NOTAS DE ÁLGEBRA I

AUTORES: ARIEL PACETTI Y MATÍAS GRAÑA

Índice

1. Conjuntos, relaciones y funciones 2
1.1. Conjuntos 2
1.2. Relaciones 6
1.3. Funciones 9
2. Inducción 12
2.1. Inducción como herramienta para construir sucesiones 17
3. Combinatoria 22
3.1. Bosones 27
4. Probabilidad 29
5. Números Enteros 32
5.1. Introducción 32
5.2. Divisibilidad 33
5.3. Números Primos 42
5.4. Sistemas Numéricos o Bases 45
6. congruencias 47
7. Ecuaciones diofánticas lineales 49
7.1. Ecuaciones lineales de congruencias 52
8. Estructura de $\mathbb{Z}/m\mathbb{Z}$ 53
8.1. Teorema Chino del Resto 58
8.2. RSA (Rivest-Shamir-Adleman) 62
9. Números Complejos 64
9.1. Raíces de un complejo 67

1. Conjuntos, relaciones y funciones

1.1. Conjuntos.

Definición. Un *conjunto* $\mathcal{A}$ es una colección de objetos tales que, dado un objeto cualquiera v, se puede determinar si v pertenece a $\mathcal{A}$ o no.

Ejemplos. Algunos ejemplos fáciles de conjuntos:

1. $\mathcal{A} = \{1, 2, 3\}$.
2. $\mathcal{A} = \{\bigcirc, \triangle, \square\}$.
3. $\mathcal{A} = \emptyset = \{\}$ es el conjunto vacío, que no tiene ningún elemento.
4. $\mathcal{A} = \{\text{números enteros}\}$.

Si $\mathcal{A}$ es un conjunto y v es un elemento cualquiera, notamos $v \in \mathcal{A}$ si v pertenece al conjunto $\mathcal{A}$ y $v \notin \mathcal{A}$ si el elemento v no pertenece al conjunto $\mathcal{A}$.

Definición. Si $\mathcal{A}$ y $\mathcal{B}$ son dos conjuntos cualesquiera, decimos que $\mathcal{A}$ es un subconjunto de $\mathcal{B}$ o que $\mathcal{A}$ está contenido, o incluido, en $\mathcal{B}$ (y escribimos $\mathcal{A} \subset \mathcal{B}$) si todo elemento $v \in \mathcal{A}$ satisface que $v \in \mathcal{B}$.

Muchas veces es útil tener en claro qué quiere decir que un conjunto **no** esté incluido en otro. Lo contrario de *"todo elemento de $\mathcal{A}$ está en $\mathcal{B}$"* es *"existe al menos un elemento en $\mathcal{A}$ que no está en $\mathcal{B}$"*. Esto es, para probar que $\mathcal{A} \not\subset \mathcal{A}$, es necesario encontrar (o probar que existe) un elemento $x \in \mathcal{A}$ tal que $x \notin \mathcal{B}$.

Ejercicios. Decidir si son ciertas las siguientes afirmaciones y en caso afirmativo demostrarlas:

1. $\{1, 2\} \subset \{1, 2, 3\}$.
2. $\{1, 2, 3\} \subset \{\{1\}, 2, 3, 4\}$.
3. $\emptyset \subset \{1, \{1\}\}$.

¿Cómo podemos explicitar un conjunto $\mathcal{A}$? Hasta aquí conocemos una única manera: listando todos sus elementos. ¿Cómo podemos explicitar un conjunto de otra manera? La respuesta es *por comprensión*. Esto es, dando alguna propiedad que cumplen los elementos que están en el conjunto y no cumplen los elementos que no están en el conjunto. Un primer ejemplo (que presenta problemas) es $\mathcal{B} = \{n : n \text{ es par}\}$. Este ejemplo tiene el problema de que no se dice qué números se consideran. Todos entendemos que $2 \in \mathcal{B}$. Pero ¿$-2 \in \mathcal{B}$? Cuando se escribe n en la definición de $\mathcal{B}$, se consideran también números negativos? ¿Y otro tipo de números? La solución a este problema es decir precisamente a qué tipo de elementos nos referimos cuando decimos "n es par". La forma correcta entonces de definir este conjunto es $\mathcal{B} = \{n \in \mathbb{N} : n \text{ es par}\}$ (si es que queremos trabajar solo con números positivos), o $\mathcal{B} = \{n \in \mathbb{Z} : n \text{ es par}\}$ (si es que queremos trabajar también con números negativos).

Un ejemplo clásico que muestra la necesidad de especificar el conjunto de los objetos sobre los que miramos la propiedad es la paradoja de Russell y Zermelo (1901), sea $\mathcal{A} = \{\mathcal{B} : \mathcal{B} \notin \mathcal{B}\}$. ¿Es cierto que $\mathcal{A} \in \mathcal{A}$?

Ejemplos de conjuntos definidos por comprensión son

- $\mathcal{A} = \left\{x \in \mathbb{R} : x^2 < 2\right\}$.
- $\mathcal{A} = \left\{x \in \mathbb{Q} : x^2 < 2\right\}$.
- $\mathcal{A} = \{n \in \mathbb{N} : n \text{ es primo}\}$.
- $\mathcal{A} = \{n + 1 : n \in \mathbb{Z} \text{ y } n \text{ es primo}\} = \{n \in \mathbb{Z} : n - 1 \text{ es primo}\}$.

Definición. Si $\mathcal{A}$ y $\mathcal{B}$ son dos conjuntos, decimos que $\mathcal{A} = \mathcal{B}$ si tienen exactamente los mismos elementos. En otras palabras, $\mathcal{A} = \mathcal{B}$ si $\mathcal{A} \subset \mathcal{B}$ y $\mathcal{B} \subset \mathcal{A}$.

Al trabajar con conjuntos, uno quiere poder definir ciertas *operaciones* entre ellos. Los ejemplos básicos de operaciones de conjuntos son:

- La *unión* (notada $\cup$): dados conjuntos $\mathcal{A}$ y $\mathcal{B}$, $\mathcal{A} \cup \mathcal{B}$ es el conjunto formado por los elementos que están en el conjunto $\mathcal{A}$ o están en el conjunto $\mathcal{B}$. Recordemos que *"o"* en matemática significa que es verdadera *al menos* una de las dos afirmaciones.
- La *intersección* (notada $\cap$): dados conjuntos $\mathcal{A}$ y $\mathcal{B}$, $\mathcal{A} \cap \mathcal{B}$ es el conjunto formado por los elementos que están en $\mathcal{A}$ y están en $\mathcal{B}$.
- La *diferencia* (notada $\mathcal{A} - \mathcal{B}$ ó $\mathcal{A} \backslash \mathcal{B}$): son los elementos que están en $\mathcal{A}$ y que no están en $\mathcal{B}$.

Ejemplos. Tomemos los conjuntos:

- $\mathcal{A} = \{1, 2, 8, -1\}$, $\mathcal{B} = \{\{1\}, 2, 10, 15\}$. Entonces
$$\mathcal{A} \cup \mathcal{B} = \{1, 2, 8, -1, \{1\}, 10, 15\}, \quad \mathcal{A} \cap \mathcal{B} = \{2\},$$
$$\mathcal{A} - \mathcal{B} = \{1, 8, -1\}, \quad \mathcal{B} - \mathcal{A} = \{\{1\}, 10, 15\}.$$
- $\mathcal{A} = \{\text{enteros pares}\}$, $\mathcal{B} = \{\text{enteros impares}\}$. Entonces $\mathcal{A} \cup \mathcal{B} = \mathbb{Z}$, $\mathcal{A} \cap \mathcal{B} = \emptyset$, $\mathcal{A} - \mathcal{B} = \mathcal{A}$ y $\mathcal{B} - \mathcal{A} = \mathcal{B}$.
- $\mathcal{A}$ un conjunto cualquiera y $\mathcal{B} = \emptyset$. Entonces $\mathcal{A} \cup \emptyset = \mathcal{A}$, $\mathcal{A} \cap \emptyset = \emptyset$, $\mathcal{A} - \emptyset = \mathcal{A}$ y $\emptyset - \mathcal{A} = \emptyset$.
- Si $\mathcal{A} = \mathcal{B}$ ¿cómo son $\mathcal{A} \cup \mathcal{B}$, $\mathcal{A} \cap \mathcal{B}$ y $\mathcal{A} \setminus \mathcal{B}$?

Definición. Dos conjuntos $\mathcal{A}$ y $\mathcal{B}$ se dicen disjuntos si $\mathcal{A} \cap \mathcal{B} = \emptyset$; Es decir, si no tienen elementos en común. ¿Cómo son $\mathcal{A} \setminus \mathcal{B}$ y $\mathcal{B} \setminus \mathcal{A}$ si $\mathcal{A}$ y $\mathcal{B}$ son disjuntos?

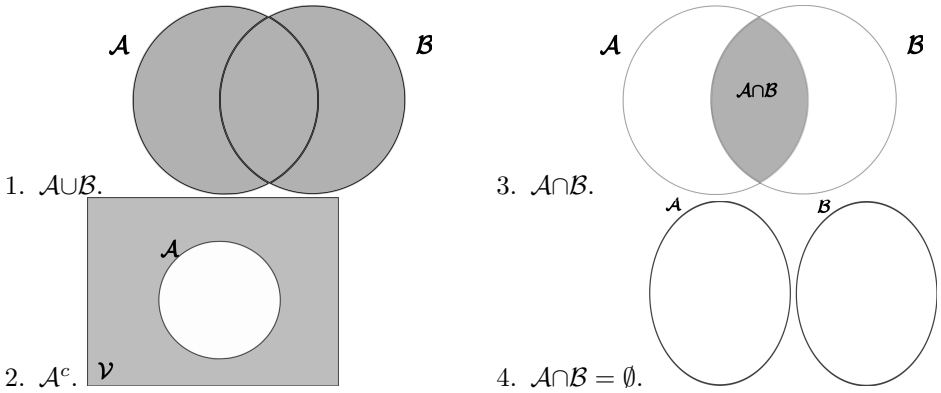
Un procedimiento usual es trabajar dentro de un conjunto *referencial* V. Si $\mathcal{A}$ y $\mathcal{B}$ son subconjuntos de V, entonces $\mathcal{A} \cup \mathcal{B}$, $\mathcal{A} \cap \mathcal{B}$ y $\mathcal{A} \setminus \mathcal{B}$ están también dentro de V. La existencia de un conjunto referencial permite hablar de *complementos*:

Definición. Si $\mathcal{A}$ es un subconjunto de un conjunto referencial V, el *complemento* de $\mathcal{A}$ (notado $\mathcal{A}^c$) es el conjunto de los elementos de V que no están en $\mathcal{A}$, o sea $\mathcal{A}^c = V - \mathcal{A}$.

Ejemplo. Consideremos el conjunto $V = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ y $\mathcal{A} = \{1, 9, 5, 3\}$. Entonces, $\mathcal{A}^c = \{2, 4, 6, 7, 8, 10\}$. Si miramos el conjunto $(\mathcal{A}^c)^c = \{1, 3, 5, 9\} = \mathcal{A}$, ¿será esto siempre cierto? O sea, si $\mathcal{A}$ es un subconjunto de un conjunto referencial V, ¿es cierto que $(\mathcal{A}^c)^c = \mathcal{A}$?

Aquí surge el siguiente problema: ¿cómo podemos probar una igualdad entre dos conjuntos cualesquiera? Una herramienta muy útil (para probar igualdades entre pocos conjuntos) es considerar los *diagramas de Venn*[1] . Un diagrama de Venn es una manera gráfica de representar conjuntos y elementos en estos conjuntos, por ejemplo:

[1] J. Venn, On the Diagrammatic and Mechanical Representation of Propositions and Reasonings, Philosophical Magazine and Journal of Science, Series 5, vol. **10**, No. 59, (1880).



Veamos el diagrama de Venn de la siguiente situación: tomamos el conjunto de alumnos que ingresaron en la facultad de ciencias exactas en el año 2008. De los 550 alumnos que entraron, 300 cursan Análisis I y Álgebra I, 150 cursan Análisis I y Física I, 20 cursan las 3 materias, 30 cursan sólo Álgebra I, 25 cursan sólo Análisis I, 15 cursan sólo Física I y 10 no cursan ninguna de estas materias.

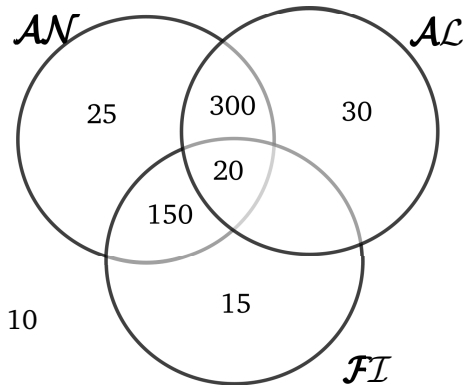


FIGURA 1. Cantidades de alumnos cursando cada materia

Un ejemplo de uso de los diagramas de Venn para probar una igualdad entre conjuntos es:

Teorema 1.1 (Ley de de Morgan)**.** *Si $\mathcal{A}$ y $\mathcal{B}$ son conjuntos, entonces $(\mathcal{A}\cup\mathcal{B})^c = \mathcal{A}^c\cap\mathcal{B}^c$.*

Dem: Miramos los diagramas de Venn de los conjuntos correspondientes y vemos que coinciden! □

Antes de hacer varios otros ejemplos de diagramas de Venn (y sus demostraciones), veamos otra manera de demostrar una igualdad entre conjuntos: la llamada *tabla de verdad*. Supongamos que queremos probar que una operación entre un cierto número de conjuntos es igual a otra operación de los mismos (por ejemplo la Ley de de Morgan). El método entonces consiste en considerar, dado un elemento, todas las posibilidades de pertenecer o no a cada uno de los conjuntos involucrados.

Luego, se debe estudiar para cada caso si el elemento pertenece a los conjuntos que se quiere comparar. Veamos cómo sería la Ley de de Morgan:

$x \in \mathcal{A}$	$x \in \mathcal{B}$	$x \in (\mathcal{A} \cup \mathcal{B})$	$x \in (\mathcal{A} \cup \mathcal{B})^c$	$x \in \mathcal{A}^c \cap \mathcal{B}^c$
V	V	V	F	F
V	F	V	F	F
F	V	V	F	F
F	F	F	V	V

Para hacer la notación mas sencilla, en general simplemente escribimos $\mathcal{A} \cup \mathcal{B}$ en lugar de la afirmación $x \in \mathcal{A} \cup \mathcal{B}$. Es claro que dos operaciones de conjuntos dan el mismo conjunto si y solo si tienen la misma tabla de verdad, y esto ocurre si y solo si tienen el mismo diagrama de Venn.

Ejemplos. Probar o dar un contraejemplo de las siguientes afirmaciones:

1. $\mathcal{A} \cap (\mathcal{B} \cup \mathcal{C}) = (\mathcal{A} \cap \mathcal{B}) \cup (\mathcal{A} \cap \mathcal{C})$.
2. $\mathcal{A} - \mathcal{B} = \mathcal{A} \cap \mathcal{B}^c$.
3. Dados dos conjuntos $\mathcal{A}$ y $\mathcal{B}$, definimos la operación *diferencia simétrica* entre ellos (y la notamos $\mathcal{A} \triangle \mathcal{B}$) , como $\mathcal{A} \triangle \mathcal{B} = (\mathcal{A} \cup \mathcal{B}) - (\mathcal{A} \cap \mathcal{B})$. Calcular la tabla de verdad de está operación. ¿Cómo se puede definir en términos de los elementos de $\mathcal{A}$ y de $\mathcal{B}$?

Un gran problema de los diagramas de Venn es que se vuelven impracticables al realizar operaciones entre muchos conjuntos. Las tablas de verdad se pueden hacer en cualquier caso, pero el número de casos a considerar crece "demasiado" con el número de conjuntos (ya veremos en el próximo capítulo qué quiere decir esto).

Consideremos el siguiente problema: vamos al kiosco a comprar algunas cosas, y cuando llegamos la persona que atiende nos informa que no disponen de cambio alguno, con lo cual sólo nos pueden vender cosas si pagamos justo. Mirando la billetera encontramos que traemos una moneda de \$1, un billete de \$2 y un billete de \$5. ¿Qué cosas podemos pagar con estos billetes?

El resultado surge de hacer una cuenta que seguramente todos hicimos en alguna circunstancia. Una opción es irnos sin comprar nada (o sea dándole nada al kiosquero), y las otras opciones son juntar \$1, \$2, \$3, \$5, \$6, \$7 u \$8. Lo que hicimos fue calcular del conjunto $\{1, 2, 5\}$ todos sus posibles subconjuntos, y luego sumar los elementos de cada subconjunto, así obtuvimos los subconjuntos: $\emptyset$, $\{1\}$, $\{2\}$, $\{1, 2\}$, $\{5\}$, $\{1, 5\}$, $\{2, 5\}$ y $\{1, 2, 5\}$.

Definición. Si $\mathcal{A}$ es un conjunto, notamos con $\mathcal{P}(\mathcal{A})$ el conjunto de *partes de* $\mathcal{A}$ que es el conjunto formado por todos los subconjuntos del conjunto $\mathcal{A}$.

Ejercicios

1. ¿Quién es $\mathcal{P}(\emptyset)$?
2. Si $\mathcal{A} = \{1, \{1\}, \{1, 2\}, -3\}$, ¿quién es $\mathcal{P}(\mathcal{A})$?

Por último, otra operación importante entre dos conjuntos es el *producto cartesiano*. Dados $\mathcal{A}, \mathcal{B}$ conjuntos, el producto cartesiano de ambos (denotado por $\mathcal{A} \times \mathcal{B}$) es el conjunto de pares (a, b) donde $a \in \mathcal{A}$ y $b \in \mathcal{B}$.

Ejemplos.

- Si $\mathcal{A}$ y $\mathcal{B}$ es el conjunto de números reales, su producto cartesiano es el plano Euclídeo (donde constantemente hacemos gráficos de funciones).

- Si $\mathcal{A} = \{1, \pi, -8\}$ y $\mathcal{B} = \left\{\frac{3}{4}, 0\right\}$, su producto cartesiano es

$$\mathcal{A} \times \mathcal{B} = \{(1, \frac{3}{4}), (1, 0), (\pi, \frac{3}{4}), (\pi, 0), (-8, \frac{3}{4}), (-8, 0)\}$$

Para asegurarnos de que no nos olvidamos ningún elemento, podemos listar los elementos de $\mathcal{A} \times \mathcal{B}$ en una tabla, donde en las columnas ponemos los elementos de un conjunto y en las filas los elementos del otro. En el ejemplo anterior quedaría

$A \backslash B$	$3/4$	0
1	$(1, 3/4)$	$(1, 0)$
π	$(\pi, 3/4)$	$(\pi, 0)$
-8	$(-8, 3/4)$	$(-8, 0)$

El producto cartesiano lo utilizamos en más cosas de las que pensamos. Por ejemplo, si al levantarnos decidimos vestirnos, tenemos ciertas alternativas de pantalones (o polleras), distintas alternativas de remeras, zapatos, etc. Luego tenemos un conjunto que podemos llamar de "calzado", otro conjunto de "ropa inferior" y un último conjunto de "ropa superior". Cada opción de vestimenta corresponde a un elemento del producto cartesiano de estos tres conjuntos.

Definición. Definimos el *cardinal* de un conjunto como el número de elementos que posee.

Pregunta. ¿Qué cardinal tiene el producto cartesiano de dos conjuntos finitos?

En breve volveremos al cálculo de cardinales de conjuntos.

1.2. Relaciones.

Definición. Dados dos conjuntos $\mathcal{A}$ y $\mathcal{B}$ una relación (binaria) de $\mathcal{A}$ en $\mathcal{B}$ es un subconjunto $\mathcal{R}$ de $\mathcal{A} \times \mathcal{B}$.

Dado $a \in \mathcal{A}$ y $b \in \mathcal{B}$, decimos que a está relacionado con b (y lo escribimos $a\mathcal{R}b$) si el par $(a, b) \in \mathcal{R}$.

Ejemplos. Tomamos como conjunto $\mathcal{A} = \{a, b, c\}$ y $\mathcal{B} = \{1, 2\}$.

- Consideremos $\mathcal{R} = \mathcal{A} \times \mathcal{B}$. O sea todo elemento del conjunto $\mathcal{A}$ está relacionado con todo elemento del conjunto $\mathcal{B}$.
- Consideremos $\mathcal{R} = \{(a, 1), (b, 1), (c, 2)\}$. ¿Es cierto que $a\mathcal{R}2$? ¿Y que $b\mathcal{R}1$?
- Consideremos $\mathcal{R} = \emptyset$. ¿Es cierto que $a\mathcal{R}2$?

Consideramos ahora relaciones $\mathcal{R} \subset \mathcal{A} \times \mathcal{A}$. La ventaja de estas relaciones es que (si $\mathcal{A}$ es finito) las podemos representar mediante un *grafo dirigido*. Un grafo dirigido es un conjunto de puntos (llamados vértices) y un conjunto de flechas entre los vértices. Por ejemplo, el grafo $1 \to 2$, $2 \to 3$ del conjunto $\{1, 2, 3, 4\}$ (ver la Figura 2). No vamos a hacer uso de la teoría de grafos, aunque ésta juega un rol

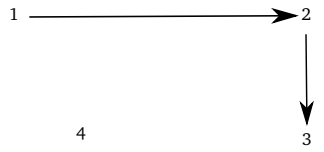


FIGURA 2. El grafo de una relación

esencial en varias ramas de la matemática y la computación (como el estudio de circuitos, en las simulaciones de epidemias, etc).

La manera de asociarle un grafo a una relación $\mathcal{R} \subset \mathcal{A} \times \mathcal{A}$ es poner como vértices los elementos del conjunto $\mathcal{A}$ y luego una flecha por cada elemento de $\mathcal{R}$. Si $(a, b) \in \mathcal{R}$, la flecha asociada es la que parte del vértice a y llega al vértice b. Por ejemplo, tomemos como conjunto $\mathcal{A} = \{1, 2, 3, 4\}$.

- La relación $\mathcal{R} = \{(1, 1), (1, 3), (3, 2), (2, 4)\}$ se grafica en la Figura 3.

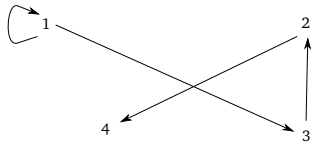


FIGURA 3. Grafo de la relación $\{(1, 1), (1, 3), (3, 2), (2, 4)\}$

- A la relación $\mathcal{R} = \emptyset$ le corresponde un grafo sin flechas.
- ¿Qué relación le corresponde al grafo de la Figura 4?



FIGURA 4

Las relaciones entre un conjunto y sí mismo son especialmente importantes, y algunas de sus posibles propiedades merecen un nombre. Consideremos entonces una relación $\mathcal{R} \subseteq \mathcal{A} \times \mathcal{A}$.

- $\mathcal{R}$ se dice *reflexiva* si $(a, a) \in \mathcal{R}$ para todo elemento $a \in \mathcal{A}$. En términos del grafo de la relación, $\mathcal{R}$ es reflexiva si en cada vértice hay una flecha que parte y termina en él.
- $\mathcal{R}$ se dice *simétrica* si para todo par $(a, b) \in \mathcal{R}$ el par $(b, a) \in \mathcal{R}$ (o sea si $a\mathcal{R}b$ entonces $b\mathcal{R}a$). En términos del grafo, $\mathcal{R}$ es simétrica si por cada flecha en una dirección hay otra en la dirección opuesta.
- $\mathcal{R}$ se dice *antisimétrica* si para todos los elementos $a, b \in \mathcal{A}$ vale la siguiente afirmación: si $(a, b) \in \mathcal{R}$ y $(b, a) \in \mathcal{R}$ entonces $a = b$ (o sea, si $a \neq b$ entonces no puede a la vez ser $a\mathcal{R}b$ y $b\mathcal{R}a$). En términos del grafo, $\mathcal{R}$ es antisimétrica si no hay ningún par de flechas en sentidos opuestos.
- $\mathcal{R}$ se dice *transitiva* si para toda terna de elementos $a, b, c \in \mathcal{A}$ tales que $(a, b) \in \mathcal{R}$ y $(b, c) \in \mathcal{R}$ se tiene que $(a, c) \in \mathcal{R}$ (o sea si $a\mathcal{R}b$ y $b\mathcal{R}c$ entonces $a\mathcal{R}c$). En términos del grafo, $\mathcal{R}$ es transitiva si hay un "camino directo" por cada "camino en etapas".

Preguntas. ¿Puede una relación ser simétrica y antisimétrica? Si una relación es simétrica y transitiva, ¿es reflexiva?

Ejercicio 1.1. Uno puede definir una operación de "inversión" en el conjunto de relaciones $\mathcal{R} \subset \mathcal{A} \times \mathcal{A}$ donde $\mathcal{R}^{-1} := \{(b, a) : (a, b) \in \mathcal{R}\}$ (o sea permutar las

coordenadas de los elementos de la relación $\mathcal{R}$). ¿Qué tiene que satisfacer $\mathcal{R}$ para que $\mathcal{R}^{-1} = \mathcal{R}$?

Algunas combinaciones de las propiedades anteriores son importantes, y tienen una teoría rica de fondo, razón por la cual se les da un nombre.

Definición. Una relación $\mathcal{R} \subset \mathcal{A} \times \mathcal{A}$ se dice:

1. de *equivalencia* si es reflexiva, simétrica y transitiva.
2. de *orden* (u *orden parcial*) si es reflexiva, antisimétrica y transitiva.
3. de *orden total* si es una relación de orden parcial y además, dados $a, b \in \mathcal{A}$ vale que $a\mathcal{R}b$ ó $b\mathcal{R}a$ (o sea los elementos se pueden comparar dos a dos).

Un ejemplo a tener en mente son: si $\mathcal{A}$ es el conjunto de los números reales (o naturales, o racionales) entonces $=$ es una relación de equivalencia y $\leq$ es una relación de orden total.

Tomamos el conjunto $\mathcal{A} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ y definimos la relación $\mathcal{R}$ por $a\mathcal{R}b$ si a divide a b. Por ejemplo, $(2, 4) \in \mathcal{R}$, $(2, 10) \in \mathcal{R}$, $(2, 7) \notin \mathcal{R}$. Entonces $\mathcal{R}$ es una relación de orden. Pero no es de orden total ya que, por ejemplo, ni $2\mathcal{R}3$ ni $3\mathcal{R}2$.

Otro ejemplo: si miramos el conjunto de partes de un conjunto, y tomamos la relación dada por la inclusión (o sea $\mathcal{A}\mathcal{R}\mathcal{B}$ si $\mathcal{A} \subset \mathcal{B}$) obtenemos una relación de orden parcial. ¿Por qué no es total?

Las relaciones de equivalencia son muy importantes. Una relación $\sim$ de equivalencia en un conjunto $\mathcal{A}$ parte al conjunto en las llamadas *clases de equivalencia*. Veamos un ejemplo. Tomamos $\mathcal{A} = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ y $\sim \subset \mathcal{A} \times \mathcal{A}$ dada por $a \sim b$ si, al dividirlos por 3, a y b tienen el mismo resto. Por ejemplo, $1 \sim 4$ porque 1 dividido 3 es 0 y el resto es 1, y 4 dividido 3 es 1 y el resto es 1. También $1 \sim 7$ y $1 \sim 10$. El grafo de $\sim$ está en la Figura 5.

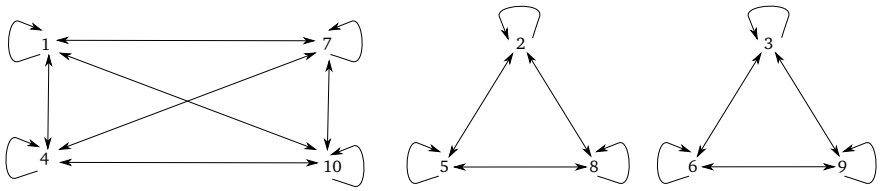


FIGURA 5. Grafo de la relación $\sim$

Si $a \in \mathcal{A}$, su clase de equivalencia es $\bar{a} = \{b \in \mathcal{A} : a \sim b\}$. Notar que $a \in \bar{a}$ por ser reflexiva. En el ejemplo de la Figura 5, $\overline{1} = \{1, 4, 7, 10\}$, $\overline{2} = \{2, 5, 8\}$, $\overline{3} = \{3, 6, 9\}$. Además, $\overline{1} = \overline{4} = \overline{7} = \overline{10}$, $\overline{2} = \overline{5} = \overline{8}$, $\overline{3} = \overline{6} = \overline{9}$.

Proposición 1.2. *Si $\mathcal{R}$ es una relación de equivalencia en $\mathcal{A} \times \mathcal{A}$, y $a, b \in \mathcal{A}$ entonces o bien $\bar{a} = \bar{b}$, o bien $\bar{a}$ y $\bar{b}$ son disjuntas.*

Demostración. Supongamos que no son disjuntas; entonces se puede tomar algún $c \in \bar{a} \cap \bar{b}$. Veamos que $\bar{a} \subset \bar{b}$. Si $d \in \bar{a}$, queremos probar que $d \in \bar{b}$. Para esto, sabemos que $a \sim d$, $a \sim c$ y $b \sim c$. Por simetría, sabemos que $c \sim a$. Entonces, por transitividad, como $b \sim c$, $c \sim a$ y $a \sim d$, tenemos que $b \sim d$. Esto prueba que $d \in \bar{b}$. Y como este razonamiento lo hicimos para cualquier $d \in \bar{a}$, hemos probado que $\bar{a} \subset \bar{b}$. Si hacemos el mismo razonamiento comenzando con elementos de $\bar{b}$, obtenemos la otra inclusión y la igualdad de ambos conjuntos. □

Luego si $\mathcal{A}$ es un conjunto y $\sim$ es una relación de equivalencia en $\mathcal{A}$, podemos considerar el *conjunto de clases de equivalencia*. Este es un nuevo conjunto, cuyos elementos son subconjuntos de $\mathcal{A}$. Como ejemplo, si tomamos el caso de la figura 5, el conjunto de clases de equivalencia es

$$\{\{1,4,7,10\},\{2,5,8\},\{3,6,9\}\},$$

que tiene tres elementos.

Ejercicios. 1. Decidir si las siguientes relaciones son de equivalencia y en caso de serlo, calcular el conjunto de clases.
   a) $\mathcal{A}$ es un conjunto cualquiera y $\mathcal{R} = \{(a,a) \ : \ a \in \mathcal{A}\}$.
   b) La relación de la figura 6.

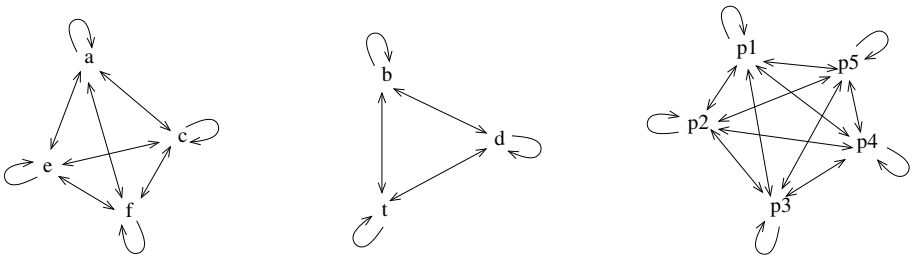


FIGURA 6

   c) $\mathcal{A} = \mathbb{N}$ y definimos $\mathcal{R}$ de la siguiente manera: si n, $m \in \mathbb{N}$, $n\mathcal{R}m$ si y solo si $n+m$ es par.
   d) En el conjunto de alumnos de la facultad definimos una relación diciendo que dos alumnos están relacionados si cursan una materia en común.
   e) ¿Qué pasa si en el ítem anterior ponemos como relación la condición de cursar exactamente las mismas materias?
2. Si $\mathcal{A} = \{1,2,3,4,5\}$ y $\mathcal{R}$ es una relación de equivalencia tal que las clases son $\{\{1,3\},\{2,5\},\{4\}\}$, graficar $\mathcal{R}$.
3. ¿Puede el conjunto $\{\{1,3\},\{2,5\},\{1,4\}\}$ ser el conjunto de clases para alguna relación de equivalencia en el conjunto $\mathcal{A}$ del ítem anterior?

1.3. Funciones. Otra familia importante de relaciones son las llamadas *funciones*. Dados dos conjuntos $\mathcal{A}, \mathcal{B}$, una función de $\mathcal{A}$ en $\mathcal{B}$ es una relación $f \subset \mathcal{A} \times \mathcal{B}$ con las siguientes dos propiedades:

- Para todo elemento $a \in \mathcal{A}$ existe un elemento $b \in \mathcal{B}$ tal que afb.
- Si $a \in \mathcal{A}$ es tal que existen b_1, $b_2 \in \mathcal{B}$ con afb_1 y afb_2 entonces $b_1 = b_2$ (o sea el elemento del ítem anterior es único).

En general notaremos por $f(a)$ al único $b \in \mathcal{B}$ tal que afb, y notamos $f : \mathcal{A} \to \mathcal{B}$ a una función del conjunto $\mathcal{A}$ en el conjunto $\mathcal{B}$.

Observación. Si $\mathcal{A}$ y $\mathcal{B}$ son finitos, una función $f : \mathcal{A} \to \mathcal{B}$ se puede dar mediante un diagrama, lo que evita tener que listar toda la relación.

Ejemplos. Determinar si son funciones las siguientes relaciones:

1. La relación de la figura 7.
2. $F \subset \mathbb{N} \times \mathbb{N}$, $F = \{(n, n+1) \ : \ n \in \mathbb{N}\}$.
3. $F \subset \mathbb{N} \times \mathbb{N}$, $F = \{(n, n-1) \ : \ n \in \mathbb{N}\}$.

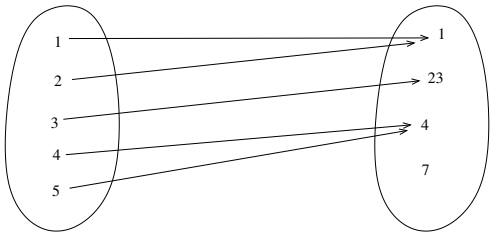


FIGURA 7

4. $F \subset \mathbb{N} \times \mathbb{Z}$, $F = \{(n, m) \ : \ n = m^2\}$.
5. $F \subset \mathbb{N} \times \mathbb{Z}$, $F = \{(n, m) \ : \ m = n^2\}$.
6. ¿Cuándo $\mathcal{R} \subset \mathcal{A} \times \mathcal{A}$ es una función?
7. En un equipo de fútbol ¿es una función la relación en el conjunto

$$\{\text{jugadores del equipo}\} \times \{\text{camisetas numeradas}\}$$

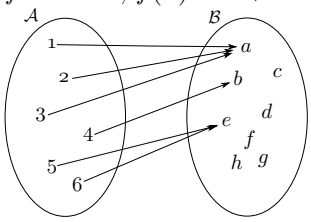
dada por $(\text{jugador}, \text{número de camiseta})$?

Si $f : \mathcal{A} \to \mathcal{B}$ es una función, llamamos *dominio* de f al conjunto $\mathcal{A}$ y *codominio* de f al conjunto $\mathcal{B}$. Esto nos permite hablar de una función f sin tener que estar especificando constantemente qué conjuntos están involucrados en su definición.

Definición. Si $f : \mathcal{A} \to \mathcal{B}$, definimos la *imagen* de f como el subconjunto de $\mathcal{B}$ dado por $\text{Im}(f) = \{b \in \mathcal{B} \ : \ \text{existe } a \in \mathcal{A} \text{ con } f(a) = b\}$.

En términos del diagrama de la función, la imagen es el conjunto de elementos a los que les llega (al menos) una flecha.

Ejercicios. Encontrar la imagen de las siguientes funciones:

1. $f : \mathbb{N} \to \mathbb{N}$, $f(n) = n + 1$.
2. $f : \mathbb{Z} \to \mathbb{Z}$, $f(n) = n + 1$.
3. 

4. $f : \mathbb{Z} \to \mathbb{N}$, $f(n) = |n|$.
5. $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$.

Algunas propiedades importantes que pueden satisfacer las funciones son:

- Una función f es *inyectiva* si satisface la siguiente propiedad: si $f(a) = f(b)$ entonces $a = b$. Equivalentemente, para que f sea inyectiva, dos elementos distintos deben tener imágenes distintas.
- Una función f es *suryectiva* o *sobreyectiva* si para todo $b \in \mathcal{B}$, existe $a \in \mathcal{A}$ tal que $f(a) = b$. Equivalentemente, para que f sea suryectiva, debe ser $\mathcal{B} = \text{Im}(f)$ (o sea, el codominio debe ser igual a la imagen).
- Una función f es *biyectiva* si es inyectiva y suryectiva.

Ejercicios. Determinar si cada una de las funciones del ejercicio anterior es inyectiva, suryectiva o biyectiva.

Como en el caso anterior, si $\mathcal{R}$ es una relación en $\mathcal{A} \times \mathcal{B}$, definimos su "inversa" como $\mathcal{R}^{-1} \subset \mathcal{B} \times \mathcal{A}$ como $\mathcal{R}^{-1} := \{(b, a) : (a, b) \in \mathcal{R}\}$. Si $f : \mathcal{A} \to \mathcal{B}$ es una función, que propiedades debe satisfacer para que la relación f^{-1} sea una función?

Respuesta: es preciso que f se biyectiva.

Definición. Si $f : \mathcal{A} \to \mathcal{B}$ es una función biyectiva, llamamos *función inversa* de f a la función f^{-1}.

1.3.1. Composición de Funciones. Cuando trabajamos con conjuntos, definimos algunas operaciones entre conjuntos. Nos gustaría poder definir algunas operaciones entre funciones. El problema es que no se pueden operar funciones cualesquiera. Por ejemplo, pudimos definir la operación *inversa* en el subconjunto de las funciones biyectivas (no en todo el conjunto de las funciones).

Supongamos que tenemos tres conjuntos $\mathcal{A}, \mathcal{B}, \mathcal{C}$, y dos funciones $f : \mathcal{A} \to \mathcal{B}$ y $g : \mathcal{B} \to \mathcal{C}$. Definimos la *composición* de g con f (y notamos $g \circ f$) como la función $g \circ f : \mathcal{A} \to \mathcal{C}$ dada por $(g \circ f)(a) = g(f(a))$ (ver la ilustración en la figura 8).

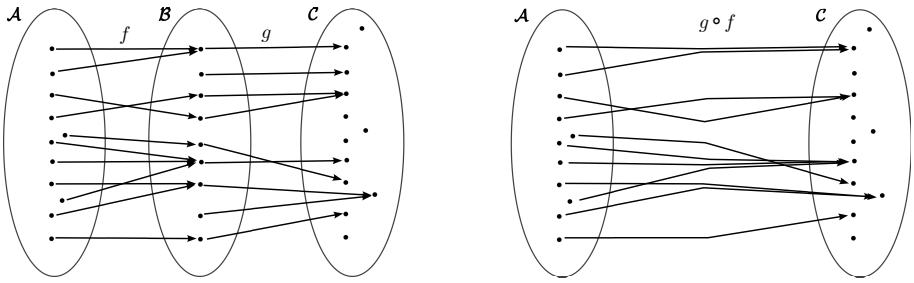


FIGURA 8. Composición de dos funciones $g \circ f$

Pregunta: Supongamos que $f : \mathcal{A} \to \mathcal{B}$ y $g : \mathcal{C} \to \mathcal{D}$. ¿Que condición hay que pedirle a f y g para poder componer g con f?

Respuesta: Si queremos definir $g \circ f(a) := g(f(a))$, entonces precisamos que $f(a) \in \mathcal{C}$. Luego la condición necesaria y suficiente para poder componer g con f es que $\mathrm{Im}(f) \subset \mathcal{C}$, o sea que la imagen de f esté contenida en el dominio de g.

Notar que la composición de funciones es una operación binaria de $\{f : \mathcal{A} \to \mathcal{B}\} \times \{g : \mathcal{B} \to \mathcal{C}\}$ en $\{h : \mathcal{A} \to \mathcal{C}\}$.

Ejemplos.

1. Consideremos las funciones $f : \mathbb{Z} \to \mathbb{Z}$, $g : \mathbb{Z} \to \mathbb{Z}$ dada por $f(n) = |n|$ y $g(n) = n^2$. Calcular $g \circ f$ y $f \circ g$.
2. Consideremos $f : \mathbb{N} \cup \{0\} \to \mathbb{Z}$ y $g : \mathbb{Z} \to \mathbb{N} \cup \{0\}$ dadas por

$$f(n) = \begin{cases} n/2 & \text{si } n \text{ es par} \\ -\frac{(n+1)}{2} & \text{si } n \text{ es impar} \end{cases}$$

y

$$g(n) = \begin{cases} 2n & \text{si } n \geq 0 \\ -2n - 1 & \text{si } n < 0. \end{cases}$$

Calcular $f \circ g$. ¿Qué se puede deducir de f y de g?

3. Dado $\mathcal{A}$ un conjunto cualquiera, consideremos la función *identidad*, $\mathrm{id}_{\mathcal{A}} : \mathcal{A} \to \mathcal{A}$ dada por $\mathrm{id}_{\mathcal{A}}(a) = a$. Probar que $\mathrm{id}_{\mathcal{A}}$ es el neutro para la composición en $\{f : \mathcal{A} \to \mathcal{A}\}$, o sea $\mathrm{id}_{\mathcal{A}} \circ f = f \circ \mathrm{id}_{\mathcal{A}} = f$.

Proposición 1.3. *Si $f : \mathcal{A} \to \mathcal{B}$ es una función biyectiva, entonces existe una única función $g : \mathcal{B} \to \mathcal{A}$ tal que $f \circ g = \mathrm{id}_{\mathcal{B}}$ y $g \circ f = \mathrm{id}_{\mathcal{A}}$.*

A dicha función g la llamamos la *inversa de* f y la notamos f^{-1}.

Dem: Como f es biyectiva, ya vimos que podemos definir la relación inversa f^{-1} y esta relación resulta ser una función también. Veamos que f^{-1} satisface las dos condiciones, y que es la única función que lo hace.

Si $b \in \mathcal{B}$, $f^{-1}(b)$ por definición es el único elemento $a \in \mathcal{A}$ tal que $f(a) = b$. Luego $(f \circ f^{-1})(b) = f(a) = b$ y se sigue que $f \circ f^{-1} = \mathrm{id}_{\mathcal{B}}$. Similarmente, $(f^{-1} \circ f)(a) = f^{-1}(f(a))$ que es el único elemento $\tilde{a} \in \mathcal{A}$ tal que $f(\tilde{a}) = f(a)$. Pero el único tal elemento es $\tilde{a} = a$, con lo cual $(f^{-1} \circ f)(a) = a$ y se sigue que $f^{-1} \circ f = \mathrm{id}_{\mathcal{A}}$.

Veamos la unicidad de g. Supongamos que tenemos dos funciones $g, h : \mathcal{B} \to \mathcal{A}$ tales que $f \circ g = f \circ h = \mathrm{id}_{\mathcal{B}}$ y $g \circ f = h \circ f = \mathrm{id}_{\mathcal{A}}$. Dado $b \in \mathcal{B}$, como f es biyectiva, existe un único $a \in \mathcal{A}$ tal que $f(a) = b$. Luego $g(b) = g(f(a)) = a = h(f(a)) = h(b)$ con lo cual $h = g$ pues toman el mismo valor en todos los elementos de $\mathcal{B}$. □

Ejercicio 1.2. Probar que si $f : \mathcal{A} \to \mathcal{B}$ tiene una función inversa, o sea existe una única $g : \mathcal{B} \to \mathcal{A}$ tal que $f \circ g = \mathrm{id}_{\mathcal{B}}$ y $g \circ f = \mathrm{id}_{\mathcal{A}}$ entonces f es biyectiva.

Preguntas: Supongamos que $\mathcal{A}$ y $\mathcal{B}$ son dos conjuntos finitos. Si $f : \mathcal{A} \to \mathcal{B}$ es una función cualquiera, ¿se puede dar alguna relación entre $|\mathcal{A}|$ y $|\mathcal{B}|$? ¿y si f es inyectiva? ¿y si f es suryectiva? ¿y si f es biyectiva? Ya discutiremos las respuestas en la parte de combinatoria.

2. Inducción

Comencemos viendo el siguiente ejercicio:

Ejercicio 2.1. Calculemos la suma de los 5 primeros números naturales, ¿cuánto da? Calculemos ahora la suma de los primeros 6 números naturales. ¿Cuánto da? Miremos ahora la función $f : \mathbb{N} \to \mathbb{N}$, dada por $f(n) = \frac{n(n+1)}{2}$. ¿Cuánto vale en 5? ¿Y en 6? ¿Qué podemos "conjeturar"? Verificar que esta conjetura es cierta para $n = 7, 8, 9$.

Ahora bien, tenemos una afirmación que suponemos cierta (porque lo es en algunos ejemplos calculados) y nos gustaría poder saber si la fórmula vale en general o no. ¡No podemos chequear para cada número natural que la fórmula es cierta! Estamos tratando de demostrar una afirmación para cada número natural (que la suma de los números de 1 hasta n es $\frac{n(n+1)}{2}$). Pero ¿que son los números naturales? Tenemos una noción intuitiva de ellos, pero para poder probar algo sobre los naturales necesitamos una definición formal.

A principios del siglo XX, Peano dio la siguiente definición axiomática de los números naturales:

Definición. El conjunto de números naturales es un conjunto que posee una función "sucesor" que satisfacen los siguientes cinco axiomas:

1. El 1 es un número natural.
2. Todo número natural tiene un sucesor.
3. El 1 no es sucesor de nadie.
4. La función sucesor es inyectiva. Es decir, si $a \neq b$ son números naturales, el sucesor de a es distinto del sucesor de b.
5. Si S es un conjunto cualquiera tal que $1 \in S$ y vale que el sucesor de cualquier elemento de S también está en S, entonces $\mathbb{N} \subset S$.

El último axioma es de una naturaleza distinta a los otros. Puede parecer superfluo, pero si no lo agregamos estaremos considerando conjuntos que no se comportan como los naturales. Por ejemplo, el conjunto $\mathbb{N} \cup \{\mathbb{Z} + 1/2\}$ satisface los primeros cuatro axiomas pero no el quinto.

La ventaja de tener una definición axiomática de los números naturales es que nos permite demostrar algunas propiedades sobre tal conjunto. El caso más importante es el *principio de inducción*.

Teorema 2.1 (Principio de Inducción)**.** *Supongamos que tenemos una afirmación $P(n)$ para cada número natural n y queremos probar que la afirmación es cierta para todo $n \in \mathbb{N}$. Si logramos probar que*

- *(primer caso) $P(1)$ es cierta,*
- *(paso inductivo) si $P(n)$ es cierta entonces $P(n+1)$ también lo es,*

entonces la afirmación vale para todo $n \in \mathbb{N}$.

El principio de inducción es como tener una hilera de piezas de dominó, una parada detrás de la otra, a una distancia tal que cada pieza, si cae, tira a la siguiente. Si tramos la primera pieza, podemos asegurar que todas las piezas caerán.

El principio de inducción es una consecuencia de los axiomas de Peano. Antes de ver la demostración, veamos cómo funciona el principio para el ejemplo con el que comenzamos.

Ejemplo. Para todo $n \in \mathbb{N}$ vale que $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.
Demostración: Para $n \in \mathbb{N}$ llamemos $P(n)$ a la afirmación anterior. Debemos probar el primer caso, $P(1)$, y el paso inductivo, $P(n) \Rightarrow P(n+1)$.

- $P(1)$ es cierta, ya que $1 = \frac{1 \cdot 2}{2}$.
- Supongamos que $P(n)$ es cierta (o sea, supongamos que $1 + \cdots + n = \frac{n(n+1)}{2}$, esto se llama la *hipótesis inductiva*) y probemos que $1 + \cdots + (n+1) = \frac{(n+1)(n+2)}{2}$. Como $P(n)$ es cierta (por hipótesis inductiva),

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

que es lo que queríamos probar.

Ahora sí, veamos por qué el principio de inducción funciona. Llamemos $\mathcal{P}$ al conjunto donde vale la propiedad P. Es decir, $\mathcal{P} = \{n \in \mathbb{N} : P(n) \text{ es cierta}\}$. Queremos ver que $\mathcal{P} = \mathbb{N}$. Para probar esto, alcanza con ver que $\mathcal{P}$ satisface el último axioma de Peano. Es decir, debemos ver que $1 \in \mathcal{P}$ y que si $n \in \mathcal{P}$ entonces $n + 1 \in \mathcal{P}$. Pero esto es justamente lo que dice el principio de inducción.

Ejemplo. ¿Cuánto vale la suma $f(n) = \sum_{i=0}^{n} 2^i$? Calculemos los primeros términos de esta sucesión: $f(1) = 3$, $f(2) = 7$, $f(3) = 15$. ¿Qué pasa si le sumamos 1 a esta sucesión? Obtenemos $4, 8, 16$. Estos números son conocidos: son potencias de 2. Es

decir, $f(1) = 2^2 - 1$, $f(2) = 2^3 - 1$, $f(3) = 2^4 - 1$. Probemos por inducción que $f(n) = 2^{n+1} - 1$. Es claro que para $n = 1$ la fórmula vale; de hecho, ya lo vimos. Veamos que, si es cierta para n, entonces es cierta para $n + 1$.

$$\sum_{i=0}^{n+1} 2^i = \sum_{i=0}^{n} 2^i + 2^{n+1} \underset{\text{H.I.}}{=} 2^{n+1} - 1 + 2^{n+1} = 2 \cdot 2^{n+1} - 1 = 2^{n+2} - 1$$

como queríamos ver.

La sigla "H.I." significa "hipótesis inductiva". Se suele utilizar para indicar que, precisamente en ese paso, hemos usado que la afirmación $P(n)$ es cierta.

Ejemplo. Probar que $2n^3 + n + 31 \geq 3n^2$ para todo $n \geq -2$.

Este ejercicio nos plantea probar una proposición que no es cierta sólo para el conjunto de números naturales, sino para todos los números enteros mayores o iguales que -2. ¿Cómo podemos probar esto? Una manera fácil (aunque no muy útil en general) es aplicar el principio de inducción para el conjunto de números naturales, y después probar que la fórmula es cierta para $n = -2, -1$ y 0. La desventaja de este método es que si queremos probar una afirmación para los enteros mayores o iguales que -10.000, tenemos que verificar a mano 10.001 casos. ¿Será cierto que podemos usar el mismo proceso de inducción, verificando que el primer caso a considerar es cierto y que si la afirmación es cierta para un número entonces también lo es para el siguiente?

La respuesta es "sí", y es bastante intuitivo que éste es el caso (si uno piensa en el dominó, realmente no importa cómo llamamos a la primera pieza). Si tenemos una afirmación $P(n)$ de la cual queremos probar su veracidad en un conjunto $\mathcal{P} = \{n \in \mathbb{Z} : n \geq n_0\}$ para algún n_0 entero, lo que podemos hacer es el cambio de variables $m = n + 1 - n_0$. Entonces $n \geq n_0 \iff m \geq 1$. Entonces podemos probar la afirmación $P(m)$ para $m \geq 1$, y esto se puede hacer usando inducción. En el ejemplo anterior, $m = n + 1 - (-2) = n + 3$, o $n = m - 3$, por lo que $P(m)$ es la afirmación $2(m-3)^3 + (m-3) + 31 \geq 3(m-3)^2$. Podemos probar que esto es verdadero por inducción para $m \geq 1$. Pero también podemos simplemente adaptar el principio de inducción a conjuntos como el mencionado, $\mathcal{P} = \{n \in \mathbb{Z} : n \geq n_0\}$.

Para ilustrar, resolvamos el ejercicio:

- $P(-2)$ es cierta, ya que $2 \cdot (-8) + (-2) + 31 = 13 \geq 3 \cdot 4 = 12$.
- Supongamos que $P(n)$ es cierta y veamos que $P(n+1)$ también lo es.

$$\begin{aligned} 2(n+1)^3 + (n+1) + 31 &= 2n^3 + n + 31 + 6n^2 + 6n + 2 + 1 \\ &\underset{\text{H.I.}}{\geq} 3n^2 + 6n^2 + 6n + 3 = 3(n+1)^2 + 6n^2 \geq 3(n+1)^2 \end{aligned}$$

Lo que acabamos de hacer es usar lo que muchas veces se llama *principio de inducción corrida*. Enunciemos este principio, cuya demostración no es otra cosa que el cambio de variables que mencionamos.

Teorema 2.2 (Principio de inducción corrida)**.** *Sea n_0 un número entero y supongamos que tenemos una afirmación $P(n)$ para cada número entero $n \geq n_0$. Si queremos probar que $P(n)$ es cierta para todo $n \geq n_0$, y logramos probar que*

- *(primer caso) $P(n_0)$ es cierta,*
- *(paso inductivo) para todo $n \geq n_0$ vale que si $P(n)$ es cierta entonces $P(n+1)$ también lo es,*

entonces la afirmación vale para todo $n \geq n_0$.

Ejemplo. Consideremos la siguiente afirmación: *Si en un conjunto de alumnos de Álgebra I, un alumno está anotado en la Licenciatura en Matemática, todos lo están.*

Veamos la demostración: la vamos a hacer por inducción en el número de alumnos. Esto es, probaremos que si n es un número natural, hay n alumnos en Álgebra I y uno está anotado en Matemática, todos lo están. El primer caso es $n = 1$, es decir, el conjunto es de un solo alumno. Es claro que si tenemos un conjunto con un solo alumno, y es alumno de la Licenciatura en Matemáticas, entonces todos lo son.

Supongamos ahora que tenemos un conjunto de $n + 1$ alumnos y que al menos uno de ellos hace Matemática. Tomemos de los $n + 1$ alumnos un subconjunto (cualquiera) de n de ellos, con la condición de que tenga al alumno de Matemática. Luego, por hipótesis inductiva, esos n alumnos hacen la Licenciatura en Matemática. Ya hemos probado que todos salvo quizás un alumno están en la Licenciatura en Matemática. Saquemos de nuestro conjunto de n alumnos a uno de ellos, y agreguemos al alumno que nos quedó sin incluir en la hipótesis inductiva. Nuevamente tenemos un conjunto de n alumnos, con uno de ellos que hace Matemática, con lo cual el alumno no considerado en el paso inductivo anterior también debe hacer la Licenciatura en Matemática. ¿Qué está mal en esta demostración?

Ejercicio 2.2. Si r es un número natural cualquiera, probar que para todo $n \in \mathbb{N}$ vale que $1^r + \cdots + n^r \geq \int_0^n x^r dx$.

Hay otros dos principios "equivalentes" al principio de inducción. Uno de ellos es el *Principio de inducción completa o global*, que dice:

Teorema 2.3 (Principio de inducción completa (o global))**.** *Dada una afirmación $P(n)$, $n \in \mathbb{N}$, supongamos que*

1. *$P(1)$ es verdadera, y*
2. *si $P(k)$ es cierta para todo $1 \leq k \leq n$ entonces $P(n+1)$ es cierta.*

Entonces la afirmación es cierta para todo $n \in \mathbb{N}$.

Notar que la diferencia con el principio de inducción es que para demostrar $P(n + 1)$ no solo se puede usar $P(n)$ sino también todos los anteriores. El otro principio es el llamado *Principio de Buena Ordenación*, que dice:

Teorema 2.4 (Principio de Buena Ordenación)**.** *Todo subconjunto no vacío del conjunto de números naturales tiene un primer elemento.*

Veamos la equivalencia de estos principios:

- Veamos que el Principio de Inducción implica el Principio de Inducción Global. Supongamos que para todo natural n, $P(1) \wedge P(2) \wedge \cdots \wedge P(n) \Rightarrow P(n+1)$. Llamemos Q a la propiedad $Q(n) = P(1) \wedge P(2) \wedge \cdots \wedge P(n)$. Entonces, si vale $Q(n)$, valen $P(1)$, $P(2)$, $\ldots P(n)$, y por lo tanto vale $P(n + 1)$, por lo que vale $Q(n+1)$. El Principio de Inducción dice que $Q(n)$ es verdadera para todo $n \in \mathbb{N}$. Esto dice que $P(n)$ es verdadera para todo $n \in \mathbb{N}$. Esto es, vale el Principio de Inducción Global.

- Veamos ahora que el Principio de Inducción Global implica el Principio de Buena Ordenación. Sea $\mathcal{P} \subseteq \mathbb{N}$ y supongamos que $\mathcal{P}$ no tiene primer elemento. Queremos probar que entonces $\mathcal{P}$ es vacío. Para esto, consideramos la afirmación $P(n) : n \notin \mathcal{P}$. Nuestro objetivo es probar que $P(n)$ es cierta para todo $n \in \mathbb{N}$, porque en ese caso $\mathcal{P}$ es vacío. Para esto, usamos inducción global.
  - Si fuese $1 \in \mathcal{P}$ entonces $\mathcal{P}$ tendría un primer elemento y tendríamos una contradicción. Por lo tanto $1 \notin \mathcal{P}$ y $P(1)$ es verdadera.
  - Supongamos que $P(1), \ldots, P(n)$ son verdaderas. Esto es, $1 \notin \mathcal{P}$, $2 \notin \mathcal{P}$,$\ldots n \notin \mathcal{P}$. Si fuese falsa $P(n+1)$ tendríamos $n+1 \in \mathcal{P}$ y $\mathcal{P}$ tendría un primer elemento, $n+1$, lo que sería una contradicción. Luego, $n+1 \notin \mathcal{P}$ y $P(n+1)$ es verdadera.

  Hemos entonces probado que $P(n)$ es verdadera $\forall n \in \mathbb{N}$ y por lo tanto $\mathcal{P}$ es vacío.
- Veamos por último que el Principio de Buena Ordenación implica el Principio de Inducción. Si tenemos las afirmaciones $P(n)$ con $n \in \mathbb{N}$, supongamos que $P(1)$ es verdadera y que $P(n) \Rightarrow P(n+1)$ para todo $n \in \mathbb{N}$. Queremos ver que $P(n)$ es verdadera $\forall n \in \mathbb{N}$. Consideremos el conjunto $\mathcal{P} = \{n \in \mathbb{N} : P(n) \text{ es falsa}\}$. Por el Principio de Buena Ordenación, si $\mathcal{P}$ no es vacío, entonces tiene un primer elemento. Llamémoslo N. No puede ser $N = 1$ porque sabemos que $P(1)$ es verdera, por lo que $1 \notin \mathcal{P}$. Entonces $N-1$ es natural y $N-1 \notin \mathcal{P}$; es decir $P(N-1)$ es verdadera. Pero entonces $P(N)$ es verdadera, por lo que $N \in \mathcal{P}$. Hemos llegado a una contradicción, que provino de suponer que $\mathcal{P}$ es no vacío. Luego, $\mathcal{P}$ es vacío y $P(n)$ es verdadera $\forall n \in \mathbb{N}$.

Ejemplo. Tomemos la función $f : \mathbb{N} \to \mathbb{N}$ dada por:

$$f(n) = \begin{cases} n/2 & \text{si } n \text{ es par,} \\ n+1 & \text{si } n \text{ es impar.} \end{cases}$$

Si $m \in \mathbb{N}$, vamos a llamar f^m a la composición $f^m = \underbrace{(f \circ \cdots \circ f)}_{m \text{ veces}}$. Veamos que, para todo $n \in \mathbb{N}$, existe un m tal que $f^m(n) = 1$.

Demostración. Hacemos inducción global en n.

- Si $n = 1$, $f(1) = 2$, y $f(2) = 1$ con lo cual $(f \circ f)(1) = 1$ o sea podemos tomar $m = 2$.
- Supongamos que la afirmación vale para $1 \leq k \leq n$ y veamos que vale para $n+1$. Para poder calcular $f(n+1)$ tenemos que separar en casos según la paridad de n.
  - Si n es impar, $n+1$ es par con lo cual $f(n+1) = \frac{n+1}{2}$. Como $\frac{n+1}{2} \leq n$ para todo $n \in \mathbb{N}$, podemos aplicar la Hipótesis Inductiva a $k = \frac{n+1}{2}$. Existe entonces $m \in \mathbb{N}$ tal que $f^m\left(\frac{n+1}{2}\right) = 1$, con lo cual $f^{m+1}(n+1) = 1$.
  - Si n es par, $n+1$ es impar, con lo cual $f(n+1) = n+2$ y $f^2(n+1) = f(n+2) = \frac{n+2}{2} = \frac{n}{2} + 1$. Pero si $n \geq 2$ (que es el caso por ser n par), $\frac{n}{2} + 1 \leq n$, con lo cual podemos aplicar la Hipótesis Inductiva a $\frac{n}{2} + 1$. Luego existe $m \in \mathbb{N}$ tal que $1 = f^m\left(\frac{n}{2} + 1\right) = f^{m+2}(n+1)$.

□

Problema abierto: Consideremos una modificación de la función anterior, y definamos $g : \mathbb{N} \to \mathbb{N}$ dada por:

$$g(n) = \begin{cases} n/2 & \text{si } n \text{ es par,} \\ 3n+1 & \text{si } n \text{ es impar.} \end{cases}$$

¿Es cierto que para todo $n \in \mathbb{N}$ existe un $m \in \mathbb{N}$ tal que $f^m(n) = 1$? Este problema es conocido como *Problema de Collatz*, y la respuesta no se conoce. Se "conjetura" que la respuesta es "sí", pero no hay una demostración. Numéricamente, está probado que es cierto para $n \leq 5 \cdot 10^{18}$.

Ejemplo. Todo subconjunto acotado T de los naturales tiene un máximo elemento. Para probarlo, llamemos $\mathcal{P} = \{n \in \mathbb{N} \ : \ t \leq n \, \forall t \in T\}$. Como T es acotado, sabemos que el conjunto $\mathcal{P}$ es no vacío, con lo cual tiene un primer elemento. Queda como ejercicio para el lector verificar que este primer elemento pertenece al conjunto T (y por lo tanto es un máximo).

2.1. Inducción como herramienta para construir sucesiones. Hasta ahora usamos el principio de inducción como herramienta para probar afirmaciones. Este es un uso "pasivo" de la inducción. Pero el principio de inducción tiene también un lado constructivo. Recordemos la definición de sucesiones:

Definición. Una *sucesión* (en el conjunto $\mathcal{A}$) es una función $f : \mathbb{N} \to \mathcal{A}$.

En general tomaremos como conjunto $\mathcal{A}$ el cuerpo de números reales. Si $f : \mathbb{N} \to \mathcal{A}$ es una sucesión, vamos a escribir a_n en lugar de $f(n)$, y a la función f la escribiremos $(a_n)_{n\in\mathbb{N}}$. Hasta aquí hemos visto cómo definir sucesiones de manera "explícita", o sea diciendo cuánto vale la función en cada número natural (por ejemplo $a_n = n^2$).

Una manera alternativa de definir una función es darla de manera *recursiva*. Esto es, se definen algunos valores (iniciales) de la función y se da una fórmula para calcular el resto de los valores a partir de los ya conocidos. Por ejemplo, definimos la función $f : \mathbb{N} \to \mathbb{N}$ dada por $f(1) = 1$ y $f(n) = n \cdot f(n-1)$. Luego el valor $f(3) = 3 \cdot f(2) = 3 \cdot 2 \cdot f(1) = 3 \cdot 2 \cdot 1 = 6$. Veremos más adelante que para todo $n \in \mathbb{N}$, $f(n) = n! = \prod_{i=1}^{n} i$.

Las sucesiones cuyos valores dependen de valores ya conocidos se llaman *sucesiones recursivas* o *sucesiones por recurrencia*. Las preguntas que uno se hace sobre ellas, y que debemos contestar, son: ¿están bien definidas? O sea, ¿esto que definimos es realmente una función? Y por otro lado, ¿se pueden definir de manera explícita?

Antes de avanzar con estas preguntas, veamos otro ejemplo. Definimos $a : \mathbb{N} \to \mathbb{Z}$ de la siguiente manera:

$$a_1 = 2, \quad a_2 = 4, \quad a_3 = 14, \quad a_{n+1} = 10a_n - 31a_{n-1} + 30a_{n-2} \text{ si } n \geq 3.$$

Se puede ver que el valor de a_4 depende del de a_3, a_2 y a_1, que están definidos. Una vez que está calculado a_4, con ese valor y el de a_3 y a_2 calculamos a_5, etc. Podemos calcular los primeros valores de a:

$$a_1 = 2, \ a_2 = 4, \ a_3 = 14, \ a_4 = 76, \ a_5 = 446,$$
$$a_6 = 2524, \ a_7 = 13694, \ a_8 = 72076, \ a_9 = 371966.$$

Sin embargo, estos números no dicen mucho. Si con estos valores queremos calcular a_{10} será sencillo. En cambio, si queremos calcular a_{100}, deberemos calcular todos los

números a_i con $i \leq 99$. Esto no es muy cómodo. Lo que nos convendría en ese caso es contar con una *fórmula cerrada*. Esto es, una fórmula en la que a_n no dependa de los anteriores sino solo de n.

Supongamos por un momento que nos dicen que para todo $n \in \mathbb{N}$, $a_n = 2^{n+1} - 3^n + 5^{n-1}$. Si esto es cierto, tendremos una fórmula cerrada para a_n. Podemos intentar ver si coinciden algunos valores. Llamemos $b_n = 2^{n+1} - 3^n + 5^{n-1}$. Queremos entonces ver si $a_n = b_n$, y calculamos b_1: $b_1 = 2^2 - 3^1 + 5^0 = 4 - 3 + 1 = 2$, es decir que $b_1 = a_1$. Podemos hacer lo mismo con b_2 y b_3: $b_2 = 2^3 - 3^2 + 5^1 = 8 - 9 + 5 = 4$, $b_3 = 2^4 - 3^3 + 5^2 = 16 - 27 + 25 = 14$, es decir que también coinciden. Tenemos entonces la sospecha de que efectivamente $a_n = b_n$ para todos los $n \in \mathbb{N}$. Pero solo vimos tres casos. Para probarlo en general, debemos usar inducción global.

- El primer paso, con $n = 1$, ya lo vimos.
- Supongamos entonces que $a_k = b_k$ para $k \leq n$ y veamos que es cierto para $k = n + 1$. Si $n + 1 = 2$ ó $n + 1 = 3$ (es decir, si $n = 1$ ó $n = 2$), ya vimos que $a_{n+1} = b_{n+1}$. Podemos entonces suponer que $n \geq 3$, lo que nos permite usar la definición recursiva de a:

$$\begin{aligned} a_{n+1} &= 10a_n - 31a_{n-1} + 30a_{n-2} \\ &\underset{\text{H.I.}}{=} 10(2^{n+1} - 3^n + 5^{n-1}) - 31(2^n - 3^{n-1} + 5^{n-2}) \\ &\qquad + 30(2^{n-1} - 3^{n-2} + 5^{n-3}) \\ &= 2^{n-1}(10 \cdot 4 - 31 \cdot 2 + 30 \cdot 1) - 3^{n-2}(10 \cdot 9 - 31 \cdot 3 + 30 \cdot 1) \\ &\qquad + 5^{n-3}(10 \cdot 25 - 31 \cdot 5 + 30 \cdot 1) \\ &= 2^{n-1} \cdot 8 - 3^{n-2} \cdot 27 + 5^{n-3} \cdot 125 \\ &= 2^{n+2} - 3^{n+1} + 5^n = b_{n+1} \end{aligned}$$

No es cierto que toda sucesión recursiva tenga una fórmula cerrada, pero en la mayoría de los ejemplos que consideraremos ese será el caso. Por otra parte, aun cuando una sucesión definida de manera recursiva tenga una fórmula cerrada, no siempre será sencillo hallarla. En el ejemplo anterior la fórmula cerrada nos fue dada. Más adelante veremos métodos que pueden ser útiles para calcular una fórmula cerrada de una función recursiva.

Concentrémonos ahora en el otro problema. ¿Está bien definida una función recursiva? Veamos que una sucesión recursiva que dependa de r términos anteriores está bien definida.

Proposición 2.5. *Dado $\mathcal{A}$ un conjunto cualquiera, una r-upla $(a_1, \ldots, a_r)$ de elementos de $\mathcal{A}$ y una función*

$$G : \mathbb{N} \times \underbrace{\mathcal{A} \times \cdots \times \mathcal{A}}_{r \text{ veces}} \to \mathcal{A},$$

existe una única función $f : \mathbb{N} \to \mathcal{A}$ tal que $f(i) = a_i$ para $1 \leq i \leq r$ y tal que $f(n) = G(n, f(n-1), \ldots, f(n-r))$.

En el ejemplo anterior, el conjunto $\mathcal{A}$ era el de los enteros y la función G era $G(n, x, y, z) = 10x - 31y + 30z$. De hecho, si reemplazamos x, y, z por a_{n-1}, a_{n-2} y a_{n-3}, obtenemos la definición recursiva de a.

Probemos entonces la proposición.

Demostración. Veamos que existe una función f definida en todos los números naturales que satisface la propiedad enunciada. Llamemos

$$\mathcal{P} = \{n \in \mathbb{N} \ : \ f \text{ está definida en } n\}.$$

Queremos ver que $\mathcal{P} = \mathbb{N}$. Lo probaremos por inducción global.

- Para $i \leq r$, hemos definido $f(i) = a_i$. Esto dice que $1, 2, \ldots, r \in \mathcal{P}$.
- Por H.I., f está definida para todos los números $1, 2, \ldots, k$ (con $k < n$). Por otra parte, podemos usar que $n > r$ porque el caso $n \leq r$ ya lo vimos. Pero entonces $f(n) = G(n, f(n-1), \ldots, f(n-r))$, por lo que f está definida en n y luego $n \in \mathcal{P}$.

La unicidad se ve de manera similar: si f, g son dos funciones que satisfacen las hipótesis, queremos ver que toman los mismos valores. Es claro para los primeros r números. Supongamos que $f(i) = g(i)$ para $1 \leq k < n$, entonces

$$f(n) = G(n, f(n-1), \ldots, f(n-r)) = G(n, g(n-1), \ldots, g(n-r) = g(n).$$

□

Dar una sucesión de manera recursiva tiene sus ventajas y sus desventajas. En algunos ejemplos es más rápido calcular el valor de la función en n de manera recursiva que de manera explícita (por ejemplo $n!$) mientras que en otros ejemplos es lo contrario (por ejemplo $f(n) = n(n+1)/2 = n + f(n-1)$). En muchas casos la fórmula recursiva permite probar ciertas propiedades de la sucesión que no se ven tan claramente en una fórmula explícita. Por eso es bueno tener las dos definiciones.

Consideremos el siguiente problema (llamado el problema de Torres de Hanoi e inventado por Edouard Lucas en 1883): Supongamos que tenemos tres postes, y un número N de discos de distinto tamaño. Comenzamos con todos los discos en el poste de la izquierda, ordenados por tamaño, con el más grande abajo. Queremos mover los discos al poste de la derecha. En cada movimiento se puede llevar el disco que está más arriba en un poste a otro poste, ubicándolo encima de los discos que estén ahí. La regla principal es que sobre un disco no puede haber otro mayor.

Si tenemos dos discos, movemos el superior al medio, el inferior a la derecha y el del medio a la derecha para transferir todo. Pregunta: ¿cuál es el mínimo número de movimientos necesarios para pasar todos los discos al poste de la derecha? ¿Hay una fórmula cerrada para esta sucesión?

El punto fundamental es que si sabemos resolver el problema con n discos, lo podemos resolver con $n+1$ de la manera que sigue: movemos primero los n discos de arriba al poste del medio (esto lo sabemos hacer, es simplemente intercambiar el rol de los postes del medio y de la derecha); luego, movemos el $n+1$-ésimo disco a la derecha, y por último movemos los n discos del medio a la derecha. Esto dice que si H_n cuenta cuántos movimientos son necesarios si tenemos n discos, entonces $H_{n+1} = 2H_n + 1$. Además, es claro que $H_1 = 1$, pues si tenemos un solo disco lo pasamos en un solo movimiento. Con esta regla recursiva, obtenemos los primeros valores de H:

$$\begin{array}{lll} H_1 = 1, & H_3 = 2 \cdot 3 + 1 = 7, & H_5 = 2 \cdot 15 + 1 = 31, \\ H_2 = 2 \cdot 1 + 1 = 3, & H_4 = 2 \cdot 7 + 1 = 15, & H_6 = 2 \cdot 31 + 1 = 63, \end{array}$$

lo cual indica que posiblemente sea $H_n = 2^n - 1$.

Ejercicio 2.3. Probar que efectivamente $H_n = 2^n - 1$.

Según la leyenda, hay en un templo de Hanoi monjes que mueven 64 discos de oro siguiendo las reglas de este juego. La leyenda dice que una vez que terminen de mover la última pieza será el fin del mundo. Suponiendo que mueven un disco por segundo, ¿cuanto tiempo tardarán en moverlos todos?

La sucesión de *Fibonacci*. La famosa sucesión de Fibonacci debe su nombre a Leonardo Pisano Bigollo, más conocido como "Fibonacci" (aprox. 1170-1240). Fibonacci publicó en el año 1202 un libro, Liber Abaci, donde entre otras cosas propuso el siguiente problema: si colocamos una pareja de conejos en un área cerrada, ¿cuántos conejos habrá luego de n meses si cada pareja de conejos produce una nueva pareja de conejos cada mes, los conejos nunca mueren y una pareja a los dos meses de nacida puede comenzar a tener hijos?

En el mes primer mes, cuando los ponemos, tenemos una pareja de conejos bebés. En el segundo mes tenemos la misma única pareja, pero son adultos. En el tercer mes, tenemos una pareja original más una pareja bebé (hijos de la pareja original), o sea tenemos dos parejas. En el cuarto mes, la pareja original tiene otra pareja de bebés, y además la pareja del mes 2 se convierte en adulta (tenemos tres parejas). En el quinto mes, las dos parejas adultas que hay tienen parejas bebés, y tenemos cinco parejas. Si calculamos algunos números más, vemos que los siguientes meses tenemos: 8, 13, 21, 34...

Para encontrar una fórmula para esta sucesión, llamenos A_n al número de parejas adultas en el mes n y B_n al número de parejas bebés. Llamamos también F_n al total de parejas, $F_n = A_n + B_n$.

mes	A_n	B_n	F_n
1	0	1	1
2	1	0	1
3	1	1	2
$\vdots$	$\vdots$	$\vdots$	$\vdots$
n	A_n	B_n	$A_n + B_n$
$n+1$	$A_n + B_n$	A_n	$2A_n + B_n$
$n+2$	$2A_n + B_n$	$A_n + B_n$	$3A_n + 2B_n$

Notar que el número de conejos en el mes $n+2$ es el número que había en el mes $n+1$ más el número de parejas adultas del mes $n+1$, que es el número de parejas del mes n. Luego la sucesión F_n satisface la recurrencia $F_{n+1} = F_n + F_{n-1}$ para todo $n \geq 2$. Además, los primeros dos valores de F son $F_1 = 1$, $F_2 = 1$. Por la proposición 2.5, estas condiciones definen una única sucesión, a la que llamamos *sucesión de Fibonacci*. A los números de la sucesión se los conoce como *números de Fibonacci*.

¿Habrá una fórmula que dé F_n? La respuesta (aunque no natural) es "sí". Para sucesiones dadas por recurrencias con coeficientes constantes (o sea

$$f(n) = a_1 f(n-1) + \cdots + a_r f(n-r)$$

donde a_i son números reales fijos) existen métodos generales para calcular fórmulas cerradas. En estas notas nos conformaremos con calcular (a mano) una fórmula para los números de Fibonacci. Notar que los números crecen de manera muy rápida, con lo cual uno podría esperar que $F_n = ar^n$, o sea que sean (salvo una constante) potencias de un número. Veremos que este no es exactamente el caso, pero "casi".

Si suponemos por un instante que son potencias de un número r, ¿quién es r? Una forma de calcularlo es mirar el cociente de dos números consecutivos de Fibonacci.

Si miramos los primeros valores de la sucesión, vemos que los cocientes sucesivos no dan siempre lo mismo $(2, 3/2, 5/3, 8/5, \dots)$, con lo cual nuestro primer enfoque no funciona. Pero $5/3 = 1.666$, $8/5 = 1.6$, $13/8 = 1.625$, $21/13 = 1.615$, $34/21 = 1.619$ y así siguiendo. Estos cocientes, parecen estar acercándose a un número, pero ¿a cuál? ¿Por qué existe este límite?

Dentro de las muchas propiedades que satisfacen los números de Fibonacci (en la web hay muchísima información al respecto) una importante es la siguiente:

Proposición 2.6 (Identidad de Cassini)**.** *$F_{n+1}F_{n-1} - F_n^2 = (-1)^n$ para todo $n \geq 2$.*

Dejamos como ejercicio probar (por inducción) tal identidad. Luego, "veamos" que $\frac{F_{n+1}}{F_n}$ es de Cauchy. Si miramos dos términos consecutivos,

$$\frac{F_{n+1}}{F_n} - \frac{F_n}{F_{n-1}} = \frac{(-1)^n}{F_n F_{n-1}}.$$

Dejamos como ejercicio ver que esto implica que la sucesión es de Cauchy, es decir, que para todo $\varepsilon > 0$ existe $N \in \mathbb{N}$ tal que si n, m son ambos $> N$, entonces $|\frac{F_{n+1}}{F_n} - \frac{F_{m+1}}{F_m}| < \varepsilon$. Esto dice que existe el límite de los cocientes sucesivos de números de Fibonacci. Ahora

$$\Phi := \lim_{n\to\infty} \frac{F_{n+1}}{F_n} = \lim_{n\to\infty} \frac{F_n + F_{n-1}}{F_n} = 1 + \lim_{n\to\infty} \frac{F_{n-1}}{F_n} = 1 + \frac{1}{\Phi}.$$

Multiplicando por Φ, obtenemos que $\Phi^2 = \Phi + 1$, o sea Φ es raíz del polinomio $x^2 - x - 1$. Usando la fórmula para las raíces de un polinomio cuadrático, vemos que $\Phi = \frac{1 \pm \sqrt{5}}{2}$. Como debe ser positivo, tenemos que $\Phi = \frac{1+\sqrt{5}}{2} = 1,618...$

Este número Φ es el llamado *número de oro* o la *proporción divina*. Si tenemos un segmento partido en dos lados de longitudes a y b ($a \geq b$) nos podemos preguntar cómo tienen que ser a y b para que la proporción entre todo el segmento y a sea la misma que entre a y b. En ecuaciones, si llamamos x a esta proporción, tenemos que $x = \frac{a}{b} = \frac{a+b}{a} = 1 + \frac{b}{a} = 1 + \frac{1}{x}$. Entonces debe ser $x = \Phi$. El número de oro aparece en muchos contextos en medicina, biología, en el arte (por ejemplo Leonardo Da Vinci observó que es la relación aproximada entre los miembros del cuerpo humano y la longitud total de los mismos).

Volviendo a nuestro problema, queremos ver cómo dar una fórmula para F_n, y parece que el número Φ debería tener algo que ver. Ya vimos que F_n no puede ser una constante por Φ (porque los cocientes sucesivos no son constantes), pero observemos qué pasa si planteamos

$$F_n = a\left(\frac{1+\sqrt{5}}{2}\right)^n + b\left(\frac{1-\sqrt{5}}{2}\right)^n$$

para un par de números a, b. Como F_n es entero, es bastante natural plantear este tipo de ecuación (ya volveremos a esto cuando hablemos de polinomios). Si miramos los primeros valores de F_n, tenemos el sistema:

$$\begin{pmatrix} \frac{1+\sqrt{5}}{2} & \frac{1-\sqrt{5}}{2} \\ \frac{3+\sqrt{5}}{2} & \frac{3-\sqrt{5}}{2} \end{pmatrix} \begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$$

Si utilizamos la regla de Cramer, tenemos que $a = \frac{1}{\sqrt{5}}$ y $b = \frac{-1}{\sqrt{5}}$, o sea

$$F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right)$$

Se deja como ejercicio ver por inducción que esta fórmula es válida para todo $n \in \mathbb{N}$.

Como comentario al margen, se puede observar que Φ es raíz del polinomio $x^2 - (x+1)$. Este polinomio está fuertemente relacionado con la recurrencia. El lector interesado puede pensar cómo resolver una recurrencia del estilo $a_{n+2} = \alpha a_{n+1} + \beta a_n$ en términos del polinomio $x^2 - (\alpha x + \beta)$.

3. Combinatoria

En el primer capítulo, al trabajar con conjuntos finitos, hablamos de su cardinal. Recordemos que el cardinal de un conjunto es el número de elementos que posee dicho conjunto. En este capítulo nos dedicaremos a "contar" elementos de un conjunto, viendo la dificultad que esto puede tener.

Comencemos con algunos casos sencillos:

Ejemplos.
1. ¿Cuántos elementos tiene el conjunto $\{0, \ldots, 9\}$?
2. ¿Y el conjunto $\{0, \ldots, 99\}$?

Es claro que las respuestas son 10 y 100 respectivamente. Pero pensemos el segundo problema a partir del primero. Cada número de dos cifras lo podemos ver como un par ordenado de dos números de una cifra cada uno. Esto es, podemos pensar al conjunto $\{0, \cdots, 99\}$ como el producto cartesiano $\{0, \cdots, 9\} \times \{0, \cdots, 9\}$.

¿Qué pasa si queremos contar cuántos números hay de tres dígitos cuyas cifras estén en el conjunto $\{2, 4, 7\}$? Lo que estamos haciendo es interpretar el conjunto buscado como el producto cartesiano del conjunto $\{2, 4, 7\}$ consigo mismo tres veces.

Proposición 3.1. *Si $\mathcal{A}$, $\mathcal{B}$ son conjuntos finitos, entonces $|\mathcal{A} \times \mathcal{B}| = |\mathcal{A}||\mathcal{B}|$.*

Demostración. Si $\mathcal{A} = \{a_1, \cdots, a_n\}$ y $\mathcal{B} = \{b_1, \cdots, b_m\}$, donde los a_i son distintos y los b_j son distintos (o sea $n = |\mathcal{A}|$ y $m = |\mathcal{B}|$), entonces por definición,

$$\mathcal{A} \times \mathcal{B} = \{(a_1, b_1), \ldots, (a_n, b_1), \ldots, (a_1, b_m), \ldots, (a_n, b_m)\}.$$

Es claro que estos nm elementos son todos distintos, con lo cual $|\mathcal{A} \times \mathcal{B}| = nm$. □

Ejercicio 3.1. ¿Qué pasa si tomamos el producto cartesiano de más conjuntos? Dar una fórmula y probarla por inducción.

Ejemplo. Supongamos que tenemos en nuestro placard 3 camisas, 4 pantalones y 2 pares de zapatos. ¿De cuántas maneras distintas podemos vestirnos?

Ejemplo. Paseando por la calle, entramos a un Pumpernic, y encontramos el siguiente anuncio: "Armá tu hamburguesa con lechuga, tomate, queso y cebolla de cualquiera de las 16 maneras posibles". ¿Es correcto el enunciado?

Lo que estamos haciendo al fin de cuentas es tomar el conjunto de "extras" de la hamburguesa (en este caso el conjunto {lechuga, tomate, queso, cebolla}) y eligiendo algún subconjunto de él. Generalizando el argumento, si $\mathcal{A}$ es un conjunto de n elementos, ¿cuántos subconjuntos tiene $\mathcal{A}$? O dicho de otra forma, ¿cuántos elementos tiene $\mathcal{P}(\mathcal{A})$?

Ejemplo. ¿Cuántos números de exactamente tres cifras hay? Podemos pensar este ejemplo como sigue: debemos proceder en tres pasos. En el primer paso elegimos la primera cifra, que no puede ser cero. Es decir, tenemos 9 posibilidades. Luego, elegimos la segunda cifra, que puede ser cualquiera. Tenemos 10 posibilidades. Por último, elegimos la tercera cifra, que otra vez puede ser cualquiera. Tenemos 10 posibilidades. En total, son $9 \cdot 10 \cdot 10 = 900$ números.

Una manera de resumir los ejemplos considerados hasta aquí es la siguiente: si tenemos que contar un proceso de k pasos, donde en cada paso tenemos que hacer una elección y tal que las elecciones son "independientes" (es decir, la elección de un paso no influye en los otros), y si tenemos n_1 posibilidades para la primer elección, n_2 para la segunda, ..., n_k posibilidades para la k-ésima, entonces en total tenemos $n_1 \times \cdots \times n_k$ casos posibles.

Si las elecciones *son* dependientes, este razonamiento ya no vale.

Ejemplo. Aceptando números que empiecen con 0, ¿cuántos números de 4 cifras hay con todos los dígitos distintos?

En este ejemplo, la elección del segundo dígito depende de cuál fue la elección del primero, con lo cual el conjunto que estamos considerando no es un producto cartesiando de conjuntos. De todas maneras, podemos nuevamente proceder por pasos. Para el primer dígito tenemos 10 posibilidades, dado que no tenemos restricción alguna hasta aquí. Si llamamos a_1 al dígito elegido, ¿qué dígitos podemos poner en el segundo lugar? Es claro que cualquier dígito que no sea a_1 nos sirve, luego para el segundo dígito tenemos 9 posibilidades. Si ahora llamamos a_2 al segundo dígito, para el tercer dígito podemos poner cualquiera salvo a_1 y a_2 (que son distintos), por lo que tenemos 8 posibilidades. Para el cuarto tenemos 7. Como todos los números contruidos son distintos (y dan todos los posibles resultados), tenemos $10 \cdot 9 \cdot 8 \cdot 7 = 5040$ números.

Ejemplo. ¿De cuántas maneras se pueden sentar 50 alumnos en 200 asientos?

Podemos pensar que los alumnos están ordenados (por ejemplo, alfabéticamente, o por fecha de nacimiento, o de cualquier otra manera). El primer alumno se puede sentar en 200 asientos. El segundo, en 199. El tercero, en 198. Así siguiendo, el último tiene 151 asientos para sentarse. Las maneras entonces son

$$200 \cdot 199 \cdot 198 \cdots 151 = \frac{200!}{150!}.$$

Ejercicios. Decidir en cada caso cuántos elementos tienen los siguientes conjuntos:

1. Funciones de un conjunto de n elementos en un conjunto de m elementos.
2. Funciones inyectivas de un conjunto de n elementos en un conjunto de m elementos.
3. Funciones biyectivas de un conjunto de n elementos en un conjunto de n elementos.

En todos los ejemplos que vimos hasta ahora el *orden* de los elementos a contar era importante (no es lo mismo el número 192 que el número 291 a pesar de que ambos poseen los mismos dígitos). ¿Qué pasa si el orden no importa? Por ejemplo, supongamos que estamos jugando a un juego de naipes (con 40 cartas) y queremos contar las posibles manos (de 3 cartas) que podemos obtener. ¿Cómo hacemos?

Siguiendo los razonamientos hechos hasta acá, uno diría: al repartir las cartas, tengo 40 posibilidades para la primera carta, 39 para la segunda y 38 para la tercera, y entonces las posibles manos son $40 \cdot 39 \cdot 38$. Sin embargo, esto no es correcto, como se puede ver con el siguiente ejemplo: si en la primer mano sacamos el as de espadas, en la segunda el 7 de oros en la tercera el 7 de espadas es lo mismo que haber sacado primero el 7 de espadas, luego el 7 de oros y por último el as de espadas. ¿Cuántas veces estamos contando esta mano? Si pensamos que contarla muchas veces es cambiar el orden en que aparecieron las cartas, vemos que la contamos tantas veces como permutaciones de las tres cartas hay, es decir, $3! = 6$ veces. Ahora, la cantidad de veces que contamos el mismo caso (la mano) no depende de las cartas que obtuvimos, con lo cual el número de manos por seis es $40 \cdot 39 \cdot 38$, o sea el número de manos es $\frac{40 \cdot 39 \cdot 38}{3 \cdot 2 \cdot 1} = 9880$.

Resolvimos el problema utilizando (esencialmente) el caso anterior, pero hay otra forma de pensar este problema. Una mano es un subconjunto de 3 elementos del conjunto de naipes (recordar que un conjunto no posee información del orden en que listamos sus elementos). Luego lo que queremos hacer es contar cuántos subconjuntos de 3 elementos tiene un conjunto de 40 elementos. Ya sabemos que el número de formas es $\frac{40!}{37!3!}$. Esto motiva la siguiente definición:

Definición. Si n, m son números naturales, con $n \geq m$, definimos el *número combinatorio* $\binom{n}{m} := \frac{n!}{m!(n-m)!}$.

Proposición 3.2. *Si $\mathcal{A}$ es un conjunto de n elementos, el número de subconjuntos de $\mathcal{A}$ de m elementos es $\binom{n}{m}$.*

Demostración. (de manera combinatoria) Si razonamos como antes, si extraemos del conjunto m elementos de manera ordenada, tenemos $\frac{n!}{(n-m)!}$ maneras de hacerlo. Como no nos interesa el orden en que elegimos los elementos, cada caso lo estamos contando $m!$ veces (el número de permutaciones de un conjunto de m elementos), de donde se sigue el enunciado. □

Más abajo haremos otra demostración de este enunciado usando inducción. Notar en particular que $\binom{n}{m}$ es un número natural para cualquier elección de n y m (cosa que no es para nada obvia de su definición). Una propiedad importante de los números combinatorios es la que sigue:

Lema 3.3. *Si $n \in \mathbb{N}$ y $1 \leq m \leq n$ entonces $\binom{n}{m} + \binom{n}{m+1} = \binom{n+1}{m+1}$.*

Demostración. Si escribimos la definición de los términos de la izquierda y sacamos común denominador, tenemos

$$\binom{n}{m} + \binom{n}{m+1} = \frac{n!}{m!(n-m)!} + \frac{n!}{(m+1)!(n-m-1)!} =$$
$$= \frac{n!(m+1) + n!(n-m)}{(m+1)!(n-m)!} = \frac{(n+1)!}{(m+1)!(n-m)!} = \binom{n+1}{m+1}$$

□

Ejercicio 3.2. Probar (por inducción) que para todo $n \in \mathbb{N}$ y m natural con $1 \leq m \leq n$, $\binom{n}{m}$ es un número natural.

Podemos ahora demostrar la proposición anterior por inducción en n.

Dem. de la Prop.3.2. (por inducción) El caso base es $n = 1$. Si el conjunto tiene 1 elemento, entonces como $0 \leq m \leq n$, m puede ser 0 ó 1. Es claro que la cantidad de subconjuntos de 0 elementos es 1 (¡el conjunto vacío!) y la cantidad de subconjuntos de 1 elemento es también 1 (todo el conjunto). En ambos casos coincide con el combinatorio $\binom{1}{m}$.

Supongamos entonces que para conjuntos de n elementos vale la proposición, y supongamos que $\mathcal{A}$ tiene $n+1$ elementos. Entonces $0 \leq m \leq n+1$. Los casos $m = 0$ y $m = n+1$ son como antes: en ambos casos hay un solo subconjunto de m elementos. Supongamos entonces que $1 \leq m \leq n$. Podemos tomar un elemento particular de $\mathcal{A}$; llamémoslo x_0. Los subconjuntos de $\mathcal{A}$ los dividimos en dos: los que tienen a x_0 como elemento y los que no. Los subconjuntos de $\mathcal{A}$ de m elementos que no contienen a x_0 son los mismos que los subconjuntos de m elementos de $\mathcal{A} \setminus \{x_0\}$. Como $\mathcal{A} \setminus \{x_0\}$ tiene n elementos, podemos aplicar la hipótesis inductiva y decir que hay $\binom{n}{m}$ de tales subconjuntos. Por otra parte, hay la misma cantidad de subconjuntos de m elementos que contienen a x_0 que de subconjuntos de $m-1$ elementos de $\mathcal{A} \setminus \{x_0\}$, por lo que nuevamente por hipótesis inductiva éstos son $\binom{n}{m-1}$. Entonces, la cantidad de subconjuntos de $\mathcal{A}$ de m elementos es $\binom{n}{m} + \binom{n}{m-1}$, que por el lema coincide con $\binom{n+1}{m}$. □

Ejercicio 3.3. El Quini 6 consiste en elegir 6 números del conjunto de números $\{1, \ldots, 46\}$. ¿Cuántos posibles resultados hay? (Rta: 9.366.819)

La fórmula del binomio de Newton (probada en la práctica de inducción) dice que si a, b son números reales y n es un número natural,

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

Podemos interpretar esto de la siguiente manera, $(a+b)^n = \underbrace{(a+b)\cdots(a+b)}_{n}$ con lo cual, al aplicar la propiedad distributiva, para obtener $a^i b^{n-i}$ tenemos que elegir en i lugares el número a y en los restantes el número b. Ahora si tenemos n términos y tenemos que elegir i de ellos para tomar el número a, tenemos $\binom{n}{i}$ maneras de hacerlo, que es lo enunciado.

Antes de pasar al último caso general, veamos cómo podemos combinar lo aprendido hasta acá en casos más complejos. Por ejemplo, ¿cuántos números de 2 cifras hay mayores que 12?

Este ejercicio se puede resolver de dos maneras distintas, pero que nos llevan a lo mismo.

Una manera de responder a la pregunta es la siguiente: los números de 2 dígitos sabemos que son 100. Los números menores o iguales a 12 son 13 (recordar que estamos considerando el 0), luego los otros son mayores que 12 y tenemos $100 - 13 = 87$ casos.

Pero también se puede pensar de otra manera, separando en casos:

- Si elijo el primer dígito mayor que 1 (y tengo 8 posibilidades), ya el número obtenido será mayor que 12. Luego acá tengo $8 \cdot 10 = 80$ casos posibles.
- Si el primer dígito es 1, el segundo dígito debe ser mayor que dos. Hay 7 números mayores que 2, con lo cual en este caso tengo 7 posibilidades.

Como hemos considerado todos los casos posibles, tenemos 87 posibilidades.

¿Qué tienen en común las dos formas de resolverlo? En ambos usamos el siguiente principio: si tenemos dos conjuntos finitos y disjuntos, el cardinal de la unión es la suma de los cardinales. En la primera resolución dijimos: {números de dos dígitos} = {números de dos dígitos > 12} $\cup$ {números ≤ 12}. Luego $100 = X + 13$, siendo X el número que queremos calcular.

En la segunda resolución consideramos como conjunto $\mathcal{A} =$ {números con primer dígito ≥ 2} y $\mathcal{B} =$ {números ≥ 12 con primer dígito 1}. Claramente $\mathcal{A} \cap \mathcal{B} = \emptyset$ y $\mathcal{A} \cup \mathcal{B}$ es el conjunto que buscamos.

¿Qué pasa si $\mathcal{A}$ y $\mathcal{B}$ no son disjuntos? ¿Qué podemos decir de $|\mathcal{A} \cup \mathcal{B}|$ en este caso?

Proposición 3.4. *Si $\mathcal{A}$ y $\mathcal{B}$ son dos conjuntos finitos, $|\mathcal{A} \cup \mathcal{B}| = |\mathcal{A}| + |\mathcal{B}| - |\mathcal{A} \cap \mathcal{B}|$.*

Demostración: Llamemos $\mathcal{C} = \mathcal{A} \cap \mathcal{B}$. Luego $\mathcal{A} = \mathcal{C} \cup (\mathcal{A} \backslash \mathcal{C})$. Al ser la unión disjunta, $|\mathcal{A}| = |\mathcal{C}| + |\mathcal{A} \backslash \mathcal{C}|$. Análogamente, $|\mathcal{B}| = |\mathcal{C}| + |\mathcal{B} \backslash \mathcal{C}|$. Como $\mathcal{A} \cup \mathcal{B} = (\mathcal{A} \backslash \mathcal{C}) \cup (\mathcal{B} \backslash \mathcal{C}) \cup \mathcal{C}$ y dichas uniones son disjuntas, obtenemos que $|\mathcal{A} \cup \mathcal{B}| = |\mathcal{A} \backslash \mathcal{C}| + |\mathcal{B} \backslash \mathcal{C}| + |\mathcal{C}| = |\mathcal{A}| + |\mathcal{B}| - |\mathcal{C}|$. □

Ejercicio 3.4. Deducir y probar una fórmula para la unión de 3 conjuntos.

Ejercicio 3.5. Generalizando los dos casos anteriores, probar (por inducción) que si tenemos n conjuntos $\mathcal{A}_1, \ldots, \mathcal{A}_n$, entonces

$$|\bigcup_{i=1}^{n} \mathcal{A}_i| = \sum_{\emptyset \neq I \subset \{1,\ldots,n\}} (-1)^{|I|+1} |\cap_{j \in I} \mathcal{A}_j|.$$

Ejemplo. ¿Cuántos anagramas de la palabra "PIANO" podemos formar si pedimos que la letra A esté al lado de otra vocal?

Una manera de resolver este problema es la siguiente: comenzamos viendo al lado de qué letra ubicamos a la A. Definamos $\mathcal{A} =$ {palabras con A pegada a I}. Los elementos de este conjunto satisfacen que en algún lugar de la palabra aparece "AI" ó "IA". Si pensamos que estas dos letras son un solo caracter, y dejamos que las otras letras se ubiquen donde quieran, tenemos 4! posibles palabras (que es el número de permutar este bloque que formamos y las otras 3 letras). Como podemos formas palabras con "AI" ó con "IA" (y estos casos son disjuntos), $|\mathcal{A}| = 2.4!$. De manera análoga, podemos definir $\mathcal{B} =$ {palabras con A pegada a O} y $|\mathcal{B}| = 2.4!$ también. ¿Quién es $\mathcal{A} \cap \mathcal{B}$? Son las palabras que la letra A esta pegada a la letra I y a la letra O. Luego $\mathcal{A} \cap \mathcal{B} =$ {palabras con "IAO" ó con "OAI" en algún lugar}. Contando como antes, $|\mathcal{A} \cap \mathcal{B}| = 2.3!$ (justificar esto). Luego la respuesta es $4.4! - 2.3! = 84$.

Ejercicio 3.6. Si tiramos un dado 4 veces, ¿cuántos resultados posibles tenemos? ¿Cuántos tal que en dos tiros consecutivos aparecen números iguales? ¿Cuántos tal que en dos tiros consecutivos aparecen dos números distintos?

Ejercicio 3.7. Vamos 3 parejas al cine, y al llegar debemos decidir como sentarnos. El problema es que dos hombres estamos peleados (por cuestiones futbolísticas) y no queremos sentarnos juntos. ¿De cuántas maneras podemos sentarnos si cada persona tiene que estar con su pareja? (rta: 40).

Ejemplo. Invitamos a 7 amigos a casa a cenar, y queremos sentarnos en una mesa redonda, ¿de cuántas formas podemos hacerlo si no importa la silla en que nos sentamos sino solamente cómo nos ubicamos entre nosotros?

El problema que tienen las mesas redondas es que no se puede marcar un "primer" lugar ni un "último" lugar. Una manera de resolver estos problemas es elegir una persona como referencia (por ejemplo me siento yo primero, y luego veo cómo se van sentando las otras personas mirando para la derecha). Si lo pensamos así, es claro que la respuesta es 6!. Otra manera (a veces más difícil) de pensar este problema es que marcamos una silla y contamos cómo nos sentamos contando las posiciones a partir de esa silla para la derecha (o para la izquierda, claro). El número de formas es el número de permutaciones de las 7 personas, con lo cual hay 7! casos. Pero al estar sentados en una mesa redonda, si nos movemos todos un asiento para la derecha, la forma de sentarnos no cambió. Lo mismo pasa moviéndonos $2, 3, 4, 5$ ó 6 lugares a la derecha. Luego cada forma de sentarnos la contamos 7 veces, con lo cual la respuesta es $\frac{7!}{7} = 6!$.

Ejemplo. ¿Cuántas funciones suryectivas hay de un conjunto $\mathcal{A}$ de n elementos en un conjunto $\mathcal{B}$ de m elementos?

Este problema a pesar de parecer sencillo no lo es tanto. Podemos tratar de contar las funciones que no son suryectivas. Digamos que $\mathcal{B} = \{b_1, \ldots, b_m\}$. Definimos el conjunto $\mathcal{C}_i = \{f : \mathcal{A} \to \mathcal{B} \text{ tales que } b_i \text{ no está en la imagen de } f\}$. Queremos contar $|\bigcup_{i=1}^m \mathcal{C}_i|$. Para usar el principio de inclusión-exclusión, necesitamos saber cuantos elementos tiene la intersección de varios de estos conjuntos, pero $\bigcap_{i=1}^r \mathcal{C}_i$ es el conjunto de funciones que no tiene los primeros r elementos en la imagen, o sea que la imagen tiene (a lo sumo) $m - r$ elementos. Ya sabemos que (independientemente de los índices), hay $(m-r)^n$ tales funciones. Luego, por el principio de inclusión-exclusión, el número de funciones suryectivas es

$$m^n - \sum_{r=1}^{m} (-1)^{r+1} \binom{m}{r} (m-r)^n = \sum_{r=0}^{n} (-1)^r \binom{m}{r} (m-r)^n.$$

Notar que el número binomial representa todos los subconjuntos de $\{1, \ldots, m\}$ que hay con r elementos.

3.1. Bosones. El caso que vamos a considerar fue estudiado por el físico Satyendra Bose mirando cómo se comportan las partículas. Las partículas tienen asociados *números cuánticos*. Los fermiones son ciertas partículas que satisfacen que dos de ellas no pueden estar en el mismo lugar y tener los mismos números cuánticos. Si tenemos n partículas (que son indistinguibles) y las queremos ubicar en k *estados cuánticos*, tenemos $\binom{k}{n}$ maneras de hacerlo.

Otra clase importante de partículas son las llamadas bosones (llamadas así precisamente en honor a Bose), que sí pueden compartir el estado cuántico. Si tenemos n bosones, y los queremos ubicar en k estados, ¿de cuántas maneras podemos hacerlo? Un problema análogo (y tal vez mas intuitivo) es el siguiente: ¿de cuántas maneras podemos poner n bolitas indistinguibles en k cajas?

Comencemos suponiendo que tenemos 2 cajas y 2 bolitas. Luego todas las maneras de poner las bolitas en las cajas son:

$$[\circ\circ][\quad], \qquad [\circ][\circ], \qquad [\quad][\circ\circ]$$

O sea la respuesta es 3. La manera de resolver este problema consiste en encontrar una "representación" del mismo que nos facilite la forma de contar. Para facilitar la notación, representemos por una barra vertical | las paredes de las cajas. Luego los casos anteriores son

$$|\circ\circ|\quad|,\qquad|\circ|\circ|,\qquad|\quad|\circ\circ|$$

Podemos pensar que tenemos dos símbolos distintos, a saber | y $\circ$ (en nuestro caso, dos $\circ$ y tres |), y que lo que estamos haciendo es mirar todas las permutaciones que podemos obtener con estos dos objetos. Esta idea a pesar de ser muy buena, no funciona correctamente, porque al permutar todos, tenemos casos que no corresponden a posiciones permitidas. Por ejemplo,

$$\circ|\quad|\quad|\circ$$

no tiene interpretación en términos de nuestras cajas. En los casos que miramos, las permutaciones tienen necesariamente una barra vertical al comienzo y una barra vertical al final, por lo que podemos no ponerlas. Luego podemos pensar que lo que queremos hacer variar las | interiores y las $\circ$. Así para dos cajas y dos bolitas, lo que queremos es ver todas las permutaciones de una barra vertical y dos círculos. El número de tales permutaciones es $\binom{3}{1} = \frac{3!}{2!1!} = 3$ (es elegir de los 3 lugares uno para poner la barra vertical). Este razonamiento demuestra la siguiente proposición:

Proposición 3.5. *Si tenemos n bolitas indistinguibles y las queremos repartir en k cajas, hay $\frac{(n+k-1)!}{n!(k-1)!} = \binom{n+k-1}{k-1} = \binom{n+k-1}{n}$ formas de hacerlo.*

Veamos algunos ejemplos de aplicaciones de esto:

Ejemplo. Tenemos 200 vacantes para Algebra I, y queremos armar 3 turnos con estas vacantes, ¿de cuántas maneras podemos hacerlo?

Podemos pensar que cada turno es una caja, y el número de vacantes asociado a cada turno es el número de bolitas que ponemos en cada caja. Luego es un problema de bosones con 3 cajas y 200 bolitas, con lo cual hay $\binom{202}{2} = \frac{202.201}{2} = 20301$.

Ejemplo. ¿De cuántas maneras se pueden distribuir las 200 vacantes si queremos un mínimo de 20 alumnos por turno?

Una manera fácil de conseguir esta condición es poner 20 vacantes en cada turno, y luego repartir (por bosones nuevamente) las 140 vacantes restantes en los 3 turnos, luego la respuesta es $\binom{142}{2} = 10011$.

Ejemplo. ¿De cuántas maneras si no puede haber más de 80 alumnos por curso?

Una manera conocida de resolver este problema es contar su complemento, o sea de cuántas formas podemos armar los turnos tal que alguno tenga más de 80 alumnos. Llamemos $\mathcal{A}_i$ a las distribuciones tales que el turno i tiene más de 80 alumnos. ¿Cuántos elementos tiene $\mathcal{A}_i$? Siguiendo el razonamiento anterior, ponemos 81 vacantes en el turno i, y distribuimos las 119 vacantes restantes entre los tres turnos, con lo cual $|\mathcal{A}_i| = \binom{121}{2} = 7260$. La intersección de dos conjuntos son las distribuciones tales que dos turnos tienen más de 80 alumnos. Supongamos (por simplicidad) que miramos cuántas distribuciones de alumnos tienen más de 80 alumnos en el turno 1 y 2. Esto corresponde a poner 81 bolitas en la primera caja y 81 bolitas en la segunda. Luego nos quedan 38 bolitas para repartir entre las tres cajas, con lo cual $|\mathcal{A}_1 \cap \mathcal{A}_2| = \binom{40}{2} = 780$. Por último, los tres conjuntos tienen intersección vacía, dado que no hay suficientes vacantes para que haya 81

alumnos en cada turno. Usando el principio de inclusión exclusión, tenemos que el complemento de nuestro problema tiene cardinal

$$3\binom{121}{2} - 3\binom{40}{2} = 19440.$$

Luego las distribuciones con menos de 80 alumnos por clase son $20301 - 19440 = 861$.

Observación: el resultado coincide con $\binom{42}{2}$, que es la cantidad de maneras de poner 40 bolitas en 3 cajas. ¿Por qué?

Ejemplo. ¿Cuántas formaciones "razonables" de un equipo de fútbol hay? Llamamos formación razonable a una formación que tiene al menos 2 defensores, 1 mediocampista y 1 delantero (además del arquero, por supuesto).

Nuevamente ¡tenemos un problema de bosones! Tenemos 11 jugadores en un equipo de fútbol. Estudiamos formaciones, es decir, cuántos jugadores son defensores, cuántos mediocampistas y cuántos delanteros. Esto es, en este ejemplo los jugadores son "indistinguibles". Además del arquero, tenemos 10 jugadores para repartir entre defensores, mediocampistas y delanteros. Podemos pensar que tenemos estas tres cajas, y queremos repartir las 10 bolitas en ellas. Ponemos dos bolitas en la defensa, una en el mediocampo y otra en la delantera, y nos quedan 6 bolitas para repartir en 3 cajas, luego la respuesta es $\binom{8}{2} = 28$.

Ejercicio 3.8. ¿Cuántas funciones crecientes hay del conjunto $\{1, \ldots, n\}$ en el conjunto $\{1, \ldots, m\}$?

Ejercicio 3.9. Si tenemos 5 pesos y queremos apostarlos en la lotería, ¿de cuántas maneras podemos hacerlo si las apuestas son siempre un número natural de pesos?

Ejercicio 3.10. ¿De cuántas maneras se puede partir un número natural n como suma de k números naturales? (suponiendo por supuesto que $k \leq n$).

4. Probabilidad

Supongamos que queremos realizar un experimento en el que los posibles resultados son finitos (digamos que hay n posibles resultados). Supongamos, además, que todos los posibles resultados son "equiprobables" o, dicho de otra manera, todos los resultados tienen la misma probabilidad de salir. Si tenemos, dentro de los posibles resultados, k de ellos que nos resultan "favorables" (o sea, queremos que salgan), entonces la probabilidad de éxito del experimento es $\frac{k}{n}$.

Observación. La probabilidad en los casos que consideramos es siempre un número racional entre 0 y 1. Además, la probabilidad es 1 si en nuestro experimento todos los casos son favorables y es 0 si ninguno lo es.

Utilizando algunas técnicas de análisis, se puede extender estos conceptos a casos en que el conjunto de resultados no es finito, ni son necesariamente equiprobables. Estas nociones están mas allá del presente curso, sin embargo.

Ejemplos. Veamos cómo la combinatoria nos permite calcular varias probabilidades (muchas de ellas de juegos de azar).

1. Tomemos una moneda equilibrada, y la tiramos al aire. Supongamos que no hay condiciones externas que influyan en la moneda (como viento), ¿qué probabilidad hay de que salga cara?

Si miramos la definición de probabilidad, lo que debemos hacer es contar el número de resultados posibles para tirar la moneda, y el número de resultados favorables que tenemos. Dado que una moneda tiene dos caras, el número de experimentos es 2, y hay un único resultado favorable. Luego la probabilidad es 1/2.

2. En las mismas condiciones, ¿qué probabilidad hay de que salga ceca?
3. Supongamos que tomamos una moneda y la tiramos dos veces. ¿Qué probabilidad hay de que salga una cara y una ceca?

   Contemos los resultados en base a qué sale cada vez que uno tira la moneda. Para cada tiro tenemos dos posibilidades, por lo que el número total de resultados es $2 \cdot 2 = 4$. El número de casos favorables es 2 (cara-ceca y ceca-cara). Luego, la probabilidad es 1/2.
4. Un argumento (falaz) para el ejercicio anterior es el siguiente: cuando tiramos las monedas, los resultados son: obtener dos caras, dos cecas o una y una. Luego, de los 3 casos hay uno solo favorable con lo cual la probabilidad es 1/3. ¿Qué está mal en esta respuesta?
5. ¿Cuál es la probabilidad de ganar el Quini6? (rta: 1.06×10^{-7}).
6. ¿Qué probabilidad hay de ganar la lotería?
7. ¿Qué probabilidad hay de que salga rojo en la ruleta? (¿cuánto nos pagan si sale rojo?).
8. En un juego de dados (no cargados), ¿qué probabilidad hay de hacer generala servida? (rta: $\frac{6}{6^5} \sim 0.00077$) ¿y de hacer escalera servida? (rta: $\frac{40}{6^4} \sim 0.03$).
9. Supongamos que debemos hacer escalera, y luego del segundo tiro tenemos los números $\{3, 3, 4, 4, 4\}$. ¿Qué nos conviene? ¿tirar todo de nuevo o sólo 3 dados? (tirar 3 tiene probabilidad 0.055).

Proposición 4.1. *Si tenemos un experimento y dos conjuntos de resultados distintos $\mathcal{A}$ y $\mathcal{B}$ que consideramos favorables, $\mathcal{P}(\mathcal{A} \cup \mathcal{B}) = \mathcal{P}(\mathcal{A}) + \mathcal{P}(\mathcal{B}) - \mathcal{P}(\mathcal{A} \cap \mathcal{B})$.*

Demostración. Si contamos el número de casos favorables, debemos calcular $|\mathcal{A} \cup \mathcal{B}| = |\mathcal{A}| + |\mathcal{B}| - |\mathcal{A} \cap \mathcal{B}|$ por el principio de inclusión exclusión. Si dividimos esta igualdad por el número total de casos, tenemos el resultado buscado. □

Corolario 4.2. *Si un evento $\mathcal{A}$ tiene probabilidad $\mathcal{P}(\mathcal{A})$ de salir, la probabilidad de que $\mathcal{A}$ no salga es $1 - \mathcal{P}(\mathcal{A})$.*

Ejemplo. ¿Cuál es la probabilidad de que de un grupo de n personas haya al menos dos que cumplen años el mismo día?

Calculemos la probabilidad del complemento, o sea de que en un conjunto de n personas, todas ellas cumplan años en días distintos. Dado que las personas son "distinguibles", podemos pensar que a cada persona tenemos que asignarle un día del año. Luego debemos contar el número de funciones inyectivas de un conjunto de n elementos en uno de 365 (para hacer la cuenta más fácil, olvidemos los 29 de febrero). Sabemos que hay $\frac{365!}{(365-n)!}$ tales formas, con lo cual la probabilidad buscada es

$$1 - \frac{365!}{(365-n)!365^n} = f(n)$$

Si miramos los primeros valores de esta función, vemos que es creciente (es claro que mientras más personas hay, más probabilidad hay de que dos cumplan el mismo día), y para 23 personas esta probabilidad es aproximadamente 0.5073, o sea es más probable que en 23 personas dos de ellas cumplan el mismo día de que no pase. Si

uno calcula un par más de valores, se da cuenta (por ejemplo) que para 30 personas, hay más del 70 % de probabilidad de que dos cumplan el mismo día.

Ejemplo. El Prode (pronóstico deportivo) "antiguo" (hasta 1998) consistía en predecir el resultado de 13 partidos de fútbol (los 10 de primera división y los 3 más importantes de la Primera B Nacional). Para ello uno debía predecir en cada partido si ganaba el equipo local, el equipo visitante, o si empataban. Además (para facilitar el juego), se podían marcar dos *dobles*, es decir, elegir dos opciones "extras" en cualquiera de los 13 partidos. Así por ejemplo uno podía predecir que un partido ganaba el local o que era empate, y si cualquiera de esos dos resultados se cumplía se consideraba como correcta la predicción (la restricción era que los dobles debían utilizarse en partidos distintos, no pudiéndose marcar las tres opciones de un partido). En el Prode moderno, se retiraron los dobles, y uno debe acertar exactamente los 13 juegos. Calcular la probabilidad de ganar en las dos modalidades.

El cálculo del Prode moderno es sencillo, y la probabilidad es cercana a $6,3 \times 10^{-7}$. Veamos qué pasa con el antiguo Prode. Comencemos contando los casos "favorables". Imaginemos que sabemos cuál será el resultado de cada partido, y queremos construir tarjetas ganadoras. Para tal fin, comenzamos eligiendo los partidos donde pondremos los dobles. Tenemos $\binom{13}{2}$ elecciones, y en estos dos partidos hay 2 formas de ubicar las cruces extras (es decir, en estos partidos debemos marcar la opción correcta, y luego nos quedan dos posibilidades para la segunda opción). Del resto de los lugares tenemos que elegir exactamente el resultado correcto, con lo cual el número de casos favorables es

$$2 \cdot 2\binom{13}{2} = 13 \cdot 24 = 312$$

Para contar el número total de resultados, podemos pensar de una manera similar: de los 13 partidos elegimos dos de ellos donde usar la opción extra. Tenemos $\binom{13}{2}$ formas de hacerlo. Una vez escogidos estos lugares, tenemos 3 formas de dejar un lugar desmarcado en cada uno de ellos, (es decir, 9 opciones para los dobles una vez que elegimos dónde ponerlos) y 3^{11} formas de marcar los 11 lugares restantes, con lo cual el número de casos totales es $\binom{13}{2}3^{13}$. Calculando la probabilidad, tenemos

$$\frac{312}{\binom{13}{2}3^{13}} = \frac{312}{124357194} \sim 2,5 \times 10^{-6}$$

O sea con el sistema viejo teníamos 4 veces más chances de ganar que ahora.

Observación: dado un resultado para cada partido, contamos cuántas tarjetas de Prode nos hubiesen servido para ganar. Se puede hacer una cuenta distinta: dada una tarjeta de Prode que armamos, se cuenta cuántas combinaciones de resultados hacen que ganemos. ¿Hay alguna diferencia en el resultado final?

Ejercicio 4.1. Tenemos el siguiente juego: se tiran dos dados (no cargados), y se suman los resultados obtenidos. Si tenemos que apostar entre que la suma sea 9 ó 10, ¿qué nos conviene hacer?

Ejercicio 4.2. Se tiran dos dados repetidas veces hasta que suman 4 ó 7, en cuyo caso el juego se termina. ¿Cuál es la probabilidad de que se haya terminado por sumar 4 y cuál por sumar 7?

5. Números Enteros

Este capítulo está basado "fuertemente" en las notas de enteros de Teresa Krick (disponibles en la página web `http://mate.dm.uba.ar/~krick/algebra1-04.htm`).

5.1. Introducción. El conjunto de números enteros es

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\} = -\mathbb{N} \cup \{0\} \cup \mathbb{N}$$

(donde $-\mathbb{N} := \{-n \ : \ n \in \mathbb{N}\}$). ¿Por qué es útil trabajar con los números enteros? Si miramos el conjunto de números naturales, podemos considerar la operación de suma $+ : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$, que

1. es *asociativa*: para toda terna de números naturales (a, b, c) vale que $(a + b) + c = a + (b + c)$, y
2. es *conmutativa*: para todo par de números naturales (a, b) vale que $a + b = b + a$.

La operación inversa a la suma es la *resta*. El problema con la resta en los números naturales es que no se puede hacer siempre. Si $n > m$, hay un único natural x tal que $n = m + x$, y se define $x = n - m$. Pero si $n \leq m$, tal natural no existe y no se puede hacer la resta $n - m$. Precisamente, para poder hacer restas con cualquier par de números naturales, se introducen los negativos (y el 0). Una vez hecho esto, en $\mathbb{Z}$ se pueden hacer sumas y restas entre dos elementos cualesquiera. Con la suma, $\mathbb{Z}$ es un *grupo abeliano*.

Definición. Un grupo abeliano es un conjunto $\mathcal{A}$ con una operación binaria $*$ tal que

1. es *asociativa*: para toda terna de números naturales (a, b, c) vale que $(a * b) * c = a * (b * c)$,
2. es *conmutativa*: para todo par de números naturales (a, b) vale que $a*b = b*a$,
3. tiene *elemento neutro*: existe $e \in \mathcal{A}$ tal que para todo elemento $a \in \mathcal{A}$ se tiene $e * a = a$ (y como $*$ es conmutativa, también $a * e = a$),
4. tiene *inversos*: para todo a hay un elemento, $\bar{a}$, tal que $a * \bar{a} = e$.

El elemento neutro de la suma en el grupo $\mathbb{Z}$ es el 0, y si $n \in \mathbb{Z}$, su inverso (para la suma) es $\bar{n} = -n$. No es difícil probar usando las propiedades 1–4 la función $i : \mathcal{A} \to \mathcal{A}$ definida por $i(a) = \bar{a}$ es biyectiva.

Además de $(\mathbb{Z}, +)$, otros ejemplos de grupos abelianos son $(\mathbb{Q}\backslash\{0\}, \cdot)$ $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, etc.

El conjunto $\mathbb{Z}$ tiene dos operaciones importantes. Una de ellas es la suma, que lo hace un grupo conmutativo, como vimos. La otra, es el producto. Con el producto $\mathbb{Z}$ no es un grupo (sólo satisface las propiedades 1, 2 y 3, pero no hay inversos de elementos). Estas dos operaciones tienen una relación entre ellas:

- *Propiedad distributiva*: para toda terna (a, b, c) de elementos de $\mathbb{Z}$ vale que $a \cdot (b + c) = a \cdot b + a \cdot c$.

Con la suma y el producto, $\mathbb{Z}$ es un *anillo conmutativo*:

Definición. Un anillo conmutativo es una terna $(\mathcal{A}, +, \cdot)$ donde $\mathcal{A}$ es un conjunto y $+, \cdot$ son dos operaciones binarias tales que:

- $(\mathcal{A}, +)$ es un grupo abeliano,
- $(\mathcal{A}, \cdot)$ satisface las propiedades 1, 2 y 3,
- se cumple la propiedad distributiva.

Los anillos conmutativos juegan un rol muy importante en la matemática. Hay definiciones similares relajando un poco las propiedades anteriores (por ejemplo la existencia de neutro para el producto o la conmutatividad del producto) que tienen una rica teoría también, pero más complicada. Ejemplos de anillos conmutativos son $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$, los polinomios $(\mathbb{R}[x], +, \cdot)$, etc.

5.2. Divisibilidad.

Definición. Dados $a, b \in \mathbb{Z}$, decimos que a *divide* a b (y notamos $a \mid b$) si existe $q \in \mathbb{Z}$ tal que $b = qa$.

Ejemplos.
- $0 \mid 0$, y si $0 \mid n$ entonces $n = 0$.
- $1 \mid 9$ porque $9 = 9 \cdot 1$.
- $2 \mid -4$ porque $-4 = (-2) \cdot 2$.
- $3 \nmid 2$, ¿por qué?
- $n \mid 0$ para todo $n \in \mathbb{Z}$.

En este momento no podemos probar que $3 \nmid 2$, porque la definición nos dice cuándo un número divide a otro, pero para probar que $3 \nmid 2$ debemos ver que para ningún número entero q vale $3q = 2$. A continuación veremos algunas propiedades de la divisibilidad que nos permitirán concluir esto (y varias cosas más).

Propiedades 5.1. Dados a, b, c números enteros, vale que

1. Si $a \mid b$ entonces $a \mid bc$.
2. Si $a \mid b$ y $b \mid c$ entonces $a \mid c$.
3. Si $a \mid b$ y $a \mid c$ entonces $a \mid rb + sc$ para cualquier $r, s \in \mathbb{Z}$.
4. Si $a \mid b$ y $b \neq 0$ entonces $|a| \leq |b|$.
5. Dado $m \in \mathbb{Z}$ no nulo, $a \mid b$ si y sólo si $ma \mid mb$.
6. Si $a, b \in \mathbb{Z}$ son tales que $a \mid b$ y $b \mid a$ entonces $a = \pm b$.
7. $a \mid b \iff -a \mid b \iff a \mid -b \iff -a \mid -b$.

Demostración. Veamos cómo demostrar algunas de las propiedades y dejamos las restantes como ejercicio.

1. Como $a \mid b$ entonces $b = qa$ para algún $q \in \mathbb{Z}$. Multiplicando esta igualdad por c, obtenemos $bc = (qc)a$ con lo cual $a \mid bc$ (Observación: usamos aquí las propiedades conmutativa y asociativa del producto. ¿Dónde?).

4. Como antes, $b = qa$ para algún $q \in \mathbb{Z}$. Si tomamos valor absoluto, tenemos que $|b| = |a| \cdot |q|$. Como $b \neq 0$, debe ser $q \neq 0$ y $|q| \geq 1$, con lo cual $|b| = |a| \cdot |q| \geq |a|$.

5. Una implicación es fácil: si $a \mid b$ entonces $ma \mid mb$. La demostración es como la del punto 1, si $b = qa$, multiplicando por m, tenemos que $bm = q(am)$. Para la recíproca, si $bm = q(am)$, entonces $(b - qa)m = 0$. Como $m \neq 0$, tenemos que $b - qa = 0$ con lo cual $b = qa$ (notar que debemos usar que m no es cero para esta implicación).

6. Si $a = 0$ entonces $b = 0$, y recíprocamente. En este caso, vale que $a = \pm b$. Podemos suponer entonces que a y b son no nulos. Como $a \mid b$, tenemos que $|a| \leq |b|$. Como $b \mid a$, tenemos que $|b| \leq |a|$, luego $|a| = |b|$, con lo cual $a = \pm b$. □

En particular, la propiedad 4 nos permite probar que $3 \nmid 2$, dado que si $3 \mid 2$, entonces $|3| \leq |2|$, lo cual es falso.

Definición. Si $a \in \mathbb{Z}$, definimos el *conjunto de divisores de* a como $Div(a) = \{d \in \mathbb{Z} \,:\, d \mid a\}$. De manera análoga, $Div_+(a)$ es el conjunto de divisores positivos de a.

Ejercicio 5.1. Probar que si $a \neq 0$ el conjunto $Div(a)$ es finito y no vacío. ¿Cuántos elementos tiene como mínimo? ¿Quiénes son los divisores de 0?

Ejemplo. ¿Para qué valores enteros de n vale que $5n+1 \mid 7n+3$?
Por la propiedad 3 de 5.1, como $5n+1 \mid 5n+1$ y también $5n+1 \mid 7n+3$, tomando $r=-7$ y $s=5$, resulta que $5n+1 \mid (-7)(5n+1)+5(7n+3) = 8$. Luego $5n+1 \in Div(8)$, pero $Div(8) = \{\pm 1, \pm 2, \pm 4, \pm 8\}$. Si resolvemos cada ecuación lineal, tenemos que las única soluciones (enteras) son $n=-1$ y $n=0$.

Ejercicio 5.2. ¿Para qué valores de n, $(n+1) \mid (n^2-7)$?

Definición. Un número entero m se dice *irreducible* si tiene exactamente 4 divisores. Un número que no es irreducible se llama *compuesto*.

Notar que todo número $m \neq \pm 1$ tiene al menos 4 divisores: $m, -m, 1, -1$. Notar también que 1 y -1 no son irreducibles. Una definición equivalente entonces es: m es irreducible si $m \neq \pm 1$ y $Div(m) = \{\pm m, \pm 1\}$.

Definición. Un número entero $p \neq \pm 1, 0$ se dice *primo* si cada vez que $p \mid ab$ para un par de números enteros a, b, se tiene que $p \mid a$ ó $p \mid b$.

La noción de número primo que se suele aprender en la escuela es la de irreducible. Ambas nociones coinciden, como veremos. Esto es, $p \in \mathbb{Z}$ es primo si y solo si es irreducible. Se usan ambos nombres porque hay anillos en los que las dos nociones son distintas. Lo que vale en cualquier anillo es que p primo implica p irreducible.

Proposición 5.2. *Si p es primo entonces es irreducible.*

Demostración. Supongamos que $a \in \mathbb{Z}$ es un divisor de p. Luego $p = qa$ para algún $q \in \mathbb{Z}$. En particular, $p \mid qa$. Luego, al ser p primo, vale que $p \mid a$ ó $p \mid q$. Si $p \mid a$, $a = \pm p$ por la propiedad 6 de 5.1. Si $p \mid q$, nuevamente por la propiedad 6, $q = \pm p$ con lo cual $a = \pm 1$. Luego los únicos divisores de p son ± 1 y $\pm p$. □

Ejemplo. Verifiquemos que 3 y 5 son irreducibles, pero 4 no lo es (a esta altura no tenemos manera sencilla de probar que un número es primo). Como los divisores de n están entre $-|n|$ y $|n|$ para todo $n \neq 0$, para ver que 3 es irreducible alcanza con ver si 2 y -2 lo dividen. Como no lo dividen, se tiene $Div(3) = \{\pm 1, \pm 3\}$ y por lo tanto es irreducible. Con 5 es similar, hay que chequear que $2 \nmid 5$, $3 \nmid 5$ y $4 \nmid 5$ (esto automáticamente probaría que $-2 \nmid 5$, $-3 \nmid 5$ y $-4 \nmid 5$, por la propiedad 7).

Teorema 5.3 (Algoritmo de división)**.** *Dados $a, b \in \mathbb{Z}$ con $a \neq 0$, existen únicos $q, r \in \mathbb{Z}$ tales que*

$$b = qa + r \qquad y \qquad 0 \leq r < |a|$$

Al número q se lo llama *el cociente* de la división de b por a y al número r *el resto*. A veces el resto lo notaremos $r_a(b)$.

En la demostración, para un número $x \neq 0$ tomamos $\text{signo}(x) = 1$ si $x > 0$ y $\text{signo}(x) = -1$ si $x < 0$. Observemos que $x\,\text{signo}(x) = |x|$.

Demostración. Consideremos el conjunto $\mathcal{P} = \{b - qa \,:\, q \in \mathbb{Z}\} \cap (\mathbb{N} \cup \{0\})$. Este es claramente un subconjunto de $\mathbb{N}_0$. Veamos que $\mathcal{P}$ es no vacío. Si tomamos $q =$

$-(|b|+1)\,\text{signo}(a)$, al calcular $b - qa = b + (|b|+1)|a| > 0$ por ser a un entero no nulo. Luego, por el Principio de Buena Ordenación, el conjunto $\mathcal{P}$ tiene un primer elemento, al que llamamos r. Ese primer elemento es de la forma $r = b - q_0 a$ para algún $q_0 \in \mathbb{Z}$. Afirmamos que esta elección satisface las condiciones y además es la única que lo hace.

• Veamos que $0 \leq r < |a|$. Si no es así, $b - aq_0 \geq |a|$, con lo cual $0 \leq b - aq_0 - |a| < r$. Pero $b - q_0 a - |a| = b - (q_0 - \text{signo}(a))a$, por lo que $b - q_0 a - |a| \in \mathcal{P}$ y entonces r no es el menor elemento de $\mathcal{P}$, lo que es un absurdo. Luego $0 \leq r < |a|$.

• Veamos la unicidad del resto y el cociente. Si $b = q_1 a + r_1 = q_2 a + r_2$ con $0 \leq r_i < |a|$, entonces tenemos que $r_1 - r_2 = a(q_2 - q_1)$, con lo cual $a \mid r_1 - r_2$. Por la Propiedad 4, tenemos que $r_1 - r_2 = 0$ ó $|a| \leq |r_1 - r_2|$. Como $|r_1 - r_2| < |a|$ (porque $-a < -r_2 \leq r_1 - r_2 \leq r_1 < a$), debemos tener $r_1 - r_2 = 0$, es decir $r_1 = r_2$. Esto, a su vez, implica que $b - q_1 a = b - q_2 a$, por lo que $(q_1 - q_2)a = 0$. Como $a \neq 0$, esto significa que $q_1 - q_2 = 0$, es decir, $q_1 = q_2$. □

Ejemplo. Calculemos el cociente y resto de la división de 27 por 4. Tenemos que considerar los números de la forma $27 - 4q$ que sean ≥ 0 y tomar el más chico de ellos. Si tomamos $q = 0, 1, 2, \ldots$ obtenemos $27, 23, 19, 15, 11, 7, 3$. El 3 se obtiene para $q = 6$, y con $q \geq 7$ ya se tienen números negativos. Esto dice que el cociente es 6 y el resto es 3. Es interesante observar que el algoritmo es una formalización del concepto intuitivo, o informal, que uno tiene de la división. La división consiste en repartir. Si se quiere repartir 27 objetos entre 4 personas, se le distribuye un objeto a cada una. Quedan 23, por lo que se puede seguir repartiendo. Se distribuye un segundo objeto, y quedan 19, por lo que se puede seguir repartiendo. Se distribuye un tercer objeto y quedan 15, etc. Esto se hace hasta que se reparten 6 objetos y quedan 3, y no se pueden repartir más. Precisamente, esto es considerar los números de la forma $27 - 4q$.

Es importante entender, según la definición, qué sucede en los casos en que a ó b son negativos.

Ejemplo. Calculemos el cociente y el resto de dividir -17 por -3. Queremos que $0 \leq -17 + 3 \cdot q < 3$, es decir $17 \leq 3q < 20$. Es claro que $q = 6$, y $r = 1$.

Proposición 5.4. *Si $a, b \in \mathbb{Z}$, $a \neq 0$, entonces $a \mid b$ si y solo si $r_a(b) = 0$.*

Demostración. Es claro de la unicidad del resto. □

Definición. Dados $a, b \in \mathbb{Z}$ con a ó b no nulo, definimos el *máximo común divisor de a y b* como

$$\text{mcd}(a, b) = (a : b) = \text{máx}\,\{d \in \mathbb{Z} \ : \ d \mid a \text{ y } d \mid b\}$$

Observación. Esta definición tiene sentido porque $Div(a) \cap Div(b)$ es no vacío (está al menos el número 1 en ambos) y alguno de ellos es acotado (porque $a \neq 0$ ó $b \neq 0$).

Ejemplos. Calculemos algunos mcd (se pueden encontrar a mano):

1. $(2 : 5) = 1$, porque $Div(2) = \{\pm 1, \pm 2\}$ y $2 \nmid 5$.
2. $(4 : 6) = 2$.
3. $(-10 : -14) = 2$.

Observación. Si $a, b \in \mathbb{Z}$, alguno no nulo, entonces:

- $(a : b) \geq 1$.

- $(a : b) = (-a : b) = (a : -b) = (-a, -b)$.
- $(a : 0) = |a|$.
- $(a : b) = |a|$ si y sólo si $a \mid b$.

La segunda igualdad y la última nos dicen que solo precisamos poder calcular de manera eficiente el máximo común divisor de números naturales. El siguiente lema es fundamental para probar las propiedades del máximo común divisor:

Lema 5.5. *Dados $a, b \in \mathbb{Z}$ con alguno no nulo, $(a : b) = (a : b + ka)$ para cualquier $k \in \mathbb{Z}$.*

Demostración. Definimos

$$\mathcal{P}_1 = \{d \in \mathbb{Z} \ : \ d \mid a \text{ y } d \mid b\}, \qquad \mathcal{P}_2 = \{d \in \mathbb{Z} \ : \ d \mid a \text{ y } d \mid b + ka\}.$$

Veremos que estos dos conjuntos son iguales. Es claro que eso termina la demostración.

- $\mathcal{P}_1 \subset \mathcal{P}_2$, ya que por la Propiedad 3 de divisibilidad, si $d \mid a$ y $d \mid b$ entonces $d \mid b + ka$ para cualquier $k \in \mathbb{Z}$.
- $\mathcal{P}_2 \subset \mathcal{P}_1$, ya que por la misma propiedad, si $d \mid a$ y $d \mid b + ka$, entonces $d \mid (b + ka) + (-k)a = b$.

□

Es computacionalmente muy costoso conocer los divisores de un número. Dados dos números, entonces, podría pensarse que calcular el mcd es más difícil, porque si se aplica la definición, hay que calcular los divisores de ambos números. Sorprendentemente, no es así.

Teorema 5.6 (Algoritmo de Euclides)**.** *Dados $a, b \in \mathbb{N}$, construimos una sucesión de cocientes y restos sucesivos de la siguiente manera:*

$$\begin{aligned}
a &= bq_1 + r_1 && 0 < r_1 < b \\
b &= r_1 q_2 + r_2 && 0 < r_2 < r_1 \\
r_1 &= r_2 q_3 + r_3 && 0 < r_3 < r_2 \\
&\vdots && \vdots \\
r_n &= r_{n+1} q_{n+2} + r_{n+2} && 0 < r_{n+2} < r_{n+1} \\
r_{n+1} &= r_{n+2} q_{n+3}
\end{aligned}$$

Luego $(a : b) = r_{n+2}$. Además, reescribiendo cada r_i en términos de los anteriores, encontramos $r, s \in \mathbb{Z}$ tales que $(a : b) = ar + bs$.

Antes de hacer la demostración, veamos un ejemplo de lo que estamos afirmando para entenderlo mejor. Supongamos que queremos calcular $(1272 : 708)$. Luego comenzamos a calcular los cocientes sucesivos, y tenemos:

$$\begin{aligned}
1272 &= 708 \cdot 1 + 564 \\
708 &= 564 \cdot 1 + 144 \\
564 &= 144 \cdot 3 + 132 \\
144 &= 132 \cdot 1 + 12 \\
132 &= 12 \cdot 11
\end{aligned}$$

Luego $(1272 : 708) = 12$. Además,

$$\begin{aligned} 12 = 144 - 132 = 144 - (564 - 144 \cdot 3) = 144 \cdot 4 - 564 \\ = (708 - 564) \cdot 4 - 564 = 708 \cdot 4 - 564 \cdot 5 \\ = 708 \cdot 4 - (1272 - 708) \cdot 5 = 708 \cdot 9 - 1272 \cdot 5. \end{aligned}$$

O sea logramos escribir el 12 como combinación lineal de 1272 y 708.

Demostración del Algoritmo. Veamos primero que $r_{n+2} = (a : b)$. Utilizando el lema 5.5, vemos que $(a : b) = (bq_1 + r_1 : b) = (r_1 : b)$. De manera análoga, $(r_1 : b) = (r_1 : r_2) = \cdots = (r_{n+1} : r_{n+2}) = r_{n+2}$ porque $r_{n+2} \mid r_{n+1}$.

Veamos entonces que $(a : b)$ es combinación lineal de a y de b. Afirmamos que cada r_i es combinación lineal de a y de b, y probaremos esto por inducción.

$$\begin{aligned} r_1 &= a \cdot 1 + b(-q_1) \\ r_2 &= r_1(-q_2) + b = (a \cdot 1 + b(-q_1))(-q_2) + b = a(-q_2) + b(1 + q_1 q_2). \end{aligned}$$

Supongamos que

$$\begin{aligned} r_i &= at_i + bs_i \\ r_{i+1} &= at_{i+1} + bs_{i+1}, \end{aligned}$$

luego $r_i = q_{i+2} r_{i+1} + r_{i+2}$, con lo cual

$$\begin{aligned} r_{i+2} = r_i - q_{i+2} r_{i+1} = at_i + bs_i - q_{i+2}(at_{i+1} + bs_{i+1}) \\ = a(t_i - q_{i+2} t_{i+1}) + b(s_i - q_{i+2} s_{i+1}). \end{aligned}$$

□

Teorema 5.7. *Sean $a, b \in \mathbb{Z}$, no ambos nulos. Si $\mathcal{P} = \{xa + yb \,:\, x, y \in \mathbb{Z}\} \cap \mathbb{N}$, entonces $(a : b)$ es el primer elemento de $\mathcal{P}$.*

Dicho en otras palabras, $(a : b)$ es el menor número natural que se puede escribir como combinación lineal de a y de b.

Demostración. Como $(a : b) \in \mathcal{P}$, el conjunto $\mathcal{P}$ es no vacío y tiene un primer elemento d_0. Si $r \in \mathcal{P}$, entonces $r = ax_0 + by_0$ para algún par de elementos $x_0, y_0 \in \mathbb{Z}$. Como $(a : b) \mid a$ y $(a : b) \mid b$, se tiene que $(a : b) \mid r$. Luego todos los elementos de $\mathcal{P}$ son divisibles por $(a : b)$, en particular $(a : b) \mid d_0$. Luego $(a : b) \leq d_0$ por ser ambos números naturales. Al estar $(a : b)$ en $\mathcal{P}$, resulta $(a : b) = d_0$. □

Dado $n \in \mathbb{Z}$, escribamos $\langle n \rangle = \{kn \,:\, k \in \mathbb{Z}\}$ el conjunto de los múltiplos de n. La demostración anterior dice que el conjunto $\mathcal{P} = \{xa + yb \,:\, x, y \in \mathbb{Z}\}$ coincide con el conjunto $\langle (a : b) \rangle$. Más aun: se puede definir $(a : b)$ como el número $d \geq 0$ tal que $\langle d \rangle = \{xa + yb\}$. Esto sugiere que extendamos la definición del máximo común divisor al caso en que ambos números son 0 por $(0 : 0) = 0$.

El hecho de poder escribir el máximo común divisor de dos números como combinación lineal implica otras propiedades importantes.

Proposición 5.8. *Sean $a, b, c \in \mathbb{Z}$.*

1. *Si $a \mid bc$ y $(a : b) = 1$, entonces $a \mid c$.*
2. *Si $(a : b) = 1$, $a \mid c$ y $b \mid c$, entonces $ab \mid c$.*
3. *$(ac : bc) = |c|(a : b)$.*
4. *Si a, b no son ambos nulos, entonces $\left(\frac{a}{(a:b)} : \frac{b}{(a:b)}\right) = 1$*

Demostración. 1. Como $a \mid bc$, existe $q \in \mathbb{Z}$ tal que $bc = aq$. Además, como $(a : b) = 1$, existen enteros r, s tales que $ra + sb = 1$. Multiplicando esta igualdad por c, tenemos

$$c = rac + sbc = acr + saq = a(cr + qs).$$

2. Como $a \mid c$ y $b \mid c$, existen $q_1, q_2 \in \mathbb{Z}$ tales que $c = aq_1$ y $c = bq_2$. Por otra parte, existen $r, s \in \mathbb{Z}$ tales que $1 = ar + bs$. Multiplicando por c, tenemos que

$$c = acr + bcs = abq_2r + baq_1s = ab(q_2r + q_1s).$$

3. Por el teorema anterior, $(ac : bc)$ es el menor natural en el conjunto

$$\{xac + ybc \ : \ x, y \in \mathbb{Z}\}.$$

Pero este conjunto coincide con el conjunto $\{|c|(xa + yb) \ : \ x, y \in \mathbb{Z}\}$, que a su vez coincide con multiplicar por $|c|$ a todos los elementos del conjunto $\{xa + yb \ : \ x, y \in \mathbb{Z}\}$. Luego, el menor natural de $\{xac + ybc\}$ es el producto entre $|c|$ y el menor natural de $\{xa + yb\}$.

4. $(a : b) = \left(\frac{a}{(a:b)}(a : b) : \frac{b}{(a:b)}(a : b)\right) = (a : b)\left(\frac{a}{(a:b)} : \frac{b}{(a:b)}\right)$, donde la última igualdad sale del ítem anterior. Como $(a : b) \neq 0$ porque a, b no son ambos nulos, podemos simplificar y obtenemos lo buscado.

□

Como se ve en la proposición anterior, el caso en que el máximo común divisor de dos números es 1 es particularmente importante; es por eso que tiene un nombre.

Definición. Dados $a, b \in \mathbb{Z}$ no nulos, decimos que son *coprimos* si $(a : b) = 1$.

Ahora sí estamos en las condiciones de probar uno de los resultados más importantes de los números enteros:

Teorema 5.9. *Si p es un número irreducible entonces es primo.*

Demostración. Tomemos dos enteros a, b cualesquiera tal que $p \mid ab$. Queremos probar que $p \mid a$ o $p \mid b$.

Sea $d = (p : a)$. Como p es irreducible, $d \mid p$ y $d \geq 0$, entonces $d = 1$ ó $d = |p|$. Si $d = |p|$, entonces $p \mid a$ y listo. En caso contrario, $(p : a) = 1$. La parte 1 de la proposición anterior nos dice que como $p \mid ab$ y es coprimo con a, debe dividir a b. □

Vamos a usar este resultado para probar que todo entero no nulo se factoriza de manera única. Pero antes, recordemos la definición de mínimo común múltiplo.

Definición. Si $a, b \in \mathbb{Z}$, ambos no nulos, definimos el *mínimo común múltiplo* de a y b (y lo notamos $[a : b]$ o $\operatorname{mcm}(a, b)$) como el mínimo del conjunto $\langle a \rangle \cap \langle b \rangle \cap \mathbb{N}$. En otras palabras, $[a : b]$ es el menor número natural que es a la vez múltiplo de a y de b. Como $|ab| \in \langle a \rangle \cap \langle b \rangle \cap \mathbb{N}$, el conjunto es no vacío y por lo tanto tiene mínimo, por el principio de buena ordenación.

Proposición 5.10. *Dados $a, b \in \mathbb{Z}$ no nulos, $[a : b](a : b) = |ab|$.*

Demostración. Si $M = [a : b]$, entonces $a \mid M$ y $b \mid M$. Digamos $M = aq_1 = bq_2$. Luego $b \mid aq_1$ con lo cual $\frac{b}{(a:b)} \mid q_1$ y $\frac{ab}{(a:b)} \mid M$. Al ser M no nulo, $M \geq \frac{|ab|}{(a:b)}$. Pero M es el más chico de los múltiplos comunes positivos, y $\frac{|ab|}{(a:b)}$ es un tal múltiplo, con lo cual $M = \frac{|ab|}{(a:b)}$. □

Veamos ahora sí la factorización de enteros en primos.

Proposición 5.11. *Todo entero $a \neq 0, \pm 1$ es divisible por un número primo.*

Demostración. Como los primos que dividen a a son los mismos que dividena $|a|$, podemos suponer que $a \in \mathbb{N}$ y $a \geq 2$. En este conjunto podemos usar inducción global.

- Si $a = 2$, es primo, en particular hay un número primo que lo divide.
- Supongamos que todos los números a con $2 \leq a \leq k$ son divisibles por un número primo, y veamos que $k+1$ también lo es. Si $k+1$ no tiene divisores positivos además del 1 y $k+1$, es irreducible y por lo tanto, primo. En este caso hay un primo que lo divide (él mismo). Si no, hay un número d, con $2 \leq d \leq k$ tal que $d \mid k+1$. Por hipótesis inductiva, existe un número primo p tal que $p \mid d$, luego (por transitividad), $p \mid k+1$.

□

Teorema 5.12 (Teorema Fundamental de la Aritmética)**.** *Todo número $a \in \mathbb{Z}$, con $a \neq 0, \pm 1$, se escribe de forma única como*

$$a = s \cdot p_1^{r_1} \cdots p_n^{r_n}$$

donde $s = \pm 1$, los p_i son números primos positivos distintos, y $r_i \in \mathbb{N}$ para $1 \leq i \leq n$.

Es importante entender qué quiere decir *única* en el enunciado. Consideramos aquí que dos factorizaciones son iguales si difieren únicamente en el orden en que aparecen los primos. En otras palabras, el teorema asegura que si

$$a = s \cdot p_1^{r_1} \dots p_n^{r_n} = s' \cdot q_1^{t_1} \dots q_m^{t_m},$$

donde los p_i son primos distintos entre sí y los q_i son primos distintos entre sí, entonces $s = s'$ (es decir, los signos coinciden), $n = m$ (es decir, la cantidad de factores coincide) y existe una función biyectiva $\sigma : \{1, \dots, n\} \to \{1, \dots, n\}$ tal que para todo $i \in \{1, \dots, n\}$ se cumple que $p_i = q_{\sigma(i)}$ y $r_i = t_{\sigma(i)}$ (es decir, los primos y sus potencias coinciden).

Demostración. Comencemos por probar la existencia de la factorización. Como todo número entero a no nulo se escribe como $a = \text{signo}(a)|a|$ y $\text{signo}(a) = \pm 1$, podemos suponer que $a \geq 2$. Hacemos inducción global en a:

- Si $a = 2$, como 2 es primo, a se escribe como producto de primos a potencias: $a = 1 \cdot 2^1$.
- Supongamos que todos los números $2 \leq a \leq k$ se escriben como producto de primos a potencias, y veamos que $k+1$ también. Si $k+1$ es primo, listo. Si no, existe un primo que lo divide, por la proposición anterior. Digamos $2 \leq p \leq k$, y $p \mid k+1$. Es decir, $k+1 = p \cdot m$. Como $p > 1$, resulta $m < k+1$. Por Hipótesis Inductiva, $m = p_1^{r_1} \dots p_n^{r_n}$ con lo cual $k+1 = p.p_1^{r_1} \dots p_n^{r_n}$, que es un producto de primos a potencias. Lo único que falta ver es que se puede escribir como producto de potencias de primos *distintos*. Si p no es ninguno de los otros primos, es decir, si $p \neq p_i$ para todo i, entonces ya tenemos la factorización buscada. En cambio, si $p = p_j$ para algún j, entonces la factorización será $k+1 = p_1^{r_1} \dots p_j^{r_j+1} \dots p_n^{r_n}$.

Nos resta probar la unicidad. Para esto, podemos "estirar" las factorizaciones, y escribir $a = p_1 \cdots p_N = q_1 \cdots q_M$. Aquí las potencias son todas 1, pero los primos pueden repetirse (o sea p_1 puede coincidir con p_2, etc.). Es claro que si probamos que las factorizaciones "estiradas" son únicas, entonces habremos probado que las factorizaciones como en el enunciado también son únicas. Queremos hacer inducción en el número de primos de la factorización de a. En concreto, miremos la siguiente afirmación:
Afirmación: $P(k)$: Si un número entero $a \geq 2$ tiene una factorización con k números primos, entonces la factorización es única.

- Miremos $k = 1$, $P(1)$ es la afirmación "si a tiene una factorización con un solo número primo, entonces esta factorización es única".

  Pero si a tiene un único primo en su factorización, entonces a es primo. Luego si $a = q_1 \dots q_r$, como un número primo tiene sólo 2 divisores positivos, $r = 1$, y $a = q_1$.
- Supongamos que es cierto para k, y veámoslo para $k+1$: Supongamos que

  $$a = p_1 \dots p_{k+1} = q_1 \dots q_m.$$

  Entonces $p_1 \mid q_1 \dots q_m$. Como p_1 es primo, si divide a un producto de números, divide a alguno de ellos, con lo cual $p_1 \mid q_i$ para algún $1 \leq i \leq m$. Al ser q_i primo, tiene un único divisor positivo distinto de 1, luego $p_1 = q_i$. Si cancelamos p_1, tenemos que

  $$p_2 \dots p_{k+1} = \prod_{\substack{1 \leq j \leq m \\ j \neq i}} q_j$$

  Luego tenemos dos factorizaciones que coinciden, y la factorización de la izquierda tiene k términos, con lo cual, por hipótesis inductiva, $m - 1 = k$, y los primos son los mismos.

□

Ejemplos. Calculemos algunas factorizaciones:

1. $28 = 2^2 \cdot 7$.
2. $-45 = (-1) \cdot 3^2 \cdot 5$.

Veamos algunas aplicaciones directas del Teorema Fundamental de la Aritmética:

Ejercicio 5.3. ¿Quiénes son los divisores de 28?

Si $a \mid 28$, entonces $28 = aq$ con algún $q \in \mathbb{Z}$. Supongamos que a es positivo, y miremos su factorización, digamos que $a = p_1^{r_1} \cdots p_n^{r_n}$, vemos que

$$2^2 \cdot 7 = p_1^{r_1} \cdots p_n^{r_n} q$$

A pesar de que no conocemos la factorización de q, esta sólo puede agrandar los exponentes de los primos, y tal vez agregar nuevos primos. Como la factorización de 28 es única, $p_i = 2$ ó 7 para todos los primos de a. Luego $a = 2^{r_1} \cdot 7^{r_2}$. Además, si miramos los exponentes del primo 2 en a y en q, su suma debe ser el exponente del primo 2 en 28, que es 2. Luego, $0 \leq r_1 \leq 2$ y $0 \leq r_2 \leq 1$. Para cada elección de potencias para a, tenemos una elección de potencias para q que nos da la igualdad, a saber $q = 2^{2-r_1} \cdot 7^{1-r_2}$ (notar que $2 - r_1 \geq 0$ y $1 - r_2 \geq 0$). En definitiva, pudimos calcular todos los divisores positivos de 28, a saber: $\{2^{r_1} \cdot 7^{r_2} \ : \ 0 \leq r_1 \leq 2, \ 0 \leq r_2 \leq 1\} = \{1, 2, 4, 7, 14, 28\}$.

Ejercicio 5.4. Si $b = p_1^{r_1} \cdots p_n^{r_n}$, ¿quiénes son los divisores de b? ¿Cuántos hay?

Definición. Si $a \in \mathbb{Z}$ es no nulo, y p es un número primo, definimos la *valuación* de p en a (y la notamos $v_p(a)$) como la máxima potencia de p que divide a a, o sea

$$v_p(a) = \max \{n \in \mathbb{N}_0 \ : \ p^n \mid a\}$$

Así, $v_2(12) = 2$, $v_3(12) = 1$ y $v_5(12) = 0$.

Ejercicio 5.5. Si $a = p_1^{r_1} \cdots p_n^{r_n}$, donde los primos de la factorización son distintos, ¿cuánto vale $v_{p_1}(a)$?

Luego si $a \in \mathbb{Z}$, y $a \neq 0$, podemos escribir

$$a = \text{signo}(a) \prod_{p \text{ primo}} p^{v_p(a)}$$

Proposición 5.13. *La valuación satisface las siguientes propiedades:*

1. *Si $p^n \mid a$ entonces $v_p(a) \geq n$.*
2. *$a \mid b \iff v_p(a) \leq v_p(b)$ para todo primo p.*
3. *$v_p(ab) = v_p(a) + v_p(b)$ para todo primo p.*

Dejamos como ejercicio la demostración de estas propiedades ya que son consecuencia inmediata del Teorema Fundamental de la Aritmética.

Corolario 5.14. *Si $a, b \in \mathbb{Z}$ entonces $a \mid b$ si y sólo si $a^n \mid b^n$ para todo $n \in \mathbb{N}$.*

Demostración: $a \mid b \iff v_p(a) \leq v_p(b)$ para todo primo p. Multiplicando por n, esto es equivalente a pedir que $nv_p(a) \leq nv_p(b)$ para todo primo p. Como $v_p(a^n) = nv_p(a)$, esto último pasa si y sólo si $a^n \mid b^n$. □

Corolario 5.15. *$\sqrt{2}$ no es un número racional.*

Demostración: Supongamos que $\sqrt{2} = \frac{a}{b}$. Luego, multiplicando por b y elevando al cuadrado tenemos que $2b^2 = a^2$. Mirando la valuación en 2, venemos que $1 + 2v_2(b) = 2v_2(a)$. Pero el número de la izquierda es impar, y el de la derecha es par, lo que es un absurdo. □

Ejercicio: ¿Qué números $a \in \mathbb{Z}$ satisfacen que $a^2 \mid 108$?

Solución: Si $a^2 \mid 108$, para todo primo p, $2v_p(a) \leq v_p(108)$. Como $108 = 2^2.3^3$, $v_2(108) = 2$, $v_3(108) = 3$ y $v_p(108) = 0$ para todo primo $p \neq 2, 3$. Luego $a = 2^r.3^s$ con $2r \leq 2$ y $2s \leq 3$, o sea $r = 0, 1$ y $s = 0, 1$. Estos números son los 8 números enteros: $-6, -3, -2, -1, 1, 2, 3, 6$.

Ejercicio: Si $n \in \mathbb{N}$, y $a \in \mathbb{N}$, probar que $\sqrt[n]{a} \in \mathbb{N}$ si y sólo si $n \mid v_p(a)$ para todo primo p.

Ejercicio: ¿Cuál es la mayor potencia de 3 que divide a 38!?

Solución: $38! = 1 \cdot 2 \cdot 3 \cdots 38$, luego debemos contar cuantas potencias de 3 aparecen en este producto. O sea debemos calcular $v_3(1) + \cdots + v_3(38)$. Los números que son divisibles por 3 y no por 9 tienen valuación 1, los que son divisibles por 9 pero no por 27 tienen valuación 2 y lo que son divisibles por 27 tienen valuación 3 (no hay múltiplos de 81 en este rango).

Si n es múltiplo de 3, $n = 3q$. Como $1 \leq n \leq 38$, $1 \leq q \leq 12$. Luego hay 12 múltiplos de 3. De igual manera, vemos que hay el cociente de dividir 38 por 9, o

sea 4 múltiplos de 9 y un sólo múltiplo de 27. Luego nuestra suma es: $1.(12-4)+2.(4-1)+3 = 12+4+1 = 17$. ¿Cuál es la mayor potencia de 5 que divide a 100!?

Proposición 5.16. *Si $a, b \in \mathbb{Z}$ con alguno no nulo, entonces*

$$(a:b) = \prod_{p \text{ primos}} p^{\min\{v_p(a), v_p(b)\}}.$$

Demostración: Si llamamos $d = \prod_{p \text{ primos}} p^{\min\{v_p(a), v_p(b)\}}$, es claro que $d \mid a$ y $d \mid b$. Si $d' \in \mathbb{N}$ es tal que $d' \mid a$ y $d' \mid b$, entonces $v_p(d') \leq v_p(a)$ y $v_p(d') \leq v_p(b)$ para todo p primo. Luego $v_p(d') \leq \min\{v_p(a), v_p(b)\} = v_p(d)$, o sea $d' \mid d$. Esto implica que $d' \leq d$ como queríamos ver. □

Ejercicio: Enunciar y demostrar un resultado análogo para el mínimo común múltiplo.

5.3. Números Primos. Gracias al Teorema Fundamental de la Aritmética, muchas cuentas se simplifican mirando los primos que aparecen en la factorización de un número. Luego los primos son como "los ladrillos" con los que se construyen todos los enteros (con el producto). En particular, una pregunta natural es saber cosas sobre los primos, por ejemplo ¿cuantos hay? Como construirlos? ¿Hay fórmulas?

La mayoría de estas preguntas son mucho mas difíciles de lo pensado, y su naturaleza es muchas veces mas analítica que algebraica (muchos resultados utilizan herramientas de análisis en sus demostraciones). Comenzemos calculando los primos entre 1 y 20 usando la Criba de Eratóstenes: listamos todos los números entre 2 y 20. Tomamos el primer número no tachado p (en este caso $p = 2$), y ese número es primo. Vamos tachando cada número que obtenemos al movernos desde p por la lista de números p lugares hacia la derecha hasta llegar al final de la lista. Una vez hecho esto, tomamos el primer número no tachado a la derecha de p, y debe también ser primo. Llamamos p a este nuevo número, y repetimos el proceso.

Si uno hace este proceso un par de veces, se da cuenta que con los últimos números primos no tacha nada de la lista que tiene, luego uno se puede preguntar si puede cortar antes el proceso, y deducir que todos los números a la derecha de donde estamos parados son primos. Por ejemplo, el 14 lo tachamos con el número 2, luego no hizo falta usar el número 7. ¿Cuál es el primer número múltiplo de 7 que tachamos por primera vez con el 7? ¿Será que siempre podemos mirar hasta $\sqrt{n}$? La respuesta a esta pregunta es el ejercicio 6 de la práctica 4, que dice que la respuesta es afirmativa. En particular, para calcular los número primos menores que 10.000, basta con tachar los múltiplos de los primos que aparecen antes de 100. Una vez que tachamos todos los múltiplos de los primos menores que 100, todo lo que quedo sin tachar es necesariamente un número primo.

La desventaja de este método es que si tenemos la criba armada para los números menores que 100 y la queremos extender hasta 120, debemos comenzar de nuevo con los primos para tachar los números agregados.

Pregunta: ¿Cuántos primos hay?

Teorema 5.17 (Euclídes)**.** *Existen infinitos números primos.*

Demostración: Existen muchas demostraciones de esta afirmación, algunas usando métodos realmente ingeniosos. La que presentaremos es la demostración original de Euclídes. Supongamos que son finitos, digamos que $p_1, \ldots, p_n$ son todos los primos. Miremos el número $N = p_1 \cdots p_n + 1$. Por el T.F.A. existe un número primo q que divide a N. Como estamos suponiendo que hay finitos primos, $q = p_i$ para algún i. Luego $q \mid p_1 \cdots p_n$ y $q \mid p_1 \cdots p_n + 1$ con lo cual $q \mid 1$ lo que es un absurdo. □

Si definimos $f(n) = n$-ésimo número primo, no se conoce una fórmula para calcular $f(n)$. Por ejemplo, ¿existe un polinomio $P(n)$ que al ser evaluado en los números naturales produzca los números primos? O pidiendo un poco menos, ¿existe un polinomio $P(n)$ que al ser evaluado en los naturales produzca siempre números primos? (aunque no necesariamente todos ellos).

En 1772 Euler encontró que el polinomio $P(n) = n^2 + n + 41$ asume valores primos para $n = 0, 1, \ldots, 39$. Desafortunadamente, $P(40) = 41^2$. No es difícil probar que un polinomio al ser evaluado en números naturales no puede dar siempre números primos a no ser que sea el polinomio constante (esto lo probaremos en el próximo capítulo). Esto muestra que si existe una fórmula para producir números primos, no puede ser muy sencilla. Una variante es estudiar "ciertos números primos". O sea tratar de calcular un subconjunto de los números primos que sea fácil (computacionalmente por ejemplo) de describir. Fue así que surgieron algunas familias con distintos intereses:

- **Primos de Fermat:** Los primos de Fermat (estudiados por Pierre de Fermat, 1601-1665) son los primos que tienen la forma $2^n + 1$. Es fácil ver (y un ejercicio de la práctica) que si $2^n + 1$ es primo, entonces n es una potencia de dos. Así, los primos de Fermat son los números de la sucesión $F_n = 2^{2^n} + 1$ que son primos.

  Para los valores $n = 0, 1, 2, 3, 4$, se obtienen los valores $3, 5, 16, 257$ y 65537 que efectivamente son primos. Al día de hoy no se conoce ningún otro número primo dentro de esta sucesión de números (usando una computadora se puede ver que $F_5 = 4294967297 = 641.6700417$). Dentro de las propiedades que satisfacen, las más importantes son las siguientes:
  1. $F_n = \prod_{i=0}^{n-1} F_i + 2$.
  2. Un polígono regular de n lados se puede construir con regla y compás si y sólo si $n = 2^k \prod F_i$ (o sea el producto de una potencia de dos con algunos primos de Fermat distintos).

  No se sabe si hay infinitos primos de Fermat o no, aunque se sospecha que la respuesta es negativa (a pesar de que algunos matemáticos no concuerdan con esta creencia general). Mirar la página web *http://www.fermatsearch.org/* para una búsqueda de tales primos.
- **Primos de Mersenne:** los primos de Mersenne (estudiados por Marin Mersenne, 1558-1648) son los primos que tienen la forma $M_n = 2^n - 1$. Los ocho primeros números primos de Mersenne son $3, 7, 31, 127, 8191, 131071$, 524287 y 2147483647. Estos números están relacionados con los llamados *números perfectos*. Un número es perfecto si es igual a la suma de sus divisores propios. Euclides probó que si M_n es primo, entonces $M_n(M_n + 1)/2$ es un número perfecto.

  No es difícil probar (y es un ejercicio de la práctica) que si M_n es primo, entonces n debe ser primo. La recíproca de esta afirmación no es cierta, por

ejemplo $M_{11} = 23.89$ a pesar de que 11 es primo. Mersenne conjeturó que M_p es primo para los primos $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$ y 257 (claramente sin tener una calculadora a mano!). Usando computadoras, se puedo verificar que estos números son primos salvo para $p = 67$ y 257. Además, en esta lista faltan los primos para $p = 61, 89$ y 107.

Una gran ventaja que tienen los primos de Mersenne es que existe un algoritmo (debido a Lucas y mejorado por Lehmer y conocido como el test de Lucas-Lehmer) que decide si M_n es primo o no dependiendo solo del tamaño de n. Así se puede probar que ciertos números de Mersenne son primos para grandes valores de n. Por ejemplo, el número primo más grande conocido corresponde al primo de Mersenne M_n con $n = 32,582,657$, que posee $9,808,358$ de dígitos.

No se sabe si existen infinitos primos de Mersenne, aunque se sospecha que la respuesta es afirmativa. Mirar la página web *http://www.mersenne.org/* para una búsqueda de tales primos.

- **Primos de Sophie-Germain:** son los primos p tal que $2p + 1$ también es primo (estudiados por Marie-Sophie Germain, 1776-1831). Por ejemplo los primoe $p = 2, 23$ son tales primos. Un tal primo es necesariamente de la forma $6k - 1$ (o sea su resto al dividirlo por 6 es 5). El primo de Sophie-Germain más grande conocido es $p = 48047305725.2^{172403} - 1$, que posee 51910 dígitos. Estos primos tienen la particularidad de que si p es un primo de Sophie-Germain que tiene resto 3 al dividirlo por 4, entonces $2p+1$ es un factor primo de M_p.

  Estos primos aparecen en varios otros contextos (el último Teorema de Fermat por ejemplo), y se conjetura que hay infinitos de ellos.

Hay varios problemas sin resolver que involucran a los números primos o cosas afines. Algunos de los problemas mas conocidos son:

- Dos números primos se dicen *gemelos* si uno de ellos es igual al otro mas dos unidades. Por ejemplo, los números 3 y 5 son primos gemelos. Otros ejemplos son los pares !! y 13, 29 y 31. A medida que uno busca números gemelos, se ve que el número de ellos va disminuyendo para primos grandes, pero aún así siguen apareciendo. El mejor resultado conocido se debe a Jing-run Chen (1973) que probo que existen infinitos números primos p tales que $p + 2$ es primo o producto de a lo sumo dos primos. Se conjetura que hay infinitos primos gemelos, mas aún, si denotamos $\pi_2(N)$ el número de primos gemelos menores que N, Hardy y Littlewood conjeturaron que
$$\pi_2(N) \simeq 2.(0,66). \int_2^N \frac{dt}{(ln\, t)^2}$$
- **Conjetura de Goldbach:** Christian Goldbach (1690-1764) conjeturó que todo número par mayor que 2 se puede escribir como suma de dos números primos positivos. Esta conjetura sigue sin haberse demostrado, y fue chequeada numéricamente para todos los números hasta 2×10^{16}. En 1966 Chen probó que todo número par mayor que 2 se escribe como un número primo y otro que es primo o producto de dos números primos. Algunos resultados similares fueron probados.
- Hay muchas preguntas abiertas sobre cómo se distribuyen los números primos. Si llamamos $\pi(N)$ a la cantidad de números primos entre 1 y N, $\pi(N)$

es del orden de $\frac{N}{log(N)}$, en el sentido de que el cociente de ambas funciones tiende a 1 cuando N tiende a infinito. Además hay estimaciones para el error entre estas dos funciones (aunque las mejores cotas dependen de un problema abierto y extremadamente difícil conocido como la hipótesis de Riemann), por ejemplo, se sabe que

$$\frac{N}{\log(N)} \leq \pi(N) \leq 1,1055.\frac{N}{\log(N)}.$$

- Una pregunta sobre la distribución de primos es la siguiente: ¿puede haber agujeros en el conjunto de números primos? O sea ¿es cierto que la distancia entre un número primo y el siguiente puede ser tan grande como uno quiere? La respuesta a esta pregunta es SI, por ejemplo, si $n \in \mathcal{N}$, el conjunto $\{n! + 2, n! + 3, \ldots, n! + n\}$ está compuesto de números consecutivos compuestos. Luego tenemos una tira de $n - 1$ números consecutivos compuestos. Ahora, ¿son estos los primeros números consecutivos compuestos? Claramente no lo son, por ejemplo si queremos 3 números consecutivos compuestos, $\{8, 9, 10\}$ lo son, mientras que la construcción anterior nos da el conjunto $\{26, 27, 28\}$ (notar la diferencia de tamaños). ¿Quiénes son los primeros n números compuestos? (no se conoce la respuesta).

Hay muchas otras preguntas que uno se puede hacer sobre los números primos y los números compuestos, y lamentablemente a la mayoría de ellas no les conocemos respuestas (a pesar de que se hizo un gran avance en esta área en los últimos años).

5.4. Sistemas Numéricos o Bases. Un sistema numérico es una manera de representar los números or símbolos. Por ejemplo, el sistema que utilizamos para representar los números enteros es el sistema *decimal* o en base 10. Este sistema fue inventado por los hindúes (Aryabhatta 476-550 y Brahmagupta 598-668) y consiste en representar un número como una tira de símbolos, cada uno en el conjunto $\{0, \ldots, 9\}$ importando el lugar en el que aparecen (estos son los conocidos *sistemas posicionales*). Así, en esta base el número 2008 por ejemplo quiere decir $8 + 0 \cdot 10 + 0 \cdot 100 + 2 \cdot 1000$.

A pesar de ser este sistema el más común hoy en día, no tiene particular razón para prevalecer sobre los otros. Tal vez el hecho de que hay 10 dedos en la mano impuso su uso (la base 20 fue utilizada por los mayas, tal vez por ser el número de dedos entre las manos y los pies). Las medidas usuales británicas usan predominantemente la base 12. Por ejemplo, cada mitad del día tiene 12 horas. También las unidades de longitud están en esta base, por ejemplo 12 pulgadas es un pie. Hasta 1971 el sistema monetario estaba basado en esta base también, siendo un "shilling" igual a 12 "pennies".

A la vez, el sistema horario usa la base 60, siendo un minuto igual a 60 segundos y una hora igual a 60 minutos, y lo mismo sucede con los ángulos. El sistema sexagesimal (de base 60) fue utilizado por los sumerios y tomado luego por los babilonios.

La pregunta natural es: ¿qué es una base d? ¿Cómo representamos un número en base d?

Supongamos que $d \in \mathbb{N}$ no es 1 (el sistema unario está dado por contar el número de símbolos simplemente). Un número en base d es una expresión del estilo

$$(a_m \ldots a_1 a_0)_d$$

donde cada a_i está en el conjunto $\{0, 1, \ldots, d-1\}$. La expresión $(a_m \ldots a_0)_d$ entonces corresponde al número natural $\sum_{i=0}^{m} a_i d^i$.

Ejemplos. El número $(101)_2$ representa al número entero $1 + 0 \cdot 2 + 1 \cdot 2^2 = 5$. El número $(11111)_2$ representa al número $1 + 2 + 4 + 8 + 16 = 31$. El número $(414)_8$ representa al número $4 + 1 \cdot 8 + 4 \cdot 8^2 = 268$. El número $(172)_{10}$ representa al número $2 + 7 \cdot 10 + 1 \cdot 10^2 = 172$. En otras palabras, la escritura en base 10 es precisamente la que usamos sin los paréntesis.

Si bien, por la experiencia que uno tiene de haber usado base 10, uno confía en que cualquier número puede escribirse (de manera única) en esta base, esto es algo que hay que probar. Además, sin mayor esfuerzo, puede probarse para cualquier base:

Teorema 5.18. *Dado $d \in \mathbb{N}$, $d > 1$, y $n \in \mathbb{N}$, n se puede representar de manera única como*

$$n = \sum_{i=0}^{m} a_i d^i \quad \text{con } 0 \leq a_i < d \text{ y } a_m \neq 0.$$

O sea $n = (a_m \ldots a_1 a_0)_d$.

Antes de demostrarlo, observemos que la unicidad en la escritura es consecuencia de exigir que el primer dígito utilizado sea no nulo. Si se acepta que la escritura de un número pueda empezar por 0, entonces ya no será única (aunque es fácil decir cuándo dos escrituras corresponden al mismo número).

Demostración. Hagamos inducción en n.

- Si $n < d$, entonces $n = (n)_1$ dado que $0 \leq n < d$. Además es claro que ésta es la única manera de escribirlo, dado que si $n = (a_m \ldots a_0)$ con $m > 0$, entonces $n \geq a_m \cdot d^m \geq 1 \cdot d = d$, que contradice la suposición $n < d$.
- Por el algoritmo de división, dados n y d, existen únicos enteros q, r tales que $n = qd + r$ y $0 \leq r < d$. Además, al ser n positivo, q también lo es. Si $q = 0$, estamos en el caso anterior. Si $q \neq 0$, $q < n$. Luego por H.I. $q = \sum_{i=0}^{m} a_i d^i$ con $0 \leq a_i < d$ de manera única. En particular

$$n = qd + r = (\sum_{i=0}^{m} a_i d^i)d + r = \sum_{i=0}^{m+1} b_i d^i$$

donde

$$b_i = \begin{cases} r & \text{si } i = 0 \\ a_{i-1} & \text{si } i > 0. \end{cases}$$

La unicidad se sigue de la unicidad de la escritura de q y de la unicidad del cociente y el resto.

□

Este algoritmo es constructivo: dice cómo escribir un número en una base. Para escribir n en base d, se divide $n = qd + r$, se pone r como el último dígito en la escritura, y antes de r se pone q escrito en base d. Para escribir q en base d se hace lo mismo: se pone $q = q_1 d + r_1$, se pone r_1 como el último dígito, y se escribe q_1 en base d, etcétera.

Ejemplo. ¿Cómo se escribe 123 en base 4? Dividiendo, tenemos $123 = 30 \cdot 4 + 3$. Luego, la escritura termina en 3. Ahora hay que escribir 30 en base 4, y para ello se vuelve a dividir: $30 = 7 \cdot 4 + 2$. Para escribir 7, nuevamente dividimos $7 = 1 \cdot 4 + 3$. Y finalmente el 1 se escribe con el dígito 1. Entonces, $123 = (1323)_4$.

Cuando la base es mayor a 10, es más cómodo escribir los dígitos $10, 11, \ldots, d-1$ con otros símbolos. Por ejemplo, usualmente en base 16 se toman como representantes los símbolos $\{0, \ldots, 9, A, B, C, D, E, F\}$ representando la letra A al número 10, la letra B el número 11 y así sucesivamente. ¿Qué número se escribe como $(A25F1)_{16}$? ¿Cómo se escribe el número 141 en base 16?

Una base muy utilizada hoy en día es la base 2 (conocida como sistema binario) por ser la utilizada por las computadoras modernas. En base 2 se usan dos dígitos, y las computadoras los simulan con dos voltajes distintos (o dos polaridades distintas en medios magnéticos). Con tres dígitos binarios se pueden representar los números de 0 a 7. De esta manera, si se agrupan dígitos binarios de a tres, se puede pasar fácilmente de base 2 a base 8 (y viceversa). Por ejemplo, $(110\ 110\ 010\ 000\ 001)_2 = (66201)_8$. La base 8 (o base *octal*) se suele usar para abreviar números escritos en base 2. También se agrupan los dígitos binarios de a 4 y se usa base 16 (o *hexadecimal*) para abreviar. El número anterior se escribe $(110\ 1100\ 1000\ 0001)_2 = (6C81)_{16} =$ `0x6C81` (la notación `0x` para comenzar un número en base 16 es también muy utilizada).

6. CONGRUENCIAS

La teoría de congruencias fue introducida por Gauss (1777-1855) y esta fuertemente relacionada con la teoría de divisibiidad.

Definición. dado m un entero no nulo y $a, b \in \mathbb{Z}$ decimos que a y b son congruentes módulo m (y lo notamos $a \equiv b \pmod{m}$) si $m \mid a - b$.

Ejemplo: $1 \equiv -6 \pmod{7}$, $1\ equiv 15 \pmod{7}$.

Ejercicio 6.1. Probar que si $m \neq 0$, entonces $a \equiv r_m(a) \pmod{m}$.

Dado $m \in \mathbb{Z}$ no nulo, definimos en $\mathbb{Z}$ la relación $a \sim b$ si y sólo si $a \equiv b \pmod{m}$.

Teorema 6.1. *La relación recién definida es una relación de equivalencia.*

Demostración: • **Reflexiva:** $a \equiv a \pmod{m}$ porque $m \mid 0$.
• **Simétrica:** Si $a \equiv b \pmod{m}$ entonces $m \mid a - b$. Luego $m \mid b - a$ con lo cual $b \equiv a \pmod{m}$.
• **Transitiva:** Si $a \equiv b \pmod{m}$ y $b \equiv c \pmod{m}$, $m \mid a - b$ y $m \mid b - c$ luego m divide a la suma de ambos números, o sea $m \mid a - c$ con lo cual $a \equiv c \pmod{m}$. □

Esto nos parte el conjunto de números enteros en clases de equivalencia. ¿Cuántas clases hay?

Proposición 6.2. *Dado $m \in \mathbb{Z}$ no nulo, $a \equiv b \pmod{m}$ si y sólo si $r_m(a) = r_m(b)$.*

Demostración: $\Rightarrow$) Como $a \equiv r_m(a) \pmod{m}$, tenemos que

$$r_m(a) \equiv a \equiv b \equiv r_m(b) \pmod{m}. \tag{1}$$

Como $0 \leq r_m(a), r_m(b) < |m|$, $-|m| < r_m(a) - r_m(b) < |m|$. Pero $m \mid r_m(a) - r_m(b)$ con lo cual $r_m(a) - r_m(b) = 0$.
$\Leftarrow$) Es inmediato de (1) □

Corolario 6.3. *El número de clases de equivalencia módulo m es $|m|$.*

Demostración: Por el Algoritmo de división, todo $n \in \mathbb{Z}$ es equivalente a un elemento del conjunto $\{0, \dots, |m|-1\}$. Además dos elementos de este conjunto no son equivalentes porque tienen distinto resto al dividirlos por m, luego hay un elemento en el conjunto por cada clase de equivalencia. □

Propiedades 6.4. Dado $m \in \mathbb{Z}$ no nulo, si $a, b, c, d \in \mathbb{Z}$ entonces:

1. Si $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$ entonces $a + c \equiv b + d \pmod{m}$.
2. Si $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$ entonces $a.c \equiv b.d \pmod{m}$.

Demostración: (1) Si $a \equiv b \pmod{m}$, entonces existe q_1 tal que $a - b = mq_1$. Análogamente, si $c \equiv d \pmod{m}$, existe q_2 tal que $c - d = mq_2$. Luego $a+c-b-d = m(q_1 + q_2)$ con lo cual $m \mid a + c - (b + d)$ o sea $a + c \equiv b + d \pmod{m}$.
(2) Como antes, si $a \equiv b \pmod{m}$, existe q_1 tal que $a - b = mq_1$. Análogamente, si $c \equiv d \pmod{m}$, existe q_2 tal que $c - d = mq_2$. Luego $ac - bd = ac - ad + ad - bd = a(c - d) + d(a - b) = m(aq_2 + dq_1)$ con lo cual $ac \equiv bd \pmod{m}$. □

Esto tiene grandes aplicaciones, por ejemplo, calculemos el resto de divdir por 7 a 351.746. Lo bueno de estas propiedades es que podemos primero calcular restos (y achicar los números) y recién ahí hacer el producto. Así, $351 \equiv 1 \pmod{7}$ y $746 \equiv 4 \pmod{7}$. Por la segunda propiedad, $351.746 \equiv 4 \pmod{7}$, o sea el resto de dividir por 7 a ese número es 4.

Corolario 6.5. *Si $p(x) = \sum_{i=0}^{n} a_i x^i$ es un polinomio con coeficientes enteros, y $b \equiv c \pmod{m}$, entonces $p(b) \equiv p(c) \pmod{m}$.*

Demostración: $p(b) = \sum_{i=0}^{n} a_i b^i = a_0 + a_1 b + \cdots + a_n b^n$. Como $b \equiv c \pmod{m}$, por la segunda propiedad $b^i \equiv c^i \pmod{m}$ y $a_i b^i \equiv a_i c^i \pmod{m}$. Si sumamos (aplicando la primer propiedad) obtenemos lo buscado. □

Corolario 6.6. *Si $p(x)$ es un polinomio no constante con coeficientes enteros, entonces no puede ser $p(n)$ primo para todo $n \in \mathbb{N}$.*

Demostración: Supongamos que hay un polinomio $p(x)$ que al evaluarlo en naturales da siempre primos. Llamemos $q = p(1)$, que es un número primo. Luego $p(q + 1) \equiv p(1) \equiv 0 \pmod{q}$. O sea $q \mid p(q + 1)$. Como $p(q + 1)$ es primo, debe ser $p(q + 1) = \pm q$. De igual forma, $p(nq + 1) \equiv 0 \pmod{q}$ para todo $n \in \mathbb{N}$. En particular, $p(x)$ toma infinitas veces el valor q o infinitas veces el valor $-q$. Esto no puede pasar por varios motivos. Uno (como veremos mas adelante) es porque el polinomio $p(x) - q$ (respectivamente $p(x) + q$) se anula un número finito de veces si es no nulo (en particular si $p(x)$ no es constante). Si uno quiere usar herramientas conocidas a esta altura, sabemos que $\lim_{x \mapsto \infty} p(x) = \infty$, con lo cual no puede alcanzar en infinitos naturales el número q ni $-q$ (¿por qué?). □

Ejemplos. Veamos algunas otras aplicaciones de las congruencias:

1. ¿En qué digito termina el número 9312^4? Como $9312 \equiv 2 \pmod{10}$, $9312^4 \equiv 2^4 \equiv 6 \pmod{10}$ con lo cual termina en 6.
2. ¿Cual es el resto de dividir 319^{21} por 10?

   Usando congruencias, $319 \equiv 9 \pmod{10}$. Una opción es calcular $9^{21} \pmod{10}$ y ver cuanto da. Una forma mas sencilla es notar que $9 \equiv -1 \pmod{10}$, luego $319^{21} \equiv (-1)^{21} \equiv -1 \pmod{10}$, con lo cual el resto es -1.

3. Probar que n^2+1 nunca es múltiplo de 4.

   Un número $n \in \mathbb{N}$ es equivalente módulo 4 a un elemento del conjunto $\{0,1,2,3\}$. Si evaluamos la expresión en estos números, vemos que

$n \pmod 4$	0	1	2	3
$n^2+1 \pmod 4$	1	2	1	2

4. Un problema conocido (y no elemental) es el siguiente: ¿que números se pueden escribir como suma de dos cuadrados? Probar que si $n \in \mathbb{N}$ tienen resto 3 al dividirlo por 4 entonces no es suma de dos cuadrados.

   La respuesta al problema general (que usa aritmética con los enteros de Gauss) es que n es suma de dos cuadrados si y sólo si los únicos primos que pueden aparecer en su factorización son el 2 y primos congruentes a 1 módulo 4. Lagrange $(1736-1813)$ probó que todo número natural es suma de cuatro cuadrados.
5. ¿Es $313^{25}+2$ divisible por 7?

Veamos otra aplicación de las congruencias:

Proposición 6.7 (Criterio de divisibilidad por 3)**.** *Un número $n \in \mathbb{Z}$ es divisible por 3 si y sólo si la suma de sus dígitos lo es.*

Demostración: Dado que $e \mid n$ si y sólo si $3 \mid -n$, podemos asumir que $n \in \mathbb{N}$ (siendo el caso $n=0$ elemental). Un número $n \in \mathbb{N}$ se puede escribir como $n = a_0 + a_1 10 + \cdots + a_n 10^n$, donde los dígitos son los números a_i y justamente $a_i \in \{0,\ldots,9\}$. Como $10 \equiv 1 \pmod 3$, $10^i \equiv 1 \pmod 3$. Luego

$$n = a_0 + a_1 10 + \cdots + a_n 10^n \equiv a_0 + a_1 + \cdots + a_n \pmod 3,$$

o sea que módulo 3 n es congruente a la suma de sus dígitos. En particular uno es congruente a 0 si y sólo si el otro lo es. □

Ejercicio: Dar y demostrar criterios para la división por $2,3,4,5,8,9$ y 11 (ejercicio 7 de la práctica 5).

7. Ecuaciones diofánticas lineales

Las ecuaciones diofánticas son sistemas de ecuaciones con coeficientes enteros a os que queremos hallarles soluciones enteras, por ejemplo: ¿que soluciones (si alguna) tiene la ecuación $x^2+y^2=z^2$?

El nombre se debe a *Diophantus of Alexandria* (~ 200 después de Cristo) quién estudió algunas de estas ecuaciones en su famoso libro *Arithmetica*. El problema general es de gran dificultad y no existe una solución general (está demostrado que no se puede dar un algoritmo que dado un sistema con muchas ecuaciones y muchas variables pueda decidir si tiene solución entera o no), sin embargo algunas familias de ecuaciones si la tienen. Entre las ecuaciones conocidas, cabe destacar el famoso *Ultimo Teorema de Fermat*, que dice que la ecuación $x^n+y^n=z^n$ no tiene soluciones enteras si $n \geq 3$ (y cuya demostración fué concluida en 1994 con los trabajos de Wiles). Nos contentaremos en este curso con dar una respuesta para el caso mas sencillo que son las ecuaciones lineales en dos variables, esto es buscar soluciones de la ecuación

$$ax + by = c$$

donde $a, b, c \in \mathbb{Z}$. Notar que las soluciones de esta ecuación es una recta en R^2, y lo que preguntarmos es si esta recta contiene algún punto con coordenadas enteras.
Preugnta: ¿tiene alguna solución entera la ecuación $2x + 4y = 1$?

La respuesta es NO. Independientemente de que valores tomemos para x y para y, el término de la izquierda será siempre un número par, con lo cual no puede dar 1.
Preugnta: ¿tiene alguna solución entera la ecuación $9x + 5y = 1$?

Si uno busca a mano una solución, encuentra que el punto $(-1, 2)$ pertenece a dicha recta. En particular esta ecuación si tiene soluciones enteras. También el punto $(4, -7)$ satisface la ecuación y si continuamos buscando a mano, encontraremos varios puntos mas. ¿Cuántas soluciones habrá? ¿Cómo podemos hallarlas todas?

Estas dos preguntas son las que trataremos de contestar en general. Si miramos como resolvemos estas soluciones sobre $\mathbb{R}$ nos dá una pista de la estrategia a utilizar: (1) hallamos (si existe) una solución (x_0, y_0) particular de la ecuación. (2) Buscamos todas las soluciones del sistema homogéneo $ax + by = 0$. Luego todas las soluciones se obtienen sumando la solución (x_0, y_0) con las soluciones del sistema homogéneo.

Teorema 7.1. *La ecuación $ax + by = c$ tiene una solución si y sólo si $(a : b) \mid c$.*

Demostración: $\Rightarrow$) Como $(a : b) \mid a$ y $(a : b) \mid b$, usando las propiedades de divisibilidad, tenemos que $(a : b) \mid ax + by$ para cualquier par de valores $x, y \in \mathbb{Z}$. En particular si existe una solución del sistema, $c = ax + by$ y $(a : b) \mid c$.
$\Leftarrow$) Por el Algoritmo de Euclídes, existen $r, s \in \mathbb{Z}$ tales que

$$ar + bs = (a : b).$$

Si $(a : b) \mid c$, entonces existe $q \in \mathbb{Z}$ tal que $c = (a : b)q$. Multiplicando la combinación lineal por q tenemos

$$c = (a : b)q = a(qr) + b(qs),$$

o sea que (qr, qs) es una solución de nuestra ecuación. □

Ejemplo: Hallar (si existe) una solución de la ecuación $21x + 12y = 15$.

Como $(21 : 12) = 3$ y $3 \mid 15$, sabemos que hay solución. ¿Cómo hallarla? Como en la demostración del Teorema, usamos el algoritmo de Euclídes. Comencemos calculando los cocientes sucesivos:

$$21 = 12.1 + 9$$
$$12 = 9.1 + 3$$

Luego $3 = 12.1+9.(-1) = 12.1+(21-12).(-1) = 12.2+21.(-1)$. Si multiplicamos la ecuación por 5, encontramos que $(-5, 10)$ es una solución de la ecuación.
Busquemos para este ejemplo todas las soluciones (para entender el caso general). Como dijimos antes (aunque sin demostrarlo aún), debemos hallar las soluciones del sistema homogéneo

$$21x + 12y = 0.$$

Lo primero que podemos hacer es dividir toda la ecuación por 3 (ya que todos los números involucrados son múltiplos de 3). Luego estamos buscando las soluciones de la ecuación

$$7x + 4y = 0.$$

Si (x_0, y_0) es una solución, $7x_0 = -4y_0$. En particular, $7 \mid 4y_0$. Como $(7 : 4) = 1$ (para esto dividimos por 3 la ecuación), $7 \mid y_0$, o sea $y_0 = 7k$. Si reemplazamos en

la ecuación, queremos que $7x_0 = -28k$. Dividiendo por 7 tenemos que $x_0 = -4k$, o sea las soluciones del sistema homogéneo son $(-4k, 7k)$, con k cualquier número entero. Como ya conocemos la solución particular, acabamos de probar que todas las soluciones de este sistema son:

$$\begin{cases} x = -5 - 4k \\ y = 10 + 7k. \end{cases}$$

Teorema 7.2. *Dada la ecuación diofántica $ax + by = c$, entonces:*

- *Si $(a : b) \nmid c$, la ecuación no tiene soluciones enteras.*
- *Si $(a : b) \mid c$ entonces la ecuación tiene infinitas soluciones enteras. Mas aún, si $r, s \in \mathbb{Z}$ son tales que $ar + bs = (a : b)$ entonces todas las soluciones son*

$$\begin{cases} x = r\frac{c}{(a:b)} - \frac{b}{(a:b)}k \\ y = s\frac{c}{(a:b)} + \frac{a}{(a:b)}k, \end{cases}$$

con $k \in \mathbb{Z}$.

Demostración: por el Teorema anterior, sabemos que si $(a : b) \nmid c$ entonces el sistema no tiene solución y que si $(a : b) \mid c$ entonces existe al menos una solución, y está dada por $x_0 = r\frac{c}{(a:b)}$, $y_0 = s\frac{c}{(a:b)}$ donde $r, s \in \mathbb{Z}$ son los que vienen del algoritmo de Euclides y satisfacen $ar + bs = (a : b)$. Lo que queremos es calcular todas las soluciones. Como al mirar sitemas de ecuaciones lineales sobre $\mathbb{R}$, si tenemos dos soluciones (x_0, y_0) y (x_1, y_1), al restarlas vale que

$$a(x_0 - x_1) + b(y_0 - y_1) = 0,$$

o sea $(x_0 - x_1, y_0 - y_1)$ es solución del sistema homogéneo. Recíprocamente, si $(\tilde{x}, \tilde{y})$ es una solución del sistema homogéneo, $(x_0 + \tilde{x}, y_0 + \tilde{y})$ es una solución del sistema original. Con esto vemos que para hallar todas las soluciones, debemos hallar todas las soluciones del sistema homogéneo

$$ax + by = 0. \tag{2}$$

Si dividimos la ecuación (2) por $(a : b)$, buscamos enteros $\tilde{x}, \tilde{y}$ tales que $\frac{a}{(a:b)}\tilde{x} = -\frac{b}{(a:b)}\tilde{y}$. En particular, $\frac{a}{(a:b)} \mid \frac{b}{(a:b)}\tilde{y}$. Como $\left(\frac{a}{(a:b)} : \frac{b}{(a:b)}\right) = 1$, $\frac{a}{(a:b)} \mid \tilde{y}$. Digamos que $\tilde{y} = \frac{a}{(a:b)}k$ con $k \in \mathbb{Z}$. Luego la igualdad se transforma en

$$\frac{a}{(a:b)}\tilde{x} = -\frac{b}{(a:b)}\frac{a}{(a:b)}k$$

y dividiendo por $\frac{a}{(a:b)}$ tenemos que $\tilde{x} = -\frac{b}{(a:b)}k$, como dice el enunciado. □

Ejemplo: Supongamos que no conseguimos monedas por ningún lado y tenemos que manejarnos con los billetes de \$2 y \$5. ¿Se puede comprar cualquier producto cuyo precio sea un número exacto de pesos? (por ejemplo, ¿podemos comprar ena gaseosa que sale \$3?)

La respuesta es que sí. Como $(2 : 5) = 1$, si tomamos un natural n cualquiera, existen $x, y \in \mathbb{Z}$ tal que $n = 2x + 5y$. Aquí la idea de "restar plata" es que pagamos con una cantidad de billetes de \$2 y \$5 y el vendedor nos da un vuelto que corresponde a números negativos de billetes.

Ejemplo: Que pasa si vamos a una librería y queremos comprar un libro que sale \$61 (nuevamente sin monedas), y el vendedor nos informa que no tiene billete alguno para darnos de vuelto. ¿Podemos pagar el libro?

Lo que buscamos acá son soluciones al sistema $2x+5y = 61$, pero con la condición extra que $x \geq 0$ y $y \geq 0$. Si buscamos todas las soluciones del sistema, debemos primero hallar una solución particular. Como $(2 : 5) = 1$ y $2(-2) + 5.1 = 1$, una solución particular es $x_0 = -122$, $y_0 = 61$. Todas las soluciones son

$$\begin{cases} x = -122 + 5k \\ y = 61 - 2k \end{cases}$$

Ahora pedimos la hipótesis extra que $-122 + 5k \geq 0$ y que $61 - 2k \geq 0$. La primer desigualdad implica que $k \geq 122/5$ con lo cual $k \geq 25$ mientras que la segunda desigualdad implica que $k \leq 61/2$ o sea $k \leq 30$. Luego cualquier valor de k con $25 \leq k \leq 30$ nos da una manera de pago. Por ejemplo $k = 25$ nos dice que demos 3 billetes de \$2 y 11 billetes de \$5. De igual manera obtenemos las otras formas de pagar.

Ejercicio: ¿de cuántas maneras puede escribirse 23 como suma de 2's y de 7's?

7.1. Ecuaciones lineales de congruencias. Un problema similar al de ecuaciones diofánticas lineales es el problema de ecuaciones lineales de congruencias. Esto es supongamos que tenemos $a, b \in \mathbb{Z}$ y $m \in \mathbb{Z}$ con $m \neq 0$, y buscamos las soluciones del sistema

$$ax \equiv b \pmod{m}.$$

Dado que si $x \equiv x' \pmod{m}$ entonces $ax \equiv ax' \pmod{m}$, si $x \in \mathbb{Z}$ es solución, su clase módulo m también lo es. Como el número de clases modulo m es finito (hay exactamente $|m|$ tales clases), si hay solución, hay infinitas soluciones, pero finitas clases de soluciones. Una forma (no muy eficiente) de saber si el sistema tiene solución o no es chequear todas las clases posibles para x y ver si alguna es solución del sistema. El problema es que si m es grande, esto demanda demasiado trabajo. Consideremos algunos ejemplos para ver como funciona este método de "fuerza bruta":

Ejemplo 1: Hallar (si existen) las soluciones de la ecuación $2x \equiv 1 \pmod{4}$.

Dado que las clases módulo 4 están representadas por $\bar{0}$, $\bar{1}$,$\bar{2}$ y $\bar{3}$, podemos probar con cada una de estas. Al hacer la cuenta vemos que ninguna de ellas satisface la ecuación, con lo cual no hay solución.

Ejemplo 2: Hallar (si existen) las soluciones de la ecuación $2x \equiv 4 \pmod{5}$.

Si hacemos el mismo procedimiento que antes, miramos las clases de $\bar{0}, \bar{1}, \bar{2}, \bar{3}$ y $\bar{4}$, vemos que la única solución es $x \equiv 2 \pmod{5}$.

Ejemplo 3: Hallar si existen as soluciones de $3x \equiv 6 \pmod{9}$.

Si buscamos dentro de las 9 clases, vemos que las soluciones son $x \equiv 2 pmod 9$, $x \equiv 5 \pmod{9}$ y $x \equiv 8 pmod 9$. O sea tiene "varias" soluciones módulo 9. ¿Cómo entendemos esto?

Si miramos la definición de congruencias, pedir

$$ax \equiv b \pmod{m}$$

es pedir que $m \mid ax - b$ que (por definición de divisibilidad) es lo mismo que pedir que exista $y \in \mathbb{Z}$ tal que $ax - b = my$ o (despejando) que tenga solución entera la ecuación diofántica

$$ax - my = b.$$

Justamente este tipo de ecuaciones son las que estudiamos en la última sección, y sabemos que tienen solución si y sólo si $(a : m) \mid b$ (esto explica por qué no tiene solución el Ejemplo 1 pero si tienen solución los otros dos ejemplos hechos). Además, tenemos una manera de hallar todas las soluciones (si tienen alguna), las soluciones son

$$\begin{cases} x = r\frac{b}{(a:m)} + \frac{m}{(a:m)}k \\ y = s\frac{b}{(a:m)} - \frac{a}{(a:m)}k \end{cases}$$

donde $ar + ms = (a : m)$. En particular, el valor de x es

$$x \equiv r\frac{b}{(a:m)} \left(\mod \frac{m}{(a:m)} \right)$$

o sea la solución es única módulo $\frac{m}{(a:m)}$. Fijensé que si buscamos soluciones módulo m, tenemos más de una, ya que distintos valores de k nos dan soluciones no congruentes módulo m. Más específicamente, si tomamos $k = 0, 1, \ldots, (a : m) - 1$ obtenemos todas las soluciones no equivalentes módulo m (¿por qué?). En particular hay $(a : m)$ tales soluciones (como pasó en los Ejemplos 2 y 3).

Una manera de interpretar esto es que si conocemos el resto de dividir un número por 9 digamos, en particular conocemos el resto al dividirlo por 3. Ahora, si sé que tengo un número n cuyo resto al dividirlo por 3 es 2, ¿que posible resto tiene al dividirlo por 9?

Dicho de otra manera, si $n \equiv m \pmod 9$, en particular $n \equiv m \pmod 3$. Si $n \equiv 2 \pmod 3$, ¿a quién es congruente n módulo 9?

Al ser $n \equiv 2 \pmod 3$, sabemos que $n = 2 + 3k$. Si miramos esto módulo 9, tenemos $n \equiv 2 + 3k \pmod 9$. Si k es divisible por 3, entonces $n \equiv 2 \pmod 9$, luego tengo que mirar valores de k módulo 3 (nuevamente, si $k_0 \equiv k_1 \pmod 3$, $2 + 3k_0 \equiv 2 + 3k_1 \pmod 9$), o sea tengo 3 posibles valores y corresponden a tomar $k = 0, 1, 2$ (que son representantes para k módulo 3 justamente).

8. Estructura de $\mathbb{Z}/m\mathbb{Z}$

Dado $m \in \mathbb{Z}$ no nulo, notamos por $\mathbb{Z}/m\mathbb{Z}$ (o en algunos lugares $\mathbb{Z}_m$) al conjunto de clases de equivalencia módulo m. O sea $\mathbb{Z}/m\mathbb{Z}$ es un conjunto con $|m|$ elementos. Lo que tiene de particular este conjunto es que es un anillo conmutativo, o sea que posee dos operaciones que satisfacen las propiedades que satisfacen los enteros (pero es finito). Las operaciones estan dadas por:

- $\bar{a} + \bar{b} = \overline{a + b}$, o sea si quiero sumar las clases de elementos $a, b \in \mathbb{Z}$, la suma de sus clases es la clase de $a + b$. Esto es independiente del elemento a en su clase por Propiedades 6.4.
- $\bar{a}.\bar{b} = \overline{a.b}$, o sea si quiero multiplicar las clases de elementos $a, b \in \mathbb{Z}$, el producto de sus clases es la clase de $a.b$. Esto es independiente del elemento a en su clase por Propiedades 6.4.

Es claro que satisface que es un grupo conmutativo para la suma (porque $\mathbb{Z}$ lo es), que el producto es asociativo, conmutativo, tiene neutro (la clase de 1) y que vale la

propiedad distributiva. A diferencia de $\mathbb{Z}$, estos anillos son mas raros, por ejemplo, si tomamos $m = 6$, $\bar{2}.\bar{3} = \bar{6} = \bar{0}$ (mód 6). O sea tenemos dos elementos no nulos (es claro que $2 \not\equiv 0$ (mód 6) y $3 \not\equiv 0$ (mód 6)) tales que su producto es cero. Dicho en términos matemáticos, $\mathbb{Z}/m\mathbb{Z}$ "no siempre" es un dominio íntegro.

Pregunta: ¿qué tiene que satisfacer m para que $\mathbb{Z}/m\mathbb{Z}$ sea un dominio íntegro? (rta: m debe ser primo. Probarlo como ejercicio)

Calculemos las tablas de multiplicación para $m = 6$ y para $m = 7$:

	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

Observaciones: Las tablas son simétricas por ser el producto conmutativo. Observar también, que la función $x \mapsto ax$ es biyectiva si $(a : m) = 1$, ¿por qué? (mirar la siguiente pregunta).

Pregunta: ¿qué elementos de $\mathbb{Z}/m\mathbb{Z}$ tienen inverso multiplicativo?

Saber si dado $\bar{a} \in \mathbb{Z}/m\mathbb{Z}$ tiene inverso multiplicativo es buscar un elemento x tal que $\bar{a}.\bar{x} = \bar{1}$. En términos de congruencia, buscamos un x tal que

$$ax \equiv 1 \pmod{m}.$$

Sabemos resolver este tipo de congruencias. El sistema tiene solución si y sólo si $(a : m) \mid 1$. Dado que el único divisor positivo de 1 es 1, tenemos solución si y sólo si $(a : m) = 1$. Esto demuestra la proposición

Proposición 8.1. *El elemento $\bar{a} \in \mathbb{Z}/m\mathbb{Z}$ tiene inverso multiplicativo si y sólo si $(a : m) = 1$.*

Además, el inverso de un elemento (si lo tiene) se calcula nuevamente con el Algoritmo de Euclídes.

Ejemplo: • Para $m = 6$, los elementos que tienen inversos son $\bar{1}$ y $\bar{5}$ (hay solo 2). • Para $m = 15$ los elementos que tienen inverso son $\bar{1}, \bar{2}, \bar{4}, \bar{7}, \bar{8}, \bar{11}, \bar{13}$ y $\bar{14}$ (hay 8 elementos).

Esto sirve también para resolver algunas ecuaciones lineales de congruencia. Si tenemos la ecuación

$$ax \equiv b \pmod{m}$$

y $(a : m) = 1$, sabemos que existe un elemento a' que es el inverso de a módulo m. Multiplicando la ecuación por a' (¿por qué se puede hacer esto?) vemos que

$$x \equiv a'ax \equiv a'b \pmod{m}.$$

O sea encontramos la solución, y es $a^{-1}b$ (como al resolver ecuaciones sobre $\mathbb{R}$). ¿Qué pasa si $(a : m) \neq 1$? Si $(a : m) \nmid b$ entonces no hay solución y no hay nada

que hacer. En cambio, si $(a : m) \mid b$, entonces dividimos todo por $(a : m)$ (¿por qué es esto cierto?) y tenemos la ecuación

$$\frac{a}{(a:m)}x \equiv \frac{b}{(a:m)} \pmod{\frac{m}{(a:m)}}$$

donde ahora $\left(\frac{a}{(a:m)} : \frac{m}{(a:m)}\right) = 1$ y podemos calcularle su inverso.

Definición. La función "fi de Euler" es la función $\varphi : \mathbb{N} \to \mathbb{N}$ dada por $\varphi(m) = \#\{n \in \mathbb{N} \ : \ 1 \leq n \leq m \text{ y } (n : m) = 1\}$.

Por la Proposición anterior, en $\mathbb{Z}/m\mathbb{Z}$ hay $\varphi(m)$ elementos inversibles.

Pregunta: ¿para qué valores de m son todos los elementos no nulos de $\mathbb{Z}/m\mathbb{Z}$ inversibles?

Notar que si todos los elementos no nulos son inversibles, en particular es un dominio íntegro, dado que si $\bar{a}\bar{b} = 0$, y $\bar{a} \neq 0$, tiene inverso y multiplicando por el inverso de $\bar{a}$ tenemos que $\bar{b} = 0$. Luego m debe ser primo (sino como vimos antes $\mathbb{Z}/m\mathbb{Z}$ no es dominio íntegro). Nos resta ver que si m es primo entonces todos los elementos no nulos tienen inverso. Pero si m es primo y tomamos $\bar{a} \neq \bar{0}$, $(m : a) = 1$ (como m es primo, el mcd es 1 o m; si es m entonces $m \mid a$ y $\bar{a} = \bar{0}$), luego $\bar{a}$ tiene inverso.

En particular, si p es primo, el anillo $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo (o sea todos los elementos no nulos tienen inverso, como sucede con $\mathbb{Q}$ y $\mathbb{R}$) con finitos elementos!

Teorema 8.2 (Pequeño Teorema de Fermat)**.** *Si $p \in \mathbb{N}$ es un número primo y $a \in \mathbb{Z}$, entonces:*

- *Si $p \nmid a$, $a^{p-1} \equiv 1 \pmod{p}$.*
- *Para cualquier a, $a^p \equiv a \pmod{p}$.*

Por ejemplo, si $p = 5$, el Teorema dice que $a^4 = equiv1 \pmod{5}$ para cualquier valor de a congruente a $1, 2, 3$ o 4 módulo 5 (sin necesidad de chequear cada caso). Antes de ver varias aplicaciones de este Teorema, veamos la demostración.

Demostración: Comencemos con el caso $(a : p) = 1$. Llamemos $\mathcal{P}$ al conjunto de elementos inversibles de $\mathbb{Z}/p\mathbb{Z}$, o sea $\mathcal{P} = \{\bar{1}, \bar{2}, \ldots, \overline{p-1}\}$. Como $(a : p) = 1$, a es inversible en $\mathbb{Z}/p\mathbb{Z}$, luego $\bar{a}\bar{1} \in \mathcal{P}, \bar{a}\bar{2} \in \mathcal{P}, \ldots, \bar{a}(\overline{p-1}) \in \mathcal{P}$. Nos gustaría ver que los elementos obtenidos al multiplicar por $\bar{a}$ el conjunto $\mathcal{P}$ son todos distintos.

¿Puede ser $\bar{a}\bar{i} \equiv \bar{a}\bar{j} \pmod{p}$?

Si $\bar{a}\bar{i} \equiv \bar{a}\bar{j} \pmod{p}$ multiplicando por $\bar{a}^{-1}$ tenemos que $i \equiv j \pmod{p}$, luego la respuesta es no. En particular, $\mathcal{P} = \{\bar{1}, \bar{2}, \ldots, \overline{p-1}\} = \{\bar{a}\bar{1}, \bar{a}\bar{2}, \ldots, \bar{a}(\overline{p-1})\}$ (vimos una contención y ambos conjuntos tienen la misma cantidad de elementos). Si multiplicamos todos los elementos del conjunto $\mathcal{P}$, tenemos que

$$1 \cdot 2 \ldots (p-1) \equiv a \cdot 1 \cdot a \cdot 2 \ldots a \cdot (p-1) \equiv a^{p-1} 1 \cdot 2 \ldots (p-1) \pmod{p}. \tag{3}$$

Llamemos $M = 1 \cdot 2 \ldots (p-1)$. Notemos que $p \nmid M$, dado que si $p \mid M$, divide a alguno de los términos y no puede ser. Luego M tiene inverso módulo p, y multiplicando por su inverso la ecuación (3) obtenemos el primer caso.

El segundo caso es inmediato, dado que si $p \nmid a$, entonces $a^p = a^{p-1}a \equiv a \pmod{p}$ por el primer caso. Si $p \mid a$, entonces la igualdad es inmediata porque ambos miembros son congruentes a cero módulo p.

□

Aplicaciones:

- Hallar el resto de dividir 2^{303} por 7.
- Hallar todas las soluciones de la ecuación $x^{22} \equiv 5 \pmod{11}$.
- ¿Existe $a \in \mathbb{Z}$ tal que a es primo y $a^{12} - 1$ también lo es? (sugerencia: mirar módulo 13).

Observación: Este resultado es "óptimo", en el sentido de que si p es primo y r es un número natural con $1 \leq r < p-1$ entonces existe $a \in \mathbb{N}$ con $p \nmid a$ y tal que $a^r \not\equiv 1 \pmod{p}$.

Otra gran aplicación de este resultado es que permite dar un "test de primalidad". Esto es un procedimiento que en algunos casos nos puede decir si un número natural n es primo o no. Por ejemplo, ¿es primo el número 4097? Supongamos que sí, luego el Teorema de Fermat nos dice que $a^{4096} \equiv 1 \pmod{4097}$ para todo a no dividible por 4097. Dado que $4096 = 2^{12}$, podemos calcular $2^{2^{12}} \pmod{4097}$ y ver a que es congruente.

La manera de calcular potencias es elevando al cuadrado cada resultado obtenido (de hecho así es como se puede calcular a^b para $b \in \mathbb{N}$ en cerca de $log(b)$ operaciones). Asi tenemos:

$$2 \mapsto 2^2 = 4 \mapsto 2^{2^2} = 16 \mapsto 2^{2^3} = 256 \mapsto 2^{2^4} \equiv 4081 \mapsto 2^{2^5} \equiv 256 \pmod{4097}$$

Notar que entramos en un loop. Si continuamos elevando al cuadrado, obtendremos sucesivamente los números 256 y 4081. En particular, $2^{2^{12}} \equiv 4081 \pmod{4097}$. Como $2^{4097-1} \not\equiv 1 \pmod{4097}$ deducimos del Teorema de Fermat que 4097 no es primo.

El mismo tipo de argumentos se pueden usar para los primos de Fermat (recordar que el n-ésimo primo de Fermat es $F_n = 2^{2^n} + 1$ con lo cual $F_n - 1$ es una potencia de 2). Verificar que F_5 no es primo (hacer lo mismo con la base 3).

La desventaja de este método es que en algunos casos nos dice si un número no es primo, pero en ningún caso puede asegurar que un número sí lo sea. A la vez, en caso de que el número no sea primo, no obtenemos información de su factorización.

Existen números m que pasan "siempre" este test, o sea para todo $a \in \mathbb{Z}$ tal que $(a : m) = 1$ vale que $a^{m-1} \equiv 1 \pmod{m}$ y m no es primo. A estos números se los conoce como *números de Carmichael* (1879-1967). El primer número de Carmichael (descubierto por él) es $561 = 3 \cdot 5 \cdot 13$. La razón de por qué pasan el test de primalidad es que para todo primo p que divide a m, $p-1$ divide a $m-1$. Usando el Teorema de Fermat y el Teorema Chino del resto (que veremos más adelante) es fácil ver que esto alcanza.

Es fácil ver que todos estos números son impares, y se puede ver (de manera no tan fácil) que son libres de cuadrados y con al menos tres divisores primos. En 1994, Alford, Granville y Pomerance provaron que hay infinitos números de Carmichael, y más aun, entre 1 y n hay al menos $n^{2/7}$ tales números (para n suficientemente grande).

Existe una versión general del Teorema de Fermat que se aplica para cualquier número m (no necesariamente primo).

Teorema 8.3 (Euler-Fermat)**.** *Si $m \in \mathbb{N}$ y $a \in \mathbb{Z}$ es coprimo con m, entonces*

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

La demostración es idéntica a la del Teorema de Fermat, pero considerando el conjunto de números comprimos con m.

Comentarios: • Si p es primo, $\varphi(p) = p-1$ con lo cual el Teorema de Euler-Fermat implica el Teorema de Fermat.
• Este Teorema no es óptimo. Por ejemplo, si $m = 15$, $\varphi(m) = 8$, pero es fácil ver (haciendo una tabla) que $a^4 \equiv 1 \pmod{15}$ para todo entero a coprimo con 15 (verificar esta afirmación). Se puede dar una versión óptima del mismo, pero requiere mas trabajo y no lo haremos en este curso.
• Para poder aplicar este Teorema a casos concretos necesitamos poder calcular $\varphi(m)$ de manera mas o menos rápida. No se conocen algoritmos rápidos para calcular $\varphi(m)$ sin factorizar m (y se sospecha que no existen, por ejemplo si m es producto de sólo dos primos, se puede probar que dan el mismo trabajo ambos problemas).

Proposición 8.4. *La función φ satisface las siguientes dos propiedades:*

1. *Si $n, m \in \mathbb{N}$ son coprimos entre sí, entonces $\varphi(nm) = \varphi(n)\varphi(m)$.*
2. *Si p es un número primo y $n \in \mathbb{N}$ entonces $\varphi(p^n) = (p-1)p^{n-1}$.*

Demostración: Para probar el primer ítem precisaremos el Teorema Chino del resto con lo cual lo haremos mas adelante. Para probar el segundo ítem, notar que $\varphi(p^n) = p^n - \#\{a \in \mathbb{N} \ : \ 1 \leq a \leq p^n \text{ y } p \mid a\}$. Pero la cantidad de números entre 1 y p^n divisibles por p es p^{n-1}. Luego $\varphi(p^n) = p^n - p^{n-1} = (p-1)p^{n-1}$. □

Corolario 8.5. *Si $m = \prod_{i=1}^{n} p_i^{r_i}$ entonces $\varphi(m) = \prod_{i=1}^{n}(p_i - 1)p_i^{r_i - 1}$.*

Ejercicio 8.1. ¿En qué dígito termina 3^{125}?

Lo que debemos hacer es calcular $3^{125} \pmod{10}$. Como $(3 : 10) = 1$, usando el Teorema de Euler-Fermat tenemos que $3^4 \equiv 1 \pmod{10}$. Luego $3^{125} = (3^4)^{31}.3 \equiv 3 \pmod{10}$.

Un resultado cuya demostración es similar a la del Pequeño Teorema de Fermat es el *Teorema de Wilson*:

Teorema 8.6. $(p-1)! \equiv -1 \pmod{p} \iff p$ *es primo*

Demostración. Supongamos que p es primo. Entonces, mirando la igualdad en $\mathbb{Z}/p\mathbb{Z}$, tenemos que probar que $1 \cdot 2 \cdot 3 \ldots (p-1) = -1$. Como $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo, para cada $i = 1, \ldots, p-1$, hay un inverso i^{-1}. Entonces, si $i \neq i^{-1}$, ambos elementos se cancelan en el producto $1 \cdot 2 \ldots (p-1)$, y solo quedan aquellos que son iguales a su inverso. Pero no hay muchos de estos elementos: si $x = x^{-1}$ (siempre mirando todo en $\mathbb{Z}/p\mathbb{Z}$) entonces multiplicando por x resulta $x^2 = 1$, es decir, $x^2 - 1 = 0$, es decir $(x-1)(x+1) = 0$. De nuevo, como $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo, si $x - 1 \neq 0$ y $x + 1 \neq 0$, resultará $(x-1)(x+1) \neq 0$. Entonces, las únicas soluciones de la ecuación $(x-1)(x+1) = 0$ son $x = 1$ y $x = -1$. Esto es, en $\mathbb{Z}/p\mathbb{Z}$, tenemos $1 \cdot 2 \cdot 3 \ldots (p-1) = 1 \cdot (-1) = -1$.

Recíprocamente, si p no es primo, entonces hay algún divisor de p entre 2 y $p-1$. Pero eso dice que d no es inversible en $\mathbb{Z}/p\mathbb{Z}$, y no puede entonces ser parte de un producto cuyo resultado es un número inversible (Ejercicio: explicar por qué). □

8.1. Teorema Chino del Resto. A diferencia de las ecuaciones en $\mathbb{Z}$, donde la solución de una ecuación en una variable es única, hemos visto que las soluciones de una ecuación de congruencias (si tiene) son infinitas (pues en cada clase de equivalencia hay infinitos números enteros). Luego podemos preguntarnos si un sistema de ecuaciones lineales tiene solución o no. Miremos el siguiente ejemplo: supongmaos que tengo un número $n \in \mathbb{N}$ tal que el resto de dividir n por 3 es 2 y el resto de dividir n por 7 es 4. ¿Puedo saber que resto tiene n al dividirlo por 21?

En otras palabras, me dicen que n es solución de las ecuaciones

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 4 \pmod 7 \end{cases}$$

¿Cómo saber si este sistema tiene solución o no? Una forma de hacerlo es encontrar todas las soluciones de la primer ecuación y ver cuales de ellas satisfacen la segunda. Así, $x \equiv 2 \pmod 3$ tiene como solución $x = 2 + 3k$ con $k \in \mathbb{Z}$. Si reemplazamos en la otra ecuación, queremos que

$$2 + 3k \equiv 4 \pmod 7 \quad \Leftrightarrow \quad 3k \equiv 2 \pmod 7.$$

Dado que $(3 : 7) = 1$ (o sea los módulos de las ecuaciones originales son coprimos), el sistema tiene solución. Además, dado que 5 es el inverso multiplicativo de 3 en $\mathbb{Z}/7\mathbb{Z}$, tenemos que

$$k \equiv 3 \pmod 7.$$

Luego $x = 2+3(3+7m) = 11+21m$, o sea las soluciones satisfacen $x \equiv 11 \pmod{21}$ (notar que 11 es solución de ambas ecuaciones). Con lo cual la respuesta es que este sistema admite infinitas soluciones, todos los números congruentes a 11 módulo 21. En particular el resto de dividir n por 21 es 11.

El Teorema Chino del Resto dá una manera de hallar todas las soluciones de un sistema de congruencias si los módulos son coprimos.

Teorema 8.7 (Teorema Chino del Resto)**.** *Dado el sistema de congruencias*

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ \quad \vdots \\ x \equiv a_n \pmod{m_n} \end{cases}$$

donde $(m_i : m_j) = 1$ *si* $i \neq j$ *entonces el sistema tiene solución única módulo* $m_1 \dots m_n$.

Demostración: Llamemos $M = m_1 \dots m_n$. Para cada $1 \leq j \leq n$, $(\frac{M}{m_j} : m_j) = 1$, dado que $\frac{M}{m_j} = \prod_{i \neq j} m_i$ y cada m_i es coprimo con m_j. Luego por el Algoritmo de Euclídes, existen r_j, s_j tales que

$$1 = \frac{M}{m_j} r_j + m_j s_j. \tag{4}$$

En particular $\frac{M}{m_j} r_j \equiv 1 \pmod{m_j}$. Definimos $x_0 = \frac{M}{m_1} r_1 a_1 + \dots + \frac{M}{m_n} r_n a_n$. Afirmo que x_0 es solución. Veamos que satisface cada congruencia. Tomemos un número i

con $1 \leq i \leq n$ y miramos x_0 módulo m_i. Como $m_i \mid \frac{M}{m_j}$ si $j \neq i$, tenemos

$$x_0 = \frac{M}{m_1} r_1 a_1 + \cdots + \frac{M}{m_n} r_n a_n \equiv \frac{M}{m_i} r_i a_i \equiv a_i \pmod{m_i}.$$

Veamos que es la única solución módulo $m_1 \dots m_n$. Si x_1 es otra solución, entonces

$$\begin{cases} x_0 \equiv x_1 \pmod{m_1} & \Rightarrow \quad m_1 \mid x_0 - x_1 \\ \qquad\qquad \vdots & \\ x_0 \equiv x_1 \pmod{m_n} & \Rightarrow \quad m_n \mid x_0 - x_1. \end{cases}$$

Como $(m_1 : m_2) = 1$, tenemos que $m_1 m_2 \mid (x_0 - x_1)$. Como $(m_1 m_2 : m_3) = 1$ entonces $m_1 m_2 m_3 \mid (x_0 - x_1)$. Inductivamente vemos que $m_1 \dots m_n \mid (x_0 - x_1)$, o sea la solución es única módulo $m_1 \dots m_n$ como queríamos. □

Ejemplo: Hallar todas las soluciones del sistema

$$\begin{cases} x \equiv 7 \pmod{4} \\ x \equiv 2 \pmod{15}. \end{cases}$$

Como $(4 : 15) = 1$, estamos en las condiciones del Teorema Chino del Resto. Luego debemos hallar r_1 y r_2 tales que $15 r_1 \equiv 1 \pmod 4$ y $4 r_2 \equiv 1 \pmod{15}$. Claramente $r_1 = 3$ y $r_2 = 4$ satisfacen lo pedido, con lo cual las soluciones del sistema son

$$x \equiv 7 \cdot 15 \cdot 3 + 2 \cdot 4 \cdot 4 \equiv 47 \pmod{60}\cdot$$

Ejercicio: hallar todas las soluciones del sistema

$$\begin{cases} x \equiv 2 \pmod 5 \\ x \equiv 1 \pmod 7 \\ x \equiv 2 \pmod{11}. \end{cases}$$

Esto tiene muchísimas aplicaciones, como veremos en breve. En particular, la idea del Teorema Chino del resto es que conocer un número módulo $N = p_1^{r_1} \dots p_n^{r_n}$ es lo mismo que conocerlo módulo $p_1^{r_1}$, ... , módulo $p_n^{r_n}$.

Proposición 8.8. *La función φ es multiplicativa, esto es si $n, m \in \mathbb{N}$ son coprimos entonces $\varphi(nm) = \varphi(n)\varphi(m)$.*

Demostración: Llamemos $\mathcal{C}_m = \{a \in \mathbb{N} \ : \ 1 \leq a \leq m \text{ y } (a : m) = 1\}$. Luego $\varphi(m) = \#\mathcal{C}_m$. Definimos la función $\Psi : \mathcal{C}_{nm} \mapsto \mathcal{C}_n \times \mathcal{C}_m$ dada por $a \mapsto (r_n(a), r_m(a))$, donde $r_n(a)$ es el resto de dividir a a por n. Veamos que Ψ está bien definida y que es biyectiva.

• **Buena definición:** Si $(a : nm) = 1$, entonces $(a : n) = 1$. Como $(a : n) = (r_n(a) : n)$, entonces $r_n(a) \in \mathcal{C}_n$. De manera análoga $r_m(a) \in \mathcal{C}_m$.

• **Inyectiva:** Si $a, b \in \mathbb{N}$ son tales que $1 \leq a, b < nm$, $r_n(a) = r_n(b)$ y $r_m(a) = r_m(b)$, queremos ver que $a = b$. Como $r_n(a) = r_n(b)$, $a \equiv b \pmod n$. Análogamente, $a \equiv b \pmod m$. O sea $n \mid (a - b)$ y $m \mid (a - b)$. Como $(n : m) = 1$, $nm \mid (a - b)$. Pero $1 \leq a, b < nm$ luego $a = b$.

• **Suryectva:** Si $a, b \in \mathbb{N}$ son tales que $1 \leq a \leq n$, $(a : n) = 1$ y $1 \leq b \leq m$,

$(b : m) = 1$, queremos ver que existe $c \in \mathbb{N}$ tal que $1 \leq c \leq nm$, $(c : nm) = 1$ y c es solución de la ecuación Luego a y b son soluciones de la ecuación

$$\begin{cases} x \equiv a \pmod{n} \\ x \equiv b \pmod{m}. \end{cases}$$

Un tal c siempre existe por el Teorema Chino del Resto. Luego el cardinal de ambos conjuntos es el mismo, o sea $\varphi(nm) = \#\mathcal{C}_{nm} = \#(\mathcal{C}_n \times \mathcal{C}_m) = \#\mathcal{C}_n.\#\mathcal{C}_m = \varphi(n)\varphi(m)$. □

Ejercicio: Probar que si $p, q \in \mathbb{N}$ son primos distintos y $a \in \mathbb{N}$ es coprimo con p y con q entonces

$$a^{[p-1:q-1]} \equiv 1 \pmod{pq},$$

donde $[p-1, q-1]$ es el mínimo común múltiplo de $p-1$ y $q-1$. Notar que esto mejora el Teorema de Euler-Fermat en este caso (que diría $a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$).

Pregunta: ¿cómo usar el Teorema Chino del Resto si los módulos no son coprimos?

Ejemplo: Supongamos que queremos hallar las soluciones del siguiente sistema (si es que tiene alguna):

$$\begin{cases} x \equiv 2 \pmod{10} \\ x \equiv 5 \pmod{15}. \end{cases}$$

Acá los módulos no son coprimos con lo cual no podemos aplicar el Teorema Chino del Resto. Sin embargo, podemos aplicarlo para separar cada una de las congruencias en congruencias que involucren primos a potencias, así son equivalentes:

$$\left\{ x \equiv 2 \pmod{10} \right. \quad \leftrightarrow \quad \begin{cases} x \equiv 2 \pmod{2} \\ x \equiv 2 \pmod{5}. \end{cases}$$

y

$$\left\{ x \equiv 5 \pmod{15} \right. \quad \leftrightarrow \quad \begin{cases} x \equiv 5 \pmod{3} \\ x \equiv 5 \pmod{5}. \end{cases}$$

Con lo cual nuestro sistema original es equivalente al sistema:

$$\begin{cases} x \equiv 2 \pmod{2} \\ x \equiv 2 \pmod{5} \\ x \equiv 5 \pmod{3} \\ x \equiv 5 \pmod{5}. \end{cases}$$

¿Tiene solución este sistema? Notar que la segunda ecuación dice que el resto de dividir a x por 5 es 2 mientras que la cuarta ecuación dice que x es divisible por 5. Luego claramente el sistema no tiene solución (o es *incompatible*).

Ejemplo: Hallar todas las soluciones del sistema:

$$\begin{cases} x \equiv 2 \pmod{15} \\ x \equiv 7 \pmod{50}. \end{cases}$$

Dado que los módulos no son coprimos (en realidad $(15 : 50) = 5$), podemos razonar como antes. Luego nuestro sistema es equivalente al sistema:

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 2 \pmod 5 \\ x \equiv 7 \pmod{25} \\ x \equiv 7 \pmod 2 \end{cases}$$

Las ecuaciones cuyos módulos no son coprimos son la segunda y la tercera. ¿Es incompatible el sistema? La respuesta es que no! La tercer ecuación nos dice que $x \equiv 7 \pmod{25}$ o sea que $25 \mid x - 7$ en particular $5 \mid x - 7$ o sea $x \equiv 7 \pmod 5$ que es lo mismo que pedir $x \equiv 2 \pmod 2$. Con lo cual la tercer ecuación implica la segunda (y es mas fuerte). Si conocemos el resto de dividir a un número por 25 en particular conocemos su resto al dividirlo por 5. Luego considerando las ecuaciones (1), (2) y (4) estamos incluyendo también la tercera. Entonces podemos mirar el sistema:

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 7 \pmod{25} \\ x \equiv 7 \pmod 2 \end{cases}$$

Ahora los módulos sí son coprimos y podemos aplicar el Teorema Chino del Resto. En realidad, dado que conocemos una solución al sistema formado por las dos últimas ecuaciones, basta considerar el sistema (mas pequeño)

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 7 \pmod{50} \end{cases}$$

Es fácil ver que $(3 : 50) = 1 = 3(17) + 50(-1)$. Con lo cual la solución del sistema es

$$x = 50.(-1).2 + 3.17.7 = 257 \equiv 107 \pmod{150}$$

Ejercicio: Para utilizar todo lo aprendido durante este capítulo, hallar (si hay) las soluciones del siguiente sistema:

$$\begin{cases} 3x \equiv 6 \pmod{18} \\ 2x \equiv 4 \pmod 5 \\ 5x^{13} \equiv 7 \pmod 9 \end{cases}$$

Comencemos resolviendo (si se puede) cada ecuación para llevarlo a un sistema del tipo del Teorema Chino del Resto.

1. $3x \equiv 6 \pmod{18}$. Como $(3 : 18) = 3 \mid 6$, sabemos que esta ecuación tiene solución. Si dividimos toda la ecuación por 3, tenemos que las soluciones son:
$$x \equiv 2 \pmod 6.$$
2. $2x \equiv 4 \pmod 5$. Dado que $(2 : 4) = 1$, hay solución. Además, como $3.2 \equiv 1 \pmod 5$ (o sea 3 es el inverso multiplicativo de 2 en $\mathbb{Z}/5\mathbb{Z}$), si multiplicamor por 3 tenemos que las soluciones son
$$x \equiv 12 \equiv 2 \pmod 5$$

3. $5x^{13} \equiv 7 \pmod 9$. Para poder aplicar Euler-Fermat, debemos probar que $(x : 9)$ debe ser 1. Como $9 = 3^2$, si $3 \mid x$ entonces $3 \mid 7$ lo que no pasa, con lo cual $(x : 9) = 1$. Como $\varphi(9) = 6$, sabemos que $x^6 \equiv 1 \pmod 9$. Luego $x^{13} = (x^6)^2.x \equiv x \pmod 9$. Así nuestra ecuación es:

$$5x \equiv 7 \pmod 9.$$

Como hicimos en el caso anterior, $(5 : 9) = 1$ y el inverso de 5 en $\mathbb{Z}/9\mathbb{Z}$ es 2. Multiplicando por 2 tenemos que

$$x \equiv 14 \equiv 5 \pmod 9.$$

Con esto hecho, nos queda que el sistema por resolver es

$$\begin{cases} x \equiv 2 \pmod 6 \\ x \equiv 2 \pmod 5 \\ x \equiv 5 \pmod 9 \end{cases} \leftrightarrow \begin{cases} x \equiv 2 \pmod 2 \\ x \equiv 2 \pmod 3 \\ x \equiv 2 \pmod 5 \\ x \equiv 5 \pmod 9 \end{cases}$$

Nuevamente, la última ecuación implica la segunda, con lo cual podemos considerar el sistema

$$\begin{cases} x \equiv 2 \pmod 2 \\ x \equiv 2 \pmod 5 \\ x \equiv 5 \pmod 9 \end{cases} \leftrightarrow \begin{cases} x \equiv 2 \pmod{10} \\ x \equiv 5 \pmod 9 \end{cases}$$

Como $(9 : 10) = 1 = 9(-1)9 + 10.1$, la solución es

$$x = 9.(-1).2 + 10.1.5 \equiv 32 \pmod{90}.$$

8.2. RSA (Rivest-Shamir-Adleman). El sistema criptográfico RSA es uno de los mas usados hoy en día. El mismo fue inventado en 1973 por Clifford Cocks. Dado que Cocks trabajaba para una agencia de seguridad nacional Británica, no pudo publicarlo hasta 1997. En 1977, Rivest, Shamir y Adleman encontraron independientemente el mismo sistema y lo patentaron.

La criptografía (de manera burda) es el estudio de cómo enviar información de manera segura entre dos personas. La idea es que cualquier persona que intercepte el mensaje no pueda saber qué información están intercambiando (como hablar un idioma extranjero adelante de personas que no lo hablan). El sistema RSA es uno de los llamados *sistemas de clave pública*. Estos métodos consisten en tener un algoritmo para "cifrar" (u ocultar) la información que se basa en algunas claves. Existen claves públicas (que son de conocimiento para cualquier persona) y claves privadas, que sólo conocen los que utilizan el algoritmo. En particular RSA posee dos claves públicas, que son un módulo m (que es un número natural con la particularidad de ser producto de dos primos p y q) y un exponente e (con la particularidad de ser coprimo con $\varphi(m)$). La factorización de m NO es pública (basándose el algoritmo en que es imposible calcularla de manera práctica). Para poder asegurar esto, los números que se utilizan son muy grandes (del orden de 2048 dígitos binarios).

El algoritmo: supongamos que tenemos un mensaje M que queremos enviarle a una persona B (por ejemplo queremos enviar el número de nuestra tarjeta de crédito al banco). El banco hace público el par (e, m) correspondiente al módulo

y al exponente. Nuestra manera de encriptar el mensaje es calcular $M^e \pmod m$ (obteniendo un número no mayor que m). Este dato es el que le enviamos a la persona B.

Desencripción: La persona B recibe un mensaje $\tilde{M}$ que sabe que es de la forma M^e para un número M desconocido. Dado que B conoce la factorización de m (en la práctica el número m es creado por B a partir de los primos p y q), puede calcular números $r, s \in \mathbb{Z}$ tales que

$$er + \varphi(m)t = (e : \varphi(m)) = 1,$$

con la condición $r \geq 0$. Luego, afirmo:

$$\tilde{M}^r = M^{er} \equiv M \pmod m.$$

Para ver esto, calculemos $\tilde{M}^r$ módulo p y módulo q. Si $p \mid M$, entonces $M \equiv 0 \equiv \tilde{M}^r \pmod p$ con lo cual la congruencia es obvia. Si $p \nmid M$, por el Teorema de Fermat, sabemos que $M^{p-1} \equiv 1 \pmod p$. Luego,

$$\tilde{M}^r = M^{er} = M^{1-(p-1)(q-1)t} = M.(M^{(p-1)})^{(1-q)t} \equiv M \pmod p$$

La congruencia módulo q se sigue del mismo razonamiento. Usando el Teorema Chino del Resto, tenemos

$$\begin{cases} \tilde{M}^r \equiv M \pmod p \\ \tilde{M}^r \equiv M \pmod q \end{cases} \quad \leftrightarrow \quad \left\{ \tilde{M}^r \equiv M \pmod{pq} \right.$$

Observación: Calcular $\varphi(pq)$ es equivalente a calcular p y q. Es claro que si conocemos p y q, entonces $\varphi(pq) = (p-1)(q-1)$. Recíprocamente, si conocemos $\varphi(pq) = (p-1)(q-1) = pq - (p+q) + 1$ y pq (esto es siempre concocido), tenemos que $p + q = pq - \varphi(pq) + 1$. O sea conocemos también cuanto vale $p + q$ con esta información. Pero si miramos el polinomio

$$(x-p)(x-q) = x^2 - (p+q)x + pq$$

tiene como raíces a p y a q y lo conocemos. Usando la fórmula de la cuadrática, recuperamos p y q.

Ejemplo: Supongamos que queremos enviarnos un mensaje con un amigo de manera secreta. Tomamos dos primos (grandes en la práctica, pero pequeños en este ejemplo para poder hacer las cuentas a mano) por ejemplo $p = 101$ y $q = 307$ con lo cual le decimos que el módulo que debe usar es 31007 (no le enviamos la factorización). Dado que $\varphi(31007) = 100 \cdot 306$, tomamos $e = 7$. Así fijadas las llaves públicas, nuestro amigo nos dice que su fecha de cumpleaños encriptada es "1867", ¿qué día cumple años?

Lo que debemos hacer es escribir 1 como combinación lineal de 7 y 30600. Usando el algoritmo de Euclídes, tenemos que:

$$30600 = 7 \cdot 4371 + 3$$
$$7 = 3 \cdot 2 + 1$$

Así, $1 = 7 \cdot 1 + 3 \cdot (-2) = 7 \cdot 1 + (30600 - 7 \cdot 4371) \cdot (-2) = 7 \cdot (8743) + 30600 \cdot (-2)$. Luego debemos calcular

$$1867^{8743} \equiv 1207 \pmod{31007}$$

(este último calculo esta hecho por computadora, pero se puede hacer de manera rápida escribiendo 8743 en base 2). Luego su cumpleaños es el 12 se Julio.