Resumen Álgebra I

Javier Vera

November 12, 2022

1 Relaciones

Dado un conjunto A una relación es un suboconjunto R de pares ordenados de A. Es decir $R \subseteq A \times A$. Dados $x, y \in A$ decimos que están relacionados si $(x, y) \in R$ (Notación: $x\ R\ y$ o $x \sim y$)
Hay diferentes tipos de relaciones sobre un conjunto A:

- Reflexivas: $\forall x \in A \quad x \sim x$
- Simétricas: $\forall x, y \in A \quad x \sim y \Rightarrow y \sim x$
- Antisimétrica: $\forall x, y \in A \quad x \sim y \wedge y \sim x \Rightarrow x = y$
- Transitiva: $\forall x, y \in A \quad x \sim y \wedge y \sim z \Rightarrow x \sim z$

Una relación Reflexiva, simétrica y transitiva se llama Relación de equivalencia
Una relación Reflexiva, antisimétrica y transitiva se llama Relación de orden

1.1 Particiones

Dada una relación de equivalencia R en un conjunto A definimos una partición

$$[a] = \{b \in A | b \sim a\} = \{b \in A | a \sim b\}$$

Llamamos a al representante de dicha partición.

Lema 1.1
Por un lado tenemos $a \in [a]$. Por otro lado dos clases de equivalencia $[a], [b]$ son disjuntas o son exactamente iguales

Proof. Si son disjuntas no hay nada que demostrar, si no lo son entonces existe $c \in [a] \cap [b]$. Ahora tomemos cualquier $x \in [a]$ sabemos que $x \sim a$ pero entonces $x \sim c$ y luego $x \sim b$ Entonces $x \in [b]$ por lo tanto $[a] \subseteq [b]$.
Análogamente probamos $[b] \subseteq [a]$ Finalmente $[a] = [b]$ □

2 Número Naturales

2.1 Axiómas de Peano

N1. El 1 no és sucesor de nadie

N2. Dos naturales distinto tienen distintos sucesores

N3. (Axioma de inducción) Si $K \subseteq \mathbb{N}$ con $1 \in K$ y además dado $x \in K$ sucede que $S(x) \in K$ (sucesors de x está en K) entonces $\mathbb{N} \subseteq K$

Hay otros axioma de Peano, pero no se han dado en la materia, se pueden buscar en Wikipedia

2.2 Inducción Matemática

Partiendo de los axiomas de Peano podemos definir $\mathbb{N}$ como el subconjunto de $\mathbb{R}$ que cumple dichos axiomas

Teorema 2.1 (Principio de inducción)
Sea $P(n)$ una función proposicional con $n \in \mathbb{N}$

1. *$P(1)$ es verdadera*
2. *Dado $n \in \mathbb{N}$ si $P(n)$ verdadera entonces $P(n+1)$ es veradera*

Entonces $P(n)$ es verdadera $\forall n \in \mathbb{N}$

Proof. Sea

$$K = \{n \in \mathbb{N} \mid P(n) \text{ es verdadera } \}$$

Por hipótesis 1. tenemos $1 \in K$, por 2. tenemos que $n \in K$ implica $n+1 \in K$ usando estos dos se cumple el axioma N3 de peano. Por lo tanto $\mathbb{N} \subseteq K$ esto implica además sabemos que $K \subseteq \mathbb{N}$ entonces tenemos $K = \mathbb{N}$. Esto implica que $P(n)$ es verdadera $\forall n \in \mathbb{N}$ □

Teorema 2.2 (Inducción Corrida)
Sea $P(n)$ una función proposicional con $n \geq N$

1. *$P(N)$ es verdadera*
2. *Si $P(n)$ verdadera implica $P(n+1)$ verdadera $\forall n \geq N$*

Entonces $P(n)$ es verdadera $\forall n \geq N$

Proof. Sea $Q(n) = P(N-1+k)$. Ahora consideremos el conjunto

$$K = \{n \in \mathbb{N} \mid Q(n) \text{ es verdadera } \}$$

Trivialmente tenemos $Q(1) = P(N)$ entonces por hipótesis es verdadera. Además dado cualquier $n \in \mathbb{N}$ tenemos $Q(n) = P(N-1+n)$ y dado que $N-1+n \geq N$ por hipótesis $P(N-1+n+1) = Q(n+1)$ es verdadera.

Pero entonces K cumple las hipótesis de el axioma N3 de peano, por lo tanto $\mathbb{N} \subseteq K$ y como sabemos $K \subseteq \mathbb{N}$ entonces $K = \mathbb{N}$.

Como cada natural $m \geq N$ se escribe de la forma $N-1+n$ tenemos que $P(n)$ es verdadera $\forall n \geq N$ □

Teorema 2.3 (Inducción Fuerte)
Sea $n \in \mathbb{N}$ y $P(n)$ una función proposicional

1. *$P(1)$ es verdadera*
2. *Si $P(1), P(2) \dots P(k)$ verdaderas implica $P(k+1)$ verdadera $\forall k \in \mathbb{N}$*

Entonces $P(n)$ es verdadera $\forall n \in \mathbb{N}$

Observación (Suma de Gauss)

$$\sum_{i=1}^{n} i = \frac{n.(n+1)}{2}$$

Se demuestra usando inducción

Observación (Suma Aritmética)
Una sucesión es aritmética si satisface $a_{n+1} = a_n + c$. Por ejemplo $a_1 = b,\ a_2 = b + c,\ a_3 = b + 2c\ \cdots a_n = b + c(n-1)$

$$\sum_{i=1}^{n} a_i = nb + \frac{(n-1)n}{2}$$

Proof. $\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} b + (i-1) = \sum_{i=1}^{n} b + \sum_{i=1}^{n} (i-1) = bn + \sum_{i=1}^{n} (i-1) = nb + \frac{(n-1)n}{2}$.
Aquí usamos la Suma de Gauss □

Observación (Suma Geométrica)
Una sucesión es geométrica si satisface $a_1 = b,\ a_2 = br,\ a_3 = br^2 \cdots a_n = br^{n-1}$

$$\sum_{i=0}^{n} br^i = b \sum_{i=0}^{n} r^i = b \frac{1 - r^{n-1}}{1 - r}$$

Lema 2.4

$$\textit{Inducción Fuerte} \iff \textit{Inducción Corrida} \iff \textit{Inducción}$$

Proof. Veamos Inducción Fuerte $\iff$ Inducción
$\Rightarrow$) Tomemos $Q(k)$ como la proposición "$P(n)$ verdadera $\forall n \leq k$". Para empezar $Q(1)$ es trivialmente verdadera.
Ahora inducción nos dice que $Q(k)$ implica $Q(k+1)$ para cualquier $k \in \mathbb{N}$

1. Luego "$P(n)$ verdadera $\forall n \leq k$" $\iff$ $Q(k)$ Verdadera.
2. Pero si $Q(k)$ verdadera entonces $Q(k+1)$ Verdadera (Inducción)
3. $Q(k+1)$ Verdadera $\iff$ "$P(n)$ verdadera $\forall n \leq k+1$"

Juntando nos queda

$P(1) \dots P(k)$ Verdaderas $\iff$ "$P(n)$ Verdadera $\forall n \leq k$" $\Rightarrow$ "$P(n)$ Verdadera $\forall n \leq k+1$" $\Rightarrow$ $P(k+1)$ Verdadera

Entonces por inducción corrida $P(n)$ es verdadera $\forall n \in \mathbb{N}$. Pero entonces $Q(k)$ es verdadera $\forall k \in \mathbb{N}$.
Por lo tanto probamos que si inducción completa vale. Las dos hipótesis de inducción implican el resultado de inducción que conocemos, que es lo mismo que decir que inducción vale.
Probar que inducción completa vale usando inducción es trivial, queda como ejercicio para el lector

□

3 Principio de buen órden

Teorema 3.1 (Principio de buen órden)
Un conjunto A se dice bien ordenado si dado cualquier $B \subseteq A$ con $B \neq \emptyset$ tiene primer elemento. Un primer elmento es un elemento menor o igual que el resto. En esta matería solo nos interesará el buen órden de los naturales

Proposición 1
$\mathbb{N}$ *es bien ordenado*

Proof. Supongamos que no es bien ordenado entonces $\exists H \subseteq \mathbb{N}$ tal que $H \neq \emptyset$, sin primer elemento
Ahora consideremos $H^c = \mathbb{N} - H$ sabemos que $1 \in H^c$, si nó estaría en H lo cual sería absurdo
Ahora consideremos $K = \{n \in \mathbb{N} \mid [1 \dots n] \subseteq H^c\}$. Por lo dicho arriba $1 \in K$
Ademas si $n \in K$ tenemos que $n+1 \in K$ por que si $n+1 \notin K$ tendríamos que todos los elementos menores o iguales que n estan en K por lo tanto estarían en H^c y $n+1 \notin K$ por lo tanto $n+1 \notin H^c$ entonces $n+1 \in H$ pero entonces $n+1$ sería primer elemento de H lo cual sería absurdo.
Entonces K cumple las hipótesis de inducción por lo tanto $K = \mathbb{N}$. Pero entonces $\mathbb{N} \subseteq H^c$ Y ya teníamos que $H^c \subseteq \mathbb{N}$ por lo cual $H^c = \mathbb{N}$. Finamente $\mathbb{N} = \mathbb{N} - H$ entonces $H = \emptyset$. Absurdo
Provino de suponer que existía dicho H no vacío sin primer elemento, entonces no existe dicho conjunto □

Proposición 2
Buen órden en $\mathbb{N}$ *implica inducción*

Proof. Sea $K = \{n \in \mathbb{N} \mid P(n) \text{ es verdadera}\}$ y miremos usando las hipótesis de inducción y el buen orden nos gustaría llegar a que $K = \mathbb{N}$ o lo que es lo mismo $K^c = \emptyset$. Supongamo que $K^c \neq \emptyset$ entonces por buen órden $\exists k \in K^c$ primer elemento.
Por inducción sabemos que $1 \in K$. Entonces dicho $k > 1$ luego tenemos que $n \in K$ para todo $n \leq k-1$. Si nó k no sería primer elemento de K^c, pero por inducción esto nos dice que $k \in K$ lo que es absurdo. Provino de suponer que $K^c \neq \emptyset$ por lo tanto $K^c = \emptyset$ Entonces $K = \mathbb{N}$ probando que $P(n)$ es verdadera $\forall n \in \mathbb{N}$ y por lo tanto probando la implicación final de inducción □

Proposición 3
Inducción implica buen órden en $\mathbb{N}$

Proof. Sea $K \subseteq \mathbb{N}$ tal que $K \neq \emptyset$ y K no tiene primer elemento. Como no tiene primer elemento $1 \in K^c$. Ahora supongamos que $1 \dots n \in K^c$ entonces $n+1 \in K^c$ por que si nó estaría en K y sería su primer elemento, pero entonces por inducción $K^c = \mathbb{N}$ por lo tanto $K = \emptyset$ abusrdo. Provino de suponer que existía dicho $K \neq \emptyset$, no vacío y sin primer elemento, entonces todo $K \neq \emptyset$ no vacío, tiene primer elemento □

Corolario 3.1.1

$$\textit{Buen órden en } \mathbb{N} \iff \textit{Inducción} \iff \textit{Inducción completa} \iff \textit{Inducción corrida}$$

4 Combinatoria

Definición 4.1
Un conjunto A tiene n elementos si y solo sí existe

$$f : A \to [1 \dots n] \textit{ biyectiva}$$

En estos casos decimos $|A| = n$ (cardinal de A es n)

Lema 4.1 (Principio de adición)
Sean A y B conjuntos disjuntos tales que $|A| = n$ y $|B| = m$ entonces

$$|A \cup B| = |A| + |B| = n + m$$

Proof. Por hipótesis tenemos $f : A \to [1 \dots n]$ y $g : B \to [1 \dots m]$ ambas biyectivas.
Definimos $h : A \cup B \to [1 \dots n+m]$

$$h(x) = \begin{cases} f(x) & \text{si } x \in A \\ g(x) + n & \text{si } x \in B \end{cases}$$

Veamos que es biyectiva. Podríamos ver que es inyectiva y suryectiva, pero es más facil dar su inversa. Sabemos que f y g tienen inversas por ser biyectivas llamemoslas f^{-1} y g^{-1}
Sea $r : [1 \dots n+m] \to A \cup B$

$$r(x) = \begin{cases} f^{-1}(x) & \text{si } x \leq n \\ g^{-1}(x-n) & \text{si } x > n \end{cases}$$

Veamos que efectivamente es su inversa mostrando que $h \circ r = id = r \circ h$
Primero supongamos $x \leq n$ entonces $h \circ r(x) = h(r(x)) = h(f^{-1}(x))$ además $f^{-1}(x) \in A$ por definición entonces $h(f^{-1}(x)) = f(f^{-1}(x)) = x$, por que f^{-1} es la inversa de f.(f tiene inversa por ser biyectiva)
Si en cambio $x > n$ entonces $h \circ r(x) = h(r(x)) = h(g^{-1}(x-n))$ además $g^{-1}(x) \in B$ por definición entonces $h(g^{-1}(x-n)) = g(g^{-1}(x-n)) + n = x - n + n = x$
$r \circ h = id$ sale con las mismas ideas, queda como ejercicio para el lector. Entonces como $h(x)$ tiene inversa por lo tanto es biyectiva
Finalmente $|A \cup B| = |[1 \dots n+m]| = n+m$ □

Corolario 4.1.1

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

Proof. Por inducción, el caso base es trivial.
Ahora si tenemos $|A_1 \cup \dots \cup A_n \cup A_{n+1}| = |(A_1 \cup \dots \cup A_n) \cup A_{n+1}| = |B \cup A_{n+1}| = |B| + |A_{n+1}|$
Por hipótesis tenemos $|B| + |A_{n+1}| = |A_1| + |A_2| + \cdots + |A_n| + |A_{n+1}|$ □

Lema 4.2 (Principio de multiplicación)
A y B conjuntos finitos entonces $|A \times B| = |A||B|$

Proof. Tenemos $A \times B = (\{a_1\} \times B) \cup (\{a_2\} \times B) \cdots \cup (\{a_n\} \times B)$
Por principio de adición $|A \times B| = |\{a_1\} \times B| + |\{a_2\} \times B| + \cdots + |\{a_n\} \times B|$
Es trivial notar que $|\{a_n\} \times B|$ es igual para cualquier n
Entonces calculemos $|\{a_1\} \times B|$. Sabemos que existe una función biyectiva $h : B \to [1 \dots |B|]$
Entonces podemos construir la función $g : \{a_1\} \times B \to [1 \dots m]$ donde $|B| = m$ dada por

$$g(a_1, b) = h(b)$$

Veamos g inyectiva. Sean $g(a_1, b_1) = g(a_1, b_2)$ entonces $h(b_1) = h(b_2)$ como h es inyectiva $b_1 = b_2$
Veamos g sobreyectiva. Sea $y \in [0 \dots |B|]$ dado que h es sobreyectiva existe $b_1 \in B$ tal que $h(b_1) = y$ pero entonces $g(a_1, b_1) = h(b_1) = y$. Finalmente dado cualquier $y \in [1 \dots |B|]$ se puede dar una preimagen por g.
Entonces g es sobreyectiva mostrando que $|\{a_n\} \cup B| = |B|$. Ahora si juntamos esto con lo que habíamos visto por principio de adición tenemos

$$|A \times B| = |\{a_1\} \times B| + |\{a_2\} \times B| + \cdots + |\{a_n\} \times B| = |B| + |B| \dots |B|$$

Donde la cantidad de sumandos es igual a la cantidad de elementos en A que es igual a $|A|$
Entonces $|A \times B| = |A||B|$

□

Lema 4.3 (Principio de complemento)
Sea $A \subseteq \mathcal{U}$ entonces $|A| = |\mathcal{U}| - |A^c|$

Lema 4.4 (Principio de inyección de Cantor)
Sean A y B finitos entonces si $|A| > |B|$ no existe ninguna función $f : A \to B$ inyectiva. Mas aún si tenemos $f : A \to B$ inyectiva entonces $|A| \leq |B|$

Proof. Tomemos el conjunto $H = \{n \in \mathbb{N} | \exists m \in \mathbb{N}, m < n \text{ y } f : [1 \dots n] \to [1 \dots m] \text{ inyectiva } \}$

Nos gustaria ver que dicho conjunto es vacío. Supongamos que nó, entonces tiene primer elemento llamémoslo h.Sabemos que $1 \notin H$ por que no existe ningún natural menor que 1. Entonces $h > 1$

Como $h \in H$ tenemos un $m \in \mathbb{N}$ con $m < h$ tal que $f : [1 \dots h] \to [1 \dots m]$ inyectiva. Supongamos que $f(h) = m$, entonces podemos restringir f y obtener $g : [1 \dots h-1] \to [1 \dots m-1]$, que es inyectiva por que restringimos una inyectiva Pero entonces $h - 1 \in H$ que sería absurdo.

Ahora si $f(h) = p < m$ podemos armar armar $\alpha : [1 \dots m] \to [1 \dots m]$ con $\alpha(p) = m$, $\alpha(m) = p$, $\alpha(i) = i \; \forall i \neq m \neq p$

Ahora podemos dar $r = \alpha \circ f : [1 \dots h] \to [1 \dots m]$ y sabemos que $r(h) = \alpha(f(h)) = \alpha(p) = m$. Pero entonces estamos en el anteriór caso restringimos r y llegamos a un absurdo □

Corolario 4.4.1
$|A| = n \wedge |A| = m$ entonces $n = m$

Proof. $|A| = n$ entonces tenemos $f : A \to [1 \dots n]$ biyectiva y $g : A \to [1 \dots m]$

Entonces tenemos $g \circ f^{-1} : [1 \dots n] \to [1 \dots m]$ inyectiva por ser composición de inyectivas entonces

$$n = |[1 \dots n]| \leq |[1 \dots m]| = m$$

analogamente tenemos una función $h : [1 \dots m] \to [1 \dots n]$ por lo cual

$$m = |[1 \dots m]| \leq |[1 \dots n]| = n$$

Entonces finalmente $n = m$ □

Observación (Permutaciones)
Sea A tal que $|A| = n$ entonces hay $n!$ formas de ordenar A. En este tipo de conteo importa el órden

Observación (Combinaciones)
Sea A tal que $|A| = n$ entonces tenemos $\binom{n}{k}$ subconjuntos de A te tamaño k. En este tipo de conteo no importa el ordan $\{1,2,3\}$ es lo mismo que $\{1,3,2\}$ por ende no lo cuento dos veces

Proof. Tengo que elejir *kelmentos* para el primer elemento tengo n opciones , para el segudno $n-1$ así hasta el k-esimo en donde tengo $n-k+1$ opciones. Por ende tengo $n.(n-1)\dots(n-k+1)$ formas de elegir k elementos entre n elementos Una vez seleccionados esos k elementos, tengo $k!$ permutaciones dentro de mi selección que no me interesan dado que dos conjuntos con diferente orden son iguales. Entonces divido por $k!$ obteniendo

$$\frac{n.(n-1)\dots(n-k+1)}{k!} = \frac{n.(n-1)\dots(n-k+1)(n-k)!}{k!(n-k)!} = \frac{n!}{k!(n-k)}$$

□

Observación (Arreglos)
Un arreglo es una selección de k elementos sobre un conjunto A. Si $|A| = n$ entonces tenemos $\frac{n!}{(n-k)!}$ arreglos

Observación
$\binom{n}{k} = \binom{n}{n-k}$

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

Otra forma alternativa es considerar $f : P_k(I_n) \to P_{n-k}(I_n)$, la función complemento. Tomas conjuntos de tamaño k y devuelve su complemento que son conjuntos de tamaño $n-k$. Resta ver que es biyectiva y eso nos diría que $\binom{n}{k} = |P_k(I_n)| = |P_{n-k}(I_n)| = \binom{n}{n-k}$

□

Teorema 4.5 (Identidad de pascal)
$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$

Proof. Una forma es aritmética, queda como ejercicio para el lector

Otra forma es mirar los conjuntos

$$B = \{K \subseteq I_{n+1} \mid |K| = k \wedge n+1 \in K\} = \{K \subseteq I_n \mid |K| = k-1\} = \mathcal{P}_{k-1}(I_n)$$

$$A = \{K \subseteq I_{n+1} \mid |K| = k \wedge n+1 \notin K\} = \{K \subseteq I_n \mid |K| = k\} = \mathcal{P}_k(I_n)$$

Notemos que $A \cup B = \mathcal{P}_k(I_{n+1})$ entonces $|A \cup B| = \binom{n+1}{k}$

Pero además tenemos $\binom{n+1}{k} = |A \cup B| = |A| + |B| = |\mathcal{P}_{k-1}(I_n)| + |\mathcal{P}_k(I_n)| = \binom{n}{k-1} + \binom{n}{k}$ □

Teorema 4.6

$|\mathcal{P}(I_n)| = 2^n$. Mas aún dado A tal que $|A| = n$ entonces $|\mathcal{P}(A)| = 2^n$

Proof. Ahora notemos que $|\{f \mid f : I_n \to \{0,1\}\}| = 2^n$. Esto sale facil usando combinatoria, particularmente permutaciones dado el primer elemento de I_n tenemos 2 opciones y así sucesivamente entonces tenemos 2.2.2 . . . 2 n veces cantidad de funciones en dicho conjunto

Ahora veamos $g : \mathcal{P}(I_n) \to \{f \mid f : I_n \to \{0,1\}\}$ dada por

$$X \to f_X(x) \quad f_X(x) = \begin{cases} 0 & \text{si } x \notin X \\ 1 & \text{si } x \in X \end{cases}$$

Inyectividad dados X, Y supongamos que $g(X) = f_x = f_y = g(Y)$. Ahora tomemos $x \in X$ sabemos entonces que $f_x(x) = 1$ entonces como $f_x = f_y$ sabemos que $f_y(x) = 1$ por lo tanto $x \in Y$ esto nos dice $X \subseteq Y$ y analogamente vemos que $Y \subseteq X$ mostrando que $X = Y$ mostrando inyectividad

La sobreyectividad es trivial, dada cualquier función f_x en $Im(g)$ podemos tomar X y sabemos que $g(X) = f_x$

Finalmente g es biyectiva, por lo tanto $|\mathcal{P}(I_n)| = |\{f \mid f : I_n \to \{0,1\}\}| = 2^n$

Hay otra prueba alternativa, veámosla Sabemos que $|\mathcal{P}(I_n)| = \sum_{i=0}^{n} |\mathcal{P}_i(I_n)| = \sum_{i=0}^{n} \binom{n}{i}$

Veamos que $\sum_{i=0}^{n} \binom{n}{i} = 2^n$ por inducción. El caso base es trivial

Como hipotesis inductiva tenemos $\sum_{i=0}^{n} \binom{n}{i} = 2^n$. Miremos

$$\left[\sum_{i=0}^{n+1} \binom{n+1}{i}\right] = [\sum_{i=1}^{n} \binom{n+1}{i}] + \binom{n+1}{n+1} + \binom{n+1}{0}$$

Usando la identidad de pascal

$$\left[\sum_{i=1}^{n} \binom{n+1}{i}\right] + \binom{n+1}{n+1} + \binom{n+1}{0} = \left(\sum_{i=1}^{n} \binom{n}{i} + \binom{n}{i-1}\right) + \binom{n+1}{n+1} + \binom{n+1}{0}$$

Separando la suma

$$\left(\sum_{i=1}^{n} \binom{n}{i} + \sum_{i=1}^{n} \binom{n}{i-1}\right) + \binom{n+1}{n+1} + \binom{n+1}{0}$$

Ademas sabemos

$$\binom{n+1}{0} = \binom{n}{0} \quad \wedge \quad \sum_{i=1}^{n} \binom{n}{i-1} = \sum_{i=0}^{n-1} \quad \wedge \quad \binom{n}{n}\binom{n+1}{n+1} = \binom{n}{n}$$

Juntando todo con cuidado queda

$$\sum_{i=0}^{n+1} \binom{n+1}{i} = \sum_{i=0}^{n} \binom{n}{n} + \sum_{i=0}^{n} \binom{n}{n}$$

Que por hipótesis es $2^n + 2^n = 2.2^n = 2^{n+1}$. Probando así la inducción □

Teorema 4.7 (Binomio de Newton)

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

Proof. Sabemos que $(x+y)^n$ es una suma de productos de x con y con cada producto $x^{n-k}y^k$ con $0 \leq k \leq n$

Ahora la pregunta es cuantos de cada uno de estos productos tenemos, primero seleccionamos $\binom{n}{k}$ esto nos dice las posiciones de las y en el producto y una vez definidas estas lo espacios restantes son para x

Entonces sabemos que tenemos $\binom{n}{k}$ formas de armar un producto de la pinta $x^{n-k}y^k$.

Ahora si sumamos todo tenemos $\sum_0^n \binom{n}{k} x^{n-k}y^k$ como queríamos mostrar □

5 Aritmética Entera

Definimos a $\mathbb{Z} = -\mathbb{N} \cup \{0\} \cup \mathbb{N}$

Y damos dos operaciones $(Producto) * : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ y suma $(Suma) + : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$

Estas operaciones las definimos como la restricción de las mismas en $\mathbb{R}$

Tenemos entonces que $(\mathbb{Z}, (*, +))$ es un anillo conmutativo. Más aún es un anillo conmutativo al que le podemos dar un orden estricto

Definición 5.1
En todo anillo ordenado valen:

1. $a < b \Rightarrow a + c < b + c$
2. $c > 0 \wedge a > b \Rightarrow ca > cb$
3. $-a.b = -(ab)$

Proposición 4
En todo anillo ordenado valen:

1. $c > 0 \iff -c < 0$
2. $c < 0 \wedge a > b \Rightarrow ac < bc$
3. $ab = 0 \iff a = 0 \vee b = 0$
4. $c \neq 0 \wedge ac = bc \Rightarrow a = b$

Proof. 1. $c > 0 \iff c - c > 0 - c \iff 0 > -c$ (usando la prop 1 dada por órden)

2. $c < 0 \Rightarrow -c > 0 \wedge a > b \Rightarrow -c.a > -c.b \iff -(ca) > -(cb) \iff cb > ca$
   (usando la propiedad 2 y 3 dadas por órden)
3. Ida. Supongamos que $a \neq 0 \wedge b \neq 0$
   Hay que dividir en casos
   (a) $a > 0 \wedge b > 0 \Rightarrow ab > b.0 \iff ab > 0$
   (b) $a > 0 \wedge b < 0 \Rightarrow a.b < b.0 \iff ab < 0$
   (c) Los otros dos caso son iguales
   Finalmente en todos los casos llegamos a que $ab \neq 0$ que es absurdo, provino de suponer $a \neq 0 \wedge b \neq 0$
   Entonces vale el complemento $a = 0 \vee b = 0$

   La vuelta es trivial
4. $ac = bc \Rightarrow ac - bc = 0 \Rightarrow c(a - b) = 0$ por la prop anteriór $c = 0 \vee a - b = 0 \Rightarrow a - b = 0 \Rightarrow a = b$

□

6 Divisibilidad

Definición 6.1
Decimos que a divide a b sii $\exists k \in \mathbb{Z}$ tal que $a.k = b$ lo notamos $a|b$ y este k es único dado que si $ak = b = ak'$ entonces $ak - ak' = 0 \iff a(k - k') = 0$ como $a \neq 0$ entonces $k = k'$. Si $a = 0$ entonces $b = 0$ en ese caso k no es necesariamente único, pero es un caso que no nos interesa mucho

Proposición 5
$\forall a, b \in \mathbb{Z}$ valen:

1. $1| \pm a \wedge -1| \pm a$
2. $a| \pm a \wedge -a| \pm a$
3. $a|b \iff a| \pm b \iff -a| \pm b$
4. $a|0$
5. $0|a \iff a = 0$

Las demostraciones son triviales y salen usando la definición

Proposición 6 1. $a|b \wedge b|c \Rightarrow a|c$

2. $a|b \wedge b|a \Rightarrow b = a \vee a = -b$
3. $a|b \wedge a|c \Rightarrow a|b \pm c$
4. $a|b \pm c \wedge a|b \Rightarrow a|c$
5. $a|b \Rightarrow a|bc$

Definición 6.2
El conjunto de divisores de n se nota $div(n) = \{d \in \mathbb{Z} \mid d|n\}$. *Y cumple ciertas propiedades*

1. *Además* $\{1, -1, n, -n\} \subseteq div(n)$
2. *Además* $div(1) = \{1, -1\}$
3. $div(0) = \mathbb{Z}$
4. $a \in div(n) \iff -a \in div(n)$
5. $div(n) = div(-n)$
6. $div(a) = div(b) \iff a = |b|$

Lema 6.1
Si $b \neq 0$ *y* $a|b \Rightarrow |a| \leq |b|$

Proof. $a|b \Rightarrow b = ak \Rightarrow |b| = |ak| = |a||k| \geq |a|$ esto último vale por que $|k| \in \mathbb{Z}$ □

Corolario 6.1.1
Sea $n \in \mathbb{Z}$ *con* $n \neq 0$ *entonces* $Div(n)$ *es finito y más aún* $Div(n) \subseteq [-n, n]$

7 Números Primos

Todo número entero a tiene cuatro divisores triviales $\{a, -a, 1, -1\}$. Un número natural mayor que 1 es primo si tiene solo divisores triviales.

Observación
Veamos un par de detalles

1. *1 no es primo*
2. *2 es primo (-2 no)*
3. *0 no es primo*
4. *si p y q son primo entonces o no se dividen o son el mismo primo (p|q con p y q primos entonces p = q)*

Teorema 7.1 (Teorema fundamental de la aritmética)
Todo numero natural mayor que 1 se puede escribir como producto único de primos salvo permutaciones de orden Además si el número es entero no natual menor que -1 se puede escribir como producto de primos multiplicados por -1

Proof. Veamos la existencia usando inducción fuerte. el caso base es trivial por que es 2 que ya és primo

Veamos la inducción, nuestra hipótesis es que todo numero $2 \leq k \leq n$ se puede escribir como producto de primos

Ahora tenemos $n + 1$ si es primo ya está escrito como producto de primos, si no és primo tiene algún divisor no trivial j entonces $n + 1 = jl$ con $2 < j < n + 1$ y $2 < l < n + 1$ por lo tanto j y l por hipótesis pueden ser escritos como productos de primos.

Pero entonces k puede ser escrito multiplicando j y l como producto de primosz

□

Proposición 7
Directamente del TFA tenemos que todo entero diferente de ± 1 *es divisible por un primo*

Observación
Habría que correjirlo para números negativos, pero es directo. Si tenemos un número negativo lo multiplicamos por -1, ahora usamos TFA y el primo divisor que obtenemos, nos sirve para el número negativo también por que $p|a \iff p|-a$

Teorema 7.2
Existen infinitos primos

Proof. Supongamos que hay finitos primos si los multiplicamos todos tenemos $p = p_1 p_2 \dots p_n$. Ahora $p+1$ no es primo, por que es mas grande que p_n que era el primo mas grande. Pero por el inciso anteriór sucede que entonces existe p_i entre nuestros primos tal que $p_i|p+1$ además $p_i|p$ pero entonces $p_i|1$ lo que es absurdo □

Lema 7.3
Dados dos enteros positivos a,b existen k y r con $0 \leq r \leq b$ *tales que* $a = bk + r$. *Mas aún q y r son únicos.*

Proof. Sea $H\{n \in \mathbb{N} | a < nb\}$ sabemos que $H \neq \emptyset$ entonces tiene primer elemento

sea n su primer elemento y $q = n-1$ entonces $qb \leq a < nb = (q+1)b$, si nó $qb \leq a$ por que si fuera $a < qb = (n-1)b$ entonces $n-1 \in H$ por lo cual n no sería primer elemento

Ahora tenemos que $0 \leq a - qb < b$ llamando $a - qb = r$ tenemos que $0 \leq r < b$ y $a = bq + r$

Veamos que son únicos, supongamos $bq + r = bq' + r'$ entonces $b(q - q') = r' - r$. sin pérdida de generalidades supongamos $r' > r$ entonces $r' - r \geq 0$ y además dado que $r' < b$ por definición entonces $r' - r < b$.

Pero entonces tengo que b por un entero es igual a algo menor que b y mayor igual que 0, la única forma de que esto suceda es que dicho algo sea cero y b por un entero también sea cero.

Entonces $r' - r = 0$ mostrando que $r = r'$ y $b(q - q') = 0$ como $b \neq 0$ entonces $q = q'$ □

Corolario 7.3.1 (Algoritmo de la división)
Dados $a, b \in \mathbb{Z}$ *con* $b \neq 0$ *existen únicos enteros q y r tales que* $a = bq + r$ *con* $0 \leq r < |b|$.

Notación: dicho r se nota $r_b(a)$ *que sería resto de dividir a por b*

Proof. Veamos por casos $a > 0 \wedge b > 0$ es lo mismo que la anteriór y $b = |b|$ entonces ya está demostra $a < 0 y b > 0$ tenemos que $-a > 0$ entonces por inciso anteriór $-a = bk + r$ entonces

$$a = -bk - r = -bk - r - b + b = b(-k-1) - r + b$$

Ahora sabemos si llamamos $b - r = r' \wedge -k - 1 = q$ tenemos $a = bq + r'$ con $0 \leq r' < b = |b|$.

La unicidad vale sale de la misma forma que el inciso anteriór

Caso $a > 0 \wedge b < 0$ entonces $-b > 0$ entonces $a = -bj + r'$ si tomamos $-j = q$ tenemos $a = bq + r'$ con $0 \leq r' < -b < |b|$

La unicidad sale igual

Caso $a < 0 \wedge b < 0$ entonces $-a > 0 \wedge -b > 0$ por lo tanto $-a = -bk + r'$ entonces $a = bk - r' = bk - b + b - r' = b(k-1) - r' - b = bq + r$ con $0 \leq r < |b|$ □

8 Máximo común divisór

Definición 8.1
El máximo común divisór (MCD) entre dos enteros a y b es valga la rebundancia el mas grande de los divisores comunes entre a y b. Notación $(a : b)$

Otra forma de verlo es $max(div(a) \cap div(b))$

Observación
el MCD está bien definido por que $div(a) \cap div(b)$ *seguro es no vacío, dado que el 1 pertenece a ambos conjuntos y son finitos ambos siempre y cuando* $a \neq 0 \neq b$ *por lo tanto la intersección es finita también. Por otro lado todos los divisores de a y b son enteros,entonces su intersección seran enteros*

Observación
Propiedades

1. $(a : b) \geq 1$
2. $(a : b) = (b : a)$

3. $(1 : a) = 1 \quad \forall a \in \mathbb{Z}$

4. $(a : b) = (-a : b) = (a : -b) = (-a : -b) = (|a| : |b|)$

5. *Dos números a,b se dicen coprimos si* $(a : b = 1)$

8.1 Combinaciones Lineales

Definición 8.2
$(a : b)$ *tiene como propiedad relevante que puede ser escrito como combinación lineal de a y b, es decir*

$$\exists k, j \in \mathbb{Z} \ \ tal\ que \ \ (a : b) = aj + bk$$

Lema 8.1 (Caracterización I del MCD)
Dados a y b no nulos $(a : b)$ *es el menor natural que puede ser escrito como combinación lineal entre a y b.*

Proof. Sea $e = na + mb$ el menór natural que puede ser escrito como combinación lineal entre a y b. Veamos primero que divide a b y a a. Supongamos que no divide a b entonces $b = qe + r$ con $0 < r \leq |e| = e$. Luego $b = qna + qmb + r$ por lo tanto $r = b - qna - qmb = b(1 - qm) + (-qn)a$, pero entonces r es una combinación lineal de a y b mas chica que e lo cual es absurdo Lo mismo sucede con a, entonces e es divisr común, veamos ahora que es el más grande Tomemos otro divisor común d ahora $d|a \Rightarrow d|na$ y $d|b \Rightarrow d|mb$ entonces $d|nm + mb = e$
Por lo tanto $d \leq |e| = e$. Entonces cualquier otro divisor común es mas peqeño que e □

Corolario 8.1.1 1. *Si* $a|bc \wedge (a : c) = 1 \Rightarrow a|b$

2. *Si* $a|c \wedge b|c \wedge (a : b) = 1 \Rightarrow ab|c$

Proof. 1. Como $(a : c) = 1$ entonces existen $n, m \in \mathbb{Z}$ tales que $1 = am + cn$ entonces $b = bam + bcn$
Ahora $a|bc \wedge a|bam \Rightarrow a|bam + bcn = b$

2. $am + bn = 1$ entonces $cam + cbn = c$ pero $a|c$ entonces $ab|cb$ y $b|c$ entoces $ab|ca$.
Juntando todo tenemos que $ab|cbn + cam = c$

□

Corolario 8.1.2
Dados $a, b \in \mathbb{Z}$ $\frac{a}{(a:b)}$, $\frac{b}{(a:b)}$ *son coprimos*

Proof. Sea $(a : b) = am + bn$ entonces $1 = \frac{am}{(a:b)} + \frac{bn}{(a:b)} = 1 = m\frac{a}{(a:b)} + n\frac{b}{(a:b)}$
Lo que implica que $1 = (\frac{a}{(a:b)} : \frac{b}{(a:b)})$, por que no hay combinación lineal posible mas pequéna que 1 □

Lema 8.2
Sea $a, b \in \mathbb{Z}$ *entonces* $(a : b) = (a : b + ma)$ *para cualquier* $n \in \mathbb{Z}$

Proof. $(a : b) = aj + bk = aj + bk - kma + kma = (j - km)a + k(b + ma)$. Entoces escribi a a y a $b + ma$ como combinación lineal. Supongamos que dicha combinación lineal no es la mas chica, entonces existe $k', j' \in \mathbb{Z}$ tal que $ak' + (b + ma)j' < (j - km)a + k(b + ma) = (a : b)$ entonces reordenando $a(k' + mj) + bj' < (a : b)$ Pero esto es absurdo, no podemos tener una combinación de a y b mas chica que $(a : b)$ □

Lema 8.3 (Caracterización 2 del MCD)
Sean a, b *y sea* $d \in \mathbb{N}$ *tal que*

1. $d|a \wedge d|b$

2. $d'|a \wedge d'|b \Rightarrow d'|d$

Entonces $d = (a : b)$

Observación
Vale la recíproca también, si $d(a : b)$ *entonces cumple 1 y 2*

Corolario 8.3.1
Sean $a, b \in \mathbb{Z}$ *con* $a \geq b$ *sabemos que existen* q, r *tales que* $a = qb + r$ *con* $0 \leq r < b$. *Entonces* $(a : b) = (b : r)$

Proof. $(a : b) = (b : a) = (b : a + mb)$ ahora si tomamos $q = -m$ tenemos $(b : a + mb) = (b : a - qb)$ pero $a - qb = r_b(a)$ entonces

$$(a : b) = (b : a) = (b : a + mb) = (b : a - qb) = (b : r_b(a))$$

□

Proposición 8
Usando este último resultado podemos tenemos una forma de calcular $(a : b)$ llamada algoritmo de euclides
$(a : b) = (b : r_1) = (r_1 : r_2) = \ldots = (r_n : 0)$ *con* $|b| > r_1 > r_2 > \ldots > 0$
Como son todos números naturales esta sucesión debe ser finita y nos quedamos. Finalmente $(a : b) = r_{n-1}$

9 Mínimo Común Múltiplo

Definición 9.1
Dados dos enteros no nulos a y b el mínimo común multiplo es el primer elemento de $div(a) \cap div(b)$. Notación [a:b] (mcd)

Proposición 9
Algunas propiedades

1. $[a : b] = [b : a]$
2. $[1 : b] = |b|$
3. $[0, b] = 0$
4. $[a : b] = [|a| : |b|]$
5. *Si k es un múltiplo de a y b entonces* $[a : b]|k$

Proof. Demostremos el último item. k es múltiplo de a y b por lo tanto es mas grande que $[a : b]$ que es el mínimo común múltiplo
Ahora tenemos que $k = [a : b]q + r$ con $0 \leq r < [a : b]$ pero $a|k \wedge b|k \wedge a|[a : b] \wedge b|[a : b]$ entonces $a|r \wedge b|r$
Lo que nos dice que r es un común múltiplo, pero entonces $r \geq [a : b] \vee r = 0$ finalmente $r = 0$ mostrando que $[a : b]|k$ □

Definición 9.2
Caracterización del mínimo común múltiplo

1. *k es múltiplo de a y b*
2. *sea k′ múltiplo de a y b entonces k|k′*

si y solo si $k = [a : b]$

Proposición 10
Sean a, b dos naturales (uno de ellos puede ser 0) entonces $ab = (a : b)[a : b]$

Proof. Análogamente queremos ver $\frac{ab}{(a:b)} = [a : b]$. Para empezar $\frac{ab}{(a:b)}$ es múltiplo común de a y de por que $\frac{ab}{(a:b)} = b\frac{a}{(a:b)}$ mostrando que es múltiplo de b y análogamente probamos que es múltiplo de a. Restaría ver que divide a todo otro mcd. sea m un múltiplo común de a y b entonces $m = ra = kb$ entonces $\frac{ra}{(a:b)} = \frac{kb}{(a:b)}$ ahora tenemos que $\frac{ra}{(a:b)} = k\frac{b}{(a:b)}$ por lo tanto $\frac{b}{(a:b)}|r\frac{a}{(a:b)}$ pero sabemos que $\frac{a}{(a:b)}, \frac{b}{(a:b)}$ son coprimos entonces $\frac{b}{(a:b)}|r$ entonces puedo escribir $r = \ell\frac{b}{(a:b)}$
Finalmente $m = ra = \ell\frac{b}{(a:b)}a = \ell\frac{ab}{(a:b)}$ que es obviamente divisible por $\frac{ab}{(a:b)}$ □

Proposición 11
Sea $a = p_1^{k_1}p_2^{k_2}\ldots p_n^{k_n}$ *y* $b = p_1^{j_1}p_2^{j_2}\ldots p_n^{j_n}$ *números expresados como factores primos entonces* $a|b \iff k_i \leq j_i \quad \forall i \leq n$

Proof. Ida, como $a|b$ entonces $b = ca$ como son iguales ambos lados tienen los mismos primos a las mismas potencias, ahora si $c = 1 \iff a = b$ pero el caso interesante es si $a \neq b$ esto implica que c o bien es primo o se escribe como producto de primos, en ambos casos a no puede tener todos los primos a las potencias iguales que los de b, por que si no $ca \neq b$ entonces debe tener alguna potencia menor

La vuelta. Si $k_i \leq j_i \quad \forall i \leq n$ entonces basta con usar un c que corrija y emparece todos los exponentes para que $b = ac$ dicho c sería $c = p_1^{j_1-k_1} p_2^{j_2 k_2} \dots p_n^{j_n-k_n}$ □

Corolario 9.0.1
Sale directo de la proposicón anteriór Si $a = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$ *entonces* $div(a) = \{\pm p_1^{j_1} p_2^{j_2} \dots p_n^{j_n} : j_i \leq k_i \quad \forall i \leq n\}$

Corolario 9.0.2
Si $a = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$ *entonces a tiene* $(k_1+1)(k_2+1)\dots(k_n+1)$ *divisores*

Lema 9.1
Sea $a = p_1^{k_1} p_2^{k_2} \dots p_n^{k_n}$ *y* $b = p_1^{j_1} p_2^{j_2} \dots p_n^{j_n}$ *entonces:*

1. $(a : b) = p_1^{min(j_1,k_1)} p_2^{min(j_2,k_2)} \dots p_n^{min(j_n,k_n)}$
2. $[a : b] = p_1^{max(j_1,k_1)} p_2^{max(j_2,k_2)} \dots p_n^{max(j_n,k_n)}$

Corolario 9.1.1
Si $a|c \wedge b|c$ *y* $(a : b) = 1$ *entonces* $ab|c$

Proof. $(a : b) = 1$ entonces existen $m, n \in \mathbb{Z}$ tal que $1 = ma + nb$ entonces $c = mac + nbc$. Por otro lado sabemos que $a|c$ entonces $ab|cb$ entonces $ab|cbn$ también $b|c$ entonces $ba|ca \Rightarrow ab|cam$ entonces $ab|mac + nbc = c$ □

10 Desarrollos P-Ádicos

Proposición 12
Dado cualquier $n \in \mathbb{N}$ *y dado* $s \in \mathbb{N}$ *con* $s \geq 2$, *para* $n \in \mathbb{N}$ *tenemos que* $\exists!\ a_0, a_1, \cdots, a_k$ *con* $0 \leq a_i < s$ *tales que*

$$n = a_k s^k + a_{k-1} s^k - 1 + \cdots + a_1 s + a_0$$

.

En estos casos s es llamada la base. Notamos $n = (a_k a_{k-1} \dots a_0)_s$

Proof. Unicidad: Supongamos $n = b_k s^k + b_{k-1} s^k - 1 + \cdots + b_1 s + b_0 = a_k s^k + a_{k-1} s^k - 1 + \ldots + a_1 s + a_0$ Entonces

$$n = s(a_k s^{k-1} + a_{k-1} s^k - 2 + \cdots + a_1) + a_0 = sq_1 + a_0 \text{ con } 0 \leq a_0 < s$$

por otro lado

$$n = s(b_k s^{k-1} + b_{k-2} s^k - 1 + \cdots + b_1) + b_0 = sq_2 + b_0 \text{ con } 0 \leq b_0 < s$$

Entonces $sq_1 + a_0 = sq_2 + b_0$ pero por algoritmo de división q_2, q_1, b_0, a_0 son únicos entonces

$$q_1 = q_2 \wedge b_0 = a_0$$

Mostrando que ambas formas eran exactamente iguales

Existencia: si $n < s$ entonces $n = a_0$ ya nos queda lo que queríamos con su notación $n = (a_0)_s$.

Si $n > s$ entonces algoritmo de división tenemos $q_1, r_1 \in \mathbb{Z}$ tales que $n = sq_1 + r_1$. Ahora si $q_1 < s$ ya tenemos lo que necesitamos, nos queda $n = (q_1 r_1)_s$.

Si $q_1 > s$ entonces devuelta por algoritmo de divisón existen $q_2, r_2 \in \mathbb{Z}$ tales que $q_1 = q_2 s + r_2$. Juntando todo nos queda $n = s(q_2 s + r_2) + r_1 = q_2 s^2 + r_2 s + r_1$ devuelta si $q_2 < s$ ya tenemos lo que necesitamos y $n = (q_2 r_2 r_1)_s$

Notemos que $q_1 > q_2 > \cdots > q_n > 0$ (son estrictamente decrecientes por algoritmo de división y son mayores que cero por que s y n son números naturales y por algoritmo de divisón (pensar)).

Entonces en algún momento $q_n < s$ por que son todos naturales y no hay infinitos naturales entre dos números naturales

□

11 Congruencia de Enteros

Definición 11.1
Dada $m \in \mathbb{N}$ y $a, b \in \mathbb{Z}$ decimos que a es congruente con b módulo m si $m|a-b$. Lo escribimos $a \equiv b(m)$

Proposición 13
Es trivial notar que congruencia es una relación de equivalencia

Proposición 14
Algunas propiedades

1. $a \equiv b(m) \wedge c \equiv d(m)$ *entonces* $a + c \equiv b + d(m) \wedge ac \equiv bd(m)$
2. *Si* $a \equiv b(m) \wedge \alpha \equiv \beta(m)$ *entonces:*
   (a) $ax + \alpha y \equiv bx + \beta y$
   (b) $a^n \equiv b^n(m) \quad \forall n \in \mathbb{N}$
   (c) *(Polinomios)* $f(a) \equiv f(b)(m) \quad \forall f \in \mathbb{Z}[X]$

Proposición 15
$a \equiv b(m) \iff ac \equiv bc(mc)$

Proof. $m|a-b \Rightarrow a - b = km \iff ca - cb = k(cm)$ finalmente $cm|ca - cb$ entonces $ca \equiv cb(mc)$ □

Proposición 16
Si $ac \equiv bc(m)$ *y* $d = (m : c)$ *entonces* $a \equiv b(\frac{m}{d})$

Proof. $ac - bc = mk \iff \frac{c}{d}a - \frac{c}{d}b = k\frac{m}{d} \iff \frac{c}{d}(a-b) = k\frac{m}{d}$
Entonces $\frac{m}{d}|\frac{c}{d}(a-b)$ como $\frac{m}{d}$ es coprimo con $\frac{c}{d}$ concluimos que $\frac{m}{d}|(a-b)$ o lo que es lo mismo $a \equiv b(\frac{m}{d})$ □

Corolario 11.0.1
Algunos resultados

1. *Del la anteriór proposición se sigue* $ac \equiv bc(mc) \iff a \equiv b(m)$
2. *Si* $(m : c) = 1$ *entonces* $ac \equiv bc(m) \iff a \equiv b(m)$
3. *Si p primo y* $p \neq m$ *entonces* $ap \equiv bp(m) \iff a \equiv b(m)$

Observación
Para el segundo y tercer item: las vueltas valen siempre, pero las idas requieren $(m : c) = 1 \wedge p \neq m$ respectivamente si no se cumplen estamos en el caso mostrado en la proposición anteriór

Lema 11.1
Si $a \equiv b(m)$ *y* $0 \leq |b-a| < m$ *entonces* $a = b$

Proof. $a - b = km \Rightarrow |a-b| = |k|m$ pero por hipótesis $0 \leq |a-b| < m$ entonces $k = 0$ necesariamente □

Lema 11.2
Dos enteros son congruentes módulo m si y sólo si tienen el mismo resto dividio por m

Proof. Ida. Tenemos $a \equiv b(m)$ con $a = q_1m + r_1 \wedge b = q_2m + r_2$. Sabemos que $m|a-b$
Equivalentemente $m|(q_1 - q_2)m + r_1 - r_2$ y $m|(q_1 - q_2)m$ entonces $m|r_1 - r_2$ o lo mismo $r_1 \equiv r_2(m)$
.Pero además sabemos que $0 < r_1 < m \wedge 0 < r_2 < m$ entonces sabemos que $r_1 - r_2 < m$ por lo tanto $0 < |r_1 - r_2| < |m| = m$
Entonces $r_1 = r_2$ usando el lema anteriór
Vuelta. Sabemos que $a = q_1m + r_1$ y $b = q_2m + r_2$ con $r_1 = r_2$ entonces $a - b = (q_1 - q_2)m$
Entonces $m|a-b$ mostrando que $a \equiv b(m)$ □

Proposición 17
Si $a \equiv b(m)$ *y* $a \equiv b(n)$ *y* $(m : n) = 1$ *entonces* $a \equiv b(mn)$

Proof. $m|a-b \wedge n|a-b$ como $(m : n) = 1$ entonces $mn|a-b$ mostrandoq ue $a \equiv b(mn)$ □

Observación
La recíproca también vale

Corolario 11.2.1
Sea $m = p_1^{j_1} p_2^{j_2} \dots p_n^{j_n}$ *sus factores primos entonces* $a \equiv b(m) \iff a \equiv b(p_i^{j_i})$

Corolario 11.2.2 (Sistemas equivalentes)
$a_1 \equiv b(c_1) \wedge a_2 \equiv b(c_2) \dots a_n \equiv b(c_n)$ *con* $c_1 \dots c_n$ *coprimos 2 a 2* $\iff a_1 a_2 \dots a_n \equiv b(c_1 c_2 \dots c_n)$

Lema 11.3
Sea $a \in K$ *con* $a \neq 0$ *entonces existe un* $a' \in \mathbb{Z}$ *no nulo tq* $aa' \equiv 1(m) \iff (a : m) = 1$. *Mas aún* a' *es único congruente* m

Proof. Unicidad supongamos exsiten $a', a'' \in \mathbb{Z}$ tal que $aa' \equiv 1(m) \wedge aa'' \equiv 1(m)$
Entonces $aa' \equiv aa''(m)$ como $(a : m) = 1$ puedo dividir de ambos lados por lo tanto $a' \equiv a''(m)$
Ida. $m|aa' - 1$ entonces si $d = (a : m)$ sabemos que $d|m$ por lo tanto $d|aa' - 1$ pero además $d|a$ y entonces $d|1$ y $d \geq 1$ entonces $d = 1$
Vuelta. Existen $k, p \in \mathbb{Z}$ tales que $1 = ka + pm$ entonces $ka - 1 = -pm$ entonces $m|ka - 1$ o lo que es lo mismo $ka \equiv 1(m)$ ahora tomamos $k = a'$ y obtenemos lo que queríamos □

Observación
Si $a \equiv b(m) \wedge (b : m) = 1 \Rightarrow (a : m) = 1$

Proof. $a = b + km$ como si $d|a \wedge d|m$ entonces $d|b$ luego d es divisor común de b y m por lo tanto es $d = 1$ □

12 Teorema de Euler

Definición 12.1 (Phi de Euler)
$\phi(n) = |\{a \in \mathbb{Z} \mid 1 < a \leq n \wedge (a : n) = 1\}|$

Observación
Algunas propiedades. Si p primo

1. $\phi(p) = p - 1$
2. $\phi(p^2) = p^2 - p$
3. $\phi(p^k) = p^k - p^{k-1}$
4. $m, n \in \mathbb{N}$ *entonces* $\phi(n)\phi(m) = \phi(nm)$ *si* $(m : n) = 1$

Definición 12.2
Una forma de calcular $\phi(m)$

$$\phi(m) = m \prod_{p|m}^{n} (1 - \frac{1}{p_i})$$

Definición 12.3
Un sistema residual completo (de ahora en mas llamado sistema residual) es un conjunto con m elementos, cada uno un representante de cada una de las m clases de equivalencia módulo m
Un sistema residual reducido es un subconjunto del anteriór donde solo estan los representantes coprimos con m

Lema 12.1
Sea $(k : m) = 1$

1. *Si* $\{a_1, a_2, \dots a_n\}$ *es un sistema residual módulo m entonces* $\{ka_1, ka_2, \dots ka_n\}$ *es un sistema residual*
2. *Si* $\{b_1, b_2, \dots b_{\phi(m)}\}$ *es un sistema reducido entonces* $\{kb_1, kb_2, \dots kb_{\phi(m)}\}$ *es un sistema reducido*

Proof. 1. Probemos que son todos no congruentes en $\{ka_1, ka_2, \dots ka_n\}$. Supongamos que tenemos $ka_i \equiv ka_j(m)$ en el conjunto, por un lado sabemos que a_i y a_j deben estar en $\{a_1, a_2, \dots a_n\}$ pero como $(k : m) = 1$ tenemos que $a_i \equiv a_j(m)$ pero no puedo tener dos número equivalentes en el mismo sistema por como se define sistema residual (un representante de cada clase de equivalencia)

Entonces $\{ka_1, ka_2, \dots ka_n\}$ tiene elementos NO equivalentes entre si y tiene la misma cantidad de elementos que $\{a_1, a_2, \dots a_n\}$ mostrando que es sistema residual módulo m

2. Sabemos,usando la misma idea que el ejericio anteriór que ningún par de $k_i, k_j \in \{kb_1, kb_2, \dots kb_n\}$ son equivalentes. Además ambos sistemas tiene la misma cantidad de elementos.

   Por otro lado
   $$(b_i : m) = 1 \quad \forall i \in \mathbb{N} \quad 1 \leq i \leq \phi(m)$$
   justamente por definición de sistema reducido. Además, por hipótesis $(k : m) = 1$ entonces
   $$(kb_i : m) = 1 \quad \forall i \in \mathbb{N} \quad 1 \leq i \leq \phi(m)$$

   Luego $\{kb_1, kb_2, \dots kb_{\phi(m)}\}$ es un sistema reducido

□

Teorema 12.2 (Teorema de Euler Fermat)
Si $(a : m) = 1$ *entonces*
$$a^{\phi(m)} \equiv 1(m)$$

Proof. Sea
$$\{b_1 \dots b_{\phi(m)}\}$$
un sistema reducido mod m entonces
$$\{ab_1 \dots ab_{\phi(m)}\}$$
También lo és por ser $(a : m) = 1$
Pero entonces
$$b_1 \dots b_{\phi(m)} \equiv ab_1 \dots ab_{\phi(m)}(m)$$
Esto vale por que ambos conjuntos tienen representantes modulo m y los representantes son equivalentes mod m
Entonces
$$b_1 \dots b_{\phi(m)} \equiv a^{\phi(m)}(b_1 \dots b_{\phi(m)})(m)$$
Sabemos que todos los b_i son coprimos con m por definición de sistema residual reducido, entonces
$$1 \equiv a^{\phi(m)}(m)$$

□

Corolario 12.2.1 (Pequeño teorema de Fermat)
Si p primo entonces $\phi(p) = p - 1$ *por lo tanto tendríamos que* $(p : a) = 1$
$$a^{p-1} \equiv 1(p)$$

que es el pequeño teorema de fermat, como caso particular de Euler , por lo tanto ya quedó demostrado

Teorema 12.3 (Teorema de Wilson)
Si p primo entonces $(p-1)! \equiv -1(p)$

Proof. queremos ver que $1.2 \dots (p-2)(p-1) \equiv -1(p)$ sabemos que $p - 1 \equiv -1(p)$ entonces queremos ver que $1.2 \dots (p-2) \equiv 1(p)$.

Sabemos que si $1 \leq a \leq p-2$ entonces $(a : p) = 1$ por lo tanto usando lema anteriór tenemos que para cada a existe un $a*$ tal que $aa* \equiv 1(p)$ y si $a_1 \neq a_2$ entonces $a_1* \neq a_2*$ por unicidad además es único congruente p por lo tanto tenemos un representante menor estricto que p

** Veamos que para cada factor a de $(p-2)!$ a es distinto de su inverso $a*$. Supongamos que no, entonces tenemos un $a \in [2, p-2]$ tal que $a = a*$ entonces $a^2 = aa* \equiv 1(p)$.

Luego $(a-1)(a+1) = a^2 - 1 \equiv 0(p)$ entonces $a-1 \equiv 0(p)$ o $a+1 \equiv 0(p)$. Pero sabemos que $a-1 \wedge a+1$ son menores que p entonces $a = 1$ o $a = p-1$ lo cual es absurdo en ambos casos. Además es facil ver que 1 es inverso de si mismo y $(p-1)(p-1) = p^2 - 2p + 1 \equiv 1(p)$ entonces $p-1$ es inverso de si mismo también.

Pero entonces todos los otros inversos seran menores que $p-1$ y mayores que 1, por que ya dijimos no pueden ser inversos de dos numeros diferentes, entonces para a tal que $1 < a < p-1$, existe $a*$ inverso de a modulo p

Entonces podemos reescribir y reordenar $(p-2)! = 1.(a_1 a*_1) \dots (a_q a*_q) \equiv 1(p)$

Entonces $(p-1)! = (p-1)(p-2)! \equiv (p-1)(p)$ y $p-1 \equiv -1(p)$

** Esta es una demostración también de que $p-1 \wedge 1$ son inversos de si mismo modulo p. Es por esto que no lo podemos simplificar y al resto si □

Definición 12.4
Dado $n \in \mathbb{N}$ definimos $\mathbb{Z}_n$ como el conjunto de clases de equivalencia módulo m $Z_n = \{[0]_m, [1]_m, \dots, [n-1]_m\} = \{[1]_m, [2]_m \dots [m-1]_m\}$

Definición 12.5
Definimos

1. $+ : Z_n \times Z_n \to Z_n$ *dada por* $[a] + [b] = [a+b]$
2. $* : Z_n \times Z_n \to Z_n$ *dada por* $[a] * [b] = [a*b]$

Definición 12.6
Usando esto se puede probar que $(Z_n, +, *)$ es un anillo conmutativ es un anillo conmutativoo

Definición 12.7
Sea $n \in \mathbb{N}$ y $[a] \in \mathbb{Z}_n$

1. $[a]$ *es unidad si* $\exists [b]$ *tq* $[a] * [b] = [1]$
2. $[a]$ *es un divisor de cero si* $\exists [b] \in \mathbb{Z}_n$ *diferente de* $[0]$ *tq* $[a] * [b] = 0$

Proposición 18
Algunas propiedades

1. $[n-1]$ *es unidad modulo n*
2. *Si* $a|m$ *entonces* $[a]$ *es divisor de cero módulo n*
3. *Si* $(a : m) > 1$ *entonces* $[a]$ *es divisor de cero módulo n*
4. $[a]$ *es unidad módulo m* iff $(a : m) = 1$, *ya lo habíamos visto*

Corolario 12.3.1
$\mathbb{Z}_n$ no tiene divisor de cero o equivalentemente todos sus elementos no nulos son unidades (son invertibles) si y sólo si m es primo. (Otra forma de decirlo $\mathbb{Z}_p$ es un cuerpo si y sólo si p es primo)

13 Ecuaciones lineales de congruencia

Definición 13.1
Una ecuación lineal de congruencia tiene esta pinta

$$ax \equiv b(m)$$

y tiene solución si y sólo si $(a : m)|b$. Si tiene solución tiene infinitas, aunque ya veremos que módulo m no son infinitas

Teorema 13.1
Consideremos $ax \equiv b(m)$

1. $(a : m) = 1$ *entonces la ecuacíon tiene solución y es única módulo m*
2. $(a : m) = d \neq 1$ *entonces la ecuación tiene solución si sólo si $d|b$. Y dicha solución es única módulo $\frac{m}{d}$*

Proof. Tenemos $ax \equiv b(m)$

1. $(a : m) = 1$ entonces tenemos $ak + mj = 1$ por lo tanto $akb + mjb = b$ entonces si tomamos $jb = q \wedge kb = x'$ tenemos $ax' - b = qm$ entonces tenemos que x' cumple la ecuación.

   Veamos que es única módulo m. Supongamos que tenemos dos soluciones distintas $c \wedge c'$ modulo m entonces $c < m \wedge c' < m$. Pero $ac \equiv b \equiv ac'(m)$ entonces $ac \equiv ac'(m)$ como $(a : m) = 1$ tenemos $c \equiv c'(m)$ como ambas son menores que m entonces $c = c'$ absurdo

2. Ida la ecuación tiene solución entonces $ax - b = km$ ahora como $d = (a : m)$ entonces $d| - ax \wedge d|km$ entonces $d|b$.

   La vuelta $d|b$ y $(a : m) = 1$ entonces $ax \equiv b(m)$ tiene solución si y sólo si existe $k \in \mathbb{Z}$ tal que $mk = ax - b$ si y sólo si $k\frac{m}{d} = \frac{a}{d}x - \frac{b}{d}$ si y sólo si $\frac{a}{d}x \equiv \frac{b}{d}(\frac{m}{d})$, pero sabemos que $(\frac{a}{d} : \frac{m}{d}) = 1$ entonces estamos en el caso 1, por lo tanto tiene solucíon Como la última ecuación tiene solucíon entonces por la cadena $ax \equiv b(m)$ también tiene.

   Veamos que es única sean x_0, x_1 soluciones, entonces $ax_0 \equiv b(m)$ y $ax_1 \equiv b(m)$ usando la misma cadena que el párrafo anteriór llegamos a $\frac{a}{d}x_0 \equiv \frac{b}{d}(\frac{m}{d})$ y $\frac{a}{d}x_1 \equiv \frac{b}{d}(\frac{m}{d})$ entonces $\frac{a}{d}x_0 \equiv \frac{a}{d}x_1(\frac{m}{d})$ como $(\frac{a}{d} : \frac{m}{d}) = 1$ entonces $x_0 \equiv x_1(\frac{m}{d})$. Mostrando que la solución es única modulo $\frac{m}{d}$

□

Proposición 19
El sistema $x \equiv b_1(n_1)$ y $x \equiv b_2(n_2)$ tiene solución si y sólo si $(n_1 : n_2)|b_1 - b_2$
Además la solución es única mod $[n_1 : n_2]$

Proof. Ida: Supongamos x_0 es solución entonces $n_1|x_0 - b_1$ y $n_2|x_0 - b_2$ entonces $(n_1 : n_2)|x_0 - b_2 - (x_0 - b_1) = b_1 - b_2$
Vuelta: $(n_1 : n_2)|b_1 - b_2$ entonces $n_1x \equiv b_1 - b_2(n_2)$ tiene solución
Por lo tanto existe x_0 tal que $n_1x_0 = b_1 - b_2 + n_2l$. Pero entonces tomo $k_0 = n_2l - b_2 = n_1x_0 - b_1$ y k_0 satisface $k_0 \equiv b_2(n_2)$ y $k_0 \equiv b_1(n_1)$ Mostrando que dicho sistema tiene solución
Finalmente si tenemos dos soluciones x_0, x_1 entonces $x_0 - x_1 \equiv 0(n_1)$ y $x_0 - x_1 \equiv 0(n_2)$. Entonces $n_1|x_0 - x_1$ y $n_2|x_0 - x_1$ entonces $x_0 - x_1$ es común múltiplo de n_1 y n_2 por lo tanto $[n_1 : n_2]|x_0 - x_1$
Equivalentemente $x_0 \equiv x_1([n_1 : n_2])$ □

Teorema 13.2 (Teorema Chino del Resto)
Sean $n_1, n_2 \dots n_k \in \mathbb{N}$ coprimos dos a dos el sistema de congruencia $x \equiv b_1(n_1)$

$$\begin{cases} x \equiv b_1(n_1) \\ x \equiv b_2(n_2) \\ \vdots \\ x \equiv b_k(n_k) \end{cases}$$

Tiene solución y es única mod $\prod_{i=1}^{k} n_i$

Proof. Sea $n = n_1n_2 \dots n_k$ y para cada $i \in \mathbb{N}$ tal que $1 \leq i \leq k$ sea $a_i = \frac{n}{n_i}$ como $(n : a_i) = 1$ tenemos que $a_ix \equiv b_1(n)$ tiene solución llamemos a dicha solución x_i ahora si tomamos $z = \sum_{i=1}^{k} a_ix_i$ tenemos que $z \equiv a_ix_i(n_i)$ (por que n_i va a dividir a todos los a_j tal que $j \neq i$) entonces $z \equiv b_i(n_i)$ y esto vale para cualquier $i \in \mathbb{N}$ tal que $0 \leq i \leq k$ Por lo tanto z es solución de todas las ecuaciones del sistema.
Veamos que es unica mod $\prod_{i=1}^{k} n_i$. Sea x_0 y x_1 dos soluciones, entonces $x_0 \equiv b_i(n_i)$ y $x_1 \equiv b_i(n_i)$ para todo $i \in \mathbb{N}$ con $0 \leq i \leq k$ Entonces $x_0 \equiv x_1(n_i)$ para todo $i \in \mathbb{N}$ con $0 \leq i \leq k$ Entonces $n_i|x_0 - x_1$ para todo $i \in \mathbb{N}$ con $0 \leq i \leq k$, como son todos coprimos $n_1n_2 \dots n_k|x_0 - x_1$ lo que me dice que $x_1 \equiv x_0(n_1n_2 \dots n_k)$ □

14 Números Reales

Definición 14.1 (Axiomas de cuerpo)
Teniendo un conjunto A y las dos operaciones típica $(+, *)$ Entonces si $(A, +, *)$ es un cuerpo cumple Sobre la suma

1. *Asociativa*
2. *Conmutativa*
3. *Tiene elemento neutro*
4. *Existe opuesto*

Sobre la multiplicación

1. *Asociativa*
2. *Conmutativa*
3. *Tiene elemento neutro*
4. *Existe opuesto*

Sobre la suma y la multiplicación, la ley de la distributiva

Observación
Todo cuerpo es un anillo en particular, $\mathbb{R}$ es un cuerpo

Definición 14.2 (Axiomas de cuerpo ordenado)
Todos los del cuerpo y estas otras

1. *Tricotomia y transitividad*
2. *Compatibilidad en la suma: $a \geq b \Rightarrow a + c \geq b + c$*
3. *Compatibilidad en la multiplicación: $c > 0 \wedge a > b \Rightarrow ca > cb$*

Observación
$\mathbb{R}$ resulta un cuerpo ordenado (dándole el órden tradicional). Pero $\mathbb{Z}_p$ es un cuerpo no ordenado $\mathbb{C}$ tampoco

Definición 14.3 (Axiomas de cuerpos ordenados y completos)
Tiene todos los del cuerpo ordenado y además cumple el axioma de completitud
Axioma de completitud: Todo conjunto no vacío y acotado superiormente tiene supremo

Observación
$\mathbb{R}$ es completo, pero $\mathbb{Q}$ no lo és

Proposición 20
En todo cuerpo (en particular en $\mathbb{R}$) valen

1. $x0 = 0$
2. $x + y = x + z \Rightarrow y = z$
3. $\exists\, !x \text{ tq } a + x = b$
4. $ab = 0 \Rightarrow a = 0 \vee b = 0$
5. $-(-x) = x$
6. $-(x + y) = (-x) + (-y)$
7. $= -(xy) = (-x).y = x.(-y)$
8. $(-x)(-y) = xy$

Todas salen usando que un cuerpo es anillo conmutativo

Proposición 21
En todo cuerpo valen

1. $(x^{-1})^{-1} = x$
2. $(xy)^{-1} = x^{-1}y^{-1}$
3. $(-1)^{-1} = -1$
4. $(-x)^{-1} = -x^{-1}$

Proof. Veamos cada una

1. $(x^{-1})^{-1} = x \iff (x^{-1})^{-1}x^{-1} = 1$ y el de la derecha vale por definición
2. tenemos que $(xy)^{-1} = x^{-1}y^{-1} \iff (xy)^{-1}(xy) = 1$. Entonces $(xy)^{-1}$ es inverso de xy entonces $(xy)^{-1} = x^{-1}y^{-1}$

□

Proposición 22
En todo cuerpo vale

1. $xy = 0 \Rightarrow x = 0 \vee y = 0$
2. *En particular* $xy = \neq 0 \Rightarrow x \neq 0 \vee y \neq 0$ *En particular*
   (a) $x^2 = 0 \iff x = 0$
   (b) $x^2 = 1 \iff x = 1 \vee x = -1$
   (c) $x^{-1} = x \iff x = 1 \vee x = -1$

Proof. Demostremoslas

1. Ya lo vimos arriba
2. Supongamos $x \neq 0$ entonces como $xy = 0$ sucede $x^{-1}xy = 0$ por lo tanto $y = 0$
   (a) $x^2 = 0 \Rightarrow x.x = 0 \Rightarrow x = 0 \vee x = 0$ usando la de arriba
   (b) $x^2 = 1 \iff x^2 - 1 = 0 \iff (x-1)(x+1) = 0 \iff x - 1 = 0 \vee x + 1 = 0$
   (c) $x^{-1} = x \iff x^2 = 1 \iff x = 1 \vee x = -1$ usando b

□

Proposición 23
En todo cuerpo ordenado valen

1. $0 < 1$
2. $x > 0 \iff -x < 0$
3. $x < y \iff -x > -y$
4. $x < y \wedge m < b \Rightarrow x + m > y + b$
5. $x < y \wedge z < 0 \Rightarrow xz > yz$
6. *(a)* $x > 0 \wedge y > 0 \Rightarrow xy > 0$
   (b) $x > 0 \wedge y < 0 \Rightarrow xy < 0$
   (c) $x < 0 \wedge y < 0 \Rightarrow xy > 0$
   (d) $x < 0 \wedge y > 0 \Rightarrow xy < 0$
7. $x > 0 \iff x^{-1} > 0$

Proof. 1. Trivial

2. $x > 0 \iff -x + x > -x + 0 \iff 0 > -x$
3. $x < y \iff -x - y + x < -x - y + y \iff -y < -x$
4. $x + m < y + m < y + b$
5. $x < y$ por 2 $-z > 0$ entonces $-zx < -zy$ por 3 $xz > yz$
6. Salen todas con el 5.
7. $x > 0$ suponemos $x^{-1} < 0$ entonces $xx^{-1} < 0x^{-1} \iff 1 < 0$ abs

□

Proposición 24
En todo cuerpo ordenado valen:

1. $x^2 \geq 0 \quad \forall x$ *en dicho cuerpo y* $x^2 = 0 \iff x = 0$
2. $x^2 + y^2 \iff x = 0 \wedge y = 0$
3. $0 < x < y \Rightarrow x^2 < y^2$
4. $x < y < 0 \Rightarrow x^2 > y^2$
5. $0 < x < y \Rightarrow y^{-1} < x^{-1}$
6. $x < 0 < y \Rightarrow x^{-1} < y^{-1}$
7. $x < y < 0 \Rightarrow y^{-1} < x^{-1}$

Proof. Veamos las demostraciones

1. Se sigue de 6 de la prop anteriór y la segunda parte ya la habíamos probado
2. Si $x^2 = -y^2$ pero $x^2 \geq 0 \wedge y^2 \geq 0$ entonces $y = 0 = x$ por que si $y > 0$ entoncse $y^2 > 0$ entonces $-y^2 < 0$ entonces $x^2 = -y^2 < 0$ que es absurdo
3. Por hipótesis $xx < yx < yy$
4. Como $x < 0$ tenemos $xx > yx$ como $y < 0$ tenemos $xy > yy$ entonces $x^2 > y^2$
5. $x > 0 \wedge y > 0 \Rightarrow 1 < yx^{-1} \Rightarrow y^{-1} < x^{-1}$
6. $x < 0 \Rightarrow 1 > x^{-1}y \Rightarrow y^{-1} > x^{-1}$
7. Sale con la misma idea que los otros dos

□

15 Números Complejos