Álgebra I. 525140 - DIM - CFM
25 de mayo de 2021
Prof.: L. Badilla, I. Donoso, A. Gajardo, J. Moya
A. Pérez, C. Rivas, M. Selva, F. Thiele, G. Torres

Teoría de números

En este capítulo recordaremos cosas del colegio, junto con sus demostraciones. Muchas de esas cosas las hemos repasado cuando vimos relaciones, de manera que no hay muchas cosas nuevas. Sin embargo les recomiendo leer este apunte con cuidado pues tomaremos un enfoque más teórico y nos servirá para practicar la lógica matemática más rigurosa. Veremos todos los conceptos en los enteros, aunque el enfoque más tradicional lo ve en los naturales, no es un problema, solo hay que ser más cuidadoso con algunas cosas.

Definición 1. Dados dos números enteros $a, b \in \mathbb{Z}$ decimos que a *divide* a b si existe un entero $k \in \mathbb{Z}$ tal que

$$ka = b,$$

en tal caso también decimos que b es múltiplo de a, y denotamos $a|b$

Ejemplo 2.

- 3 divide a -24, ya que $-8 \cdot 3 = -24$.
- 5 no divide a 16 ya que si multiplico 5 por $1, 2, 3$ obtengo $5, 10, 15$ respectivamente, y si multiplico por $k \geq 4$, obtengo un número mayor que 16, en efecto:

$$\begin{aligned} k &\geq 4 \qquad / \cdot 5 \\ k5 &\geq 20 > 16. \end{aligned}$$

- 3 divide a 0, ya que $0 \cdot 3 = 0$, de hecho, según la definición que aquí se da, 0 es múltiplo de todos los números. Esta definición no es la más usual, en general estos conceptos se definen solo en $\mathbb{N}$, pero acá nos conviene hacerlo así.
- 0 no divide más que a sí mismo, ya que cualquiera sea $k \in \mathbb{Z}$ se tiene $k \cdot 0 = 0$.

Lema 3. Dados dos números enteros no nulos $a, b \in \mathbb{Z} \setminus \{0\}$, se cumple que

$$a|b \Leftrightarrow \frac{b}{a} \in \mathbb{Z} \setminus \{0\}$$

Demostración.

$$\begin{aligned} a|b &\Leftrightarrow \exists k \in \mathbb{Z} \setminus \{0\},\ ka = b && \text{si } b \neq 0 \text{ entonces } k \neq 0, \text{ por eso lo podemos excluir} \\ &\Leftrightarrow \exists k \in \mathbb{Z} \setminus \{0\},\ k = \frac{b}{a} && \text{ya que } a \neq 0 \\ &\Leftrightarrow \frac{b}{a} \in \mathbb{Z} \setminus \{0\} \end{aligned}$$

□

Ejemplo 4.

- 3 divide a -24, ya que $\frac{-24}{3} = -8 \in \mathbb{Z} \setminus \{0\}$.
- 5 no divide a 16 ya que $\frac{16}{5} = 3,2 \notin \mathbb{Z} \setminus \{0\}$.

Ya habíamos definido la relación "divide a" en $\mathbb{N}$, y ya habíamos demostrado que es una relación de orden. Repetimos de todas formas la demostración.

Proposición 5. La relación *divide a* en $\mathbb{N}$ es una relación de orden.

Demostración.

- **Es refleja.** Sea $a \in \mathbb{N}$ cualquiera. Es claro que a divide a a ya que basta tomar $k = 1$, se cumple $1 \cdot a = a$, ya que 1 es el neutro multiplicativo.
- **Es transitiva.** Sea $a, b, c \in \mathbb{N}$ tales que a divide a b y b divide a c (hipótesis), Vamos a demostrar que a divide a c, para eso interpretamos la hipótesis según la definición: existe $k \in \mathbb{N}$ tal que $ka = b$, y existe $k' \in \mathbb{N}$ tal que $k'b = c$, tomamos una letra distinta al aplicar la definición pues tomar la misma letra sería equivalente a asumir que las constantes son iguales, pero no tendrían porque serlo, siempre tomaremos variables con nombres diferentes para representar objetos independientes.

  Si ahora reemplazamos $b = ka$ en la segunda ecuación obtenemos $k'ka = c$, dado que k y k' son enteros, kk' también es entero, entonces a divide a c.
- **Es antisimétrica.** Sea $a, b \in \mathbb{N}$ tales que a divide a b y $a \neq b$ (hipótesis), vamos a demostrar que entonces b no divide a a. Partimos traduciendo la hipótesis: existe $k \in \mathbb{N}$ tal que $ka = b$ y $a \neq b$. Razonamos por contradicción: si se tuviera que b divide a a tendríamos que existe $k' \in \mathbb{Z}$ tal que $k'b = a$. Si reemplazamos $a = k'b$ en la primera ecuación obtenemos: $kk'b = b$, de donde se obtiene que $kk' = 1$, es decir, k' es el inverso multiplicativo de k, pero en $\mathbb{N}$ el único números que tiene inverso multiplicativo es 1, por lo tanto $k = k' = 1$, así $a = b$, lo cual es una contradicción. □

Notamos que en $\mathbb{Z}$ la relación NO cumple la antisimetría, ya que 2 divide a -2 y -2 divide a 2, por lo tanto, en $\mathbb{Z}$ NO es una relación de orden (ni tampoco de equivalencia).

El siguiente teorema permite entender mejor la relación de divisibilidad y describir mejor lo que ocurre cuando a no divide a b. Su demostración se basa en el método de la división.

Teorema 6. Para todo par de naturales $a \in \mathbb{N}$, $b \in \mathbb{N}$, existe un único entero $q \in \mathbb{N}$ y $r \in \{0, 1, ..., b-1\}$ tales que

$$a = qb + r.$$

Tal q se llama *cuociente entero* entre a y b, mientras que r se denomina *resto* de la división de a por b.

Demostración. Lo primero es observar que los naturales se pueden expresar como unión de intervalos disjuntos como sigue:

$$\mathbb{N} = \{1, \ldots, b-1\} \cup \{b, \ldots, 2b-1\} \cup \{2b, \ldots, 3b-1\} \cup \cdots \cup \{kb, \ldots, (k+1)b-1\} \cup \cdots$$

es claro que $a \in \mathbb{N}$ pertenece a uno y solo uno de estos intervalos. Sea $q \in \mathbb{N}$ tal que:

$$a \in \{qb, \ldots, (q+1)b-1\}.$$

Esto significa que $qb \leq a \leq qb + b - 1$. Si restamos qb a ambos lados de estas dos inecuaciones obtenemos que:

$$0 \leq a - qb \leq b - 1.$$

Si ahora definimos $r = a - qb$, concluimos que:

$$a = qb + r \text{ y } 0 \leq r \leq b - 1,$$

que era lo que se quería demostrar. □

Ejemplo 7. Si $a = 16$ y $b = 5$, entonces $16 = 3 \cdot 5 + 1$, pero cómo obtenemos esto normalmente, lo que hacemos es preguntarnos ¿cuántas veces cabe 5 en 16? lo cual quiere decir ¿cuál es la mayor cantidad de veces que 5 cabe en 16? la respuesta es 3, pues $3 \cdot 5 = 15$, cabe 3 veces pero más veces no cabe, ¿por qué? por que lo que sobra es 1, y 5 no cabe en 1.

La división entera, entonces es la división sin sacar decimales, y reportando lo que sobra como el "resto".

Esta definición permite tener otra caracterización de la relación de divisibilidad.

Proposición 8. Dados dos números enteros no nulos $a, b \in \mathbb{Z} \setminus \{0\}$, se cumple que

$$b|a \Leftrightarrow \text{ el resto de dividir } |a| \text{ por } |b| \text{ es nulo } (r = 0)$$

Demostración. En efecto, si $b|a$, entonces existe $k \in \mathbb{Z}$ tal que $kb = a$ lo cual implica que $|k||b| = |a|$, es decir $|a| = |k||b| + 0$.

Recíprocamente, si el resto de dividir $|a|$ por $|b|$ es nulo, entonces existe $q \in \mathbb{N}$ tal que $|a| = q|b| + 0$, entonces puedo tomar $k \in \mathbb{Z}$ como sigue:

$$k = \begin{cases} q & \text{si } a \text{ y } b \text{ tienen el mismo signo} \\ -q & \text{si } a \text{ y } b \text{ tienen distinto signo} \end{cases}$$

Con esta definición es claro que se tiene $a = qb$, por lo tanto $b|a$. □

La relación de divisibilidad es central en el estudio de los números, y permite definir un concepto fundamental: el concepto de numero primo.

Definición 9. Dado un número $a \in \mathbb{N}$ se define el conjunto de los *divisores de* a por $\text{Div}(a)$ como sigue:

$$\text{Div}(a) = \{n \in \mathbb{N} \ : \ n|a\}.$$

Un número $p \in \mathbb{N}$ se dice *primo* si $|\text{Div}(p)| = 2$. Si $|\text{Div}(p)| > 2$ entonces se dice que n es *compuesto*.

Ejemplo 10.
- $\text{Div}(16) = \{1, 2, 4, 8, 16\}$, 16 es compuesto.
- $\text{Div}(1) = \{1\}$, 1 no es primo ni compuesto.
- $\text{Div}(31) = \{1, 31\}$, 31 es primo.

Todo número es divisible por 1 y por si mismo: $n = 1 \cdot n$. Cuando $n = 1$, n tiene un solo divisor. Si no, n tiene al menos 2 divisores. Si tiene más de 2, entonces hay un divisor d que no es ni 1 ni n, por lo tanto existe $k \in \mathbb{N}$ tal que $n = kd$, donde k no es ni 1 ni n, es decir, n es multiplicación de otros dos números, por eso es que en ese caso se le llama compuesto.

Los número primos permiten analizar de manera muy fina a los números y abren las puertas a grandes descubrimientos, incluso son centrales en el funcionamiento del mundo digital. Pero no son de uso exclusivo humano, insectos se sirven de los número primos para evitar ser depredados. Esto es tan importante que se dice que si hubiera vida inteligente en otros planetas, una manera de comunicarnos con ellos sería a travez de los números primos.

Nos acercaremos al teorema más importante de la aritmética, que permite demostrar y analizar un montón de cosas. Para hacerlo necesitamos recordar las nociones de *mínimo común múltiplo* y *máximo común divisor*[1] .

Definición 11. Dados dos números naturales a, $b \in \mathbb{N}$, se definen los dos números siguientes.

$\text{mcd}(a, b)$ = el divisor común a a y b que es más grande que todos los demás divisores comunes

$\text{mcm}(a, b)$ = el múltiplo común a a y b que es más pequeño que todos los demás múltiplos comunes

Ambos, escogidos dentro de los número naturales.

Ejemplo 12. Tomemos $a = 12$ y $b = 20$, y veamos cuáles son sus divisores y cuales son sus múltiplos.

$$\text{Div}(12) = \{1, 2, 3, 4, 6, 12\}$$
$$\text{Div}(20) = \{1, 2, 4, 5, 10, 20\}$$

Sus divisores comunes son los siguientes.

$$\text{Div}(12) \cap \text{Div}(20) = \{1, 2, 4\}$$

Por lo tanto el mayor de sus divisores comunes es 4: $\text{mcd}(12, 20) = 4$.

Los múltiplos son los siguientes.

$$\text{Múltiplos de } 12 = \{12, 24, 36, 48, 60, 72, ...\} = \{12k \ : \ k \in \mathbb{N}\}$$
$$\text{Múltiplos de } 20 = \{20, 40, 60, 80, 100, ...\} = \{20k \ : \ k \in \mathbb{N}\}$$

Por lo tanto el menor de sus múltiplos comunes es 60: $\text{mcm}(12, 20) = 60$.

Observamos también que si queremos enumerar los múltiplos comunes de 12 y 20 pareciera ser que todos son múltiplos de 60:

$$\text{Múltiplos de } 12 \cap \text{Múltiplos de } 20 = \{60, 120, 180, ...\} = \text{múltiplos de } 60.$$

¿Pero esto será realmente cierto?

[1] La teoría que siguie fue extraida del libro "Números" del profesor Xavier Vidaux, en preparación.

Teorema 13. Dados dos números naturales a, $b \in \mathbb{N}$ cualesquiera, se cumple que

$$\text{Múltiplos de } a \cap \text{Múltiplos de } b = \text{Múltiplos de } \operatorname{mcm}(a, b).$$

Demostración. Sea $M = \operatorname{mcm}(a, b)$, esto implica que existe k, $k' \in \mathbb{N}$ tales que $M = ka$ y $M = k'b$ (hipótesis). Debemos demostrar una igualdad de conjuntos, demostramos la inclusión hacia un lado primero y luego la inclusión hacia el otro lado.

- $\supseteq$ Si n es múltiplo de M, es claro que n ha de ser múltiplo de a y de b también, ya que entonces existe $l \in \mathbb{N}$ tal que $n = lM = lka = lk'b$.
- $\subseteq$ Si n es múltiplo de a y es múltiplo de b (segunda hipótesis) debemos demostrar que entonces n es múltiplo de M, lo único que sabemos es que, por definición de mcm, $M \leq n$. Usemos la división entera para analizar el problema, y tomemos $q, r \in \mathbb{N}$ tales que:

  $$n = qM + r \quad \wedge \quad r \in \{0, 1, ..., M-1\}$$

  Esto implica que $r = n - qM$. Como tanto n como M son múltiplos comunes de a y de b, concluimos que r también es múltiplo común de a y b. Por lo tanto $r \geq M$ o bien $r \notin \mathbb{N}$, pero lo primero no puede ser pues $r \leq M-1$, entonces $r = 0$, con lo cual $M|n$ y hemos demostrado lo que queríamos. □

Esto muestra que era verdad lo observado en el ejemplo anterior: que todos los múltiplos comunes de 12 y 20 son múltiplos de 60.

En el ejemplo anterior también vemos que todos los divisores comunes de 12 y 20 son divisores de 4. Esto también es cierto en general y es un corolario del teorema anterior.

Teorema 14. Dados dos números naturales a, $b \in \mathbb{N}$ cualesquiera, se cumple que

$$\operatorname{Div}(a) \cap \operatorname{Div}(b) = \operatorname{Div}(\operatorname{mcd}(a, b))$$

Demostración. Sea $D = \operatorname{mcd}(a, b)$, esto implica que existe k, $k' \in \mathbb{N}$ tales que $kD = a$ y $k'D = b$ (hipótesis). Debemos demostrar una igualdad de conjuntos, demostramos la inclusión hacia un lado primero y luego la inclusión hacia el otro lado.

- $\supseteq$ Si n es es divisor de D, es claro que n ha de ser divisor de a y de b también, ya que la relación de divisibilidad es transitiva.
- $\subseteq$ Si n es divisor de a y de b (segunda hipótesis) debemos demostrar que entonces n es divisor de D. Sabemos, por definición de mcd, que $n \leq D$. También sabemos que a y b son múltiplos tanto de n como de D, es decir, ambos son múltiplos comunes de n y D. Por el teorema anterior, esto nos dice qua a y b son múltiplos de $\operatorname{mcm}(n, D)$, o dicho de otra forma $\operatorname{mcm}(n, D)$ es un divisor común de a y b. Por lo tanto

  $$D \leq \operatorname{mcm}(n, D) \leq \operatorname{mcd}(a, b) = D,$$

  es decir $D = \operatorname{mcm}(n, D)$!! pero esto implica que $n|D$. □

Estos dos últimos teoremas establece una simetría casi total entre los conceptos de máximo común divisor y mínimo común múltiplo, la cual se ve coronada con el siguiente teorema.

Teorema 15. Dados dos números naturales a, $b \in \mathbb{N}$ cualesquiera, se cumple que

$$\text{mcm}(a,b) \cdot \text{mcd}(a,b) = a \cdot b.$$

Demostración. Sean $D = \text{mcd}(a,b)$ y $M = \text{mcm}(a,b)$.

Sabemos que ab es múltiplo común de a y b, por lo tanto $M|(ab)$. Por lo tanto existe $k \in \mathbb{N}$ tal que $kM = ab$.

También sabemos que por ser M un múltiplo común de a y b, existen $n, m \in \mathbb{N}$ tales que $M = na = mb$, es decir

$$kM = kna = kmb = ab.$$

De aquí se obtiene que

$$km = a \ \wedge \ kn = b$$

Por lo tanto k es divisor común de a y b, entonces

$$k|D. \tag{1}$$

Por otra parte, al ser D un divisor común de a y b, existen $i, j \in \mathbb{N}$ tales que $iD = a$ y $jD = b$. Así $ijD = ja = ib$ es múltiplo común de a y b, y el Teorema 13 nos dice que $M|(ijD)$, desarrollamos:

$$\begin{aligned} M|(ijD) &\Rightarrow \frac{ijD}{M} \in \mathbb{Z} \\ &\Rightarrow \frac{iDjD}{DM} \in \mathbb{Z} \\ &\Rightarrow \frac{ab}{DM} \in \mathbb{Z} \\ &\Rightarrow \frac{kM}{DM} \in \mathbb{Z} \\ &\Rightarrow \frac{k}{D} \in \mathbb{Z} \\ &\Rightarrow D|k \end{aligned}$$

Juntando esta última con la ecuación (1) concluimos que $k = D$, es decir $DM = ab$. □

Este teorema nos da una manera de obtener el mínimo común múltiplo si es que ya hemos encontrado em máximo común divisor.

Ejemplo 16. Consideremos $a = 36$ y $b = 40$, listamos sus divisores:

$$\text{Div}(36) = \{1, 2, 3, 4, 6, 9, 12, 18, 36\}$$

$$\text{Div}(40) = \{1, 2, 4, 5, 8, 10, 20, 40\}$$

Sus divisores comunes son los siguientes.

$$\text{Div}(36) \cap \text{Div}(40) = \{1, 2, 4\}$$

Por lo tanto el mayor de sus divisores comunes es 4.

Del teorema anterior calculamos el mínimo común múltiplo sin mayores cavilaciones como

$$\text{mcm}(36, 40) = \frac{36 \cdot 40}{4} = 360.$$

La noción de máximo común divisor permite definir otro importante concepto: *primos relativos*

Definición 17. Dos naturales a y b son *primos relativos* si y solo si $\text{mcd}(a, b) = 1$

Ejemplo 18.

- $\text{mcd}(8, 15) = 1$, entonces 8 y 15 son primos relativos, o primos entre sí, a pesar que ninguno de los dos son primos, lo que ocurre es que no tienen divisores comunes salvo el 1.
- $\text{mcd}(8, 6) = 2$, entonces 8 y 6 no son primos relativos ya que 2 es divisor común de estos.

Concluimos esta sección con el Lema de Euclides, el cual será clave para obtener el teorema Fundamental de la Aritmética, o Teorema de Descomposición Única.

Lema 19 (Lema de Euclides)**.** Si $a, b, c \in \mathbb{N}$ son números tales que $a|(bc)$ y $\text{mcd}(a, b) = 1$, entonces $a|c$.

Demostración. Como a divide a bc y b también divide a bc se tiene que $\text{mcm}(a, b)$ divide a bc, gracias al teorema 13. Ahora bien, dado que nos dicen que $\text{mcd}(a, b) = 1$, del teorema 15, se tiene $\text{mcm}(a, b) \cdot 1 = \text{mcm}(a, b) \cdot 1 = ab$. Entonces $\frac{bc}{ba} \in \mathbb{Z}$, pero $\frac{bc}{ba} = \frac{c}{a}$, por lo tanto $a|c$. □

Destacamos que la hipótesis $\text{mcd}(a, b) = 1$ es muy importante, por ejemplo $6|(4 \cdot 15)$, pero $6 \nmid 4$ ni $6 \nmid 15$. Esto ocurre ya que $\text{mcd}(6, 4) = 2 \neq 1$, por lo tanto el Lema de Euclides no aplica ya que sus hipótesis no se cumplen.

Podemos aplicar el Lema de Euclides por ejemplo si nos dicen que, $6|(5a)$, podemos de inmediato deducir que a es múltiplo de 6 ya que $\text{mcd}(6, 5) = 1$.

Teorema de descomposición prima

Al fin llegamos al teorema que hemos anunciado desde el comienzo del capítulo. El *el teorema de descomposición prima* establece que todo número se escriba de una única manera como multiplicación de números primos.

$$\begin{aligned} 6 &= 2 \cdot 3 \\ 15 &= 3 \cdot 5 \\ 12 &= 2^2 \cdot 3 \\ 360 &= 2^3 \cdot 3^2 \cdot 5 \end{aligned}$$

No es dificil ver que la descomposición existe, algo más complejo es demostrar que es única, y es justamente esto lo que la hace tremendamente útil.

Teorema 20. Para todo número natural $n > 1$ existen únicos números primos p_1, ... , p_k, salvo el orden, tales que

$$n = p_1 p_2 \cdot p_k$$

Siendo $k = 1$, es decir un producto con un solo factor, si n mismo es primo.

Demostración. Sea $n \in \mathbb{N}$.

- (Existencia) Lo demostraremos por inducción fuerte.
  - (Base de inducción) $n = 2$: como 2 es primo, es producto de solo un primo.
  - (Paso de inducción) Tomamos n cualquiera, y suponemos que la descomposición existe para todos los naturales $m \leq n$. Demostraremos que la descomposición existe también para $n + 1$. Podemos separarla en dos casos.
    - (Caso 1) $n + 1$ es primo. Este caso es trivial, ya que al ser primo se descompone trivialmente como producto de solo un factor.
    - (Caso 2) $n + 1$ no es primo. Si $n + 1$ no es primo, entonces tiene algún divisor d, distinto de $n + 1$ y distinto de 1, por lo tanto podemos afirmar que $2 \leq d \leq n$. Esto implica que existe $c \in \mathbb{N}$ tal que $n + 1 = cd$. Observamos que $c \neq 1$ pues si lo fuera se tendría $n + 1 = d$ lo cual ya dijimos que no es así. También observamos que $c < n + 1$ pues dado que $d \geq 2$ se tendría que $n + 1 = cd = (n + 1)d > n + 1$ lo cual es una contradicción.
      Concluimos que $n + 1$ se descompone en la multiplicación de dos números naturales $2 \leq d, c \leq n$. Aplicamos entonces la hipótesis de inducción a estos dos números d y c, la cual nos dice que existen números primos $p_1, p_2, \ldots, p_k$ y $q_1, q_2, \ldots, q_l$ tales que $c = p_1 p_2 \cdots p_k$ y $d = q_1 q_2 \cdots q_l$. Por lo tanto $n + 1 = cd = p_1 p_2 \cdots p_k q_1 q_2 \cdots q_l$, con lo cual hemos demostrado que $n + 1$ es producto de primos.
- (Unicidad) Debemos demostrar que no hay dos maneras distintas de escribir un número como multiplicacion de primos, a no ser por un mero cambio de orden. Nuevamente razonamos por inducción fuerte.
  - (Base de inducción) $n = 2$: 2 no tiene más factores pues es el menor de todos los números primos, por lo tanto la unicidad de la descomposición es evidente en este caso.

- (Paso de inducción) Tomamos n cualquiera, y suponemos que la descomposición de todos los naturales $m \leq n$ es única. Demostraremos que la descomposición es única también para $n+1$. Razonaremos por contradicción suponiendo que hay dos maneras distintas de escribir $n+1$ como producto de primos:

$$n+1 = p_1 \cdot p_2 \cdots p_k = q_1 \cdot q_2 \cdots q_l. \tag{2}$$

  Aparecen dos casos.

  - (Caso 1) Existen i, j tales que $p_i = q_j$. En ese caso podemos dividir la ecuación (**??**) por p_i, y obtenemos la siguietne igualdad.

$$\frac{n+1}{p_i} = \frac{p_1 \cdot p_2 \cdots p_k}{p_i} = \frac{q_1 \cdot q_2 \cdots q_l}{q_j}$$

    Dado que p_i es primo, $p_i \geq 2$, por lo tanto $\frac{n+1}{p_i}$ es un natural menor o igual a n, por lo tanto, de la hipótesis de inducción, tiene una descomposición única como producto de números primos. De aquí concluimos que $k = l$ y que en realidad las dos descomposiciones de $n+1$ no eran dos si no una sola.
  - (Caso 2) No hay primos en común en los conjuntos $\{p_1, p_2, \ldots, p_k\}$ y $\{q_1, q_2, \ldots, q_l\}$. En este caso podemos afirmar que $p_1 | p_1 \cdots p_k$ ya que es uno de sus factores. Pero de la ecuación (2) concluimos que $p_1 | q_1 \cdots q_l$. Como $q_1 \neq p_1$ podemos afirmar que $\text{mcd}(p_1, q_1) = 1$, y entonces podemos aplicar el Lema de Euclides para concluir que:

$$p_1 | q_2 \cdots q_l.$$

    No es difícil ver que el argumento se puede repetir una y otra vez y terminar concluyendo que $p_1 | q_l$, lo cual es una contradicción con la primalidad de q_l, lo cual termina la demostración. Pero hagamos esto bien, por inducciónen j, es decir, demostremos que

$$\forall j \in \{2, \ldots, l\},\ p_1 | q_j q_{j+1} \ldots q_l.$$

    - ◇ (Base de inducción) $p_1 | q_2 \cdots q_l$, ya lo hemos demostrado.
    - ◇ Tomemos $j < l$, supongamos que es verdad que $p_1 | q_j q_{j+1} \ldots q_l$, demostremos ahora que $p_1 | q_{j+1} \cdots q_l$. Pero eso se cumple gracias al Lema de Euclides ya que tanto p_1 como q_j son primos y por lo tanto se tiene que $\text{mcd}(p_1, q_j)$.

□

Corolario 21. Existen infinitos números primos.

Demostración. Razonemos por contradicción y supongamos que solo hay una cantidad finita de números primos, y digamos que estos son $\{p_1, \ldots, p_k\}$. Consideremos ahora el número siguiente.

$$N = p_1 p_2 \cdots p_k + 1$$

Es claro que $p+1$ es un número y que es mas grande que todos los primos existentes, ya que el producto de estos ya es al menos el doble más grande que cualquiera de ellos pues 2, 3 y 5 son factores de ese producto.

Por lo tanto $N \notin \{p_1, \ldots, p_k\}$ y entonces no puede ser primo.

N tampoco es igual a 1, entonces N debe des componerse como producto de primos. Por lo tanto alguno de los primos ha de ser divisor de N, es decir, existe j tal que:

$$\frac{N}{p_j} = \underbrace{\frac{p_1 p_2 \cdots p_k}{p_j}}_{\in \mathbb{N}} + \underbrace{\frac{1}{p_j}}_{\in]0,1[} \in \mathbb{N},$$

pero un natural no puede ser suma de otro natural más un úna fracción no entera, entonces nuestra suposición de finitud es falsa, es decir, existen infinitos número primos. □

Congruencias modulares

Lo que viene a continuación es un bello tópico, que tiene que ver con los números que e usan en las telecomunicaciones y en la informática, pero no forma arte de los *resultados de aprendizaje* del curso, por lo tanto no será evaluado. Por esta razón lo coloreamos con tinta azul.

Congruencias módulo p

Podemos definir otra relación usando el concepto de divisibilidad y la resta de números enteros, la relación de *congruencia modulo p*.

Definición 22. Dado un número $p \in \mathbb{N}$, se define la relación de *congruencia modulo p* en $\mathbb{Z}$, denotada por $\sim_p$, como sigue.

$$a \sim_p b \;\Leftrightarrow\; p|(a-b).$$

Ejemplo 23.

- Si tomamos $p = 2$, vemos que $a \sim_2 b$ si y solo si $a - b$ es múltiplo de 2, lo cual equivale a decir que a y b tiene la misma paridad.
- Si tomamos $p = 5$, vemos que $2 \sim_5 7$ ya que $2 - 7 = -5 = -1 \cdot 5$, por otra parte $2 \not\sim_5 5$ ya que $2 - 5 = -3$ que no es múltiplo de 5. Observamos que el resto de dividir 2 y 7 por 5 es siempre 2: $2 = 0 \cdot 5 + 2$ y $7 = 1 \cdot 5 + 2$.

No es una si no infinitas relaciones, una para cada natural p, resulta que cada una de estas relaciones es de equivalencia.

Proposición 24. Dado un número $p \in \mathbb{N}$, la relación de *congruencia modulo p* es relación de equivalencia en $\mathbb{Z}$.

Demostración.

- **Es refleja.** Sea $a \in \mathbb{Z}$ cualquiera, vemos que $a \sim_p a$ ya que $a - a = 0$ y $p|0$.
- **Es simétrica.** Sean $a, b \in \mathbb{Z}$ tales que $a \sim_p b$ (hipótesis), eso significa que $a - b$ es múltiplo de p, es decir, existe $k \in \mathbb{Z}$ tal que $a - b = kp$, pero entonces $b - a = (-k)p$, con lo cual tenemos que $b \sim_p a$.
- **Es transitiva.** Sean $a, b, c \in \mathbb{Z}$ tales que $a \sim_p b$ y $b \sim_p c$ (hipótesis). Vamos a demostrar que $a \sim_p c$. Pero trabajemos la hipótesis un poco más. Tenemos que $p|(a - b)$ y $p|(b - c)$, por lo tanto existen $k, k' \in \mathbb{Z}$ tales que $kp = a - b$ y $k'p = b - c$. Despejamos b de la segunda ecuación y lo reemplazamos en la primera:

  $$kp = a - k'p - c.$$

  De donde se obtiene:

  $$(k - k')p = a - c.$$

  Como $k, k' \in \mathbb{Z}$ se cumple que $k - k' \in \mathbb{Z}$ también, por lo tanto la última ecuación nos dice que $p|(a - c)$ y entonces $a \sim_p c$. □

Al ser una relación de equivalencia nos permite definir clases de equivalencia. Partamos con $p = 2$ (¿qué pasa si $p = 1$?). Tenemos que la diferencia entre dos pares es siempre par, es decir, es siempre múltiplo de 2, por lo tanto todos los pares están relacionados entre sí.

$$[0] = \{2k \ : \ k \in \mathbb{Z}\}$$

Por su parte, al restar dos impares también me da un par, por lo tanto todos los impares están relacionados entre sí.

$$\begin{aligned} [1] &= \{n \ : \ \exists k \in \mathbb{Z}, \ n - 1 = 2k\} \\ &= \{2k + 1 \ : \ k \in \mathbb{Z}\} \end{aligned}$$

Hay solo dos clases de equivalencia para la relación $\sim_2$.

Veamos ahora el caso $p = 5$. Es claro que todos los múltiplos de 5 están relacionados entre sí, ya que la diferencia entre dos múltiplos de 5 sigue siendo múltiplo de 5.

$$[0] = \{5k \ : \ k \in \mathbb{Z}\}$$

Ahora, ¿qué queda en la clase de 1 por ejemplo?

$$\begin{aligned} [1] &= \{n \ : \ \exists k \in \mathbb{Z}, \ n - 1 = 5k\} \\ &= \{5k + 1 \ : \ k \in \mathbb{Z}\} \\ &= \{-19, -14, -9, -4, 1, 6, 11, 16, 21, \dots\} \end{aligned}$$

Son todos los números que se pueden escribir como un múltiplo de 5 más 1. Tenemos entonces más clases de equivalencia.

$$[2] = \{5k + 2 \ : \ k \in \mathbb{Z}\} = \{-18, -13, -8, -3, 2, 7, 12, 17, 22, \dots\}$$

$$[3] = \{5k+3 \ : \ k \in \mathbb{Z}\} = \{\ldots -17, -12, -7, -2, 3, 8, 13, 18, 23, \ldots\}$$
$$[4] = \{5k+4 \ : \ k \in \mathbb{Z}\} = \{\ldots -16, -11, -6, -1, 4, 9, 14, 19, 24, \ldots\}$$

Completamos un total de 5 clase de equivalencia. Notamos que sumar 3 equivale a restar 2.

$$[3] = \{5k+3 \ : \ k \in \mathbb{Z}\} = \{5(k+1)-2 \ : \ k \in \mathbb{Z}\} = \{5k-2 \ : \ k \in \mathbb{Z}\}$$

Estas relaciones de equivalencia "resisten" a las operaciones aritméticas.

Proposición 25. Dado un número $p \in \mathbb{N}$, se cumplen las siguientes propiedades.

1. $\forall a, b, c, d \in \mathbb{Z}, (a \sim_p b \wedge c \sim_p d) \Rightarrow (a+c) \sim_p (b+d)$
2. $\forall a, b, c, d \in \mathbb{Z}, (a \sim_p b \wedge c \sim_p d) \Rightarrow (ac) \sim_p (bd)$

Demostración.

1. Sean $a, b, c, d \in \mathbb{Z}$ tales que $(a \sim_p b \wedge c \sim_p d)$ (hipótesis), debemos demostrar que $(a+c) \sim_p (b+d)$. Desarrollamos la hipótesis: $p|(a-b)$ y $p|(c-d)$, es decir, existen $k, k' \in \mathbb{Z}$ tales que $kp = a-b$ y $k'p = c-d$. Sumamos ambas ecuaciones y obtenemos: $(a+c)-(b+d) = (k+k')p$, de donde $p|((a+c)-(b+d)$ y por lo tanto $a+c \sim_p b+d$.
2. Sean $a, b, c, d \in \mathbb{Z}$ tales que $(a \sim_p b \wedge c \sim_p d)$ (hipótesis), debemos demostrar que $(ac) \sim_p (bd)$. Igual que antes, tenemos que existen $k, k' \in \mathbb{Z}$ tales que $kp = a-b$ y $k'p = c-d$. Despejamos a en la primera ecuación y c en la segunda: $a = kp+b$ y $c = k'p+d$. Multiplicamos:

$$\begin{aligned} ac &= (kp+b)(k'c+d) \\ &= kk'p^2 + kpd + k'cb + bd \\ &= p(kk'p + kd + k'c) + bd \end{aligned}$$

   Lo cual implica que $ac - bd = p(kk'p + kd + k'c)$, y como el número $kk'p + kd + k'c \in \mathbb{Z}$, concluimos que $p|(ac-bd)$ y $ac \sim_p bd$. □

Con todo esto, podemos definir las operaciones aritméticas entre las clases de equivalencia, ya que al operar miembros de las clases de equivalencia entre sí, la clase resultante no depende de los miembros que hayamos escogido para hacer pa operación, si no solo de a qué clase pertenecían. Ilustremos esto con un ejemplo para $p = 5$. Tomemos $1 \sim_5 6$ y $3 \sim_5 -7$.

$$\begin{aligned} [1] + [3] &= [1+3] = [4] \\ [6] + [-7] &= [6-7] = [-1] = [4] \\ [1]\,[3] &= [1 \cdot 3] = [3] \\ [6]\,[-7] &= [6 \cdot (-7)] = [-42] = [-45+3] = [3] \end{aligned}$$

Esto nos permite definir las tablas pitagóricas de la suma y la multiplicación de clases de equivalencia. Terminemos esta clase desarrollando los dos ejemplos que hemos tratado.

Para $p = 2$

$+$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

$\cdot$	$[0]$	$[1]$
$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$

Para $p = 5$

$+$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[1]$	$[1]$	$[2]$	$[3]$	$[4]$	$[0]$
$[2]$	$[2]$	$[3]$	$[4]$	$[0]$	$[1]$
$[3]$	$[3]$	$[4]$	$[0]$	$[1]$	$[2]$
$[4]$	$[4]$	$[0]$	$[1]$	$[2]$	$[3]$

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	$[0]$	$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[2]$	$[0]$	$[2]$	$[4]$	$[1]$	$[3]$
$[3]$	$[0]$	$[3]$	$[1]$	$[4]$	$[2]$
$[4]$	$[0]$	$[4]$	$[3]$	$[2]$	$[1]$