \cdot z = 173$.

Aplicamos el algoritmo de Euclides para calcular m.c.d.$(6, 15, 10)$. En este sentido,

$$\text{m.c.d.}(6, 15, 10) = \text{m.c.d.}(\text{m.c.d.}(6, 15), 10).$$

Ahora bien, m.c.d.$(6, 15) = 3$ y

$$3 = \text{m.c.d.}(6, 15) = -2 \cdot 6 + 15. \tag{6}$$

Por otra parte, m.c.d.$(3, 10) = 1$ y

$$1 = \text{m.c.d.}(3, 10) = -3 \cdot 3 + 10. \tag{7}$$

Finalmente, teniendo en cuenta (6) y (7), resulta

$$1 = \text{m.c.d.}(6, 15, 10) = 6 \cdot 6 - 3 \cdot 15 + 10.$$

Por lo tanto una solución de la ecuación es

$$x = 6 \cdot 173 = 1038, \qquad y = -3 \cdot 173 = -519, \qquad z = 173.$$

Para obtener el total de soluciones, consideramos la ecuación homogénea

$$6 \cdot x + 15 \cdot y + 10 \cdot z = 0.$$

Despejando x se tiene

$$x = -\frac{15}{6}y - \frac{10}{6}z = -\frac{5}{2}y - \frac{5}{3}z,$$

y para que las soluciones sean enteras, tiene que ser $y = 2 \cdot k$ y $z = 3 \cdot k'$. Por lo tanto, la solución general se puede poner como

$$x = 1038 - 5 \cdot (k + k'), \qquad y = -519 + 2 \cdot k, \qquad z = 173 + 3 \cdot k', \quad k, k' \in \mathbb{Z}.$$

■

2 Combinatoria

Se entiende por *combinatoria* el estudio, técnicas y métodos para contar el número de elementos de un conjunto finito.

Contar los elementos de un conjunto A es establecer una biyección del conjunto $\mathbb{N}_n = \{1, 2, \ldots, n\}$ con A. Si tal biyección existe, se dice que el conjunto A es *finito* y que su número de elementos, o cardinal, es n. A este número lo denotamos por $\text{card}(A) = |A|$. No obstante, debemos asegurar que el cardinal de un conjunto es único, es decir, debemos probar que si existe $b : \mathbb{N}_n \longrightarrow A$ biyectiva, no existe otra aplicación biyectiva de $\mathbb{N}_m$ en A con $m \neq n$. Esto es una consecuencia directa del siguiente teorema.

Teorema 4 *Si $m < n$, no existe ninguna aplicación inyectiva de $\mathbb{N}_n$ en $\mathbb{N}_m$.*

Supongamos que el conjunto

$$S = \{\, n \in \mathbb{N} \;\big|\; \text{existe una plicación inyectiva } \; i : \mathbb{N}_n \longrightarrow \mathbb{N}_k \; \text{ para algún } \; k < n\}$$

es no vacío. Por el principio del buen orden existe mínimo, que llamamos n_0. Evidentemente, $n_0 > 1$. Consideremos, ahora, $i : \mathbb{N}_{n_0} \longrightarrow \mathbb{N}_k$ inyectiva. Resulta que $k > 1$, pues en otro caso, al ser $n_0 \geq 2$, todos los elementos tendrían como imagen $k = 1$ y, entonces, i no sería inyectiva.

Supongamos que $i(j) \neq k$ si $1 \leq j \leq n_0 - 1$, entonces la aplicación $i : \mathbb{N}_{n_0-1} \longrightarrow \mathbb{N}_{k-1}$ (restricción de i a $\mathbb{N}_{n_0-1}$) sería inyectiva. Entonces $n_0 - 1 \in S$, pero esto es absurdo, pues n_0 era el mínimo.

Supongamos que existe j, $1 \leq j \leq n_0 - 1$ tal que $i(j) = k$, entonces $i(n_0) = p < k$. Si consideramos la aplicación $i_* : \mathbb{N}_{n_0-1} \longrightarrow \mathbb{N}_{k-1}$ definida por $i_*(j) = p$; $i_*(x) = i(x)$ si $x \neq j$, sería inyectiva. De nuevo, resultaría que $n_0 - 1 \in S$, cosa que es absurda. Por lo tanto, no puede ser $S \neq \emptyset$ y el teorema queda probado. ∎

Además de justificar rigurosamente que el cardinal de un conjunto finito es único, de este teorema se deducen otras dos consecuencias importantes. Una de ellas es la existencia de conjuntos infinitos.

Definición 8 *Diremos que un conjunto no vacío A es infinito si no existe ninguna aplicación biyectiva de $\mathbb{N}_n$ en A, cualquiera que sea $n \in \mathbb{N}$ (notar que $\mathbb{N}$ es infinito).*

La propiedad más interesante de los conjuntos infinitos es que tienen subconjuntos propios con tantos elementos como el todo. Es decir, se puede establecer una biyección entre una parte del conjunto y el propio conjunto.

Ejemplo 16.- Hay tantos números pares como números naturales.

Basta ver que se puede establecer una biyección entre los números $1, 2, 3 \ldots$ y los números pares $2, 4, 6, \ldots$. Pero esto es sencillo, ya que la aplicación

$$\begin{aligned} b : \mathbb{N} &\longrightarrow \{2, 4, 6, \ldots\} \\ n &\mapsto 2n \end{aligned}$$

es claramente biyectiva. Es decir, una parte de $\mathbb{N}$ tiene tantos elementos como $\mathbb{N}$. ∎

Por otra parte, también es interesante hacer notar que no todos los conjuntos infinitos son equivalentes (en el sentido de que se pueden poner en correspondencia biyectiva). En este sentido, los números reales, $\mathbb{R}$, representan un conjunto infinito de mayor orden que los números naturales. Una prueba de ello la dio Cantor[1], estableciendo que no existe una biyección entre los números naturales y el conjunto de números decimales de la forma $0.a_1a_2a_3 \cdots a_n \cdots$.

La otra consecuencia es el llamado *principio del palomar* (también denominado principio de Dirichlet, de las cajas o del casillero).

Principio del palomar.- Si m objetos se distribuyen en n cajas y $m > nr$, enonces hay al menos una caja que tiene más de r objetos.

[1] ver apéndice 3 del libro *Matemáticas Discreta y Combinatoria* de R. P. Grimaldi, teorema A3.4

Las aplicaciones de este principio, casi obvio, son muchas, aunque no siempre triviales. Pongamos un par de ejemplos.

Ejemplo 17.- Probar que, dados 12 números enteros cualesquiera (incluso repetidos), siempre hay dos cuya diferencia es múltiplo de 11.

Por el principio de la división, todo número entero puede expresarse como $11 \cdot q + r$, con $0 \leq r < 11$. Si $a_1, a_2, \ldots, a_{12}$ son los 12 números seleccionados, entonces

$$a_k = 11 \cdot q_k + r_k, \qquad 1 \leq k \leq 12.$$

Como $0 \leq r_k < 11$, sólo hay 11 posibles restos diferentes. Ahora bien, como tenemos una colección de 12 restos, por el principio del palomar, debe haber al menos dos iguales. Sean esos restos r_i y r_j, entonces

$$a_i - a_j = 11 \cdot q_i + r_i - (11 \cdot q_j + r_j) = 11 \cdot (q_i - q_j).$$

Por lo tanto $a_i - a_j$ es múltiplo de 11. ∎

Ejemplo 18.- Sea A un subconjunto de seis elementos de $\mathbb{N}_{14}$. Probar que A tiene al menos dos subconjuntos no vacíos cuyos elementos suman lo mismo.

Como A tiene 6 elementos, el total de subconjuntos diferentes de A es 2^6 (ver más adelante el ejemplo 21), de los cuales uno es el conjunto vacío. Por lo tanto A tiene 63 subconjuntos diferentes no vacíos. A cada uno de esos subconjuntos le podemos asociar la suma de sus elementos, lo que hace un total de 63 sumas diferentes posibles.

Por otro lado, la mayor suma que puede obtenerse es la correspondiente a la suma de todos los elementos del propio conjunto A, que en el peor de los casos será

$$9 + 10 + 11 + 12 + 13 + 14 = 69.$$

Sin embargo, en este caso, la menor de las sumas sería 9, lo que hace que la suma de los elementos de los subconjuntos de A sea un número comprendido entre 9 y 69. Como esto nos da un total de 61 sumas posibles y hay 63 subconjuntos diferentes, por el principio del palomar, hay al menos dos sumas repetidas.

Dejamos como ejercicio el ver qué pasaría si el conjunto A no es $\{9, 10, 11, 12, 13, 14\}$. ∎

2.1 Principios básicos de conteo

Las técnicas combinatorias para contar o enumerar los elementos de un conjunto se basan en una serie de principios elementales.

Principio de adición.- Sean A y B dos conjuntos finitos tales que $A \cap B = \emptyset$, entonces $|A \cup B| = |A| + |B|$.

Este principio se generaliza por inducción. Así, si $A_1, A_2, \ldots, A_n$ es una colección de conjuntos disjuntos dos a dos, es decir $A_i \cap A_j = \emptyset$ si $i \neq j$, entonces

$$|A_1 \cup A_2 \cup \cdots \cup A_n| = |A_1| + |A_2| + \cdots + |A_n|.$$

Notemos que el principio del palomar es una consecuencia del principio generalizado de la suma. Así, si las cajas las denominamos $A_1, A_2, \ldots, A_n$ y cada caja contiene menos de r elementos, entonces, por el principio de adición,

$$|A_1 \cup A_2 \cup \cdots \cup A_n| \leq nr < m.$$

Es decir, el total de elementos que hay en todas las cajas, es inferior al número de objetos que hemos repartido m.

También consecuencia del principio de adición, es el *principio de inclusión-exclusión.*

Principio de inclusión-exclusión.- Sean A y B dos conjuntos finitos, entonces

$$|A \cup B| = |A| + |B| - |A \cap B|.$$

Al igual que el principio de adición, podemos generalizar este principio por inducción. En este sentido, si tenemos una colección A_i $(1 \leq i \leq n)$ de conjuntos finitos, entonces

$$|A_1 \cup A_2 \cup \cdots \cup A_n| =$$

$$\sum_{i=1}^{n} |A_i| - \sum_{1 \leq i < j \leq n} |A_i \cap A_j| + \sum_{1 \leq i < j < k \leq n} |A_i \cap A_j \cap A_k| + \cdots\cdots + (-1)^{n-1} |A_1 \cap A_2 \cap \cdots \cap A_n|.$$

Ejemplo 19.- ¿Cuántos enteros hay, entre 1 y 1000, que no son divisibles por 3, por 7 o por 11?

Sean

$$A = \{\text{enteros entre 1 y 1000 divisibles por 3}\},$$
$$B = \{\text{enteros entre 1 y 1000 divisibles por 7}\},$$
$$C = \{\text{enteros entre 1 y 1000 divisibles por 11}\}.$$

Lo que nos pide el problema es $|(A \cup B \cup C)^c| = 1000 - |A \cup B \cup C|$. Ahora bien como uno de cada tres números es múltiplo de 3, resulta[2]

$$|A| = \left\lfloor \frac{1000}{3} \right\rfloor = 333.$$

Análogamente, $|B| = \left\lfloor \frac{1000}{7} \right\rfloor = 142$ y $|C| = \left\lfloor \frac{1000}{11} \right\rfloor = 90$. Por otra parte, podemos determinar los cardinales de las intersecciones teniendo en cuenta que si $x \in |A \cap B|$, entonces x es múltiplo de 21, por tanto

$$|A \cap B| = \left\lfloor \frac{1000}{21} \right\rfloor = 47, \quad |A \cap C| = \left\lfloor \frac{1000}{33} \right\rfloor = 30, \quad |B \cap C| = \left\lfloor \frac{1000}{77} \right\rfloor = 12,$$

$$|A \cap B \cap C| = \left\lfloor \frac{1000}{231} \right\rfloor = 4.$$

Finalmente, por el principio de inclusión-exclusión

$$|A \cup B \cup C| = 333 + 142 + 90 - (47 + 30 + 12) + 4 = 480$$

y por tanto la solución del problema es $\boxed{520}$. ∎

Principio del producto.- Sean A y B dos conjuntos finitos, entonces $|A \times B| = |A| \cdot |B|$.

Este principio también se generaliza por inducción para el producto cartesiano de una colección finita de conjuntos, $A_1, A_2, \ldots, A_n$. En este sentido,

$$|A_1 \times A_2 \times \cdots \times A_n| = |A_1| \cdot |A_2| \cdots |A_n|.$$

Podría decirse que, conocidos los principios básicos del conteo, la combinatoria está estudiada. Sin embargo, aparecen con frecuencia conjuntos equipotentes a cuyo cardinal se le da un nombre especial.

2.2 Variaciones con repetición

Supongamos que queremos contar el total de posibles aplicaciones que pueden construirse de un conjunto X, de m elementos, en otro conjunto Y, de n elementos.
Una aplicación $f : X \longrightarrow Y$ queda completamente determinada si conocemos cada una de las imágenes de los m elementos de X. Es decir, debemos conocer $f(x_i)$ con $1 \leq i \leq m$. Esto equivale a dar una m-tupla

$$(f(x_1), f(x_2), \ldots, f(x_m))$$

[2] $\lfloor a \rfloor$ representa el entero m más próximo a a tal que $m < a$. Comunmente se denomina parte entera de a.

del conjunto $Y^m = \overbrace{Y \times Y \times \cdots \times Y}^{m \text{ veces}}$. También es equivalente a dar una palabra de m letras del alfabeto Y ($f(x_1)f(x_2)\cdots f(x_n)$) o a dar una selección ordenada de m elementos entre los de Y (notar que pueden repetirse elementos de Y, es decir, $f(x_i) = f(x_j)$ con $i \neq j$).

La única condición es que $f(x_i) \in Y$. Por tanto el total de aplicaciones de X en Y, o el total de *variaciones con repetición de n elementos tomados de m en m*, es igual al cardinal de Y^m que, por el principio del producto, es m^n. Si denotamos a este número por $\mathrm{VR}_m^n = \mathrm{SO}(n, m)$, entonces

$$\mathrm{VR}_m^n = \mathrm{SO}(n, m) = n^m.$$

El ejemplo más conocido sobre variaciones con repetición es el siguiente

Ejemplo 20.- ¿Cuál es la probabilidad de acertar en una quiniela el pleno al quince?

Nótese que dar una quiniela es dar una lista de 15 símbolos (1, X, 2), es decir, una palabra de longitud 15, construida con el alfabeto (1, X, 2). Por tanto, según lo visto, el total de quinielas posibles es $\mathrm{VR}(3, 15) = 3^{15}$ y la probabilidad pedida es

$$p = \frac{1}{3^{15}} = 6.969171937625632\, 10^{-8}.$$

Es interesante observar que el problema es equivalente a distribuir 15 objetos diferentes (los partidos) en tres cajas etiquetadas (1, X, 2). Más adelante volveremos al problema de las distribuciones. ∎

Otro ejemplo, no tan conocido, nos permite determinar el total de subconjuntos diferentes que tiene un conjunto dado A.

Ejemplo 21.- Dado un conjunto A, de n elementos, probar que el total de subconjuntos diferentes de A es 2^n.

Por ejemplo si $A = \{1, 2, 3\}$, el conjunto de todos los subconjuntos de A, que recibe el nombre de *partes de A*, ($\mathcal{P}(A)$), es

$$\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}.$$

En este caso se tiene $|\mathcal{P}(A)| = 2^3$ como dice el enunciado del problema. Para ver que esto es así en general, podemos identificar cada subconjunto con una palabra de longitud n del alfabeto $(0, 1)$. Un cero en la posición k significará que el elemento k-ésimo no pertenece al subconjunto, mientras que un uno indicará que sí pertenece. En este sentido, para el caso $A = \{1, 2, 3\}$, se tiene la siguiente correspondencia entre subconjuntos y palabras

$$\begin{array}{lcllcl} \emptyset & \longrightarrow & 000 & \{1,2\} & \longrightarrow & 110 \\ \{1\} & \longrightarrow & 100 & \{1,3\} & \longrightarrow & 101 \\ \{2\} & \longrightarrow & 010 & \{2,3\} & \longrightarrow & 011 \\ \{3\} & \longrightarrow & 001 & \{1,2,3\} & \longrightarrow & 111 \end{array}$$

Por lo tanto, el total de subconjuntos es el total de aplicaciones entre el conjunto A y el conjunto $\{0, 1\}$, es decir 2^n. ∎

2.3 Variaciones

Supongamos ahora que queremos contar el total de posibles aplicaciones inyectivas que pueden construirse de un conjunto X, de m elementos, en otro conjunto Y, de n elementos (notar que $m \leq n$).

Como en el caso de las variaciones con repetición, la aplicación queda determinada si conocemos las imágenes de todos los elementos de A. De nuevo podemos ver la aplicación como una m-tupla de Y^m, sólo que esta vez

$$S = \{f : A \longrightarrow B \mid f \text{ inyectiva}\}$$

no coincide con Y^m. S es un subconjunto propio de Y^m, ya que dos elementos de A no pueden tener la misma imagen. Dicho de otra forma, si consideramos la aplicación f como una palabra de m letras del alfabeto Y, ésta no tiene letras repetidas. Así, si la aplicación f es $f(x_1)f(x_2)f(x_3)\cdots f(x_n)$, entonces

$$\begin{aligned}
&f(x_1) \in Y,\\
&f(x_2) \in Y \setminus \{f(x_1)\},\\
&f(x_3) \in Y \setminus \{f(x_1), f(x_2)\},\\
&\quad\vdots\\
&f(x_n) \in Y \setminus \{f(x_1), f(x_2), \ldots, f(x_{n-1})\}.
\end{aligned}$$

Si denotamos por V_m^n al total de aplicaciones inyectivas de A en B y lo llamamos *variaciones de n elementos tomados de m en m*, entonces, por el principio del producto,

$$\mathrm{V}_m^n = n(n-1)(n-2)\cdots(n-m+1) = \frac{n!}{(n-m)!},$$

donde $n! = n \cdot (n-1) \cdot (n-2)\cdots 2 \cdot 1$ es el producto de todos los números naturales desde 1 hasta n.

Ejemplo 22.- ¿Cuál es la probabilidad de que entre un grupo de n personas haya dos que celebren el cumpleaños el mismo día?

Calcularemos la probabilidad del suceso contrario que es más sencilla. Es decir, calcularemos la probabilidad de que las n personas celebren su cumpleaños en diferentes días. Esto es equivalente a dar una lista ordenada de n días distintos de entre los 365 días del año. Por lo tanto, el total de casos favorables es

$$\text{casos favorables} = \mathrm{V}_n^{365} = \frac{365!}{(365-n)!}.$$

Por otra parte, los casos posibles son todas las posibles listas ordenadas de n días, es decir,

$$\text{casos posibles} = \mathrm{VR}_n^{365} = 365^n.$$

Finalmente, la probabilidad pedida es

$$p = 1 - \frac{\text{casos favorables}}{\text{casos posibles}} = \frac{\mathrm{V}_n^{365}}{\mathrm{VR}_n^{365}} = \frac{365!}{365^n(365-n)!}.$$

A continuación damos una pequeña tabla con algunos valores de p para distintos valores de n

Nº de personas (n)	probabilidad (p)	Nº de personas (n)	probabilidad (p)
5	0.027136	35	0.814383
10	0.116948	40	0.891232
15	0.252901	45	0.940976
20	0.411438	50	0.970374
21	0.443688	55	0.986262
22	0.475695	60	0.994123
23	0.507297	65	0.997683
24	0.538344	70	0.999160
25	0.568700	75	0.999720
26	0.598241	80	0.999914
27	0.626859	85	0.999976
28	0.654461	90	0.999994
29	0.680969	95	0.99999856
30	0.706316	100	0.99999969

Observar que a partir de 22 personas, la probabilidad es superior al 50% y que a partir de 40 personas la probabilidad es superior al 90%. ∎

2.4 Permutaciones

Una *permutación* de un conjunto A es una aplicación biyectiva de A en A. El total de permutaciones de A coincide con el total de aplicaciones inyectivas de A en A, por tanto, si $|A| = n$, el total de permutaciones será[3]

$$\mathrm{P}(n) = \mathrm{V}_n^n = n(n-1)(n-2)\cdots 2\cdot 1 = \frac{n!}{0!} = n!.$$

En general, si f es una biyección entre dos conjuntos A y B con $|A| = |B| = n$ se identifica la biyección

$$\begin{aligned} f : A &\longrightarrow B \\ a_i &\mapsto f(a_i) = b_j \end{aligned}$$

con la *permutación* $\pi : \mathbb{N}_n \longrightarrow \mathbb{N}_n$ tal que $\pi(i) = j$ si $f(a_i) = b_j$. La permutación π se escribe

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \pi(1) & \pi(2) & \pi(3) & \dots & \pi(n) \end{pmatrix}$$

Las permutaciones pueden componerse, en el sentido de que si se aplican dos permutaciones seguidas se obtiene una nueva permutación. El conjunto de permutaciones de *orden n* se denota por S_n y es evidente que $|S_n| = n!$.

Ejemplo 23.- Componer las permutaciones

$$\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 3 & 1 & 7 & 4 & 6 & 2 \end{pmatrix} \quad \text{y} \quad \pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 4 & 2 & 3 & 1 & 7 & 6 \end{pmatrix}$$

Como la primera permutación envía el 1 al 5 y la segunda envía el 5 al 1, resulta, $\pi_2 \circ \pi_1(1) = 1$ y entonces

$$\pi_2 \circ \pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 2 & 5 & 6 & 3 & 7 & 4 \end{pmatrix}$$

■

algunas permutaciones reciben nombres específicos, como los *ciclos*.

Definición 9 *Una permutación $\sigma \in S_n$ es un ciclo de longitud r si deja fijos $n - r$ elementos y permuta circularmente los otros r. Es decir, existe una ordenación $(i_1, i_2, \dots, i_r)$ tal que*

$$\begin{aligned} &\sigma(i_j) = i_{j+1}, \qquad 1 \le j \le r-1, \\ &\sigma(i_r) = i_1, \\ &\sigma(k) = k \qquad \forall k \in \mathbb{N}_n \setminus \{i_1, i_2, \dots, i_r\}. \end{aligned}$$

El ciclo se escribe como $(i_1\, i_2\, \dots\, i_r)$.

Ejemplo 24.- La permutación $\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 1 & 4 & 2 & 6 & 7 & 3 \end{pmatrix}$ es un ciclo de longitud 7 que se escribe $(1\,5\,6\,7\,3\,4\,2)$.

Ejemplo 25.- La permutación $\pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 2 & 3 & 1 & 4 \end{pmatrix}$ es un ciclo de longitud 3 que se escribe $(1\,5\,4)$.

El resultado más interesante sobre ciclos es el siguiente

Teorema 5 *Toda permutación puede ponerse como una composición de ciclos.*

La manera de demostrarlo, sin entrar en muchos detalles, es como sigue. Sea σ la permutación de S_n que queremos descomponer en ciclos. Comencemos por considerar el 1 y la secuencia $\sigma(1)$, $\sigma^2(1) = \sigma(\sigma(1))$, $\sigma^3(1)$, ..., hasta encontrar un $r \le n$ tal que $\sigma^r(1) = 1$. De esta forma tenemos el ciclo $(1\,\sigma(1)\,\sigma^2(1)\,\dots\,\sigma^{r-1}(1))$. Si $r = n$ hemos terminado y σ es un ciclo de longitud n que recibe el nombre de *permutación cíclica*. Si $r < n$, tomamos un número i_1 que no esté en el ciclo del 1 y calculamos $\sigma(i_1)$, $\sigma^2(i_1)$, ..., hasta llegar a un $s \le n - r$ tal que $\sigma(i_1) = i_1$. Obtenemos el ciclo $(i_1\,\sigma(i_1)\,\dots\,\sigma^{s-1}(i_1))$. Si $r + s = n$ hemos terminado y

$$\sigma = (1\,\sigma(1)\,\sigma^2(1)\,\dots\,\sigma^{r-1}(1)) \circ (i_1\,\sigma(i_1)\,\dots\,\sigma^{s-1}(i_1)).$$

En caso contrario, continuamos hasta incluir todos los números en algún ciclo. ■

[3] Por convenio se toma $0! = 1$

Ejemplo 26.- Descomponer en ciclos la permutación

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 5 & 7 & 8 & 4 & 6 & 1 & 2 & 9 \end{pmatrix}.$$

Siguiendo la demostración del Teorema anterior, empezamos por considerar el ciclo al que pertenece el 1. De esta forma vemos cuál es la imagen del 1, luego la imagen de la imagen y así sucesivamente hasta regresar al 1.

$$1 \longrightarrow 3 \longrightarrow 7 \longrightarrow 1 \equiv (1\,3\,7).$$

Tomamos ahora el primer número no incluido en el ciclo anterior y construimos el ciclo al que pertenece, $(2\,5\,4\,8)$. Continuamos hasta ver que

$$\sigma = (1\,3\,7)(2\,5\,4\,8)(6)(9).$$

■

Aplicaciones de la descomposición en ciclos pueden encontrarse en diferentes trucos de magia realizados con una baraja. Se trata de aparentar un desordenamiento de las cartas, cuando en realidad se están haciendo ciertas permutaciones, cuya descomposición en ciclos se conoce. Para ello, resulta útil saber que si un ciclo de longitud r se itera r veces, entonces todos los elementos quedan como al principio. Es decir, $\sigma^r(k) = k$, $1 \leq k \leq n$.

Ejemplo 27.- Los números del 1 al 15 están dispuestos en forma de matriz 3×5. Se reordenan, leyendo los números por filas y escrbiéndolos por columnas

$$\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ 6 & 7 & 8 & 9 & 10 \\ 11 & 12 & 13 & 14 & 15 \end{array} \qquad \longrightarrow \qquad \begin{array}{ccccc} 1 & 4 & 7 & 10 & 13 \\ 2 & 5 & 8 & 11 & 14 \\ 3 & 6 & 9 & 12 & 15 \end{array}$$

¿Después de cuántas repeticiones de este proceso la tabla quedará como al principio?

El reordenamiento de la tabla no es más que una permutación de S_{15}, que descompuesta en ciclos se escribe como

$$(1)(2\,4\,10\,14\,12\,6)(3\,7\,5\,13\,9\,11)(8)(15)$$

Por lo tanto como los ciclos son de longitud 1 ó 6, depués de 6 repeticiones la tabla quedará como estaba. ■

2.4.1 Números de Stirling de primera clase

Planteemos la siguiente pregunta: ¿Cuántas permutaciones de S_n se descomponen en k ciclos? Denotemos a este número por $\left[{n \atop k}\right]$, que denominaremos *número de Stirling de primera clase.*

Algunos de estos números son fáciles de calcular. Por ejemplo, $\left[{n \atop n}\right]$ representa el total de permutaciones que se descomponen en n ciclos. En este caso, cada elemento forma un ciclo de forma única y por tanto $\left[{n \atop n}\right] = 1$.

También es fácil calcular $\left[{n \atop 1}\right]$. Ahora se trata de ver cuántas permutaciones se descomponen en un sólo ciclo. Para ello, observemos que los siguientes ciclos son equivalentes

$$(A\,B\,C\,D) \equiv (B\,C\,D\,A) \equiv (C\,D\,A\,B) \equiv (D\,A\,B\,C).$$

De alguna manera, el primer elemento del ciclo lo podemos fijar y sólo es necesario cambiar los siguientes elementos de orden para obtener ciclos distintos. Por lo tanto

$$\begin{bmatrix} n \\ 1 \end{bmatrix} = (n-1)!$$

Supongamos que conocemos los números de Stirling de primera clase para el caso de las permutaciones de $n-1$ elementos y queremos calcular $\left[{n \atop k}\right]$. Distinguiremos dos situaciones:

n	$\begin{bmatrix} n \\ 1 \end{bmatrix}$		$\begin{bmatrix} n \\ 2 \end{bmatrix}$		$\begin{bmatrix} n \\ 3 \end{bmatrix}$		$\begin{bmatrix} n \\ 4 \end{bmatrix}$		$\begin{bmatrix} n \\ 5 \end{bmatrix}$		$\begin{bmatrix} n \\ 6 \end{bmatrix}$	$\begin{bmatrix} n \\ 7 \end{bmatrix}$
1	**1**											
2	**1**		**1**									
		↘	×2 ↓									
3	**2**		**3**		**1**							
		↘	×3 ↓	↘	×3 ↓							
4	**6**		**11**		**6**		**1**					
		↘	×4 ↓	↘	×4 ↓	↘	×4 ↓					
5	**24**		**50**		**35**		**10**		**1**			
		↘	×5 ↓	↘	×5 ↓	↘	×5 ↓	↘	×5 ↓			
6	**120**		**274**		**225**		**85**		**15**		**1**	
		↘	×6 ↓	↘	×6 ↓	↘	×6 ↓	↘	×6 ↓	↘	×6 ↓	
7	**720**		**1754**		**1624**		**735**		**175**		**21**	**1**

Table 2: Números de Stirling de primera clase.

En la primera supondremos que el elemento n forma un ciclo de longitud 1. Entonces, los $n-1$ elementos restantes están en $k-1$ ciclos, lo que aporta un total de $\begin{bmatrix} n-1 \\ k-1 \end{bmatrix}$ posibles descomposiciones.
En la segunda supondremos que n no es un ciclo de longitud 1. Por tanto ahora los $n-1$ elementos restantes están en k ciclos, mientras que n puede ser introducido en cualquiera de ellos de todas las formas posibles. Por ejemplo, si tenemos la descomposición

$$(A\,B\,C)(D\,E)$$

y queremos insertar un sexto elemento F, lo podemos hacer de las 5 maneras siguientes

$$\begin{gathered}(A\,F\,B\,C)(D\,E),\\ (A\,B\,F\,C)(D\,E),\\ (A\,B\,C\,F)(D\,E),\\ (A\,B\,C)(D\,F\,E),\\ (A\,B\,C)(D\,E\,F).\end{gathered}$$

Generalizando, n puede introducirse de $n-1$ formas diferentes y esto nos da $(n-1)\begin{bmatrix} n-1 \\ k \end{bmatrix}$ nuevas descomposiciones. Por lo tanto

$$\begin{bmatrix} n \\ k \end{bmatrix} = \begin{bmatrix} n-1 \\ k-1 \end{bmatrix} + (n-1)\begin{bmatrix} n-1 \\ k \end{bmatrix}. \tag{8}$$

En la tabla 2 se dan los números de Stirling hasta $n = 7$. Observar que si se suman todos los números de Stirling en una misma fila (fila k-ésima por ejemplo) se obtiene el factorial de k.

La relación de recurrencia (8) permite construir una *función generadora* de los números de Stirling. En efecto, si denotamos por $x^{\overline{n}}$ al siguiente producto

$$x^{\overline{n}} = \overbrace{x(x+1)(x+2)\dots(x+n-1)}^{n \text{ factores}},$$

entonces, aplicando (8) y utilizando el principio de inducción matemática, resulta

$$x^{\overline{n}} = \begin{bmatrix} n \\ 1 \end{bmatrix} x + \begin{bmatrix} n \\ 2 \end{bmatrix} x^2 + \begin{bmatrix} n \\ 3 \end{bmatrix} x^3 + \cdots + \begin{bmatrix} n \\ n \end{bmatrix} x^n = \sum_{k=1}^{n} \begin{bmatrix} n \\ k \end{bmatrix} x^k. \tag{9}$$

De alguna manera, la función $F(x) = x^{\overline{n}}$ genera los números de Stirling, ya que una vez desarrollada nos permitiría generar la misma tabla 2, sin necesidad de recordar la forma en que fue construida. Es

decir, la función $F(x)$ recoge la propiedad fundamental de recurrencia de estos números. De esta forma, si quisiéramos conocer los números de Stirling para $n = 8$, basta calcular $F(x)$ con $n = 8$. Así,

$$x^{\overline{8}} = 5040x + 13068x^2 + 13132x^3 + 6769x^4 + 1960x^5 + 322x^6 + 28x^7 + x^8$$

y, por ejemplo $\begin{bmatrix} 8 \\ 5 \end{bmatrix} = 1960$.

2.5 Combinaciones

Sea A un conjunto de n elementos y preguntémonos por el total de subconjuntos de k elementos diferentes que podemos formar. Cada uno de estos subconjuntos puede entenderse como una selección (no ordenada) de k elementos de los n elementos del conjunto de partida. También diremos que se trata de una *combinación de n elementos tomados de k en k, o de orden k.*

Al número de subconjuntos de k elementos ($0 \leq k \leq n$) de un conjunto de n elementos se le denota por $\binom{n}{k}$ y se dice *n sobre k*, o también, *número o coeficiente binomial* o *combinaciones de n sobre r*.

Para calcular $\binom{n}{k}$ observemos que cada aplicación inyectiva $f : \mathbb{N}_k \longrightarrow A$ define un subconjunto de k elementos de A, que es el conjunto de las imágenes de $\mathbb{N}_k$, esto es $S = \{f(1), f(2), \ldots, f(k)\}$. Ahora bien, este subconjunto está generado por $k!$ aplicaciones inyectivas diferentes (basta ordenar de todas las formas posibles las imágenes). Por tanto, se tiene que el total de aplicaciones inyectivas es $k!$ veces el total de subconjuntos de k elementos de A, es decir,

$$\mathrm{V}_k^n = k!\binom{n}{k} \Longrightarrow \binom{n}{k} = \frac{\mathrm{V}_k^n}{k!} = \frac{n!}{k!(n-k)!}.$$

Otra forma de calcular los coeficientes binomiales es apoyándose en lo que representan. Así, es fácil ver que

$$\binom{n}{0} = 1, \quad \binom{n}{1} = n, \quad \binom{n}{n} = 1, \quad \binom{n}{k} = 0,\ k > n,$$

ya que, por ejemplo, $\binom{n}{n}$ representa el total de subconjuntos de n elementos que pueden formarse a partir de un conjunto A con n elementos. Esto es, obviamente, uno. A partir de estas relaciones básicas se tiene el siguiente resultado.

Teorema 6 *Para cada k tal que* $1 \leq k \leq n$ *se verifica* $\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k}$.

Sea A un conjunto de n elementos y $x \in A$ un elemento cualquiera de A. Los subconjuntos de k elementos de A pueden dividirse en dos clases:

a) Aquellos que contienen al elemento x, que podemos escribir como

$$U = \{S \subset A \,|\, |S| = k \text{ y } x \in S\}.$$

b) Aquellos que no contienen al elemento x, esto es,

$$V = \{S \subset A \,|\, |S| = k \text{ y } x \notin S\}.$$

Es evidente que $\binom{n}{k} = |U \cup V| = |U| + |V|$ ya que $U \cap V = \emptyset$.

Observemos que $S \in U$ si y sólo si $S \setminus \{x\}$ es un subconjunto de $k-1$ elementos de $A \setminus \{x\}$. De esta froma en U hay tantos elementos como selecciones de $k-1$ elementos puedan hacerse de un conjunto de $n-1$ elementos y, por tanto, $|U| = \binom{n-1}{k-1}$.

Análogamente, $S \in V$ si y sólo si S es un subconjunto de $k-1$ elementos de $A \setminus \{x\}$. Por lo tanto $|V| = \binom{n-1}{k}$.

De lo anterior se sigue que $\binom{n}{k-1} = \binom{n-1}{k} + \binom{n-1}{k}$. ∎

Lo que este resultado nos proporciona es una forma recursiva de calcular los coeficientes binomiales como se puede ver en la tabla 3, que recibe el nombre de triángulo de Pascal o de Tartaglia. Obsérvese que la suma de cada una de las filas es igual a 2^n, es decir, el total de subconjuntos de un conjunto de n elementos (ver ejemplo 21). Esto puede probarse también gracias al teorema del binomio.

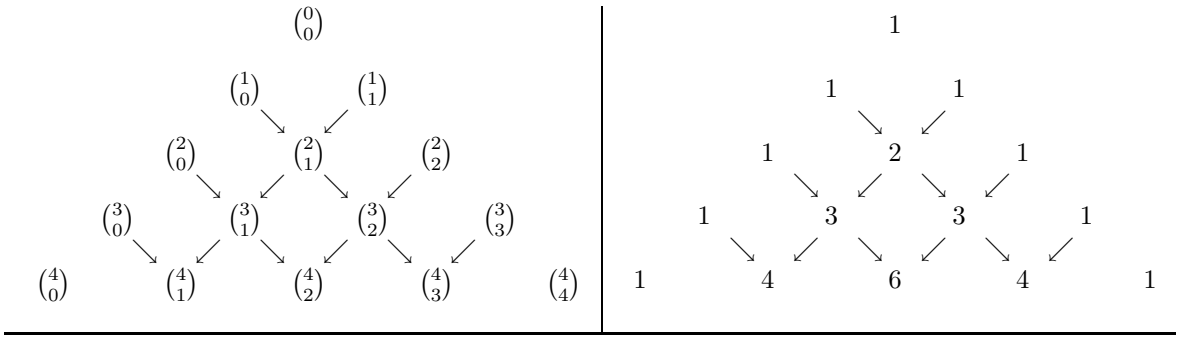

Table 3: Triángulo de Pascal para el cálculo recursivo de los coeficientes binomiales

Teorema 7 *(Teorema del binomio) Sean a y b números reales y $n \geq 1$, entonces se verifica*

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \cdots + \binom{n}{k}a^{n-k}b^k + \cdots + \binom{n}{n}b^n = \sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k.$$

Se tiene que $(a+b)^n = \overbrace{(a+b)(a+b)\cdots(a+b)}^{\text{n veces}}$. Por lo tanto, obtenemos un término de la forma $a^{n-k}b^k$ cuando multipliquemos a de $n-k$ factores y b de k factores. Pero esto puede hacerse de $\binom{n}{k}$ formas, ya que basta especificar los k factores, de los n posibles, correspondientes a las b. ∎

A partir de este teorema se pueden deducir algunas relaciones relevantes como las que se apuntan a continuación:

1.- $\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots + \binom{n}{n} = 2^n$.

2.- $\binom{n}{0} - \binom{n}{1} + \binom{n}{2} + \cdots + (-1)^{n-1}\binom{n}{n-1} + (-1)^n\binom{n}{n} = 0$.

3.- $\binom{n}{0}^2 + \binom{n}{1}^2 + \binom{n}{2}^2 + \cdots + \binom{n}{n}^2 = \binom{2n}{n}$.

Las dos primeras son inmediatas de ver sin más que tomar $a = b = 1$ en el primer caso y $a = 1$, $b = -1$ en el segundo caso. La tercera de las relaciones surge de la aplicación del teorema del binomio para $(1+x)^{2n}$, ya que

$$(1+x)^{2n} = (1+x)^n(1+x)^n$$

y entonces

$$\binom{2n}{0} + \binom{2n}{1}x + \cdots + \binom{2n}{n}x^n + \cdots + \binom{2n}{2n}x^{2n} = \left[\binom{n}{0} + \binom{n}{1}x + \cdots + \binom{n}{n}x^n\right]^2.$$

La identidad se obtiene al comparar los coeficientes de x^n.

Los ejemplos en los que podemos aplicar combinaciones son muchos. Por ejemplo, nos sirven para calcular las probabilidades de acertar en la primitiva.

Ejemplo 28.- Calcular la probabilidad de acertar en un sorteo de lotería primitiva: *a)* los 6 números, *b)* 5 y el complementario.

Como en ejemplos anteriores, la probabilidad se obtiene a través del cociente

$$p = \frac{\text{casos favorables}}{\text{casos posibes}}.$$

Ahora bien, los casos posibles son todas las posibles elecciones de 6 números de entre 49 posibles, esto es

$$\text{casos posibles} = \binom{49}{6} = 13983816.$$

Por otra parte, sólo hay un caso favorable para acertar los 6 números y entonces la probabilidad pedida es

$$p_6 = \frac{1}{13983816} = 7.151123842018516\,10^{-8}.$$

Para calcular ahora la probabilidad de acertar 5 más el complementario, notemos que deberemos haber marcado necesariamente el complementario y 5 números más de entre los otros 6 de la extracción. Por lo tanto los casos favorables son $\binom{6}{5} = 6$ y la probabilidad pedida es

$$p_{5+c} = \frac{6}{13983816} = 4.290674305211111\,10^{-7},$$

que como se ve es 6 veces mayor que la de acertar los 6 números. ∎

Como ejercicio puede verse que $p_5 = 0.0000180208$, $p_4 = 0.00096862$ y $p_3 = 0.0176504$.

Ejemplo 29.- Dado el conjunto $\mathbb{N}_{2n}$, calcular el total de sunconjuntos que tienen igual de números pares que impares.

Podemos dividir el conjunto $\mathbb{N}_{2n}$ en dos partes disjuntas, separando los números pares de los impares. De este modo, formamos los conjuntos

$$\mathcal{P} = \{k \in \mathbb{N}_{2n} \,|\, k \text{ es par}\}, \qquad \mathcal{I} = \{k \in \mathbb{N}_{2n} \,|\, k \text{ es impar}\},$$

que tienen cada uno de ellos n elementos.

Así, para formar un subconjunto con el mismo número de pares que de impares hay que tomar igual número de elementos del conjunto $\mathcal{P}$ que del $\mathcal{I}$. En este sentido, si tomamos k elementos de cada conjunto, el total de subconjuntos con k pares y k impares es $\binom{n}{k}\binom{n}{k}$. Por lo tanto el total de subconjuntos será

$$\binom{n}{0}^2 + \binom{n}{1}^2 + \binom{n}{2}^2 + \cdots + \binom{n}{n}^2$$

y por la relación 3 de los coeficientes binomiales esto es igual a $\binom{2n}{n}$.

Este resultado puede obtenerse directamente si nos fijamos en lo siguiente. Cada vez que elegimos un subconjunto de n elementos de $\mathbb{N}_{2n}$, automáticamente se forma otro con otros n elementos. Llamemos a estos subconjuntos A y B. Resulta que si A tiene k números pares entonces tiene $n-k$ impares y, por lo tanto, B tiene $n-k$ pares y k impares. Juntemos ahora los k números pares de A con los k números impares de B y entonces tenemos un subconjunto con tantos números pares como impares. Es decir, a cada elección de n elementos de $\mathbb{N}_{2n}$ le corresponde un conjunto con el mismo número de pares que de impares y, a la inversa, a cada subconjunto C con el mismo número de pares que de impares le corresponde un subconjunto de n elementos de $\mathbb{N}_{2n}$ (basta tomar $A = \{k \in C \,|\, \text{k par}\} \cup \{k \in \mathbb{N}_{2n} \setminus C \,|\, k \text{ impar}\}$). Por lo tanto el total de subconjuntos con la misma cantidad de pares que de impares es igual al total de selecciones de n elementos de entre los $2n$ de $\mathbb{N}_{2n}$, esto es, $\binom{2n}{n}$. ∎

2.6 Combinaciones con repetición

Sea $A = \{a_1, a_2, \ldots, a_n\}$ un conjunto de n elementos. Una *combinación con repetición de orden k* (o una combinación con repetición de n elementos tomados de k en k) es un conjunto de k elementos formado con elementos de A, donde éstos se pueden repetir. Esto equivale a dar una lista no ordenada de longitud k, formada con elementos de A, los cuales se pueden repetir.

Dar una lista de estas características es lo mismo que decir cuántas veces aparece en la lista cada uno de los elementos de A. De este modo hay una correspondencia uno a uno entre las combinaciones con repetición de orden k y las soluciones enteras no negativas de la ecuación

$$x_1 + x_2 + x_3 + \cdots + x_n = k.$$

Cada $x_i \geq 0$ es el número de veces que aparece en la lista el elemento a_i.

Ejemplo 30.- ¿De cuántas maneras pueden colorearse cinco pelotas con dos colores?

Esto equivale a dar una lista no ordenada de longitud 5, formadas con los dos colores disponibles, supongamos b y r. Esto es lo mismo que decir cuántas pelotas pintamos de cada color. Por lo tanto a cada solución de la ecuación

$$x_1 + x_2 = 5$$

le corresponde una combinación con repetición de 2 elementos tomados de 5 en 5. Como las posibles soluciones son

$$\begin{array}{llll} x_1 = 5, & x_2 = 0; & x_1 = 2, & x_2 = 3; \\ x_1 = 4, & x_2 = 1; & x_1 = 1, & x_2 = 4; \\ x_1 = 3, & x_2 = 2; & x_1 = 0, & x_2 = 5, \end{array}$$

el total de combinaciones con repetición de 2 elementos tomados de 5 en 5 es 6. ∎

Para calcular el total de combinaciones con repetición de n elementos de orden k ($\mathrm{CR}(n,k)$) podemos proceder de dos formas. En primer lugar observemos que toda combinación con repetición puede escribirse como una secuencia de ceros y unos. En efecto, escribamos tantos unos como veces aparezca el elemento a_1 en la combinación, a continuación escribamos un 0, para indicar que vamos a empezar a contar el elemento a_2. A continuación escribamos tantos unos como veces esté a_2 en la combinación y así sucesivamente. Al final, habremos escrito k unos y $n-1$ ceros, es decir, tantos unos como elementos hay en la combinación y tantos ceros como separadores se necesitan entre los elementos de A. Veamos la relación entre las secuencias de ceros y unos y las combinaciones con repetición para el caso del ejemplo 30.

$$\begin{array}{llllll} x_1 = 5, & x_2 = 0, & \longrightarrow & x_1x_1x_1x_1x_1 & \longrightarrow & 111110, \\ x_1 = 4, & x_2 = 1, & \longrightarrow & x_1x_1x_1x_1x_2 & \longrightarrow & 111101, \\ x_1 = 3, & x_2 = 2, & \longrightarrow & x_1x_1x_1x_2x_2 & \longrightarrow & 111011, \\ x_1 = 2, & x_2 = 3, & \longrightarrow & x_1x_1x_2x_2x_2 & \longrightarrow & 110111, \\ x_1 = 1, & x_2 = 4, & \longrightarrow & x_1x_2x_2x_2x_2 & \longrightarrow & 101111, \\ x_1 = 0, & x_2 = 5, & \longrightarrow & x_2x_2x_2x_2x_2 & \longrightarrow & 011111. \end{array}$$

Como la correspondencia entre secuencias de ceros y unos y combinaciones con repetición es biyectiva resulta

$$\mathrm{CR}(n,k) = \binom{n+k-1}{k},$$

ya que basta especificar la posición de los k unos en la secuencia de longitud $n+k-1$ de ceros y unos.

También puede calcularse $\mathrm{CR}(n,k)$ de forma recursiva. Tomemos a_1 como elemento de referencia. Las combinaciones con repetición podemos dividirlas en dos clases: las que tienen al elemento a_1 y las que no. De la primera clase es evidente que hay tantas como combinaciones con repetición de $n-1$ elementos tomados de k en k. Para saber ahora cuántas hay de la segunda clase procedemos de la siguiente forma. Puesto que hay por lo menos un elemento a_1, quitamos uno y nos queda una combinación con repetición de n elementos tomados de $k-1$ en $k-1$. Por lo tanto,

$$\mathrm{CR}(n,k) = \mathrm{CR}(n-1,k) + \mathrm{CR}(n,k-1).$$

Por otra parte, es evidente que $\mathrm{CR}(n,1) = n$ y $\mathrm{CR}(1,k) = 1$. Así, podemos calcular las combinaciones con repetición mediante el esquema que se indica en la tabla 4.

Las combinaciones con repetición también pueden entenderse como *distribuciones*. De hecho, el problema de dar una lista no ordenada de longitud k, formada con los n elementos del conjunto A, donde éstos se pueden repetir, es equivalente a distribuir k objetos idénticos en n cajas etiquetadas. Resulta evidente que una tal distribución puede asociarse con una solución en enteros no negativos de la ecuación

$$x_1 + x_2 + x_3 + \cdots + x_n = k,$$

donde x_i representa el número de objetos que recibe la caja i-ésima. Pero esto mismo sucedía con las combinaciones con repetición.

Ejemplo 31.- ¿De cuántas formas pueden distribuirse 10 objetos idénticos en 5 cajas diferentes si ninguna puede quedar vacía?

$$\begin{array}{ccccccc}
\mathrm{CR}(1,1)=1 & & \mathrm{CR}(1,2)=1 & & \mathrm{CR}(1,3)=1 & & \mathrm{CR}(1,4)=1 \\
 & & \downarrow & & \downarrow & & \downarrow \\
\mathrm{CR}(2,1)=2 & \rightarrow & \mathrm{CR}(2,2)=3 & \rightarrow & \mathrm{CR}(2,3)=4 & \rightarrow & \mathrm{CR}(2,4)=5 \\
 & & \downarrow & & \downarrow & & \downarrow \\
\mathrm{CR}(3,1)=3 & \rightarrow & \mathrm{CR}(3,2)=6 & \rightarrow & \mathrm{CR}(3,3)=10 & \rightarrow & \mathrm{CR}(3,4)=15 \\
 & & \downarrow & & \downarrow & & \downarrow \\
\mathrm{CR}(4,1)=4 & \rightarrow & \mathrm{CR}(4,2)=10 & \rightarrow & \mathrm{CR}(4,3)=20 & \rightarrow & \mathrm{CR}(4,4)=35
\end{array}$$

Table 4: Cálculo recursivo de las combinaciones con repetición.

Como acabamos de ver, si llamamos x_i al número de objetos que recibe cada caja, el problema se reduce a calcular el total de soluciones de la ecuación

$$x_1 + x_2 + x_3 + x_4 + x_5 = 10,$$

con la condición $x_i \geq 1$.

Puesto que cada caja recibe por lo menos un objeto, podemos considerar que ya tenemos 5 objetos distribuidos y nos resta distribuir los otros 5 sin ninguna restricción. Por lo tanto, el total de distribuciones será el total de soluciones de la ecuación

$$x_1 + x_2 + x_3 + x_4 + x_5 = 5,$$

con la condición $x_i \geq 0$. Pero esto es $\mathrm{CR}(5,5) = 126$. ∎

Ejemplo 32.- ¿Cuántos números menores que 1.000.000 son tales que sus cifras suman 15?

Los números menores que 1.000.000 pueden ser considerados como números de seis cifras, donde éstas pueden ser cero en cualquiera de las posiciones. Así, el número 567 puede verse como 000567. Teniendo esto en cuenta y llamando c_i a las cifras del número, se tiene que cumplir que

$$c_1 + c_2 + c_3 + c_4 + c_5 + c_6 = 15, \tag{10}$$

con la condición $0 \leq c_i \leq 9$.

Si no hubiera restricciones, el total de soluciones de (10) sería $\mathrm{CR}(6,15) = 15504$. Ahora bien aquí estamos contando soluciones para las que alguna de las cifras es mayor que 9. Por lo tanto hay que descontar todas estas posibles soluciones.

Supongamos que una de las cifras, por ejemplo la última, valiera 10, entonces, las otras 5 deberían sumar 5. Si valiera 11, las otras sumarían 4. Si valiera 12, las otras sumarían 3, y así sucesivamente. Entonces, hay que restar todas las soluciones de las ecuaciones

$$\begin{array}{l}
x_1 + x_2 + x_3 + x_4 + x_5 = 5, \\
x_1 + x_2 + x_3 + x_4 + x_5 = 4, \\
x_1 + x_2 + x_3 + x_4 + x_5 = 3, \\
x_1 + x_2 + x_3 + x_4 + x_5 = 2, \\
x_1 + x_2 + x_3 + x_4 + x_5 = 1, \\
x_1 + x_2 + x_3 + x_4 + x_5 = 0.
\end{array} \tag{11}$$

Estas son

$$\begin{aligned}
\mathrm{CR}(5,5) + \mathrm{CR}(5,4) + \mathrm{CR}(5,3) + \mathrm{CR}(5,2) + \mathrm{CR}(5,1) + \mathrm{CR}(5,0) = \\
= 126 + 70 + 35 + 15 + 5 + 1 = 252.
\end{aligned}$$

Puesto que la cifra que puede valer más de 9 es cualquiera de las 6, la solución del problema será

$$15504 - 6 \cdot 252 = \boxed{13992}.$$

Veamos una forma de encontrar una solución más compacta del sistema de ecuaciones (11). Estas 6 ecuaciones se pueden resumir en la desigualdad

$$x_1 + x_2 + x_3 + x_4 + x_5 \leq 5.$$

Si introducimos una sexta variable x_6 y transformamos la desigualdad en igualdad, tendremos la ecuación

$$x_1 + x_2 + x_3 + x_4 + x_5 + x_6 = 5. \tag{12}$$

Puesto que $0 \leq x_6 \leq 5$, resulta que cuando $x_6 = 0$, las otras cinco variables satisfacen la primera de las ecuaciones en (11). Si $x_6 = 1$ las otras cinco variables satisfacen la segunda ecuación en (11) y así sucesivamenete. Por lo tanto, las soluciones de (11) son las soluciones de (12), es decir, $\mathrm{CR}(6,5) = 252$. Haciendo la misma consideración que antes, la solución del problema es $\mathrm{CR}(6,15) - 6 \cdot \mathrm{CR}(6,5) = 13992$. ■.

2.7 Permutaciones con repetición

Consideremos un conjunto $A = \{a_1, a_2, \ldots, a_k\}$ de k elementos y una lista ordenada de longitud n donde el elmento a_1 se repite α_1 veces, el a_2 α_2 veces y, en general, el a_i, α_i veces ($\alpha_1 + \alpha_2 + \cdots + \alpha_k = n$ y $\alpha_i \geq 0$). Esto es equivalente a distribuir n objetos diferentes en k cajas, de modo que la caja i-ésima recibe α_i objetos. También puede interpretarse como una aplicación de un conjunto de n elemetos en otro conjunto de k elementos (A) tal que envía α_1 elementos a a_1, …, α_k elementos a a_k.

Ejemplo 33.- Sea el conjunto $X = \{\mathrm{A}, \mathrm{B}, \mathrm{C}, \mathrm{D}, \mathrm{R}\}$ y consideremos la lista ordenada ABRACADABRA.

ABRACADABRA es una lista ordenada de elementos de X de longitud 11, donde A se repite 5 veces, B 2 veces, C una vez, D una vez y R dos veces. Esto es lo mismo que haber construido la siguiente aplicación de $\mathbb{N}_{11}$ en X

$$\begin{aligned} f : \mathbb{N}_{11} \longrightarrow X = \{\mathrm{A}, \mathrm{B}, \mathrm{C}, \mathrm{D}, \mathrm{R}\}; \quad & f(1) = f(4) = f(6) = f(8) = f(11) = \mathrm{A} \\ & f(2) = f(9) = \mathrm{B} \\ & f(3) = f(10) = \mathrm{R} \\ & f(5) = \mathrm{C} \\ & f(7) = \mathrm{D} \end{aligned}$$

o bien haber distribuido los objetos de N_{11} en las cajas A, B, C, D, R, de forma que la caja A recibe los objetos 1, 4, 6, 8, 11, la B los objetos 2 y 9, la C el objeto 5, la D el objeto 7 y la R los objetos 3 y 10. ■

Al total de listas distintas de longitud n formadas con α_1 veces a_1, …, α_k veces a_k se le representa por

$$\binom{n}{\alpha_1 \alpha_2 \ldots \alpha_k}, \qquad \alpha_1 + \alpha_2 + \cdots \alpha_k = n, \quad \alpha_i \geq 0.$$

A este número se le conoce como *coeficiente multinomial*.

Teorema 8 *Se verifica* $\binom{n}{\alpha_1 \alpha_2 \ldots \alpha_k} = \dfrac{n!}{\alpha_1! \alpha_2! \cdots \alpha_k!}$.

Podemos probarlo de dos formas diferentes. Visto el problema como una distribución de n objetos diferentes en k cajas, de forma que la caja i-ésima recibe α_i objetos, basta con determinar cuáles son los objetos que van a parar a cada una de las cajas. Como la primera caja recibe α_1 objetos, ésta puede recibir un total de $\binom{n}{\alpha_1}$ colecciones distintas de α_1 objetos. La segunda caja podrá recibir cualquier colección de α_2 objetos de los $n - \alpha_1$ restantes y así sucesivamente. Por tanto se tiene

$$\begin{aligned} \binom{n}{\alpha_1 \alpha_2 \ldots \alpha_k} &= \binom{n}{\alpha_1}\binom{n-\alpha_1}{\alpha_2}\binom{n-\alpha_1-\alpha_2}{\alpha_3} \cdots \binom{\alpha_k}{\alpha_k} = \\ &= \frac{n!}{\alpha_1!(n-\alpha_1)!} \frac{(n-\alpha_1)!}{\alpha_2!(n-\alpha_1-\alpha_2)!} \frac{(n-\alpha_1-\alpha_2)!}{\alpha_3!(n-\alpha_1-\alpha_2-\alpha_3)!} \cdots \frac{\alpha_k!}{\alpha_k!}, \end{aligned}$$

Figure 1:

de donde se sigue el resultado, sin más que simplificar.

La otra forma de verlo es considerando las ordenaciones los n elementos. Si todos fueran diferentes habría $n!$ ordenaciones. Ahora bien, como el primer elemento (a_1) se repite α_1 veces, la ordenación no cambiará si intercambio entre sí los elementos a_1. Como puedo intercambiarlos de $\alpha_1!$ formas distintas,, el total de ordenaciones habrá que dividirlo por ese factor. Razonando análogamente con el resto de elementos, llegamos al resultado pedido

$$\binom{n}{\alpha_1\alpha_2\ldots\alpha_k} = \frac{n!}{\alpha_1!\alpha_2!\cdots\alpha_k!}.$$

■

Ejemplo 34.- Doce platillos de forma idéntica se ordenan en cuatro columnas verticales, como se muestra en la figura 1. Hay cuatro de color rojo en la primera columna, tres de color azul en la segunda columna, dos verdes en la tercera columna y tres blancos en la cuarta. Para entrar en el equipo de tiro de la universidad es necesario romper los doce platillos (usando sólo 12 balas) y, para esto, siempre se debe romper el platillo que queda en la parte inferior de la columna. En estas condiciones, ¿de cuántas formas se puede disparar y romper los 12 platillos?

El problema es equivalente a ordenar los 12 platillos. Por ejemplo, la ordenación

$$RRBAAVRVBBAR$$

significa que primero disparamos a dos platillos rojos, luego a uno blanco, después a dos azules, etc. Por tanto la solución del problema son las ordenaciones de 12 elementos del conjunto $\{R, A, V, B\}$, donde R se repite 4 veces, A tres veces, V dos veces y B tres veces, es decir

$$\binom{12}{4\,3\,2\,3} = \frac{12!}{4!3!2!3!} = 277200.$$

■

Ejemplo 35.- ¿Cuál es la probabilidad de que al repartir una mano de tute, con una baraja española de 40 cartas, cada jugador reciba un as?

Como en ejemplos anteriores, la probabilidad pedida es

$$p = \frac{\text{casos favorables}}{\text{casos posibles}}.$$

Para determinar los casos posibles, vemos que lo que tenemos que hacer es distribuir 40 cartas distintas entre 4 jugadores diferentes, de forma que cada jugador recibe 10 cartas. Esto, según hemos visto es

$$\text{casos posibles} = \binom{40}{10\,10\,10\,10} = \frac{40!}{10!^4}.$$

Otra forma de llegar al mismo resultado es viendo que el primer jugador puede recibir un total de $\binom{40}{10}$ manos distintas, el segundo $\binom{30}{10}$, el tercero $\binom{20}{10}$ y el último $\binom{10}{10}$, Es decir

$$\text{casos posibles} = \binom{40}{10}\binom{30}{10}\binom{20}{10}\binom{10}{10} = \frac{40!}{10!^4}.$$

Para determinar los casos favorables, dividimos el problema en dos partes. En primer lugar repartimos los ases entre los 4 jugadores (4! formas diferentes) y después distribuimos las 36 cartas restantes. Razonando como antes se tiene

$$\text{casos favorables} = 4!\binom{36}{9\,9\,9\,9} = 4!\frac{36!}{9!^4}.$$

Por tanto $p = \dfrac{4!\,36!\,10!^4}{40!\,9!^4} = 0.109421.$ ∎

2.8 Particiones

Una partición de un conjunto A en k partes es una familia de k subconjuntos disjuntos no vacíos de A tales que su unión es el propio conjunto A. De esta forma si A_1, A_2, ..., A_k son los subconjuntos de la partición, entonces

1.- A_j no vacío.

2.- $A_i \cap A_j = \emptyset$ si $i \neq j$.

3.- $A_1 \cup A_2 U \cdots \cup A_k = A$.

¿Cuántas particiones diferentes se pueden hacer de un conjunto de n elementos en k partes? Llamemos a tal número $\left\{{n \atop k}\right\}$ que recibe el nombre de *número de Stirling de segunda clase*.

Tratemos de determinar el número de Stirling para algún conjunto concreto para ver si somos capaces de inferir algún procedimiento general. Supongamos que queremos contar todas las particiones de un conjunto de 4 elementos en dos partes ($\left\{{4 \atop 2}\right\}$).

Primera aproximación Hay dos tipos de particiones,

a) las que están formadas por dos subconjuntos de dos elementos

b) las que están formadas por uno de tres elementos y otro de uno.

Las de tipo *b)* se pueden contar fácilmente. Habrá 4 de ellas, ya que el subconjunto que sólo tiene un elemento puede elegirse de 4 formas distintas, tantas como elementos tiene el conjunto.

Para contar las de tipo *a)* podemos pensar que elegida una de las partes, la otra queda fijada. Como elegir una parte es elegir 2 elementos entre 4, resultará que hay $\binom{4}{2}$ particiones de este tipo. Por tanto el total de particiones sería $4 + \binom{4}{2} = 10$.

Sin embargo el total de particiones es 7. De alguna manera hemos contado de más en el razonamiento anterior. En efecto, consideremos la forma en que hemos contado las particiones de tipo *a*. Hemos determinado una de las partes de todas las formas posibles con la seguridad de que la otra parte queda completamente determinada. Examinemos esto más despacio

parte seleccionada	$\{1,2\}$	$\{1,3\}$	$\{1,4\}$	$\{2,3\}$	$\{2,4\}$	$\{3,4\}$
parte que queda determinada	$\{3,4\}$	$\{2,4\}$	$\{2,3\}$	$\{1,4\}$	$\{1,3\}$	$\{1,2\}$

Como vemos, la selección $\{1,2\}$ y la $\{3,4\}$ dan lugar a la misma partición. Lo mismo sucede con la $\{1,3\}$ y la $\{2,4\}$ o la $\{1,4\}$ y la $\{2,3\}$. En realidad cada partición aparece dos veces, por lo que en realidad sólo hay 3 particiones distintas de tipo *a)*, lo que hace un total de 7.

Segunda aproximación Como antes, dividiremos las particiones en dos tipos

a) Las que el $\{4\}$ es una de las partes

b) el resto de particiones, es decir aquéllas en las que el 4 está en una de las partes junto a otros elementos.

De las del tipo *a)* sólo hay una, pues el resto de elementos tiene que formar necesariamente la otra parte.

Las del segundo tipo pueden contarse si prescindimos del 4 y nos dedicamos a distribuir los otros 3 elementos en dos partes. Esto se puede hacer de 3 formas

$$[\{1\},\quad \{2,3\}]\quad [\{2\},\quad \{1,3\}]\quad [\{3\},\quad \{1,2\}]$$

Ahora insertemos el elemento 4 de todas las formas posibles en cada una de las partes

$$\underset{\nwarrow\ \nearrow\ \ \ 4}{[\{1\},\quad \{2,3\}]}\quad \underset{\nwarrow\ \nearrow\ \ \ 4}{[\{2\},\quad \{1,3\}]}\quad \underset{\nwarrow\ \nearrow\ \ \ 4}{[\{3\},\quad \{1,2\}]}$$

Hemos generado 6 particiones, lo que hace un total de 7.

Esta segunda forma de contar las particiones es la que se puede generalizar para llegar al siguiente resultado

Teorema 9 *Se verifica* $\begin{cases} \left\{ {n \atop k} \right\} = \left\{ {n-1 \atop k-1} \right\} + k\left\{ {n-1 \atop k} \right\}, \\ \left\{ {n \atop 1} \right\} = 1, \quad \left\{ {n \atop n} \right\} = 1. \end{cases}$

Basta seguir la segunda aproximación de antes. Consideremos dos tipos de particiones

- $\{n\}$ es una de las partes. El resto de $n-1$ elementos están en $k-1$ partes. En total $\left\{ {n-1 \atop k-1} \right\}$.
- n está en alguna de las partes con más elemenos. Prescindamos de n, entonces el resto de $n-1$ elementos está en k partes. Como el elemento n puede introducirse en cualquiera de las k partes, tenemos un total de $k\left\{ {n-1 \atop k} \right\}$.

Como sólo hay estos dos tipos de particiones se sigue que

$$\left\{ {n \atop k} \right\} = \left\{ {n-1 \atop k-1} \right\} + k\left\{ {n-1 \atop k} \right\}.$$

Por otra parte es evidente que $\left\{ {n \atop 1} \right\} = 1$, ya que sólo es posible dividir un conjunto en una parte. Del mismo modo es trivial que $\left\{ {n \atop n} \right\} = 1$. ∎

Este resultado nos proporciona una forma recursiva de calcular los números de Stirling de segunda clase, como se ve en la tabla 5. Sin embargo, al igual que con los números de Stirling de primera clase, podemos encontrar estos números en otro contexto.

Consideremos el producto de potencias *decrecientes* de x

$$x^{\underline{k}} = \overbrace{x(x-1)(x-2)\dots(x-k+1)}^{k \text{ factores}},$$

y tratemos de expresar una potencia de x en términos de potencias decrecientes. Resulta que

$$\begin{aligned} x &= x^{\underline{1}}, \\ x^2 &= x^{\underline{2}} + x^{\underline{1}}, \\ x^3 &= x^{\underline{3}} + 3x^{\underline{2}} + x^{\underline{1}}, \\ x^4 &= x^{\underline{4}} + 6x^{\underline{3}} + 7x^{\underline{2}} + x^{\underline{1}}, \\ &\vdots \\ x^k &= \left\{ {k \atop k} \right\} x^{\underline{k}} + \left\{ {k \atop k-1} \right\} x^{\underline{k-1}} + \left\{ {k \atop k-2} \right\} x^{\underline{k-2}} + \cdots + \left\{ {k \atop 2} \right\} x^{\underline{2}} + \left\{ {k \atop 1} \right\} x^{\underline{1}}, \end{aligned} \tag{13}$$

ya que se cumple $x \cdot x^{\underline{k}} = x^{\underline{k+1}} + k \cdot x^{\underline{k}}$. Además, no es difícil comprobar que $x^n = \sum_{k=1}^{n} \left\{ {n \atop k} \right\} (-1)^k x^{\overline{k}}$.

De alguna forma, (13) puede verse como la forma de invertir la ecuación (9). Estas expresiones son de utilidad a la hora de sumar algunas series infinitas. Así, encontramos el siguiente algoritmo para series aritmético-geométricas

n	$\left\{ {n \atop 1} \right\}$		$\left\{ {n \atop 2} \right\}$		$\left\{ {n \atop 3} \right\}$		$\left\{ {n \atop 4} \right\}$		$\left\{ {n \atop 5} \right\}$		$\left\{ {n \atop 6} \right\}$		$\left\{ {n \atop 7} \right\}$
			$\times 2$		$\times 3$		$\times 4$		$\times 5$		$\times 6$		$\times 7$
1	1												
2	1		1										
		$\searrow$	$\downarrow$										
3	1		3		1								
		$\searrow$	$\downarrow$	$\searrow$	$\downarrow$								
4	1		7		6		1						
		$\searrow$	$\downarrow$	$\searrow$	$\downarrow$	$\searrow$	$\downarrow$						
5	1		15		25		10		1				
		$\searrow$	$\downarrow$	$\searrow$	$\downarrow$	$\searrow$	$\downarrow$	$\searrow$	$\downarrow$				
6	1		31		90		65		15		1		
		$\searrow$	$\downarrow$	$\searrow$	$\downarrow$	$\searrow$	$\downarrow$	$\searrow$	$\downarrow$	$\searrow$	$\downarrow$		
7	1		63		301		350		140		21		1

Table 5: Cálculo recursivo de los números de Stirling de segunda clase.

Algoritmo de sumación de series aritmético-geométricas.- Sea $P(n)$ un polinomio de grado k en n, tal que, expresado en términos de potencias crecientes de $(n+1)$ es de la forma

$$P(n) = \alpha_k (n+1)^{\overline{k}} + \alpha_{k-1}(n+1)^{\overline{k-1}} + \cdots + \alpha_2 (n+1)^{\overline{2}} + \alpha_1 (n+1)^{\overline{1}} + \alpha_0.$$

Entonces, resulta

$$\sum_{n=0}^{\infty} P(n)(ax)^n = \frac{\alpha_k\, k!}{(1-ax)^{k+1}} + \frac{\alpha_{k-1}\,(k-1)!}{(1-ax)^k} + \cdots + \frac{\alpha_2\, 2!}{(1-ax)^3} + \frac{\alpha_1}{(1-ax)^2} + \frac{\alpha_0}{(1-ax)}.$$

También hay un algoritmo similar para la sumación de series exponenciales de la forma $\displaystyle\sum_{n=0}^{\infty} P(n)\frac{(ax)^n}{n!}$, utilizando potencias decrecientes de n, en lugar de potencias crecientes. Así, se tiene

Algoritmo de sumación de series exponenciales.- Sea $P(n)$ un polinomio de grado k en n, tal que, expresado en términos de potencias decrecientes de n es de la forma

$$P(n) = \alpha_k n^{\underline{k}} + \alpha_{k-1} n^{\underline{k-1}} + \cdots + \alpha_2 n^{\underline{2}} + \alpha_1 n^{\underline{1}} + \alpha_0.$$

Entonces, resulta

$$\sum_{n=0}^{\infty} P(n)\frac{(ax)^n}{n!} = (\alpha_k (ax)^k + \alpha_{k-1}(ax)^{k-1} + \cdots + \alpha_2 (ax)^2 + \alpha_1 (ax) + \alpha_0) e^{ax}.$$

Además de las aplicaciones al cálculo de sumas de series, los números de Stirling también aparecen en problemas de distribuciones. Consideremos el siguiente problema.

Ejemplo 36.- ¿De cuántas maneras pueden distribuirse n objetos distintos en k cajas diferentes si ninguna caja puede estar vacía?

> Podemos pensar una de estas distribuciones como en una partición del conjunto de n elementos. De hecho, una distribución divide al conjunto en k partes. Sin embargo, al realizar una partición sólo se tiene en cuenta cuáles son las partes y no se les asigna ningún orden, cosa que sí ocurre con las distribuciones. Es por eso que distintas distribuciones pueden originar la misma partición. De hecho, cada partición da lugar a $k!$ distribuciones diferentes, ya que no hay más que ordenar de todas las formas posibles las partes para generar las distintas distribuciones. Por lo tanto el total de distribuciones será $k!\left\{ {n \atop k} \right\}$.

Puede razonarse de otro modo para ver que

$$k!\left\{ {n \atop k} \right\} = \sum_{\substack{\alpha_1+\alpha_2+\cdots\alpha_k=k \\ \alpha_j \geq 1}} \binom{n}{\alpha_1 \alpha_2 \cdots \alpha_k},$$

lo que proporciona una fórmula explícita para calcular los números de Stirling de segunda clase. ∎

3 Funciones generadoras

La resolución de problemas combinatorios no es una cuestión sencilla, pues no parecen existir métodos directos de resolución. Cada problema puede parecer distinto a los demás, a pesar de que se resuelvan utilizando las mismas herramientas. Con el ánimo de introducir métodos más o menos directos, aparecen las funciones generadoras que se revelan como una técnica de gran utilidad a la hora de resolver problemas de distribuciones con restricciones.

Definición 10 *Sea $a_0, a_1, a_2, \ldots$ una sucesión de números reales. Llamamos función generadora de la sucesión (a_n) a una función $G(x)$ tal que*

$$G(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_n x^n + \cdots.$$

La función generadora de la sucesión (a_n) debe entenderse como una forma alternativa de representarla. En este sentido, no debemos preocuparnos de la convergencia de la serie.

Ejemplo 37.- La función $G(x) = (1+x)^n$ es la función generadora de $a_k = \binom{n}{k}$.

En efecto, las funciones generadoras ya nos han aparecido con anterioridad y, gracias al teorema del bonomio, podemos escribir

$$(1+x)^n = \binom{n}{0} + \binom{n}{1} x + \binom{n}{2} x^2 + \cdots + \binom{n}{k} x^k + \cdots + \binom{n}{n} x^n.$$

De este modo, $G(x) = (1+x)^n$ es la función generadora de $a_k = \binom{n}{k}$.

Podemos decir que la función $(1+x)^n$ resume la solución de una familia de problemas, como es el de determinar el número de formas en que pueden seleccionarse k objetos de un total de n. ∎

Otro ejemplo de funciones generadoras lo encontramos en los números de Stirling de primera clase. En este caso la función

$$G(x) = x^{\overline{n}} = \overbrace{x(x+1)(x+2)\ldots(x+n-1)}^{n \text{ factores}},$$

genera la sucesión $a_k = \left[{n \atop k} \right]$, el total de formas en que una permutación de n elementos puede descomponerse en k ciclos.

Considerando las funciones generadoras como series de potencias formales, uno puede operar con ellas para obtener nuevas funciones generadoras que están relacionadas con las sucesiones a las que representan.

Entre las propiedades más importantes podemos señalar las siguientes.

Adición. Si $G_1(x)$ es la función generadora de $a_0, a_1, \ldots$ y $G_2(x)$ es la función generadora de $b_0, b_1, \ldots$, entonces $\alpha G_1(x) + \beta G_2(x)$ es la función generadora de $\alpha a_0 + \beta b_0, \alpha a_1 + \beta b_1, \ldots$. Basta tener en cuenta que las series se suman como si fueran polinomios.

Desplazamiento. Si $G(x)$ es la función generadora de $a_0, a_1, \ldots$, entonces $x^n G(x)$ es la función generadora de

$$\overbrace{0, \ldots, 0}^{n \text{ ceros}}, a_0, a_1, \ldots.$$

Análogamente,

$$(G(x) - a_0 - a_1 x - \ldots - a_{n-1} x^{n-1})/x^n$$

es la función generadora de $a_n, a_{n+1}, \ldots$.

Ejemplo 38.- $G(x) = \dfrac{1}{1-x}$ es la función generadora de la sucesión constante $a_n = 1$.

Si $G(x)$ es la función generadora de la sucesión constante $1, 1, \ldots$, entonces $xG(x)$ genera a $0, 1, 1, \ldots$, por lo que $(1-x)G(x) = 1$. Esto proporciona la importante fórmula

$$G(x) = \frac{1}{1-x} = 1 + x + x^2 + \cdots.$$

Nótese que esto, además, nos indica que una función generadora puede tener inversa, en el sentido de que existe otra función generadora $G(x)^{-1}$ tal que $G(x)G(x)^{-1} = 1$. La condición necesaria y suficiente para que esto ocurra es que $a_0 \neq 0$. ∎

Multiplicación. Si $G_1(x)$ es la función generadora de $a_0, a_1, \ldots$ y $G_2(x)$ es la función generadora de $b_0, b_1, \ldots$, entonces

$$\begin{aligned} G_1(x)G_2(x) &= (a_0 + a_1x + a_2x^2 + \cdots)(b_0 + b_1x + b_2x^2 + \cdots) \\ &= (a_0b_0) + (a_0b_1 + a_1b_0)x + (a_0b_2 + a_1b_1 + a_2b_0)x^2 + \cdots; \end{aligned}$$

es la función generadora de la sucesión $s_0, s_1, \ldots$, donde

$$s_n = \sum_{0 \leq k \leq n} a_k b_{n-k}.$$

Un caso importante es cuando (b_n) es la sucesión constante 1. En esta situación tenemos

$$\frac{1}{1-x}G(x) = a_0 + (a_0 + a_1)x + (a_0 + a_1 + a_2)x^2 + \cdots$$

que es la función generadora de la sucesión de sumas parciales de la sucesión (a_n).

Ejemplo 39.- Determinar la función generadora de la sucesión $a_n = n$.

La función $G(x) = \dfrac{1}{1-x}$ genera la sucesión constante $a_n = 1$.

Por la propiedad de multiplicación, la función $G(x)^2$ genera la sucesión de sumas parciales de a_n, es decir, genera la sucesión $b_n = \displaystyle\sum_{k=0}^{n} a_k = n + 1$. Por tanto $G(x)^2$ genera la sucesión $1, 2, 3, \ldots$. Aplicando la propiedad de desplazamiento $xG(x)^2$ genera la sucesión $0, 1, 2, 3, \ldots$, que es la que pide determinar el problema.

En resumen, $F(x) = \dfrac{x}{(1-x)^2}$ genera la sucesión $a_n = n$. ∎

Cambio de variable. Si $G(x)$ es la sucesión generadora de la sucesión $a_0, a_1, \ldots$, entonces $G(cx)$ es la función generadora de la sucesión

$$a_0, ca_1, c^2a_2, \ldots.$$

En particular, la función generadora de la sucesión $1, c, c^2, c^3, \ldots$ es $\dfrac{1}{1-cx}$.

Además de estas propiedades algebraicas las técnicas de cálculo nos proporcionan nuevas operaciones, como la derivación y la integración. Así, si $G(x)$ es la función generadora de la sucesión $a_0, a_1, \ldots$, entonces $xG'(x)$ es la función generadora de (na_n). Análogamente

$$\frac{1}{x}\int_0^x G(s)\,ds = a_0 + \tfrac{1}{2}a_1x + \frac{1}{3}a_2x^2 + \cdots$$

es la función generadora de $(a_n/(n+1))$.

Las funciones generadoras tienen múltiples aplicaciones y el poder determinarlas, para una sucesión dada, resulta de gran utilidad, especialmente si la sucesión está relacionada con la solución general de un cierto problema combinatorio. En cualquier caso, no existen métodos generales para determinar una función generadora, aunque en cierto tipo de problemas es posible dar unas reglas más o menos generales. En este sentido nos será de utilidad el teorema del binomio generalizado.

Teorema 10 *(Teorema del binomio generalizado) Si definimos*

$$\binom{\alpha}{k} = \frac{\alpha(\alpha-1)(\alpha-2)\cdots(\alpha-k+1)}{k!},$$

con $\alpha \in \mathbb{R}$*, entonces*

$$(1+x)^\alpha = \sum_{k=0}^{\infty} \binom{\alpha}{k} x^k.$$

Basta desarrollar la función $f(x) = (1+x)^\alpha$ en serie de Taylor en torno a $x = 0$.

En efecto, las derivadas sucesivas de la función f son

$$\begin{aligned} f'(x) &= \alpha(1+x)^{\alpha-1} \\ f''(x) &= \alpha(\alpha-1)(1+x)^{\alpha-2} \\ &\vdots \\ f^{k)}(x) &= \alpha(\alpha-1)\cdots(\alpha-k+1)(1+x)^{\alpha-k}. \end{aligned}$$

Puesto que

$$f(x) = f(0) + \frac{f'(0)}{1!}x + \frac{f''(0)}{2!}x^2 + \cdots + \frac{f^{k)}(0)}{k!}x^k + \cdots,$$

resulta finalmente

$$f(x) = 1 + \frac{\alpha}{1!}x + \frac{\alpha(\alpha-1)}{2!}x^2 + \cdots + \frac{\alpha(\alpha-1)\cdots(\alpha-k+1)}{k!}x^k + \cdots.$$

Es decir, $(1+x)^\alpha = \sum_{k=0}^{\infty} \binom{\alpha}{k} x^k$. ∎

Un caso especialmente interesante es cuando α es un entero negativo. Si $\alpha = -n$, entonces

$$\binom{-n}{k} = \frac{(-n)(-n-1)\cdots(-n-k+1)}{k!} = (-1)^k \frac{(n+k-1)\cdots(n+1)n}{k!} = (-1)^k \binom{n+k-1}{k}.$$

Ahora bien, $\binom{n+k-1}{k} = \mathrm{CR}(n,k)$, por lo que $\binom{-n}{k} = (-1)^k \,\mathrm{CR}(n,k)$ y entonces

$$\frac{1}{(1-x)^n} = \sum_{k=0}^{\infty} \mathrm{CR}(n,k) x^k.$$

De este modo, a partir del teorema del binomio generalizado hemos encontrado la función generadora de las combinaciones con repetición de n elementos tomados de k en k.

En realidad, la función $G(x) = \dfrac{1}{(1-x)^n}$ equivale a multiplicar n veces la serie

$$1 + x + x^2 + x^3 + \cdots + x^n + \cdots.$$

Denotemos por e_1 al exponente de x en la primera serie, por e_2 al exponente de x en la segunda serie y así sucesivamente. Obtendremos x^k, en el producto final, cada vez que se cumpla

$$e_1 + e_2 + e_3 + \cdots + e_n = k. \tag{14}$$

Por tanto, el coeficiente de x^k es el total de soluciones enteras no negativas de la ecuación (14). Pero, como ya vimos en la sección 2.6, esto equivale a $\mathrm{CR}(n,k)$.

Esta observación es muy útil a la hora de resolver problemas de combinaciones con repetición con restricciones. Podemos interpretar cada uno de los e_j como los elementos que se combinan en el problema (en un total de k) y los exponentes de la serie asignada a cada elemento como los posibles valores que pueden tomar estos elementos. Al final, la solución de nuestro problema es el coeficiente de x^k.

Ejemplo 40.- Determinar el total de enteros entre 1 y 1.000.000 tales que la suma de sus cifras sea igual a 15. (Ver Ejemplo 32)

Podemos ver los enteros entre 1 y 1.000.000 como los números de 6 dígitos que pueden empezar por 0. En este sentido uno de tales números puede escribirse como

$$c_1c_2c_3c_4c_5c_6.$$

Sus cifras sumarán 15 cuando se cumpla

$$c_1 + c_2 + c_3 + c_4 + c_5 + c_6 = 15,$$

siendo cada uno de los c_j un número comprendido entre 0 y 9. Es decir, los posibles valores que pueden tomar cada uno de los c_j son 0, 1, 2, 3, 4, 5, 6, 7, 8 ó 9.

Por tanto, asignamos a cada uno de los 6 elementos que se combina la serie

$$G(x) = 1 + x + x^2 + x^3 + x^4 + x^5 + x^6 + x^7 + x^8 + x^9.$$

El resultado del problema será el coeficiente de x^{15} en $G(x)^6$.

Ahora bien, $G(x)$ puede escribirse como

$$G(x) = \frac{1 - x^{10}}{1 - x},$$

por lo que

$$G(x)^6 = \frac{(1 - x^{10})^6}{(1 - x)^6} = (1 - x^{10})^6 \sum_{k=0}^{\infty} \mathrm{CR}(6, k)x^k.$$

Aplicando el teorema del binomio para desarrollar $(1 - x^{10})^6$, encontramos que el coeficiente de x^{15} es

$$\mathrm{CR}(6, 15) - \binom{6}{1}\mathrm{CR}(6, 5) = \binom{20}{5} - \binom{6}{1}\binom{10}{5} = 13.992,$$

que es el resultado pedido. ∎

Ejemplo 41.- Se lanza una moneda al aire 25 veces consecutivas, saliendo un total de 8 cruces. Calcular la probabilidad de que no hayan salido 6 o más caras consecutivas.

Llamemos c_1 al total de caras que han salido antes de la primera cruz, c_2 al total de caras entre la primera y segunda cruz y así sucesivamente hasta llegar a c_9, que representa el total de caras después de la octava cruz.

Como se han realizado 25 lanzamientos y el total de cruces es 8, tiene que cumplirse

$$c_1 + c_2 + c_3 + c_4 + c_5 + c_6 + c_7 + c_8 + c_9 = 17, \tag{15}$$

pues en total habrán salido 17 caras.

La probabilidad la calcularemos como siempre por el cociente entre casos favorables y casos posibles.

Los casos posibles, son el total de soluciones de la ecuación (15), es decir $\mathrm{CR}(9, 17) = \binom{25}{8}$. Nótese que el resultado es el mismo que el de determinar las ocho posiciones que han ocupado las cruces en los 25 lanzamientos.

Los casos favorables son las soluciones de (15) con la restricción de que cada uno de los c_j no puede ser mayor que 5. Asignando a cada c_j la serie

$$G(x) = 1 + x + x^2 + x^3 + x^4 + x^5,$$

los casos favorables serán el coeficiente de x^{17} en $G(x)^9$.

Como $G(x)$ puede escribirse como $G(x) = \dfrac{1-x^6}{1-x}$, resulta

$$G(x)^9 = \frac{(1-x^6)^9}{(1-x)^9} = (1-x^6)^9 \sum_{k=0}^{\infty} \mathrm{CR}(9,k)\, x^k.$$

Desarrollando $(1-x^6)^9$ mediante la fórmula del binomio obtenemos el siguiente coeficiente para x^17

$$\mathrm{CR}(9,17) - \binom{9}{1}\mathrm{CR}(9,11) + \binom{9}{2}\mathrm{CR}(9,5).$$

Finalmente, la probabilidad pedida es

$$p = \frac{\text{casos favorables}}{\text{casos posibles}} = \frac{\mathrm{CR}(9,17) - \binom{9}{1}\mathrm{CR}(9,11) + \binom{9}{2}\mathrm{CR}(9,5)}{\mathrm{CR}(9,17)} = 0.413905.$$

La resolución de este problema sin la ayuda de las funciones generadoras es bastante más complicado. Para determinar los casos posibles procedemos como en el ejemplo 32. Al total de soluciones de (15) le descontamos las soluciones que incumplen el enunciado. Es decir, descontaremos aquellas soluciones en que haya algún c_j mayor o igual que 6. Supongamos que es $c_9 \geq 6$, entonces se tiene que cumplir

$$c_1 + c_2 + c_3 + c_4 + c_5 + c_6 + c_7 + c_8 \leq 11.$$

Como ya vimos en el ejemplo 32, el total de soluciones de esta desigualdad es $\mathrm{CR}(9,11)$. Puesto que el elemento que puede ser mayor que 5 es cualquiera de los 9, habrá que descontar $9\,\mathrm{CR}(9,11)$ al total de soluciones de (15). (Notar que este es el segundo término del coeficiente de x^17 que hemos obtenido mediante las funciones generadoras.)

Sin embargo, este no es el resultado definitivo, ya que puede haber hasta dos elemetos que pueden ser mayores que 5 al mismo tiempo. En este caso habremos descontado dos veces esa posibilidad, una por cada uno de los elementos que es mayor que 5. Por tanto, debemos sumar todo lo que hemos descontado de más. Y es aquí donde hay que proceder con cuidado. A primera vista puede parecer que si hay dos elementos mayores que 5, los otros siete tienen que sumar 5 o menos y entonces habría que sumar $\binom{9}{2}\,\mathrm{CR}(8,5)$. Pero este factor no es el mismo que hemos obtenido mediante funciones generadoras. El porqué de esto es que no hemos tenido en cuanta el orden, pues si son c_8 y c_9 los que suman 13, por ejemplo, no hemos contemplado cuál de los dos es el que vale 7 y cuál el que vale 6. Esto nos conduce a la tentación de multiplicar por 2 el resultado obtenido ($\binom{9}{2}\,\mathrm{CR}(8,5)$). No obstante, esto no arregla el problema, ya que

$$2\binom{9}{2}\,\mathrm{CR}(8,5) = 1584 > \mathrm{CR}(9,5) = 1287.$$

¿Dónde está ahora el fallo?. La respuesta es que cuando ambos elementos valen lo mismo, por ejemplo 6 y 6, el orden no importa. Por eso hay que proceder con mucho cuidado, analizando cada caso concreto.

Suma 12: $6+6$, 1 caso $\longrightarrow \mathrm{CR}(7,5)$

Suma 13: $\left\{\begin{array}{l} 6+7, \\ 7+6, \end{array}\right.$ 2 casos $\longrightarrow 2\,\mathrm{CR}(7,5)$

Suma 14: $\left\{\begin{array}{l} 6+8, \\ 7+7, \\ 8+6, \end{array}\right.$ 3 casos $\longrightarrow 3\,\mathrm{CR}(7,5)$

Suma 15: $\left\{\begin{array}{l} 6+9, \\ 7+8, \\ 8+7, \\ 9+6, \end{array}\right.$ 4 casos $\longrightarrow 4\,\mathrm{CR}(7,5)$

$$\text{Suma 16:} \begin{cases} 6+10, \\ 7+9, \\ 8+8, \\ 9+7, \\ 10+6, \end{cases} \quad 5 \text{ casos} \longrightarrow 5\,\mathrm{CR}(7,5)$$

$$\text{Suma 17:} \begin{cases} 6+11, \\ 7+10, \\ 8+9, \\ 9+8, \\ 10+7, \\ 11+6, \end{cases} \quad 6 \text{ casos} \longrightarrow 6\,\mathrm{CR}(7,5)$$

La suma de todos estos valores puede comprobarse que es equivalente a $\mathrm{CR}(9,5)$, por lo que ahora si que obtendríamos el factor que aparece con las funciones generadoras. Por tanto, el resultado sería el mismo. ∎

Es importante destacar que un ataque del problema mediante combinatoria tradicional puede llevarnos a una solución equivocada. Por ello hay que ser muy cuidadoso a la hora de proceder a su resolución. Es por eso que las funciones generadoras resultan de gran utilidad, pues nos ahorran la mayor parte del razonamiento combinatorio, evitando errores innecesarios que, de otra forma, pueden producirse.

Las funciones generadoras que hemos usado para resolver los problemas correspondientes a los dos ejemplos anteriores se denominan, habitualmente, funciones generadoras ordinarias y se usan para resolver problemas relacionados con combinaciones con repetición con o sin restricciones. Este tipo de problemas es equivalente a la distribución de objetos idénticos en cajas diferentes. Cuando los objetos son diferentes el problema es esencialmente el mismo, pero se necesita modificar convenientemente el tipo de funciones generadoras que se usan.

Ejemplo 42.- Determinar el total de palabras de cuatro letras formadas con a, b y c, de forma que hay al menos dos a.

Resolvámoslo inicialmente considerando casos. De este modo, las posibles combinaciones de letras que pueden formar la palabra son $\{a,a,a,a\}$, $\{a,a,a,b\}$, $\{a,a,a,c\}$, $\{a,a,b,b\}$, $\{a,a,b,c\}$ y $\{a,a,c,c\}$. El total de palabras diferentes a los que da lugar cada conjunto de letras es un problema de permutaciones con repetición. Así tenemos que la solución es

$$\frac{4!}{4!0!0!}+\frac{4!}{3!1!0!}+\frac{4!}{3!0!1!}+\frac{4!}{2!2!0!}+\frac{4!}{2!1!1!}+\frac{4!}{2!0!2!}. \tag{16}$$

Nótese que el problema es muy parecido a los considerados anteriormente. En efecto, si denotamos por e_1 el total de as que aparecen en la palabra, por e_2 el total de bs y por e_3 el total de cs, se tiene que cumplir

$$e_1+e_2+e_3=4, \qquad e_1\geq 2, \quad e_2,e_3\geq 0.$$

La diferencia es que ahora cada solución entera de la ecuación no contribuye en uno al total de soluciones, sino en un número igual a

$$\frac{4!}{e_1!e_2!e_3!}=\frac{e_1+e_2+e_3}{e_1!e_2!e_3!}.$$

En este sentido, podemos asignar a cada elemento que se combina (en este caso las letras a, b y c) una serie de potencias en x donde el exponente representa el número de veces que dicho elemento interviene an la combinación y donde el coeficiente de x^k es $1/k!$. No es difícil ver que entonces la solución del problema será el coeficiente de x^4 (en este caso) multiplicada por $4!$.

Para el problema que nos ocupa, las series que debemos asignar a cada elemento son

$$\begin{aligned} a &\longrightarrow \frac{x^2}{2!}+\frac{x^3}{3!}+\frac{x^4}{4!}+\cdots, \\ b &\longrightarrow 1+x+\frac{x^2}{2!}+\frac{x^3}{3!}+\cdots, \\ c &\longrightarrow 1+x+\frac{x^2}{2!}+\frac{x^3}{3!}+\cdots. \end{aligned}$$

Si multiplicamos las series y buscamos el coeficiente de x^4 y lo multiplicamos por 4! obtenemos (16).

Conviene hacer notar que las series asignadas son series exponenciales, ya que

$$e^x = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots + \frac{x^k}{k!} + \cdots.$$

Por tanto, el producto de las tres series correspondientes a a, b y c las podemos expresar como

$$(e^x - x - 1)e^x e^x = e^{3x} - xe^{2x} - e^{2x}.$$

Si buscamos ahora el coeficiente de x^4 en la expresión anterior y lo multiplicamos por 4! resulta

$$3^4 - 4 \cdot 2^3 - 2^4.$$

Esto es, el total de secuencias diferentes que se pueden formar con a, b y c menos el total de secuencias que tienen una sóla a, menos el total de secuencias que no tienen ninguna a. ■