UNA GENERALIZACIÓN DE LA FUNCIÓN FACTORIAL

YOVANI CORREA PRIETO

Universidad Industrial de Santander
Facultad de Ciencias
Escuela de Matemáticas
Bucaramanga
Junio de 2005

UNA GENERALIZACIÓN DE LA FUNCIÓN FACTORIAL

YOVANI CORREA PRIETO

Trabajo de grado presentado como requisito parcial para optar al título de
Licenciado en Matemáticas

Director
M.Sc. Edilberto Reyes González

Universidad Industrial de Santander
Facultad de Ciencias
Escuela de Matemáticas
Licenciatura en Matemáticas
Bucaramanga
Junio de 2005

Culminada esta otra etapa de
mi vida, quiero dedicarle este
triunfo a mi padre celestial,
a mi querida madre ROSA PRIETO
y a mi novia YANETH LOZADA.

Agradecimientos

Agradezco muy especialmente a:

Dios por iluminarme en cada momento de este difícil pero gratificante camino.

Mi madre, por su incondicional apoyo en todo momento.

Mi novia, por su amor y compresión para logro de esta meta.

El profesor y director Edilberto Reyes, por su constante colaboración prestada en el desarrollo de este trabajo.

Todos los demás profesores, compañeros y personal de la escuela que hicieron posible este triunfo.

TITLE: A FACTORIAL FUNCTION GENERALIZATION [*]
AUTHOR: YOVANI CORREA PRIETO[**]

KEY WORDS: The factorial function and generalizations, p-ordering, associated p-sequence.

DESCRIPTION

In the present thesis the factorial functions along with a few of its most significant results basically related to theory of numbers are studied. A generalization of this function is presented with the study of some of its main characteristics.

In the first chapter are presented some basic concepts and some results of importance for the development of this task. In the second chapter the factorial function is studied along with some of its most significant results, the gamma function is presented as an extension of the factorial to the set of the real numbers showing some of its more important properties. In the third chapter are defined some new concepts which are necessary of the development of the task, the factorial generalization is presented along with a few examples, the new generalized factorial function is applied to a few theorems seen in chapter two . Finally some questions are stated as a result of the stated generalization.

The task shown here solves certain problems that were still without a solution, besides, new investigations subjects on several mathematical fields are suggested. We hope the reader to continue working on this study and through this we can together achieve a complete factorial generalization in a non very distant future. The methodology used here was the analysis of an article.

---

[*] Thesis

[**] FACULTY OF SCIENCES, LICENCIATURA EN MATEMÁTICAS.
DIRECTOR M.Sc. Edilberto Reyes González.

TITULO: UNA GENERALIZACIÓN DE LA FUNCIÓN FACTORIAL[*]
AUTOR: YOVANI CORREA PRIETO[**]

PALABRAS CLAVES: Función factorial generalizada, p-ordenamiento, p-sucesión asociada.

DESCRIPCIÓN

En el presente trabajo de grado, se estudia la función factorial junto con algunos de sus resultados más importantes relacionados básicamente con la teoría de números, se presenta una generalización de esta función y se estudian algunas de sus características.

En el primer capítulo se presentan algunos conceptos básicos y algunos resultados de gran importancia para el desarrollo de este trabajo. En el segundo capitulo se estudia la función factorial con algunos de sus resultados más importantes, se presenta la función gamma como una extensión del factorial al conjunto de los números reales mostrando algunas de sus propiedades más importantes. En el tercer capítulo se definen algunos nuevos conceptos necesarios para el desarrollo del trabajo, se presenta la generalización del factorial con algunos ejemplos, se aplica la nueva función factorial generalizada a algunos teoremas vistos en el capítulo dos y por ultimo se plantean algunos interrogantes que surgen como consecuencia de la generalización planteada.

El trabajo expuesto aquí soluciona ciertos problemas que estaban aun sin resolver, además también sugiere nuevos temas de investigación en diversos campos de la matemática. Esperamos que el lector continue trabajando sobre éste tema y así podamos llegar a una completa generalización del factorial. La metodología utilizada en éste trabajo fue el análisis de un artículo.

[*] Tesis

[**] FACULTAD DE CIENCIAS, LICENCIATURA EN MATEMÁTICAS.
DIRECTOR M.Sc. Edilberto Reyes González.

Contenido

Introducción

El factorial es sin alguna duda, una de las primeras funciones que se encuentran en el estudio de las matemáticas. Su uso se hace indispensable en algunas de sus ramas; como en la combinatoria donde interviene en el cálculo de probabilidades, en el análisis a través del desarrollo polinomial de las funciones (fórmulas de Taylor y MacLaurin), en la teoría de números en donde aparece en muchos resultados de gran importancia en este campo, y en muchas otras áreas en las cuales se convierte en una herramienta muy valiosa a la hora de interpretar y solucionar problemas.

Dada su importancia, el presente trabajo de monografía muestra una investigación reciente realizada sobre esta función; en el cual se presenta una generalización de la misma, enfocada básicamente hacia la teoría de números y cuyos resultados se han aplicado en diversos campos de la matemática como en la misma teoría de números, teoría combinatoria, teoría de anillos, problemas de interpolación, entre otros.

El objetivo general de este trabajo es mostrar una generalización de la función factorial definida en cualquier subconjunto de lo números enteros, tomando como base conceptos de la teoría de números.

Este trabajo está basado en el artículo *The Factorial Function and Generalizations* ([1, p. 565]); consta de tres capítulos: en el primero se encuentran conceptos y resultados básicos para el desarrollo de la generalización factorial planteada, en el segundo se presenta el factorial junto con algunos de sus resultados más importantes en la teoría de números, también se muestra la función gamma como una extensión de la función factorial al conjunto de los reales y finalmente en el tercer capítulo se propone la generalización del factorial, se presentan algunos ejemplos, se estudian algunas de sus propiedades y se plantean algunos interrogantes sobre dicha generalización.

Capítulo 1

Preliminares (conceptos básicos)

En este capítulo se hace un resumen de los principales conceptos, definiciones y teoremas que se utilizaran en el desarrollo de este trabajo; también se presentan algunos ejemplos para facilitar la comprensión por parte del lector.

1.1. Congruencias

El concepto de congruencia, introducido inicialmente por Gauss, permite simplificar muchos problemas relacionados con la divisibilidad de números enteros. En esta sección estudiaremos algunos resultados de gran importancia sobre este tema.

Definición 1.1. *Sean a y b enteros cualesquiera y n un entero positivo. Decimos que a y b* son congruentes módulo *n, lo cual se escribe $a \equiv b \pmod{n}$; si $a - b$ es divisible por n, es decir, que $a - b = n \cdot s$ para alguna $s \in \mathbb{Z}$.*

Por ejemplo, $17 \equiv 33 \pmod{8}$ ya que $17 - 33 = 8 \cdot (-2)$. Esta relación de de congruencia definida en el conjunto $\mathbb{Z}$ de los números enteros es reflexiva ya que para todo $a \in \mathbb{Z}$, $a - a = 0 = 0n$; también es simétrica ya que si $a - b = nk$, entonces $b - a = (-k)\, n$; finalmente es transitiva dado que si $a - b = nk$ y $b - c = ns$, tenemos que $a - c = (a - b) + (b - c) = nk + ns = n\,(k + s)$. Por tanto la relación de congruencia es una relación de equivalencia.

Podemos por tanto, considerar el conjunto cociente de $\mathbb{Z}$ mediante esta relación de equivalencia, el cual se simboliza por $\mathbb{Z}_n$ y se llama el conjunto de las clases de congruencia módulo n.

Los elementos de $\mathbb{Z}_n$ son, pues, clases de equivalencia que se denotan mediante $\overline{a}$, donde

$$\overline{a} \;=\; \{x \in \mathbb{Z} : x \equiv a \pmod{n}\},$$

$$\overline{a} \;=\; \{x \in \mathbb{Z} : x = a \; + nk \quad \text{para algún} \;\; k \in \mathbb{Z}\}\,.$$

Dada una clase de equivalencia $\overline{a} \in \mathbb{Z}_n$ siempre podemos elegir un representante x de $\overline{a}$ de manera que $\overline{a} = \overline{x}$ y $0 \leq x < n$; para esto basta con dividir a entre n y tomar x como el residuo de esta división. Entonces podemos escribir

$$\mathbb{Z}_n = \left\{\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n-1}\right\}.$$

El siguiente teorema enuncia algunas de las propiedades más importantes de las congruencias.

Teorema 1.2. *Si* $a \equiv b \pmod{n}$ *y* $c \equiv d \pmod{n}$ *entonces:*

1. *Para todo par de enteros* r *y* s, $ar + cs \equiv br + ds \pmod{n}$.
2. $a + c \equiv b + d \pmod{n}$.
3. $a - c \equiv b - d \pmod{n}$.
4. $ac \equiv bd \pmod{n}$.
5. $\forall k \in \mathbb{Z}^+,\; a^k \equiv b^k \pmod{n}$.
6. $\forall r \in \mathbb{Z},\; a + r \equiv b + r \pmod{n}$.
7. $\forall r \in \mathbb{Z},\; ar \equiv br \pmod{n}$.

La demostración de las anteriores propiedades de las congruencias son sencillas de realizar y se dejan como ejercicio al lector.

Teorema 1.3 (Teorema Chino del residuo). *Sean* $m_1, m_2, \cdots, m_r$ *enteros positivos primos relativos dos a dos y sean* $a_1, a_2, \cdots, a_r$ *enteros arbitrarios. Entonces el sistema de congruencias lineales*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

tiene solución única módulo $m = \prod_{i=1}^{r} m_i$.

La demostración de este teorema no se hará aquí, pero se puede encontrar en la mayoría de textos de teoría de números. (Véase por ejemplo [6]).

1.2. Grupos, anillos y campos

Definición 1.4. *Un grupo $\langle G, * \rangle$ es un conjunto G, junto con una operación binaria $*$ en G, tal que satisface los siguientes axiomas:*

1. *La operación binaria $*$ es asociativa.*
2. *Existe un elemento $e \in G$ tal que $e * x = x * e = x$ para todas las $x \in G$ (este elemento e es el elemento identidad para $*$ en G).*
3. *Para cada $a \in G$ existe un elemento $a' \in G$ con la propiedad de que $a' * a = a * a' = e$ (el elemento a' es el inverso de a respecto $a*$).*

Nota. Un grupo G es *abeliano* (o conmutativo) si su operación binaria $*$ es conmutativa.

El conjunto $\mathbb{Z}$ de los números enteros, el conjunto $\mathbb{Q}$ de los números racionales, el conjunto $\mathbb{R}$ de los números reales y el conjunto $\mathbb{C}$ de los números complejos; todos ellos con la operación $+$ (suma usual) son ejemplos de grupos.

Definición 1.5. *Sean $G_1, G_2, \cdots, G_n$ grupos conmutativos. Se define $\bigoplus_{i=1}^{n} G_i$ como la* suma directa de los grupos G_i; *en donde*

$$(g_1, g_2, \cdots, g_n) \oplus (h_1, h_2, \cdots, h_n) = (g_1 + h_1, g_2 + h_2, \cdots, g_n + h_n).$$

Definición 1.6. *Si H es un subconjunto de un grupo G cerrado bajo la operación de grupo de G y si H es él mismo un grupo bajo esta operación inducida, entonces H es un* subgrupo *de G.*

Por ejemplo el conjunto $\langle \mathbb{Z}, + \rangle$ es un subgrupo del grupo $\langle \mathbb{R}, + \rangle$. Pero $\langle \mathbb{Q}^+, \cdot \rangle$ no es un subgrupo de $\langle \mathbb{R}, + \rangle$ aunque $\mathbb{Q}^+ \subset \mathbb{R}$.

Definición 1.7. *Sea H un subgrupo de un grupo G y sea $a \in G$. La* clase lateral izquierda *aH de H es el conjunto $\{ah \mid h \in H\}$. La* clase lateral derecha *Ha de H se define como sigue $Ha = \{ha \mid h \in H\}$.*

Definición 1.8. *Un subgrupo H de un grupo G es un* subgrupo normal *(o invariante) de G si $g^{-1}Hg = H$ para toda $g \in G$. ($g^{-1}Hg = \{g^{-1}hg \mid h \in H\}$).*

Definición 1.9. *Si N es un subgrupo normal de un grupo G, el grupo de las clases laterales de N bajo la operación inducida es el* grupo factor *de G módulo N y se denota por G/N. Las clases laterales son las clases residuales de G módulo N.*

Si por ejemplo tomamos el grupo $\mathbb{Z}$; el subgrupo $n\mathbb{Z}$ es normal en éste y para todas las $n \in \mathbb{Z}^+$ hay las n clases residuales $0 + n\mathbb{Z}, 1 + n\mathbb{Z}, \cdots, (n-1) + n\mathbb{Z}$, entonces $\mathbb{Z}/n\mathbb{Z}$ es un grupo factor.

Definición 1.10. *Un* anillo *A es un conjunto con dos operaciones binarias (adición y multiplicación) tales que:*

1. *A es un grupo abeliano respecto a la adición (es decir A tiene un elemento cero, que se indica por 0, y cada $x \in A$ tiene un inverso aditivo y se nota $-x$).*
2. *La multiplicación es asociativa ($(xy)\,z = x\,(yz)$) y distributiva respecto a la adición ($x\,(y+z) = xy + xz, \quad (y+z)\,x = yx + zx$).*

Nota. Un anillo en donde la multiplicación es conmutativa se denomina *anillo conmutativo.*

Los conjuntos $\langle \mathbb{Z}, +, \cdot \rangle$, $\langle \mathbb{Q}, +, \cdot \rangle$, $\langle \mathbb{R}, +, \cdot \rangle$ y $\langle \mathbb{C}, +, \cdot \rangle$ son ejemplos de anillos.

Definición 1.11. *Un* ideal *I de un anillo A es un subconjunto de A que es un subgrupo aditivo y tal que si $x \in A$ y $r \in I$ implica $xr \in I$).*

El grupo cociente A/I hereda de A una multiplicación unívocamente definida que le convierte en un anillo, denominado el *anillo cociente* (o *anillo de clases de restos*) A/I. Los elementos de A/I son las clases de I en A.

Como un ejemplo sencillo consideremos el anillo $\mathbb{Z}$; se puede comprobar fácilmente que $n\mathbb{Z}$ es un ideal y las clases laterales $a + n\mathbb{Z}$ de $n\mathbb{Z}$ forman el anillo $\mathbb{Z}/n\mathbb{Z}$ bajo las operaciones inducidas de suma y multiplicación.

Definición 1.12. *Un* isomorfismo *ϕ entre un grupo G y un grupo G^* es una función $\phi : G \to G^*$ que es inyectiva, sobreyectiva y tal que para todas las x, $y \in G$,*

$$\phi\,(xy) = \phi\,(x)\,\phi\,(y)\,.$$

Si existe dicha función, se dice que G y G^* son isomorfos.

Definición 1.13. *Un isomorfismo ϕ de un anillo A en un anillo A^* es una función $\phi : A \to A^*$ que es inyectiva, sobreyectiva y tal que para todas $x, y \in A$,*

$$\phi\,(x+y) = \phi\,(x) + \phi\,(y) \qquad y \qquad \phi\,(xy) = \phi\,(x)\,\phi\,(y)\,.$$

Definición 1.14. *Un* divisor de cero *en un anillo A es un elemento x que «divide a 0», es decir, para el cual existe un $y \neq 0$ en A tal que $xy = 0$.*

Definición 1.15. *Un* dominio de integridad *es un anillo conmutativo con identidad (es decir, existe $1 \in A$ tal que $x1 = 1x = x$ para todo $x \in A$) que no contiene divisores de cero.*

Definición 1.16. *Un* campo *es un anillo conmutativo, en el cual todo elemento distinto de cero tiene inverso multiplicativo.*

El conjunto $\langle \mathbb{Z}, +, \cdot \rangle$ no es un campo pues, por ejemplo, el 2 no tiene inverso multiplicativo.

Claramente $\langle \mathbb{Q}, +, \cdot \rangle$, $\langle \mathbb{R}, +, \cdot \rangle$ y $\langle \mathbb{C}, +, \cdot \rangle$ son campos.

Teorema 1.17. *Todo dominio de integridad finito es un campo.*

Demostración. Sean $0, a_1, a_2, \cdots, a_n$ todos los elementos de un dominio de integridad finito D. Es necesario mostrar que para $a \in D$ donde $a \neq 0$, existe $b \in D$ tal que $ab = 1$. Consideremos ahora $a1, aa_1, \cdots, aa_n$. Afirmamos que todos los elementos de D son distintos pues $aa_i = aa_j$ implica que $a_i = a_j$, por las leyes de cancelación que se pueden aplicar en un dominio de integridad. Además, como D no tiene divisores de cero, ninguno de estos elementos es cero. Contando, tenemos que $a1, aa_1, \cdots, aa_n$ son los elementos $1, a_1, \cdots, a_n$ en algún orden, de manera que $a1 = 1$, esto es, $a = 1$, o bien $aa_i = 1$ para algún i. Por tanto a tiene inverso multiplicativo. □

Corolario 1.18. *Si p es primo, entonces $\mathbb{Z}_p$ es un campo.*

Demostración. La demostración resulta inmediatamente del hecho de que $\mathbb{Z}_p$ es un dominio de integridad y del teorema anterior. □

La función $f : \mathbb{Z}_n \to \mathbb{Z}/n\mathbb{Z}$ definida por $f(a) = a + n\mathbb{Z}$; claramente es una función inyectiva, sobreyectiva; tal que $f(a+b) = f(a) + f(b)$ y $f(ab) = f(a) f(b)$. Es decir $\mathbb{Z}_n$ y $\mathbb{Z}/n\mathbb{Z}$ son isomorfos. Entonces, $\mathbb{Z}_n$ bajo la suma y la multiplicación módulo n puede verse como $\mathbb{Z}/n\mathbb{Z}$ con diferentes nombres.

Definición 1.19.

1. *Un ideal P en A es* primo *si $P \neq A$ y si $xy \in P$ implica $x \in P$ o $y \in P$.*

2. *Un ideal M en A es* maximal *si $M \neq A$ y no existe ningún ideal I tal que $M \subset I \subset A$.*

Definición 1.20. *Un anillo D es un* Anillo Dedekind *si es un anillo conmutativo asociativo con unidad que no contiene divisores de cero (o sea, un dominio conmutativo de integridad), en el que todo ideal propio es representable en forma del producto de ideales primos.*

1.3. Sobre polinomios

Una de las clases de funciones más útiles y mejor conocidas dentro de las matemáticas es la de los polinomios. Debido a su expresión como sumas y productos los hacen una herramienta muy eficaz a la hora de resolver una gran cantidad de problemas en diversos campos.

Definición 1.21. *Sea* $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, *un polinomio con coeficientes enteros. Se dice que* $f(x)$ *es un* polinomio primitivo, *si el máximo común divisor* (mcd) *de* $a_0, a_1, a_2, \ldots, a_n$ *es 1.*

Ejemplo 1.22.

1. *Sea* $f(x) = 3x^2 + 5x + 1$; $f(x)$ *es primitivo ya que el* mcd *de 3, 5 y 1 es 1.*
2. $f(x) = 6x^3 + 4x$ *no es primitivo ya que el* mcd *de 6 y 4 es 2.*

Definición 1.23. *Sea* $f(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$, *un polinomio con coeficientes enteros. El* divisor fijo de f *sobre los enteros se define como el* mcd *de todos los elementos que son imagen de* f *en* $\mathbb{Z}$ *y se denota como* $d(\mathbb{Z}, f)$. *Esto es:*

$$d(\mathbb{Z}, f) = \operatorname{mcd}\{f(a) : a \in \mathbb{Z}\}.$$

Ejemplo 1.24. *Sea* $f(x) = x^3 + x$, *entonces tenemos que:*

$$\begin{aligned} f(0) &= 0; & f(1) &= 2; \\ f(2) &= 10; & f(-1) &= -2; \\ f(-2) &= -10; & f(-3) &= -30. \end{aligned}$$

En general,

1. *si* x *es par,* $x = 2k, \quad k \in \mathbb{Z}$ *y*

$$\begin{aligned} f(x) &= f(2k) = (2k)^3 + 2k \\ &= 8k^3 + 2k \\ &= 2\underbrace{\left(4k^3 + k\right)}_{\in\, \mathbb{Z}}, \end{aligned}$$

   y por tanto $f(x)$ *es par.*

2. *si* x *es impar,* $x = 2k + 1$, $k \in \mathbb{Z}$ *y*

$$\begin{aligned} f(x) &= f(2k+1) = (2k+1)^3 + 2k + 1 \\ &= 8k^3 + 4k + 1 + 2k + 1 \\ &= 8k^3 + 6k + 2 \\ &= 2\underbrace{\left(4k^3 + 3k + 1\right)}_{\in\, \mathbb{Z}}. \end{aligned}$$

   Por tanto $f(x)$ *nuevamente es par y como* $f(1) = 2$ *se tiene que* $d(\mathbb{Z}, f) = 2$.

Ahora, si tenemos $g(x) = 3x^3 + 3x$, es decir, $g(x) = 3\ f(x)$, haciendo los cálculos respectivos encontramos que $d(\mathbb{Z}, g) = 6$, o sea $d(\mathbb{Z}, g) = 3d(\mathbb{Z}, f)$. Esto se debe a propiedades del mcd. Por tanto podemos hallar el divisor fijo únicamente para polinomios primitivos.

Definición 1.25. *Si n es un entero no negativo ($n \geq 0$) el polinomio*

$$x(x-1)(x-2)\cdots(x-n+1)$$

se llama polinomio factorial *y lo denotamos por $x^{(n)}$. Y definimos también $x^{(0)} = 1$.*

Así los primeros polinomios factoriales son:

$$\begin{aligned} x^{(0)} &= 1, \\ x^{(1)} &= x, \\ x^{(2)} &= x(x-1), \\ x^{(3)} &= x(x-1)(x-2), \\ x^{(4)} &= x(x-1)(x-2)(x-3). \end{aligned}$$

Fácilmente se puede mostrar que estos polinomios son linealmente independientes y por lo tanto cualquier polinomio se puede expresar como una combinación lineal de los polinomios factoriales,lo que es muy conveniente en muchas ocasiones para algunos cálculos por su expresión como un producto.

Ejemplo 1.26. *Expresar el polinomio $4x^3 + 2x^2 + x - 1$ como una combinación lineal de polinomios factoriales.*

Fácilmente se pueden hacer los cálculos y llegar a que

$$\begin{aligned} 4x^3 + 2x^2 + x - 1 &= 4x(x-1)(x-2) + 14x(x-1) + 7x - 1. \\ &= 4x^{(3)} + 14x^{(2)} + 7x^{(1)} - x^{(0)}. \end{aligned}$$

1.4. Otros conceptos

1.4.1. Determinante de Vandermonde

El siguiente concepto le ayudará al lector a dar respuesta a uno de los interrogantes planteados al final de este trabajo.

Definición 1.27. *El* determinante de Vandermonde *de orden k está dado por:*

$$B(a_0, a_1, \cdots, a_k) = \begin{vmatrix} 1 & a_0 & a_0^2 & \cdots & a_0^k \\ 1 & a_1 & a_1^2 & \cdots & a_1^k \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & a_k & a_k^2 & \cdots & a_k^k \end{vmatrix},$$

donde $a_0, a_1, \cdots, a_k$ son elementos de un anillo conmutativo.

Se puede mostrar para cualquier $k \geq 2$ que $B(a_0, a_1, \cdots, a_k) = \prod_{i<j} (a_i - a_j)$. (Véase [5, p. 203]).

1.4.2. Interpolación

Dados los valores de una función f en $n+1$ puntos distintos $x_0, x_1, \cdots, x_n$ se desea encontrar un polinomio p de grado menor o igual a n, que satisfaga las condiciones $p(x_0) = f(x_0)$, $p(x_1) = f(x_1)$, ..., $p(x_n) = f(x_n)$.

Existen muchas maneras de construir polinomios interpolantes; definiremos aquí el polinomio interpolante de Lagrange.

Definición 1.28. *Si $x_0, x_1, \cdots, x_n$ son $n+1$ puntos y f es una función que pasa por esos puntos, existe un único polinomio p de grado a lo más n, tal que $f(x_k) = p(x_k)$ para cada $k = 0, 1, 2, \cdots, n$.*

Este polinomio está dado por

$$p(x) = f(x_0) L_{n,0}(x) + \ldots + f(x_n) L_{n,n}(x) = \sum_{k=0}^{n} f(x_k) L_{n,k}(x)$$

donde

$$L_{n,k}(x) = \frac{(x - x_0)(x - x_1) \cdots (x - x_{k-1})(x - x_{k+1}) \cdots (x - x_n)}{(x_k - x_0)(x_k - x_1) \cdots (x_k - x_{k-1})(x_k - x_{k+1}) \cdots (x_k - x_n)} = \prod_{\substack{i=0 \\ i \neq k}}^{n} \frac{(x - x_i)}{(x_k - x_i)}$$

para cada $k = 0, 1, \cdots, n$.

Capítulo 2

La función factorial

Difícilmente podríamos trabajar en algunas áreas de la matemática sin utilizar esta importante función. En el presente capítulo se muestra la función factorial junto con algunos de sus resultados más importantes en la teoría de números y también se presenta la función gamma, la cual puede considerarse como una generalización del factorial en el conjunto de los números reales.

2.1. Sobre la función factorial

Si n es un entero positivo el símbolo $n!$ que se lee "n factorial" es bastante conocido y se puede definir recursivamente por:

Definición 2.1.

$$n! = \begin{cases} 1 & si \quad n = 0 \\ (n-1)! \cdot n & si \quad n \geq 1 \end{cases}$$

De la definición tenemos que:

$$\begin{aligned} 0! &= 1 \\ 1! &= 0! \cdot 1 = 1 \cdot 1 = 1 \\ 2! &= 1! \cdot 2 = 1 \cdot 2 = 2 \\ 3! &= 2! \cdot 3 = 2 \cdot 3 = 6 \\ 4! &= 3! \cdot 4 = 6 \cdot 4 = 24 \\ &\vdots \\ n! &= (n-1)!n = n \cdot (n-1) \cdot (n-2) \cdot \ldots \cdot 1 = 1 \times 2 \times 3 \times \ldots \times n. \end{aligned}$$

De aquí, el factorial de un número se calcula como el producto de todos los números enteros desde el 1 hasta dicho número.

Son muchas las áreas de la matemática en las que aparece el número factorial, por ejemplo en combinatoria (principios básicos de conteo), en el teorema del binomio (como coeficientes binomiales) y en muchos resultados relacionados con la teoría de números. Veamos algunos de ellos:

Definición 2.2. *Si $n, k \in \mathbb{Z}$, $0 \leq k \leq n$. El número combinatorio entre n y k que se denota $\binom{n}{k}$ se define por:*

$$\binom{n}{k} = \frac{n!}{k!\,(n-k)!}.$$

Mediante los principios básicos de conteo se deduce que $\binom{n}{k}$ siempre es un número entero. Se propone acá como un buen ejercicio de inducción matemática.

Ejercicio 2.3. *Si $n, k \in \mathbb{Z}$ y $0 \leq k \leq n$, entonces $\binom{n}{k}$ es un número entero.*

Este ejercicio se puede usar para demostrar uno de los resultados más conocidos sobre divisibilidad en el que aparece el número factorial. En efecto:

Lema 2.4. *El producto de k enteros consecutivos es un múltiplo de $k!$.*

Demostración. Sea $(m+1)\cdot(m+2)\cdot(m+3)\cdots(m+k)$ el producto de k enteros consecutivos. Si $m \geq 0$, tenemos

$$\begin{aligned}\frac{(m+1)\,(m+2)\,(m+3)\cdots(m+k)}{k!} &= \frac{m!\,(m+1)\,(m+2)\,(m+3)\cdots(m+k)}{m!\cdot k!} \\ &= \frac{(m+k)!}{m!\cdot k!} = \binom{m+k}{k}.\end{aligned}$$

Luego $(m+1)\,(m+2)\,(m+3)\cdots(m+k) = \underbrace{\binom{m+k}{k}}_{\in\mathbb{Z}} k!$.

Si $m < 0$ se presentan dos casos:

1. el producto es cero; entonces $k!|0$, ya que $0 = k!\cdot 0$;
2. el producto es distinto de cero, en cuyo caso se puede expresar, salvo por un signo, como el producto de enteros positivos consecutivos y se sigue del caso para $m \geq 0$. □

Ejemplo 2.5.

1. *Sea $k = 5$, y tomemos el producto de 5 enteros consecutivos: $3 \times 4 \times 5 \times 6 \times 7$ entonces esto debe ser un múltiplo de $5! = 120$, y efectivamente*

$$3 \times 4 \times 5 \times 6 \times 7 = 2520 = 120 \times 21.$$

   Hay que ver que los enteros también pueden ser negativos.

2. $(-6) \times (-5) \times (-4) \times (-3) = -360$ *y* $-360 = 24 \times (-15)$ *lo que indica que* -360 *es múltiplo de* $4! = 24$.

3. *El caso cuando se incluye el cero es trivial porque* 0 *es múltiplo de cualquier número entero.*

Lema 2.6. *El producto de k enteros pares consecutivos es un múltiplo de $2^k k!$.*

Demostración. Dados k enteros pares consecutivos $2\,(m+1)$, $2(m+2)$, $\cdots$, $2(m+k)$, entonces:

$$2\,(m+1) \times 2(m+2) \times \ldots \times 2(m+k) = 2^k \underbrace{(m+1)\,(m+2)\ldots(m+k)}_{(*)}$$

y por el lema anterior, $(*)$ es un múltiplo de $k!$, entonces todo el producto es un múltiplo de $2^k k!$. □

Ahora veremos un resultado asociado con el Lema 2.4.

Teorema 2.7. *Para cualesquiera enteros no negativos k y m, $(k+m)!$ es un múltiplo de $k! \cdot m!$.*

Demostración.

$$\begin{aligned}(k+m)! &= 1 \times 2 \times 3 \times \ldots \times k\,(k+1)\,(k+2) \times \ldots \times (k+m) \\ &= k!\underbrace{(k+1)\,(k+2) \times \ldots \times (k+m)}_{\text{producto de } m \text{ enteros consecutivos}}\end{aligned}$$

Por tanto resulta que $(k+m)!$ es múltiplo de $k! \cdot m!$. □

El resultado anterior también puede deducirse a partir de la siguiente observación.

$$\binom{m+k}{k} = \frac{(m+k)!}{k!m!}.$$

Ejemplo 2.8. *Tomemos $(2+3)! = 5! = 120$ y según el teorema anterior 120 debe ser múltiplo de $2! \times 3! = 2 \times 6 = 12$. Lo que se comprueba fácilmente, ya que:* $120 = 12 \times 10$.

Los siguientes teoremas, en donde nuevamente aparece el factorial, son mucho más complejos que el anterior y sus demostraciones se harán de manera mas general en el siguiente capítulo.

Otro resultado en el cual aparece la función factorial en el área de la teoría de números, nos muestra la directa relación que existe entre dicha función y los posibles valores tomados por un polinomio. En 1915 Pólya descubrió una importante conexión entre los divisores fijos sobre $\mathbb{Z}$ y la función factorial. El siguiente resultado que fue probado por Pólya considerará únicamente el caso para polinomios primitivos, utiizando propiedades de divisor fijo descritas en el capítulo 1.

Teorema 2.9. *Sea f un polinomio primitivo de grado k sobre los enteros, entonces $d(\mathbb{Z}, f)$ divide a $k!$. Además existen polinomios primitivos de grado k sobre los enteros tal que $d(\mathbb{Z}, f) = k!$.*

Puesto que $d(\mathbb{Z}, f)$ divide a $k!$ tenemos que $d(\mathbb{Z}, f) \leq k!$, por lo tanto, $k!$ es una cota superior para el divisor fijo de un polinomio de grado k. Además, también tenemos que dado $k!$ (o cualquiera de sus factores) este puede ser obtenido como el divisor fijo de algún polinomio primitivo.

Ejemplo 2.10. *Tomemos el polinomio del Ejemplo 1.24; $f(x) = x^3 + x$, en el cual encontramos que $d(\mathbb{Z}, f) = 2$. Por tanto tenemos por el teorema anterior que $d(\mathbb{Z}, f) = 2$ debe dividir a $3!$; lo que se puede comprobar fácilmente.*

Otro ejemplo más en el cual aparece nuevamente el factorial es el siguiente:

Teorema 2.11. *Sean $a_0, a_1, \ldots, a_n$ $n+1$ enteros arbitrarios. Entonces el producto de sus pares de diferencias*

$$\prod_{i<j}(a_i - a_j)$$

es un múltiplo de $0! \cdot 1! \cdots n!$.

Ejemplo 2.12. *Tomemos los enteros $-2, 1, 4, 6$; entonces:*

$$\begin{aligned}\prod_{i<j}(a_i - a_j) &= (-2-1)\cdot(-2-4)\cdot(-2-6)\cdot(1-4)\cdot(1-6)\cdot(4-6) \\ &= (-3)(-6)(-8)(-3)(-5)(-2) = 4320\end{aligned}$$

y según el teorema 2.11, 4320 debe ser múltiplo de $0! \cdot 1! \cdot 2! \cdot 3! = 1 \times 1 \times 2 \times 6 = 12$, lo que es cierto ya que $4320 = 12 \times 360$.

Ahora veamos otro ejemplo más en el cual aparece la función factorial, pero en un problema de combinatoria.

Recordemos que cuando n es primo $\mathbb{Z}/n\mathbb{Z}$ es un campo (Teorema 1.17). Y así utilizando la interpolación de Lagrange encontramos que toda función de $\mathbb{Z}/n\mathbb{Z}$ en el

mismo puede ser representada por un polinomio. Dado que cuando n no es primo, no podemos utilizar los métodos tradicionales de interpolación, debido a que generalmente necesitamos hacer divisiones, pero esto no es posible en un conjunto que no sea un campo. Así la cuestión sería ¿Cuantas funciones de $\mathbb{Z}/n\mathbb{Z}$ en el mismo (o equivalentemente de $\mathbb{Z}$ en $\mathbb{Z}/n\mathbb{Z}$) pueden ser representadas por un polinomio? La respuesta para esta pregunta fue descubierta por Kempner en 1920, y nos proporciona una fórmula exacta para el número de tales aplicaciones.

Teorema 2.13. *El número de funciones polinomiales de $\mathbb{Z}$ en $\mathbb{Z}/n\mathbb{Z}$ está dado por:*

$$\prod_{k=0}^{n-1} \frac{n}{\operatorname{mcd}(n, k!)}.$$

En particular, cuando n es primo, el Teorema 2.13 afirma que hay n^n de tales funciones.

Ejemplo 2.14. *Supongamos que queremos saber cuantas funciones de $\mathbb{Z}$ en $\mathbb{Z}/4\mathbb{Z}$ pueden ser representadas por un polinomio. Entonces, por el Teorema 2.13 tenemos que:*

$$\begin{aligned}
\prod_{k=0}^{3} \frac{4}{\operatorname{mcd}(4, k!)} &= \frac{4}{\operatorname{mcd}(4, 0!)} \times \frac{4}{\operatorname{mcd}(4, 1!)} \times \frac{4}{\operatorname{mcd}(4, 2!)} \times \frac{4}{\operatorname{mcd}(4, 3!)} \\
&= \frac{4}{\operatorname{mcd}(4, 1)} \times \frac{4}{\operatorname{mcd}(4, 1)} \times \frac{4}{\operatorname{mcd}(4, 2)} \times \frac{4}{\operatorname{mcd}(4, 6)} \\
&= 4 \times 4 \times \frac{4}{2} \times \frac{4}{2} \;=\; 64
\end{aligned}$$

Y tenemos 64 *de tales funciones.*

Los resultados vistos anteriormente en donde aparece el factorial, se ampliarán a un caso más general en el siguiente capítulo.

2.2. La función Gamma

Una de las funciones no elementales más importantes es la función gamma, la cual es representada por $\Gamma(x)$.

Esta función tiene diversas aplicaciones en la física, la ingeniería y la estadística matemática entre otras áreas y, por lo tanto debemos familiarizarnos con ella y con sus propiedades.

Durante los años 1729 y 1730, Euler introdujo esta función analítica que tiene la característica de interpolar la función factorial para valores no enteros. En una carta fechada el 13 de octubre de 1729 dirigida a Christian Goldbach, Euler le propuso la siguiente definición:

Definición 2.15 (Euler, 1729). *Sea x un número real positivo, se define*

$$\Gamma_p(x) = \frac{p!p^x}{x(x+1)(x+2)\cdots(x+p)} = \frac{p^x}{x(x+1)\left(\frac{x}{2}+1\right)\cdots\left(\frac{x}{p}+1\right)},$$

entonces

$$\Gamma(x) = \lim_{p\to\infty} \Gamma_p(x).$$

Claramente

$$\Gamma_p(1) = \frac{p!}{1(1+1)(1+2)\cdots(1+p)} = \frac{p}{p+1},$$

y

$$\Gamma_p(x+1) = \frac{p!p^{x+1}}{(x+1)(x+2)\cdots(x+p+1)} = \frac{p}{x+p+1} x\Gamma_p(x),$$

por lo tanto

$$\Gamma(1) = 1, \qquad \Gamma(x+1) = x\Gamma(x).$$

La relación $\Gamma(x+1) = x\Gamma(x)$ se denomina ecuación funcional.

Euler dió la siguiente definición equivalente de la función gamma:

Definición 2.16 (Euler, 1730). *Sea x un número real positivo, entonces*

$$\Gamma(x) = \int_0^1 (-\log(t))^{x-1} dt. \tag{2.1}$$

Haciendo un cambio de variable, obtenemos el siguiente resultado:

Teorema 2.17. *Sea x un número real positivo, entonces*

$$\Gamma(x) = \int_0^\infty e^{-t} t^{x-1} dt, \tag{2.2}$$

o también

$$\Gamma(x) = 2\int_0^\infty e^{t^2} t^{2x-1} dt.$$

Demostración. Haciendo cambio de variable en la ecuación (2.1), tenemos

$$\int_0^1 (-\log(t))^{x-1} dt = \int_0^\infty u^{x-1} e^{-u} du.$$

Haciendo $u^2 = -\log(t)$, se obtiene

$$\int_0^1 (-\log(t))^{x-1} dt = 2\int_0^\infty u^{2x-1} e^{-u^2} du. \qquad \square$$

De este teorema vemos que la función gamma $\Gamma(x)$ está bien definida para $x > 0$, pero no está definida para valores enteros negativos.

Para $x = 1$ en la ecuación (2.2) tenemos

$$\Gamma(1) = \int_0^\infty e^{-t} dt = 1,$$

integrando por partes esta ecuación, para $x > 0$, se obtiene:

$$\Gamma(x+1) = \int_0^\infty e^{-t} t^x dt = -t^x e^{-t}\Big|_0^\infty + x \int_0^\infty e^{-t} t^{x-1} dt = x\Gamma(x).$$

Si n es un entero positivo la ecuación funcional se convierte en:

$$\Gamma(n+1) = n!.$$

Demostración. Aplicando inducción sobre n tenemos:

$$\Gamma(1+1) = \Gamma(2) = \int_0^\infty e^{-t} t dt$$

e integrando por partes

$$\Gamma(2) = -te^{-t}\Big|_0^\infty - \int_0^\infty e^{-t} dt = -te^{-t} - e^{-t}\Big|_0^\infty = 1 = 1!.$$

Ahora supongamos que:

$$\Gamma(n) = (n-1)!$$

en consecuencia tenemos

$$\begin{aligned} \Gamma(n+1) &= \int_0^\infty e^{-t} t^n dt = -t^n e^{-t}\Big|_0^\infty + \int_0^\infty e^{-t} t^{n-1} dt = \\ &= n \int_0^\infty e^{-t} t^{n-1} dt = n\Gamma(n) = n(n-1)! = n!. \quad \square \end{aligned}$$

De aquí que la función gamma puede considerarse como una generalización de la función factorial elemental.

También es posible ampliar esta función a valores negativos invirtiendo la ecuación funcional en la forma

$$\Gamma(x) = \frac{\Gamma(x+1)}{x}. \tag{2.3}$$

Por ejemplo $\Gamma\left(-\frac{1}{3}\right) = -3\Gamma\left(\frac{2}{3}\right)$.

Aplicando reiteradamente esta identidad obtenemos:

$$\Gamma(x) = \frac{\Gamma(x+1)}{x} = \frac{\Gamma(x+2)}{x(x+1)} = \frac{\Gamma(x+3)}{x(x+1)(x+2)} = \cdots = \frac{\Gamma(x+k+1)}{x(x+1)(x+2)\cdots(x+k)},$$

con $x \neq 0, -1, -2, -3, \cdots$.

La anterior expresión puede usarse para definir la función gamma de valores negativos de x diferentes de $0, -1, -2, -3, \cdots$, eligiendo para k el menor número natural, tal que $x + k + 1$ sea mayor que cero.

Así por ejemplo:

$$\Gamma\left(-\frac{1}{2}\right) = \frac{\Gamma\left(-\frac{1}{2}+1\right)}{-\frac{1}{2}} = -2\Gamma\left(\frac{1}{2}\right),$$

$$\Gamma\left(-3,25\right) = \frac{\Gamma\left(0,75\right)}{\left(-3,25\right)\left(-2,25\right)\left(-1,25\right)\left(-0,25\right)} = \frac{\Gamma\left(0,75\right)}{2,285}.$$

Ejercicio 2.18. *Evaluar* $\Gamma\left(\frac{1}{2}\right)$ *y probar que es igual a* $\sqrt{\pi}$.

Demostración.

$$\begin{aligned}\Gamma\left(\frac{1}{2}\right) &= \int_0^\infty e^{-t}t^{-\frac{1}{2}}dt \\ &= \int_0^\infty e^{-u^2}\left(u^2\right)^{-\frac{1}{2}}2udu \\ &= 2\int_0^\infty e^{-u^2}du \\ &= 2\int_0^\infty e^{-v^2}dv,\end{aligned}$$

por lo tanto

$$\left[\Gamma\left(\frac{1}{2}\right)\right]^2 = 4\int_0^\infty e^{-u^2}du\int_0^\infty e^{-v^2}dv = 4\int_0^\infty\int_0^\infty e^{-\left(u^2+v^2\right)}dudv$$

e introduciendo coordenadas polares $\quad u = r\cos\theta,\ v = r\,\mathrm{sen}\,\theta$

$$\left[\Gamma\left(\frac{1}{2}\right)\right]^2 = 4\int_0^{\frac{\pi}{2}} e^{-r^2}rdrd\theta = 4\frac{\pi}{2}\int_0^\infty e^{-r^2}rdr = 2\pi\left(-\frac{1}{2}\right)e^{-r^2}\Big|_0^\infty = \pi.$$

En definitiva se tiene que

$$\Gamma\left(\frac{1}{2}\right) = \sqrt{\pi}.$$ □

Aplicando este resultado junto con la ecuación funcional podemos calcular los valores de $\Gamma\left(k+\frac{1}{2}\right)$ para $k \in \mathbb{Z}^+$.

Ejemplo 2.19.

$$\Gamma\left(\frac{3}{2}\right) = \Gamma\left(\frac{1}{2}+1\right) = \frac{1}{2}\Gamma\left(\frac{1}{2}\right) = \frac{1}{2}\sqrt{\pi} = \frac{\sqrt{\pi}}{2},$$

$$\Gamma\left(\frac{5}{2}\right) = \Gamma\left(\frac{3}{2}+1\right) = \frac{3}{2}\Gamma\left(\frac{3}{2}\right) = \frac{3}{2}\frac{\sqrt{\pi}}{2} = \frac{3\sqrt{\pi}}{4}.$$

Teorema 2.20 (Weierstrass). *Para todo número real x, $x \neq -1, -2, -3, \ldots$, tenemos el producto infinito*

$$\frac{1}{\Gamma(x)} = xe^{\gamma x}\prod_{p=1}^{\infty}\left(1+\frac{x}{p}\right)e^{-\frac{x}{p}}$$

donde γ es la constante de Euler y se define

$$\gamma = \lim_{p\to\infty}\left(1+\frac{1}{2}+\frac{1}{3}+\cdots+\frac{1}{p}-\log(p)\right) \approx 0,5772156649015328$$

Aplicando este teorema a $\dfrac{1}{\Gamma(x)}\dfrac{1}{\Gamma(-x)}$, se obtiene

$$\begin{aligned}\frac{1}{\Gamma(x)}\frac{1}{\Gamma(-x)} &= -x^2e^{\gamma x}e^{-\gamma x}\prod_{p=1}^{\infty}\left[\left(1+\frac{x}{p}\right)e^{-\frac{x}{p}}\left(1-\frac{x}{p}\right)e^{\frac{x}{p}}\right] \\ &= -x^2\prod_{p=1}^{\infty}\left(1-\frac{x^2}{p^2}\right).\end{aligned}$$

Por la ecuación funcional tenemos que $\Gamma(-x) = -\dfrac{\Gamma(1-x)}{x}$, por tanto la igualdad se puede escribir como

$$\frac{1}{\Gamma(x)}\frac{1}{\Gamma(-x)} = x\prod_{p=1}^{\infty}\left(1-\frac{x^2}{p^2}\right)$$

y usando el producto infinito

$$\operatorname{sen}(\pi x) = \pi x\prod_{p=1}^{\infty}\left(1-\frac{x^2}{p^2}\right)$$

se tiene que

$$\Gamma(x)\Gamma(1-x) = \frac{\pi}{\operatorname{sen}(\pi x)}.$$

Esta última expresión se conoce como la formula del complemento y es válida para cuando x y $(1-x)$ son diferentes de cero o de enteros negativos.

Aplicando la formula del complemento para los valores de $x = \frac{1}{2}$, $x = \frac{1}{3}$ y $x = \frac{1}{4}$ obtenemos

$$\Gamma\left(\frac{1}{2}\right) = \sqrt{\pi}, \qquad \Gamma\left(\frac{1}{3}\right)\Gamma\left(\frac{2}{3}\right) = \frac{2\pi\sqrt{3}}{3} \qquad \text{y} \qquad \Gamma\left(\frac{1}{4}\right)\Gamma\left(\frac{3}{4}\right) = \pi\sqrt{2}.$$

Teorema 2.21 (Legendre, 1809). *Para todo número real x, $x \notin \mathbb{Z}^- \cup \{0\}$, se tiene que*

$$\Gamma(x)\,\Gamma\left(x + \frac{1}{2}\right) = \frac{\sqrt{\pi}}{2^{2x-1}}\Gamma(2x).$$

Esta expresión se conoce como fórmula de la duplicación.

Se han hecho tablas como la Tabla 2.1 para $\Gamma(x)$ donde $1 \leq x \leq 2$.

x	$\Gamma(x)$	x	$\Gamma(x)$	x	$\Gamma(x)$	x	$\Gamma(x)$
$1,00$	$1,000000$	$1,26$	$0,904397$	$1,52$	$0,887039$	$1,78$	$0,926227$
$1,02$	$0,988844$	1,28	$0,900718$	$1,54$	$0,888178$	$1,80$	$0,931384$
$1,04$	$0,978438$	$1,30$	$0,897471$	$1,56$	$0,889639$	$1,82$	$0,936845$
$1,06$	$0,968744$	$1,32$	$0,894640$	$1,58$	$0,891420$	$1,84$	0,942612
$1,08$	$0,959725$	$1,34$	$0,892216$	$1,60$	$0,893515$	$1,86$	$0,948687$
$1,10$	$0,951351$	$1,36$	$0,890185$	$1,62$	$0,895164$	$1,88$	$0,955071$
$1,12$	$0,943590$	$1,38$	$0,888537$	$1,64$	$0,898642$	$1,90$	$0,961766$
$1,14$	$0,936416$	$1,40$	$0,887264$	$1,66$	$0,901668$	$1,92$	$0,968774$
$1,16$	$0,929803$	$1,42$	$0,886356$	$1,68$	$0,905001$	$1,94$	$0,976099$
$1,18$	$0,923728$	$1,44$	$0,885805$	$1,70$	$0,908639$	$1,96$	$0,983743$
$1,20$	$0,918169$	$1,46$	$0,885604$	$1,72$	$0,912581$	$1,98$	$0,991708$
$1,22$	$0,913106$	$1,48$	$0,885747$	$1,74$	$0,916826$	$2,00$	$1,000000$
$1,24$	$0,908521$	$1,50$	$0,886227$	$1,76$	$0,921375$		

Cuadro 2.1: $\Gamma(x)$ para $1 \leq x \leq 2$.

En la Figura 2.1 se presenta la función $\Gamma(x)$.

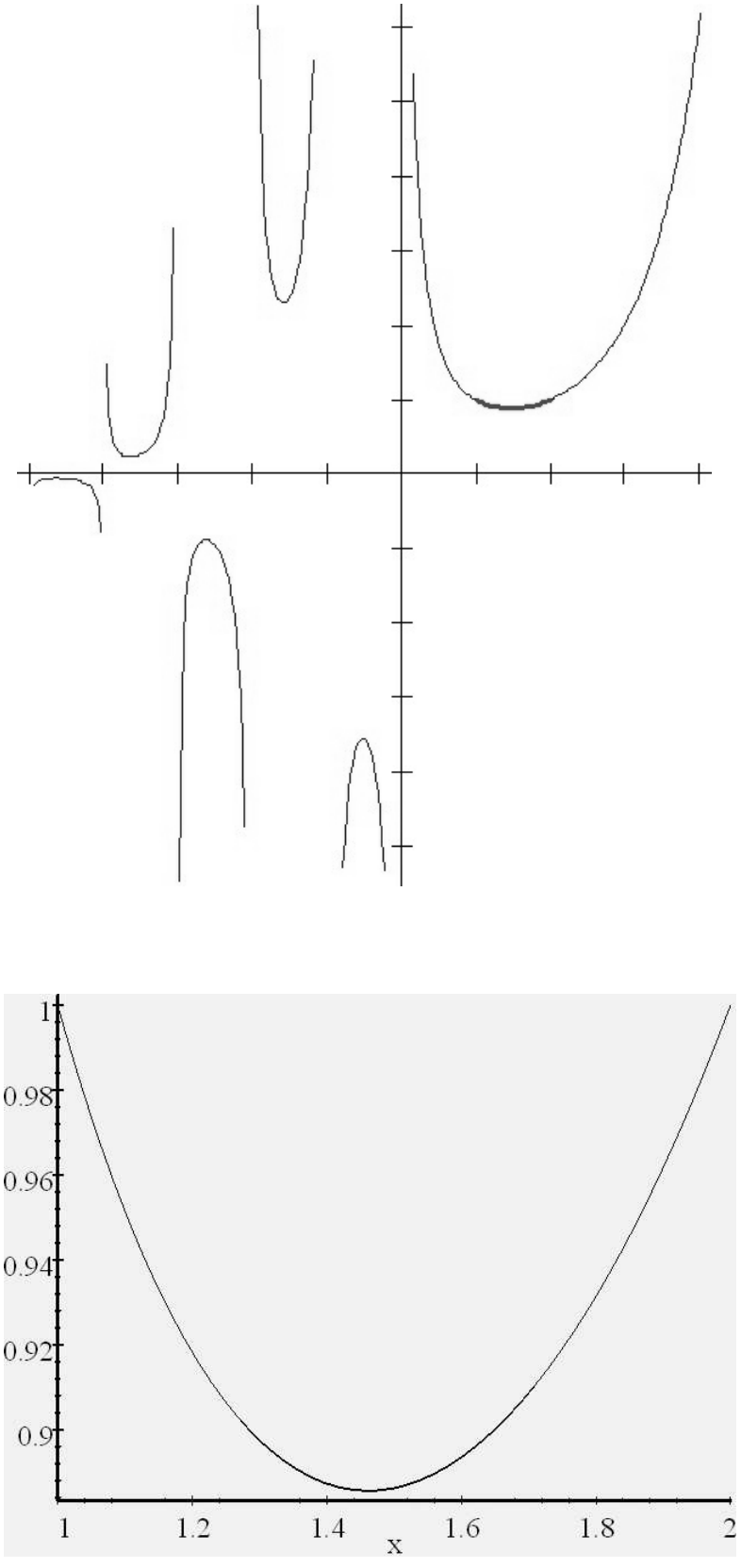

Figura 2.1: Gráfica de la función Gamma.

Capítulo 3

Una generalización del factorial

En este capítulo se presenta una posible generalización de la función factorial elemental, definida en cualquier subconjunto de los números enteros. Para empezar este trabajo necesitamos de algunas nuevas definiciones; las cuales se dan a continuación.

3.1. Nuevos conceptos

Definición 3.1. *Sea S un subconjunto no vacío de $\mathbb{Z}$ y p un primo fijo; un* p-ordenamiento *es una sucesión $\{a_i\}_{i=0}^{\infty}$ de elementos de S que se forma de la siguiente manera:*

- *se escoge un elemento $a_0 \in S$;*
- *se escoge un elemento $a_1 \in S$ que minimice la mayor potencia de p que divide a*

$$(a_1 - a_0)\,;$$

- *se escoge un elemento $a_2 \in S$ que minimice la mayor potencia de p que divide a*

$$(a_2 - a_0) \cdot (a_2 - a_1)\,.$$

Y en general, para el k-ésimo paso:

- *se escoge un elemento $a_k \in S$ que minimice la mayor potencia de p que divide a*

$$(a_k - a_0) \cdot (a_k - a_1) \cdots (a_k - a_{k-1})\,.$$

Claramente pueden existir muchos p-ordenamientos para un subconjunto S de números enteros, debido a que el elemento a_0 puede ser elegido arbitrariamente y además pueden haber varias posibles elecciones de un elemento con el cual se consigue minimizar la potencia de p, y en este caso se puede escoger cualquiera de estos.

Ejemplo 3.2. *Sea* $S = \{0, 1, 2, 3, 4, 5, 6, 7, ...\}$ *y* $p = 5$.

Elijamos $a_0 = 0$ *y tomemos* $a_1 = 1$*; ya que la mayor potencia de* 5 *que divide a*

$$(a_1 - a_0) = (1 - 0) = 1$$

es 5^0.

En el siguiente paso, podemos elegir $a_2 = 2$*, dado que la mayor potencia de* 5 *que divide a*

$$(a_2 - a_0) \cdot (a_2 - a_1) = (2 - 0) \cdot (2 - 1) = 2$$

es 5^0.

Como el elemento a_3 *podemos elegir a* 3*, debido a que la mayor potencia de* 5 *que divide a*

$$(a_3 - a_0)(a_3 - a_1)(a_3 - a_2) = (3 - 0)(3 - 1)(3 - 2) = 6$$

es 5^0.

En el siguiente paso, podemos tomar $a_4 = 4$*, dado que la mayor potencia de* 5 *que divide a*

$$(a_4 - a_0)(a_4 - a_1)(a_4 - a_2)(a_4 - a_3) = (4 - 0)(4 - 1)(4 - 2)(4 - 3) = 24$$

es nuevamente 5^0.

Y así tenemos los primeros cinco elementos de un 5*-ordenamiento de* S*; a saber* $0, 1, 2, 3, 4, \cdots$.

Como afirmamos anteriormente este no es el único 5*-ordenamiento de* S*; para tal efecto se puede comprobar que* $a_0 = 1$*,* $a_1 = 3$*,* $a_2 = 5$*,* $a_3 = 7$ *y* $a_4 = 9$ *son los primeros cinco elementos de otro* 5*-ordenamiento de* S.

Ejemplo 3.3. *Sea* $S = 2\mathbb{Z} \subset \mathbb{Z}$ *y* $p = 3$.

Tomemos $a_0 = 0$*, luego elegimos* $a_1 = 2$*, ya que la mayor potencia de* 3 *que divide a*

$$(a_1 - a_0) = (2 - 0) = 2$$

es 3^0.

Para el siguiente paso podemos elegir $a_2 = 4$ *debido a que la mayor potencia de* 3 *que divide a*

$$(a_2 - a_0) \cdot (a_2 - a_1) = (4 - 0) \cdot (4 - 2) = 4 \times 2 = 8$$

es 3^0.

Para elegir el elemento a_3 *hay que observar que:*

$$(a_3 - a_0)(a_3 - a_1)(a_3 - a_2) = (a_3 - 0)(a_3 - 2)(a_3 - 4) \tag{3.1}$$

es el producto de tres pares consecutivos y por lo tanto es un múltiplo de 3*, entonces para minimizar la potencia de* 3 *dividiendo* (3.1) *podemos elegir* $a_3 = 6$.

Exactamente con el mismo argumento anterior se pueden elegir $a_4 = 8$ *y* $a_5 = 10$.

Por tanto tenemos los primeros seis términos de un 3*-ordenamiento para* S*; a saber* $\{0, 2, 4, 6, 8, 10 \ldots\}$. *Y así podríamos seguir calculando los demás* a_k.

Como en el ejemplo anterior este no es el único 3*-ordenamiento de* S*; fácilmente se puede verificar que* $a_0 = -2$, $a_1 = 0$, $a_2 = 2$, $a_3 = -4$, $a_4 = 4$ *y* $a_5 = -6$ *son los primeros seis elementos de otro* 3*-ordenamiento de* S.

Si notamos por $V_k(S, p)$; $k = 1, 2, 3, \ldots$ la potencia de p que minimiza la elección de a_k en el k-ésimo paso de la construcción del p-ordenamiento, tenemos para el ejemplo anterior que:

$$V_1(S, 3) = 1, \quad V_2(S, 3) = 1, \quad V_3(S, 3) = 3, \quad V_4(S, 3) = 3 \quad \text{y} \quad V_5(S, 3) = 3.$$

Para el 3-ordenamiento $\{0, 2, 4, 6, 8, 10 \ldots\}$, y

$$V_1(S, 3) = 1, \quad V_2(S, 3) = 1, \quad V_3(S, 3) = 3, \quad V_4(S, 3) = 3 \quad \text{y} \quad V_5(S, 3) = 3.$$

Para el 3-ordenamiento $\{-2, 0, 2, -4, 4, -6, \ldots\}$.

Observando lo anterior podríamos pensar que las potencias de p que son minimizadas en cada uno de los pasos de la construcción de los p-ordenamientos son las mismas para cualquier p-ordenamiento de S.

Así para cada p-ordenamiento, tenemos una sucesión monótona creciente de números enteros que llamamos p-sucesión asociada correspondiente al p-ordenamiento. Exactamente tenemos:

Definición 3.4. *Sea* $S \subset \mathbb{Z}$ *y* $\{a_i\}_{i=0}^{\infty}$ *un* p*-ordenamiento de* S*,*

$$\{V_k(S, p)\}_{k=0}^{\infty}$$

es la p-sucesión asociada *de* S *correspondiente a la elección del* p*-ordenamiento* $\{a_i\}$ *de* S. *Donde* $V_k(S, p)$ *es la más alta potencia de* p *minimizada en el* k*-ésimo paso.*

Ejemplo 3.5. *Tomemos el conjunto del ejemplo anterior en el cual encontramos las potencias de* $p = 3$ *que fueron minimizadas y que forman la* 3*-sucesión asociada de* S *correspondiente al* 3*-ordenamiento:* $\{0, 2, 4, 6, 8, 10, \cdots\}$. *Así esta sucesión es*

$$\left\{3^0, 3^0, 3^1, 3^1, 3^1, \cdots\right\} = \{1, 1, 3, 3, 3, \cdots\}.$$

Nota. En adelante denotaremos por $w_p(n)$ la mayor potencia de p que divide a n, esto con el animo de facilitar algunos cálculos. Así tenemos por ejemplo que $w_2(10) = 2$, $w_2(7) = 1$, $w_5(50) = 25$. Nótese además que $\forall m \in \mathbb{Z}$, $\prod_p w_p(m) = |m|$.

Hasta ahora hemos hallado simplemente los primeros elementos de algunos p-ordenamientos; miremos un ejemplo más completo de un p-ordenamiento tomando el conjunto de los enteros como subconjunto de sí mismo.

Ejemplo 3.6. *Sea $\mathbb{Z}$ el conjunto de los enteros. Entonces el ordenamiento natural $0, 1, 2, 3, \cdots$ forma un p-ordenamiento de $\mathbb{Z}$ para todo primo p.*

Demostración. (Utilizando el principio de inducción matemática).

Para $k = 0$, elegimos $a_0 = 0$.

Para $k = 1$ elegimos $a_1 = 1$, y este valor minimiza la mayor potencia de p que divide a

$$(a_1 - a_0) = (1 - 0) = 1$$

para todo primo p.

Ahora suponemos cierto que $0, 1, 2, 3, \cdots (k-1)$ es un p-ordenamiento para los primeros $k-1$ pasos y veamos que $0, 1, 2, 3, \cdots k$ es un p-ordenamiento para los primeros k pasos.

En el k-ésimo paso necesitamos elegir a_k que minimice la mayor potencia de p que divide a

$$(a_k - 0)(a_k - 1) \cdots (a_k - (k-1)) \tag{3.2}$$

Pero esto es el producto de k enteros consecutivos, por tanto es un múltiplo de $k!$ y si elegimos $a_k = k$ encontramos $k!$, y este valor de a_k claramente minimiza la mayor potencia de p que divide (3.2) para todo primo p. □

Una característica muy importante de la p-sucesión asociada de S, como afirmamos anteriormente, es que es independiente de la elección del p-ordenamiento, es decir que eligiendo cualquiera de los p-ordenamientos la p-sucesión asociada siempre será la misma; y por tanto podemos referirnos a ella sin mencionar algún p-ordenamiento en particular (lo cual se enuncia en el siguiente teorema).

Teorema 3.7. *La p-sucesión asociada de S es independiente de la elección del p-ordenamiento.*

La demostración de este teorema se hará mas adelante, ya que necesitamos de algunos conceptos que se verán en el proceso de la generalización del factorial.

Como el teorema anterior afirma que cualquier p-ordenamiento origina la misma p-sucesión asociada, podemos calcular la p-sucesión $V_k(\mathbb{Z}, p)$ de $\mathbb{Z}$. Entonces tenemos:

$$\begin{aligned} V_k(\mathbb{Z}, p) &= w_p\left((a_k - a_0)(a_k - a_1)\cdots(a_k - a_{k-1})\right) \\ &= w_p\left((k-0)(k-1)\cdots(k-(k-1))\right) \;=\; w_p(k!) \end{aligned}$$

Tomando esta última expresión y multiplicándola para todo primo p obtenemos exactamente $k!$.

Por tanto tenemos una definición del factorial, sólo en términos de $V_k(\mathbb{Z}, p)$,

$$k! = \prod_p V_k(\mathbb{Z}, p).$$

Pero dado que para cualquier subconjunto de $\mathbb{Z}$ podemos construir p-ordenamientos y por tanto su p-sucesión asociada; podemos definir el factorial en cualquier subconjunto de los enteros.

Definición 3.8. *Sea $S \subseteq \mathbb{Z}$. Entonces la función factorial de S denotada por $k!_S$ esta definida por:*

$$\begin{aligned} 0!_S &= 1 \\ k!_S &= \prod_p V_k(S, p). \end{aligned} \tag{3.3}$$

En particular tenemos $k!_{\mathbb{Z}} = k!$.

Hay que ver que el número de factores no iguales a uno en (3.3) es necesariamente finita.

Esta definición tiene sentido para cualquier $S \subseteq \mathbb{Z}$ y cualquier $k \in \mathbb{Z}$.

Como un ejemplo sencillo calculemos algunos de los primeros factoriales en un subconjunto muy importante de $\mathbb{Z}$.

Ejemplo 3.9. *Sea S el conjunto de los números primos en $\mathbb{Z}$;*
$S = \{2, 3, 5, 7, 11, 13, \cdots\}$. Calculemos los primeros elementos de un p-ordenamiento para $p = 2$, 3, 5 y 7 con su respectiva p-sucesión asociada.

p	***p*-ordenamiento**							***p*-sucesión asociada**
	a_0	a_1	a_2	a_3	a_4	a_5	$\cdots$	
2	2	3	5	7	17	11		$\{2^0, 2^1, 2^3, 2^4, 2^7, \cdots\}$
3	2	3	7	5	13	17		$\{3^0, 3^0, 3^1, 3^1, 3^2, \cdots\}$
5	2	3	5	11	19	23		$\{5^0, 5^0, 5^0, 5^0, 5^1, \cdots\}$
7	2	3	5	7	11	13		$\{7^0, 7^0, 7^0, 7^0, 7^0, \cdots\}$

Ahora aplicando el algoritmo para calcular los factoriales tenemos:

$$
\begin{aligned}
0!_S &= 1 \\
1!_S &= \prod_p V_1(S,p) = 2^0 \times 3^0 \times 5^0 \times 7^0 = 1 \\
2!_S &= \prod_p V_2(S,p) = 2^1 \times 3^0 \times 5^0 \times 7^0 = 2 \\
3!_S &= \prod_p V_3(S,p) = 2^3 \times 3^1 \times 5^0 \times 7^0 = 24 \\
4!_S &= \prod_p V_4(S,p) = 2^4 \times 3^1 \times 5^0 \times 7^0 = 48 \\
5!_S &= \prod_p V_5(S,p) = 2^7 \times 3^2 \times 5^1 \times 7^0 = 5760
\end{aligned}
$$

Ejemplo 3.10. *Tomemos $S = 2\mathbb{Z}$. Hallemos los primeros factoriales calculando p-ordenamientos para los primeros números primos.*

Se puede verificar (y en efecto se mostrará más adelante) que $a_0 = 0$, $a_1 = 2$, $a_2 = 4$, $a_3 = 6$, $a_4 = 8$, $a_5 = 10$ y $a_6 = 12$ son los primeros términos de un p-ordenamiento para cualquier número primo. Entonces tenemos:

p	***p*-ordenamiento**								***p*-sucesión asociada**
	a_0	a_1	a_2	a_3	a_4	a_5	a_6	$\cdots$	
2	0	2	4	6	8	10	12		$\{2^1, 2^3, 2^4, 2^7, 2^8, 2^{10}, \cdots\}$
3	0	2	4	6	8	10	12		$\{3^0, 3^0, 3^1, 3^1, 3^1, 3^2, \cdots\}$
5	0	2	4	6	8	10	12		$\{5^0, 5^0, 5^0, 5^0, 5^1, 5^1, \cdots\}$
7	0	2	4	6	8	10	12		$\{7^0, 7^0, 7^0, 7^0, 7^0, 7^0, \cdots\}$
11	0	2	4	6	8	10	12		$\{11^0, 11^0, 11^0, 11^0, 11^0, 11^0, \cdots\}$

Calculando los factoriales obtenemos:

$$
\begin{aligned}
0!_S &= 1 \\
1!_S &= \prod_p V_1(S,p) = 2^1 \times 3^0 \times 5^0 \times 7^0 \times 11^0 = 2 \\
2!_S &= \prod_p V_2(S,p) = 2^3 \times 3^0 \times 5^0 \times 7^0 \times 11^0 = 8 \\
3!_S &= \prod_p V_3(S,p) = 2^4 \times 3^1 \times 5^0 \times 7^0 \times 11^0 = 48 \\
4!_S &= \prod_p V_4(S,p) = 2^7 \times 3^1 \times 5^0 \times 7^0 \times 11^0 = 384
\end{aligned}
$$

$$5!_S = \prod_p V_5(S,p) = 2^8 \times 3^1 \times 5^1 \times 7^0 \times 11^0 = 3840$$
$$6!_S = \prod_p V_6(S,p) = 2^{10} \times 3^2 \times 5^1 \times 7^0 \times 11^0 = 46080.$$

Generalmente cuando vamos a calcular factoriales en subconjuntos arbitrarios de $\mathbb{Z}$, esto es un trabajo muy dispendioso, debido a que si se quieren seguir calculando los factoriales para números más grandes; igualmente se deben seguir hallando los a_k del p-ordenamiento para valores cada vez más grandes de k.

Veamos algunos ejemplos de subconjuntos de $\mathbb{Z}$ en los cuales se hace fácil calcular factoriales, pues en ellos hay una característica especial que facilita este trabajo. Son subconjuntos en los cuales hay una sucesión que es un p-ordenamiento para todo primo p. Lo cual afirma el siguiente teorema.

Teorema 3.11. *Supongamos que $\{a_i\}$ es un p-ordenamiento de S para todo primo p. Entonces, $k!_S = |(a_k - a_0)(a_k - a_1)\cdots(a_k - a_{k-1})|$.*

Demostración. Por definición se tiene que:

$$k!_S = \prod_p V_k(S,p) = \prod_p w_p\left((a_k - a_0)(a_k - a_1)\cdots(a_k - a_{k-1})\right).$$

Aquí se presentan dos casos:

1. Si el producto $(a_k - a_0)(a_k - a_1)\cdots(a_k - a_{k-1})$ es positivo, entonces:

$$\prod_p w_p\left((a_k - a_0)(a_k - a_1)\cdots(a_k - a_{k-1})\right) = (a_k - a_0)(a_k - a_1)\cdots(a_k - a_{k-1}).$$

2. Si el producto $(a_k - a_0)(a_k - a_1)\cdots(a_k - a_{k-1})$ es negativo, entonces:

$$\prod_p w_p\left((a_k - a_0)(a_k - a_1)\cdots(a_k - a_{k-1})\right) = -(a_k - a_0)(a_k - a_1)\cdots(a_k - a_{k-1}).$$

En definitiva tenemos que:

$$k!_S = |(a_k - a_0)(a_k - a_1)\cdots(a_k - a_{k-1})|. \qquad \square$$

Ya vimos que si $S = \mathbb{Z}$, entonces $k!_{\mathbb{Z}} = k!$. Ahora veamos otros ejemplos de factoriales en diferentes subconjuntos de $\mathbb{Z}$.

Ejemplo 3.12. *Sea $S = 2\mathbb{Z}$. Mostremos que $0, 2, 4, 6, \cdots$ forma un p-ordenamiento de $2\mathbb{Z}$ para todo primo p.*

(Utilizando el principio de inducción matemática)

Para $k = 0$, tomemos $a_0 = 0$.

Para $k = 1$, elijamos $a_1 = 2$; este valor minimiza la mayor potencia de p que divide a

$$(a_1 - a_0) = (2 - 0) = 2$$

para cualquier número primo p.

Supongamos ahora que $0, 2, 4, \ldots, 2(k-1)$ forma un p-ordenamiento de S para los primeros $(k-1)$ pasos para todo primo p.

En el k-ésimo paso necesitamos elegir un elemento a_k de S que minimice la mayor potencia de p que divide a

$$(a_k - 0)(a_k - 2)(a_k - 4)\cdots(a_k - 2(k-1)) \tag{3.4}$$

Pero esto es el producto de k pares consecutivos y por tanto es un múltiplo de $2^k k!$; eligiendo $a_k = 2k$ se obtiene

$$(2k - 0)(2k - 2)(2k - 4)\cdots(2k - 2(k-1)) = 2k \cdot 2(k-1) \cdot 2(k-2) \cdot \cdots \cdot 2 = 2^k k!$$

y este valor minimiza la mayor potencia de p que divide (3.4) para todo primo p.

Por consiguiente, según el teorema anterior, se tiene que

$$\begin{aligned} k!_{2\mathbb{Z}} &= (2k - 0)(2k - 2)\cdots(2k - (2k - 2)) \\ &= 2k(2k - 2)(2k - 4)\cdots 2 \\ &= 2k \cdot 2 \cdot (k-1) \cdot 2 \cdot (k-2)\cdots 2 \cdot 1 \\ &= 2^k \cdot k!. \end{aligned}$$

Así, si queremos calcular por ejemplo 2!, 5! y 10! en $2\mathbb{Z}$, tendremos:

$$\begin{aligned} 2!_{2\mathbb{Z}} &= 2^2 \cdot 2! = 4 \times 2 = 8, \\ 5!_{2\mathbb{Z}} &= 2^5 \cdot 5! = 32 \times 120 = 3840, \\ 10!_{2\mathbb{Z}} &= 2^{10} \cdot 10! = 3715891200. \end{aligned}$$

En general, si tomamos $S = a\mathbb{Z}+b$ (enteros congruentes con b módulo a encontramos que $k!_{a\mathbb{Z}+b} = a^k \cdot k!$.

Ejemplo 3.13. *Sea S el conjunto de las potencias de 2 en $\mathbb{Z}$. Nuevamente se puede mostrar que $1, 2, 4, 8, \cdots$ forma un p-ordenamiento de S para todo primo p. Entonces tenemos que:*

$$k!_S = \left(2^k - 1\right)\left(2^k - 2\right)\cdots\left(2^k - 2^{k-1}\right).$$

Así, si queremos calcular $2!$, $3!$ *y* $5!$ *en este conjunto, tenemos:*

$$\begin{aligned} 2! &= \left(2^2-1\right)\left(2^2-2\right) = 3\times 2 = 6. \\ 3! &= \left(2^3-1\right)\left(2^3-2\right)\left(2^3-2^2\right) = 7\times 6\times 4 = 168. \\ 5! &= \left(2^5-1\right)\left(2^5-2\right)\left(2^5-2^2\right)\left(2^5-2^3\right)\left(2^5-2^4\right) \\ &= 31\times 30\times 28\times 24\times 16 = 9999360. \end{aligned}$$

Y en general, si tomamos como S *cualquier progresión geométrica en* $\mathbb{Z}$ *con razón* r *y primer término* a*, se tiene que:*

$$k!_S = a^k\cdot\left(r^k-1\right)\left(r^k-r\right)\cdots\left(r^k-r^{k-1}\right).$$

Así, si tenemos $S=\{5,15,45,135,\cdots\}$ *y queremos calcular* $2!$ *en* S*, obtenemos que*

$$2!_S = 5^2\cdot\left(3^2-1\right)\left(3^2-2\right)\left(3^2-3\right) = 25\times 8\times 7\times 6 = 8400.$$

Ejemplo 3.14. *Sea* S *el conjunto de los números cuadrados en* $\mathbb{Z}$*. Se puede verificar que* $0,1,4,9,\cdots$ *forma un* p*-ordenamiento de* S *para todo primo* p*.*

Por tanto

$$k!_S = \underbrace{\left(k^2-0\right)\left(k^2-1\right)\cdots\left(k^2-(k-1)^2\right) = \frac{(2k)!}{2}}_{\text{ver Proposición 3.15}}.$$

Entonces, para calcular por ejemplo $2!$, $3!$ *y* $5!$ *en* S*, se tiene:*

$$\begin{aligned} 2!_S &= \frac{(2\times 2)!}{2} = \frac{4!}{2} = 12. \\ 3!_S &= \frac{(2\times 3)!}{2} = \frac{6!}{2} = 360. \\ 5!_S &= \frac{(2\times 5)!}{2} = \frac{10!}{2} = 1814400. \end{aligned}$$

Proposición 3.15. *Sea* $k\in\mathbb{N}$ *entonces;* $\left(k^2-0\right)\left(k^2-1\right)\cdots\left(k^2-(k-1)^2\right) = \dfrac{(2k)!}{2}$.

Demostración. Factorizando cada uno de los términos de la izquierda se obtiene:

$$(k-0)(k+0)(k-1)(k+1)\cdots(k-(k-1))(k+(k-1)).$$

Ordenando términos encontramos

$$k(k-1)\cdots(k-(k-1))\,k(k+1)\cdots(k+(k-1)) = k!k(k+1)\cdots(2k-1)$$

multiplicando y dividiendo esta expresión por $1\cdot 2\cdot 3\cdot\ldots\cdot(k-1)\,2k$ se obtiene:

$$\begin{aligned} &\frac{k!1\cdot 2\cdot 3\cdot\ldots\cdot(k-1)\,k(k+1)\cdots(2k-1)\,2k}{1\cdot 2\cdot 3\cdot\ldots\cdot(k-1)\,2k} = \\ &= \frac{1\cdot 2\cdot 3\cdot\ldots\cdot(k-1)\,k(k+1)\cdots(2k-1)\,2kk!}{2k!} = \frac{(2k)!}{2}. \quad \square \end{aligned}$$

3.2. Nuevas versiones de resultados anteriores

En esta sección aplicaremos la definición de la extensión de la función factorial a los teoremas vistos en la sección 2.1. Para hacer las demostraciones de los nuevos teoremas, se necesitan de algunas definiciones y resultados los cuales se irán enunciando a medida que sean necesarios.

Para empezar, podemos definir el análogo polinomio factorial para cualquier subconjunto S de $\mathbb{Z}$.

Definición 3.16. *Sea $S \subseteq \mathbb{Z}$ y $\{a_i\}$ un p-ordenamiento fijo de S. El polinomio factorial $x^{(n)S,p}$ está definido como sigue*

$$\begin{aligned} x^{(0)_{S,\,p}} &= 1, \\ x^{(n)_{S,\,p}} &= (x-a_0)(x-a_1)\cdots(x-a_{n-1}). \end{aligned}$$

Ejemplo 3.17. *Sea S el conjunto de los números primos, (ver Ejemplo 3.9) y tomemos $\{2,3,5,11,19,23,\cdots\}$ como el 5-ordenamiento hallado en dicho ejemplo. Entonces tenemos que:*

$$\begin{aligned} x^{(0)_{S,\,5}} &= 1 \\ x^{(1)_{S,\,5}} &= (x-2) \\ x^{(2)_{S,\,5}} &= (x-2)(x-3) \\ x^{(3)_{S,\,5}} &= (x-2)(x-3)(x-5) \\ x^{(4)_{S,\,5}} &= (x-2)(x-3)(x-5)(x-11) \\ x^{(5)_{S,\,5}} &= (x-2)(x-3)(x-5)(x-11)(x-19) \\ &\vdots \end{aligned}$$

Cuando $S = \mathbb{Z}$ con el p-ordenamiento $0, 1, 2, 3, \cdots$, estos polinomios coinciden con los de la Definición 1.25.

Lema 3.18. *Un polinomio f sobre los enteros, escrito en la forma*

$$f(x) = \sum_{i=0}^{k} c_i x^{(i)_{S,\,p}} = \sum_{i=0}^{k} c_i (x-a_0)(x-a_1)\cdots(x-a_{i-1}) \tag{3.5}$$

se anula en S módulo p^e si y sólo sí $c_i x^{(i)_{S,\,p}}$ también se anula para cada $0 \leq i \leq k$.

Demostración.

$\Longrightarrow$: Supongamos que f se anula en S módulo p^e, pero algunos términos $c_i x^{(i)_{S,\,p}}$ no lo hacen para algún i.

Sea j el índice más pequeño para el cual $c_j x^{(j)_{S,p}}$ no se anula en S módulo p^e. Tomando $x = a_j$ en (3.5), encontramos que todos los términos en el lado derecho de (3.5) con $i > j$ se anulan idénticamente, mientras el hecho de que j es el índice más pequeño para el cual $c_j x^{(j)_{S,p}}$ no se anula, garantiza que todos los términos con $i < j$ se anulan módulo p^e. Se sigue que $c_j {a_j}^{(j)_{S,p}}$ también se anula módulo p^e, y por tanto, $c_j x^{(j)_{S,p}}$ se anula sobre todo S módulo p^e, ya que $\{a_i\}$ es un p-ordenamiento.

$\Longleftarrow$: Si cada uno de los términos $c_i x^{(i)_{S,p}}$ se anula en S módulo p^e; entonces es claro que la suma también se anula. □

Definición 3.19. *Sea $S \subseteq \mathbb{Z}$. El* divisor fijo *de f sobre S, denotado por $d(S,f)$ es el* mcd *de todos los elementos que son imagen de f en S. Esto es:*

$$d(S,f) = \operatorname{mcd}\{f(a) : a \in S\}.$$

Ejemplo 3.20. *Sea S el conjunto de los números primos en $\mathbb{Z}$ (ver Ejemplo 3.9). $S = \{2,3,5,7,11,13,\ldots\}$ y sea $f(x) = x^3 + x$.*

Debemos hallar $d(f,S)$.

Tenemos que para $p = 2$, $f(2) = 2^3 + 2 = 8 + 2 = 10$. Como los demás números primos son impares entonces $p = 2k+1$, $k \in \mathbb{Z}$ y

$$\begin{aligned} f(p) &= f(2k+1) = (2k+1)^3 + 2k + 1 \\ &= 8k^3 + 4k + 1 + 2k + 1 = 8k^3 + 6k + 2 \\ &= 2\underbrace{\left(4k^3 + 3k + 1\right)}_{\in\mathbb{Z}}. \end{aligned}$$

Lo que quiere decir que $d(f,S)$ es par.

En particular tenemos $f(11) = 11^3 + 11 = 1342$ y este valor, por el único número par y positivo menor que 10 ,por el cual es divisible es 2. En definitiva se tiene que $d(f,S) = 2$.

Empezaremos enunciando los nuevos resultados al utilizar la función factorial generalizada, con la nueva versión del Teorema 2.9.

Teorema 3.21. *Sea f un polinomio primitivo de grado k, y sea*

$$d(S,f) = \operatorname{mcd}\{f(a) : a \in S\}.$$

Entonces $d(S,f)$ divide a $k!_S$.

Como en el Teorema 2.9, el Teorema 3.21 afirma que $k!_S$ no solamente es una cota superior para un polinomio de grado k en S, sino que dado $k!_S$ (o cualquiera de sus factores) este puede ser obtenido como el divisor fijo de algún polinomio primitivo.

Demostración. Para un primo fijo p, y una elección de un p-ordenamiento $\{a_i\}$ de S escribamos f de la siguiente manera

$$f(x) = \sum_{i=0}^{k} c_i x^{(i)_{S,\,p}} = \sum_{i=0}^{k} c_i \left(x - a_0\right)\left(x - a_1\right)\cdots\left(x - a_{i-1}\right).$$

Como f es primitivo, hay una elección de j $(0 \leq j \leq k)$ tal que c_j no es múltiplo de p. Por definición, f se anula en S módulo $w_p\left(d\left(S, f\right)\right)$; y por el Lema 3.18 tenemos que $c_j x^{(j)_{S,\,p}}$ también se anula. Además, puesto que c_j es primo relativo con p, se sigue $x^{(j)_{S,\,p}}$ se anula en S módulo $w_p\left(d\left(S, f\right)\right)$. En particular, $w_p\left(d\left(S, f\right)\right)$ divide a

$$w_p\left(a_j x^{(j)_{S,\,p}}\right) = w_p\left(a_j - a_0\right)\left(a_j - a_1\right)\cdots\left(a_j - a_{j-1}\right) = w_p\left(j!_S\right);$$

de aquí $w_p\left(d\left(S, f\right)\right)$ divide a $w_p\left(k!_S\right)$, puesto que $j!_S$ divide a $k!_S$. Multiplicando sobre todo p, vemos que $d\left(S, f\right)$ divide a $k!_S$.

Para ver que $k!_S$ (y cualquiera de sus factores) puede ser obtenido como el divisor fijo de algún polinomio primitivo; construimos el polinomio factorial general como sigue:

$$B_{k,S} = \left(x - a_{0,k}\right)\left(x - a_{1,k}\right)\cdots\left(x - a_{k-1,k}\right),$$

donde $\{a_{i,k}\}_{i=0}^{\infty}$ es una sucesión en $\mathbb{Z}$ que, para cada primo p que divide a $k!_S$ es congruente término a término módulo $V_k\left(S, p\right)$ a algún p-ordenamiento de S. Entonces se tiene que $d\left(S, B_{k,S}\right) = k!_S$. Además si r es un factor de $k!_S$, entonces $d\left(S, B_{k,S} + r\right) = r$. □

Ejemplo 3.22. *Sea S y f como en el ejemplo 3.20 en donde encontramos que $d\left(f, S\right) = 2$, entonces para comprobar el Teorema 3.21 debemos ver que $d\left(f, S\right) = 2$, divide a $k!_s = 3!_s = 24$ lo que es cierto, ya que $24 = 2\left(12\right)$.*

Utilizaremos el teorema anterior para hacer la demostración del siguiente teorema que es análogo al Teorema 2.7.

Teorema 3.23. *Para cualesquiera enteros no negativos k y l, $(k + l)!_S$ es un múltiplo de $k!_S \cdot l!_S$.*

Demostración. Por el Teorema 3.21 existe un polinomio primitivo f_k (a saber $B_{k,S}$) y f_{k-n} (a saber $B_{n-k,S}$) con grado k y $n - k$ respectivamente, tal que $d\left(S, f_k\right) = k!_S$ y $d\left(S, f_{n-k}\right) = (n - k)!_S$. Si multiplicamos obtenemos un polinomio primitivo $f = f_k \cdot f_{n-k}$ de grado n tal que $k!_S \cdot (n - k)!_S$ divide a $d\left(S, f\right)$. Y nuevamente por el Teorema 3.21 sabemos que $d\left(S, f\right)$ debe dividir a $n!_S$. Por tanto $k!_S \cdot (n - k)!_S$ divide a $n!_S$. □

Ejemplo 3.24. *Tomemos nuevamente el Ejemplo 3.9, con $k = 2$ y $l = 3$; en el cual encontramos que $2!_S = 2$, $3!_S = 24$ y $5!_S = 5760$. Según el Teorema 3.23, $(2 + 3)!_S$ es múltiplo de $2!_S \cdot 3!_S$, lo cual se comprueba facilmente como sigue*

$$(2+3)!_S = 5!_S = 5760; \qquad 2!_S \cdot 3!_S = 2\,(24) = 48 \qquad y \qquad 5760 = 48\,(120)\,.$$

El siguiente resultado es de gran importancia en la generalización factorial y nos ayudará en la demostración del análogo al Teorema 2.11.

Lema 3.25. *Sea $T \subseteq S \subseteq \mathbb{Z}$. Entonces $k!_S$ divide $k!_T$ para cada $k \geq 0$.*

Demostración. Para cualquier polinomio f, claramente $d\,(S, f)$ divide a $d\,(T, f)$. Así en particular, $d\,(S, B_{k,S}) = k!_S$ divide a $d\,(T, B_{k,S})$ y por el Teorema 3.21 este debe dividir a $k!_T$. Y por tanto $k!_S$ divide a $k!_T$. □

Teorema 3.26. *Sean a_0, a_1, a_2, $\cdots$, $a_n \in S$, $n+1$ enteros cualesquiera. Entonces el producto*

$$\prod_{i<j} (a_i - a_j)$$

es un múltiplo de $0!_S \cdot 1!_S \cdot 2!_S \cdots n!_S$.

Demostración. Para un primo fijo p, asumamos que a_0, a_1, a_2, $\cdots$, a_n son los $n+1$ primeros elementos de un p-ordenamiento del conjunto $T = \{a_0, a_1, a_2, \cdots a_n\}$. Entonces puesto que para cada $0 \leq k \leq n$,

$$V_k\,(T, p) = w_p\,((a_k - a_0)\,(a_k - a_1) \cdots (a_k - a_{k-1}))\,.$$

Encontramos tomando el producto sobre todo k y por tanto sobre todo p, que

$$0!_T \cdot 1!_T \cdots n!_T = \pm \prod_{i<j} (a_j - a_i)\,,$$

ahora por el lema anterior sabemos que $k!_S$ divide a $k!_T$, por consiguiente

$$0!_S \cdot 1!_S \cdots n!_S \Big| \prod_{i<j} (a_i - a_j)\,. \qquad \square$$

Ejemplo 3.27. *En el Ejemplo 3.9 encontramos que $0!_S = 1$, $1!_S = 1$, $2!_S = 2$, $3!_S = 24$, $4!_S = 48$ y $5!_S = 5760$. Por lo tanto, si $p_0, p_1, \ldots p_5$ son seis primos cualesquiera, el Teorema 3.26 afirma que el producto de sus pares de diferencias $\prod_{i<j} (p_i - p_j)$ es múltiplo de* 13271040.

Tomemos los primeros seis números primos, a saber, 2, 3, 5, 7, 11 *y* 13. *Entonces*

$$\begin{aligned}\prod_{i<j} (p_i - p_j) = {} & (2-3)\,(2-5)\,(2-7)\,(2-11)\,(2-13)\,(3-5)\,(3-7)\,(3-11) \\ & \times (3-13)\,(5-7)\,(5-11)\,(5-13)\,(7-11)\,(7-13)\,(11-13)\end{aligned}$$

$$
\begin{aligned}
&= (-1)\,(-3)\,(-5)\,(-9)\,(-11)\,(-2)\,(-4)\,(-8) \\
&\quad \times (-10)\,(-2)\,(-6)\,(-8)\,(-4)\,(-6)\,(-2) \\
&= -\,4379443200
\end{aligned}
$$

y

$$-4379443200 = -330 \times 13271040.$$

Para facilitar la demostración del resultado análogo al Teorema 2.13 necesitamos el siguiente refinamiento del Lema 3.18.

Lema 3.28. *Un polinomio de grado d escrito en la forma*

$$f(x) = \sum_{k=0}^{d} x^{(k)_{S,p}} = \sum_{k=0}^{d} b_k\,(x - a_0)\,(x - a_1)\cdots(x - a_{k-1})$$

se anula en S módulo p^e si y sólo si b_k es un múltiplo de $\dfrac{p^e}{\operatorname{mcd}(p^e, k!_S)}$ para cada $0 \leq k \leq d$.

Demostración. Por Lema 3.25, $f(x)$ se anula en S módulo p^e si y sólo si $b_k x^{(k)_{S,p}}$ también se anula para cada $0 \leq k \leq d$. Ahora por construcción de $x^{(k)_{S,p}}$, tenemos que $w_p\left(d\left(S, x^{(k)_{S,p}}\right)\right) = V_k(S,p)$; por lo tanto $b_k x^{(k)_{S,p}}$ se anula en S módulo p^e si y sólo si b_k es un múltiplo de $\dfrac{p^e}{\operatorname{mcd}(p^e, k!_S)}$. □

Teorema 3.29. *Sea $S \subseteq \mathbb{Z}/n\mathbb{Z}$. Entonces el número de funciones polinomiales de S en $\mathbb{Z}/n\mathbb{Z}$ esta dado por*

$$\prod_{k=0}^{n-1} \frac{n}{\operatorname{mcd}(n, k!_S)}.$$

Demostración. Por el Teorema Chino del residuo (Teorema 1.3), designar una función polinómica en S módulo n es equivalente a designar la función módulo cada potencia prima que divide a n.

Ahora fácilmente se ve que la formula del Teorema 3.29 es multiplicativa, por tanto, esto basta para verificar dicho teorema cuando $n = p^e$ es una potencia de un número primo.

Sea $\{a_i\}$ un p-ordenamiento de S. Entonces se quiere mostrar que cualquier función polinómica $f : S \longrightarrow \mathbb{Z}/p^e\mathbb{Z}$ puede ser expresada únicamente en la forma

$$f(x) = \sum_{k=0}^{\infty} c_k\,(x - a_0)\,(x - a_1)\cdots(x - a_{k-1}), \tag{3.6}$$

donde $0 \leq c_k \leq \dfrac{p^e}{\operatorname{mcd}(p^e, k!_S)}$ para cada $k \geq 0$. En efecto, por el Lema 3.28 al cambiar uno de los coeficientes c_k por un múltiplo de $\dfrac{p^e}{\operatorname{mcd}(p^e, k!_S)}$ en (3.6) no cambia la función f, es decir, los c_k están determinados únicamente módulo $\dfrac{p^e}{\operatorname{mcd}(p^e, k!_S)}$, así nosotros podemos elegir los c_k en el rango $0 \leq c_k \leq \dfrac{p^e}{\operatorname{mcd}(p^e, k!_S)}$. Ahora tenemos una única representación para cada función polinómica de S en $\mathbb{Z}/p^e\mathbb{Z}$. Observando que aquí hay $\dfrac{p^e}{\operatorname{mcd}(p^e, k!_S)}$ elecciones de c_k para cada $k \geq 0$ se obtiene el resultado del teorema. □

Ahora ya estamos listos para hacer la demostración del teorema 3.7

Demostración del Teorema 3.7. Sea $d \in \mathbb{Z}$ y e un entero positivo grande tal que $p^e > V_d(S, p)$. Consideremos el grupo aditivo G_d de todos los polinomios en $(\mathbb{Z}/p^e\mathbb{Z})_{[x]}$ que se anulan sobre S módulo p^e y tienen grado a lo más d.

Entonces el Lema 3.18 implica, que el grupo abeliano G_d es isomorfo a $\bigoplus_{k=0}^{d} \mathbb{Z}/V_k(S, p)\mathbb{Z}$. Así los números $V_d(S, p)$ para $0 \leq k \leq d$ forma la estructura de coeficientes de este grupo abeliano G_d; además por el teorema para grupos abelianos finitamente generados (Véase por ejemplo [3, p. 92–93]) esas constantes dependen únicamente de ellas mismas, sobre G_d, implicando la afirmación del teorema. □

3.3. Preguntas para investigaciones posteriores

Presentamos aquí algunos de los interrogantes relacionados con la generalización factorial que surgen de manera natural.

1. Para un subconjunto S de $\mathbb{Z}$. ¿Existe una interpretación combinatoria de $k!_S$?
2. Recordemos la función Gamma vista en la sección 2.2. Para cada subconjunto S de $\mathbb{Z}$ ¿Podría existir una generalización de la función Gamma definida en los números reales? ¿Qué propiedades vistas en dicha sección seguiría conservando?
3. ¿Cuáles subconjuntos S de $\mathbb{Z}$ tienen p-ordenamientos para todo primo p?
4. Para un subconjunto S de $\mathbb{Z}$. ¿Existe un interpretación combinatoria natural para $\binom{n}{k}_S$?

5. Si reemplazamos el conjunto de los enteros por cualquier anillo Dedekind (Definición 1.20). ¿ Se sigue cumpliendo la generalización factorial propuesta aquí para subconjuntos de esta clase de anillos?

6. Observando la Definición 1.27 ¿Se podría pensar en la generalización factorial no para subconjuntos de $\mathbb{Z}$, sino para subconjuntos de $\mathbb{Z}^n$ cuando $n > 1$? ¿Que resultados vistos en este trabajo podrían redefinirse en este caso?

Esperamos que el lector se motive a tratar de dar respuesta a estos interrogantes y a muchos otros que hayan podido aparecer como consecuencia en todo el proceso de este trabajo.

Bibliografía

[1] BHARGAVA Manjul. *The factorial function and generalizations*. American Mathematical Montly 107, 2000.

[2] BHARGAVA Manjul. *Generalized factorials and fixed divisors over subsets of a Dedekind domain*. J. reine angew. Math. 490, 1997

[3] FRALEIGH Jhon B. Álgebra abstracta. Primer curso. Estados Unidos: Addison-Wesley Iberoamericana. 1982.

[4] ATIYAH M.F. and MACDONALD I.G. Introducción al álgebra conmutativa. Barcelona: Ed. Reverté:, 1980.

[5] GROSSMAN Stanley. Álgebra lineal. Ed. McGraw Hill: Mexico.1996.

[6] JIMENEZ Rafael, GORDILLO Enrique, RUBIANO Gustavo. Teoría de números para principiantes. Bogotá: Unibiblos Sección Imprenta.