Solía permitirme creer que la mente es un subproducto del cuerpo. ¿ Dónde se llega primero, al puerto o a ciudad, a la ciudad o al Estado, al Estado o al mundo?

Mi hermana y yo, Federico Nietzsche.

Capítulo 1

Los Números Enteros

1.1. Introducción

El objetivo de este capítulo es presentar las propiedades básicas de los números enteros que vamos a necesitar en los próximos capítulos. Con el fin de tener una definición formal de los números enteros, en el marco de la teoría de conjunto, mostraremos como se construyen a partir de los números naturales. Sin embargo no nos detendremos a probar todas las propiedades básicas de los enteros a partir de su definición sino que las enunciaremos y las usaremos. Invitamos al lector a realizar las pruebas de dichas propiedades que sólo requieren de las definiciones presentadas. Los números enteros se definen como clases de pares ordenados, pero para simplificar su notación y manipulación los denotaremos como se hace usualmente. Los puntos más importantes tratados en este capítulo son: el principio de buena ordenación, los principios de inducción, el algoritmo de Euclides y el teorema de descomposición en primos (teorema fundamental de la aritmética).

1.2. La Definición

Sobre el conjunto $\mathbb{N} \times \mathbb{N}$ se define la siguiente relación:

$$< a, b > \equiv < c, d > \Longleftrightarrow a + d = b + c \ . \tag{1.1}$$

Esta relación es una relación de equivalencia sobre $\mathbb{N} \times \mathbb{N}$, y por consiguiente, parte al conjunto $\mathbb{N} \times \mathbb{N}$ en clases disjuntas. Al conjunto de dichas clases, esto es, al conjunto cociente se le denomina *conjunto de los enteros racionales* y se denota por la letra Z. Entonces se tiene que

$$Z = \{[< n, 0 >] : n \in \mathbb{N}^*\} \cup \{[< 0, n >] : n \in \mathbb{N}^*\} \cup \{[< 0, 0 >]\} \ . \tag{1.2}$$

Al primero de los conjuntos de esta unión se le denomina conjunto de los enteros positivos y se le denota por Z^+, al segundo se le denomina conjunto de los enteros

negativos y se le denota por Z^- y finalmente el último de los conjunto de esta unión es un singletón cuyo único elemento es el *cero*. Al entero $[< n, 0 >]$ lo denotaremos por n o $+n$, mientras que al entero $[< 0, n >]$ lo denotaremos por $-n$. Recuerde que los corchetes significan la clase del elemento tal.

1.2.1. Aritmética Entera

Sobre el conjunto de los números enteros se definen dos operaciones que denominamos adición y multiplicación como sigue:

$$\begin{array}{rcl} [< a, b >] + [< c, d >] & = & [< a + c, b + d >] \\ [< a, b >] * [< c, d >] & = & [< ac + bd, ad + bc >] \ . \end{array} \tag{1.3}$$

Sobre la adición se pueden probar las siguientes propiedades:

1. Clausura: $(\forall x, y \in Z)(x + y \in Z)$
2. Asociatividad: $(\forall x, y, z \in Z)((x + y) + z = x + (y + z))$
3. Existencia de Neutro: $(\forall x \in Z)(x + 0 = 0 + x = x)$
4. Existencia de inverso: $(\forall x \in Z)(x + (-x) = (-x) + x = 0)$
5. Conmutatividad: $(\forall x, y \in Z)(x + y = y + x)$

y para la multiplicación se pueden probar las siguientes propiedades:

1. Clausura: $(\forall x, y \in Z)(x * y \in Z)$
2. Asociatividad: $(\forall x, y, z \in Z)((x * y) * z = x * (y * z))$
3. Existencia de Neutro: $(\forall x \in Z)(x * 1 = 1 * x = x)$
4. Conmutatividad: $(\forall x, y \in Z)(x * y = y * x)$

Además se cumplen las leyes distributivas de la multiplicación con respecto a la adición, esto es: $(\forall x, y, z \in Z)(x(y + z) = xy + xz \wedge (x + y)z = xz + yz)$

Otras dos propiedades importantes de los números enteros son las siguientes:

- En los enteros *se cumplen las leyes cancelativas*, esto es, $(\forall x, y, z \in Z)(z \neq 0 \wedge zx = zy \Rightarrow x = y)$
- En los enteros *no existen divisores de cero distintos de cero*, esto es, $(\forall x, y \in Z)(xy = 0 \Rightarrow x = 0 \vee y = 0)$

1.2.2. Un Orden en los Enteros

Sobre el conjunto de números enteros se define la siguiente relación de orden

$$< a, b > \ \leq \ < c, d > \iff \ a + d \leq b + c \ . \tag{1.4}$$

Donde el signo $\leq$ del lado derecho es la relación de orden usual en los números naturales. Puede probarse que con esta relación de orden el conjunto de los números enteros es un conjunto linealmente ordenado. Alerta: No es la única relación de orden que se puede definir sobre los enteros, pero es la que usamos con más frecuencia: la denominamos *orden usual*. A continuación mostramos algunas de las propiedades más importantes del orden en los enteros. Como es usual denotaremos al orden estricto asociado a $\leq$ por $<$, recordando que $a < b$ significa que $a \leq b \wedge a \neq b$.

Cuadro 1.1: Algunas Propiedades del orden de los Enteros

1.	$m \leq m$	5.	$m \leq n \wedge p \leq q \Longrightarrow m + p \leq n + q$
2.	$m \leq n \wedge n \leq m \Longrightarrow m = n$	6.	$m \leq n \wedge p > 0 \Longrightarrow mp \leq np$
3.	$m \leq n \wedge n \leq p \Longrightarrow m \leq p$	7.	$m \leq n \wedge p < 0 \Longrightarrow np \leq mp$
4.	$m \leq n \Longrightarrow m + p \leq n + p$	8.	$m < n \vee n < m \vee m = n$

Como para todo entero a se tiene que es cero, o bien que es positivo o bien que es negativo a continuación se define su valor absoluto.

Definición 1.1 (Valor Absoluto) *Dado un número entero a se define el valor absoluto de a y se denota por $|a|$ como cero si $a = 0$ o como el entero positivo del par no ordenado $\{a, -a\}$ si $a \neq 0$, esto es:*

$$|a| = \begin{cases} a, & si\ a \geq 0; \\ -a, & si\ a < 0. \end{cases} \tag{1.5}$$

La función valor absoluto tiene las siguientes propiedades:

$$|a| = |-a|, \qquad |ab| = |a||b|, \qquad -|a| \leq a \leq |a|, \tag{1.6}$$

Si p es un entero positivo, entonces $|a| < p \Leftrightarrow -p < a < p$. Tambiém es importante la siguiente proposición.

Teorema 1.1 (Desigualdad Triangular) *Para todo par de enteros a, b, se tiene que $|a \pm b| \leq |a| + |b|$.*

1.3. Principio de Buena Ordenación

Definición 1.2 (Conjunto Bien Ordenado) *Un conjunto parcialmente ordenado se dice que está bien ordenado si y sólo si está linealmente ordenado y cada uno de sus subconjuntos no vacíos tiene mínimo.*

El conjunto de los números enteros no es un conjunto bien ordenado porque él mismo no tiene mínimo. Sin embargo, el conjunto de los números enteros positivos Z^+ y el de los enteros no negativos son conjuntos bien ordenados.

Una consecuencia del principio de buena ordenación de los números enteros positivos o de los enteros no negativos son los principios de inducción. A continuación estudiaremos los principios de inducción para los enteros positivos o no negativos, pero los mismos son válidos en cualquier conjunto bien ordenado.

Teorema 1.2 *Todo subconjunto de enteros positivos que incluya a* 1 *y que para todo* k *si incluye* k*, también incluye a* $k+1$*, incluye a todos los enteros positivos.*

Prueba: Sea S un subconjunto de Z^+ que incluye a 1 y tal que si $k \in S$, se tiene que $k+1 \in S$. Si $S \neq Z^+$, entonces existe $x \in Z^+$ tal que $x \notin$, por lo tanto el conjunto $A = \{x \in Z^+ : x \notin S\}$ no es vacío y es subconjunto de Z^+. Luego, en base al principio de buena ordenación, tiene mínimo que llamaremos m. Se tiene que m no puede ser igual a 1 porque $1 \in S$; por lo tanto $m > 1$ y por consiguiente $m - 1 > 0$, lo cual implica que $m - 1$ por ser menor que m no pertenece a A y en consecuencia, como es positivo, pertenece a S. Pero, como $m - 1 \in S$ se tiene que $(m - 1) + 1 = m$ pertenece a S, lo cual es una contradicción que provino de considerar que A era distinto del conjunto vacío. Por lo tanto A es vacío y $S = Z^+$. □

El siguiente teorema es consecuencia del principio de buena ordenación. Su prueba es por absurdo y se deja como ejercicio.

Teorema 1.3 *No existe entero positivo entre* 0 *y* 1.

1.4. Principios de Inducción

También son consecuencia del principio de buena ordenación los siguientes dos teoremas. El primero de ellos se conoce como principio de inducción completa y es el más conocido. Su prueba es similar a la del segundo y se deja como ejercicio.

Teorema 1.4 (Principio de Inducción Completa) *Si* $P(n)$ *es una proposición que pueden o no satisfacer los enteros, se cumple que* $P(1)$ *es verdadera y para cualquier* $k > 0$*,* $P(k)$ *implica* $P(k+1)$*, entonces* $P(n)$ *es cierta para todo entero positivo.*

El siguiente teorema se conoce como segundo principio de inducción o principio de inducción generalizada.

Teorema 1.5 (Segundo Principio de Inducción) *Si* P *es una proposición que pueden o no satisfacer los enteros y para cualquier* $m > 0$ *la hipótesis de que* $P(k)$ *es verdadera para todo* $0 < k < m$ *implica que* $P(m)$ *es verdadera, entonces* $P(n)$ *es cierta para todo entero positivo.*

Prueba: Sea S el conjunto de enteros positivos para los cuales P es falsa. Si S es vacío, entonces P es verdadera para todo entero positivo. Si S no es vacío, existe en S un elemento mínimo m—Principio de buena ordenación—. Como m es el entero positivo más pequeño para el cual no se cumple P, se tiene que para todo $k < m$, $P(k)$ es verdadera; luego, se concluye que $P(m)$ también es verdadera. Esto es una contradicción, luego, S no puede ser no vacío. □

1.5. Divisibilidad en los Enteros

La ecuación $ax = b$ no siempre tiene solución en los enteros, esto es, dados $a, b \in Z$, no siempre existe $c \in Z$ tal que $ac = b$; por ejemplo, la ecuación $2x = 3$ no tiene solución en los enteros porque no existe un entero que multiplicado por 2 de 3. Cuando tal solución existe se dice que "a divide a b", que "a es divisor de b" o que "b es divisible por a". También se dice que b es múltiplo de a. Este concepto se formaliza a continuación.

Definición 1.3 *Dados dos enteros a y b, decimos que "a divide a b", y lo representamos por $a|b$, si y sólo si existe un número entero z tal que $az = b$.*

Alerta: Dado que los divisores de un entero no nulo vienen por pareja, muchos autores usan la frese "es divisor" sólo para referirse a los divisores no negativos, por ejemplo, suelen decir: "los divisores de 12 son 1,2,3,4,6,12." Nosotros usaremos explícitamente el calificativo "positivos" cuando necesitemos referirnos sólo a los divisores positivos.

Teorema 1.6 *La relación "divide a " es reflexiva y transitiva, esto es:*

reflexividad: $\forall a \in Z \quad a|a$

transitividad: $\forall a, b, c \in Z \quad (a|b \wedge b|c \Rightarrow a|c)$

Prueba: Sea $a \in Z$; se tiene que $a = a \cdot 1$, luego $a|a$. Sean $a, b, c \in Z$; si $a|b$ y $b|c$ se tiene que existen enteros z_1 y z_2 tales que $b = az_1$ y $c = bz_2$. Por lo tanto, $c = az_1z_2$, lo que indica que $a|c$. □

Si a es un divisor de b y a es un divisor de c, decimos que a es un divisor común de b y c; por ejemplo, 1, 2, 3 y 6 son divisores comunes de 18 y 24. Un resultado importante y fácil de probar sobre los divisores comunes es el siguiente: Si d es un divisor común de a y b, entonces d es un divisor de cualquier combinación lineal de a y b.

Ejercicio 1.1 *Demuestre que si $a|b$ y $a|c$, entonces $a|b \pm c$.*

Ejercicio 1.2 *Demuestre que si $a|b$ o $a|c$, entonces $a|bc$.*

Ejercicio 1.3 *Demuestre que si $a|b \pm c$ y $a|b$, entonces $a|c$.*

Definición 1.4 (Unidades) *Se denominan unidades a los divisores de* 1.

Teorema 1.7 *Las únicas unidades de Z son* ± 1.

Prueba: El entero a es una unidad de Z si y sólo si existe $b \in Z$ tal que $ab = 1$. Debemos probar que $a = \pm 1$. Si $ab = 1$ se tiene que $a \neq 0$ y que $b \neq 0$ (porque de ser alguno cero el producto sería cero) y que $|ab| = |a| \cdot |b| = 1$. Luego, como $|a| > 0$ y $|b| > 0$ y como no existe un entero k tal que $0 < k < 1$ se tiene que $|a| \geq 1$ y $|b| \geq 1$. Si $|a| > 1$, entonces se tiene que $|a| \cdot |b| > |b| \geq 1$ ($x < y \wedge c > 0 \Rightarrow cx < cy$ y transitividad). Por consiguiente $|ab| > 1$ que contradice $|ab| = 1$. Esto implica que $|a| = 1$ y en consecuencia que $a = \pm 1$. □

La relación "divide a" no es antisimétrica porque, por ejemplo, $2|-2$ y $-2|2$, pero $2 \neq -2$. El siguiente corolario muestra una propiedad parecida a la antisimetría. Él dice que los enteros mutuamente divisible son solamente los opuestos.

Corolario 1.8 *Si los enteros a y b son mutuamente divisibles, esto es, $a|b$ y $b|a$, entonces $a = \pm b$.*

Prueba: Si $a|b$, se tiene que existe $z_1 \in Z$ tal que $b = az_1$. De igual forma, $b|a$ implica que $a = bz_2$ para algún $z_2 \in Z$. Luego, sustituyendo se tiene que $a = az_1z_2$; si $a = 0$, entonces $b = 0$, y si $a \neq 0$, se tiene que $a - az_1z_2 = a(1 - z_1z_2) = 0$, y dado que Z no tiene divisores de cero distintos de cero, se concluye que $z_1z_2 = 1$ y por el teorema anterior obtenemos que $z_1 = \pm 1$, de donde concluimos que $a = \pm b$. □

Nota: si consideramos el conjunto de los enteros positivos o el conjunto de los enteros no negativos, la relación de divisibilidad es un orden parcial y no total.

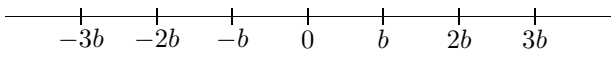
1.5.1. Algoritmo de Euclides

Teorema 1.9 (Algoritmo de la División de Euclides) *Dados dos enteros a y b tales que $b > 0$, se tiene que existen dos enteros q y r que cumplen con*

$$a = bq + r \qquad 0 \leq r < b \ .$$

Dichos enteros son únicos.

Prueba: Probaremos primero la existencia y luego la unicidad.
[Existencia] La prueba consiste en mostrar que existen múltiplos de b menores que a para concluir que el conjunto de los enteros positivos de la forma $a - bx$ no es vacío y en consecuencia tiene un elemento mínimo que probaremos es el máximo común divisor positivo entre a y b. Informalmente es claro que esto ocurre: si listaramos los múltiplos de b como se muestra en la figura, se tiene claramente, que no importa donde le corresponda ir a a, el mismo estará entre dos múltiplos de b y que todos los múltiplo a su izquieda son menores que él.



Formalicemos este argumento mostrando uno concreto: Puesto que $-|a|$ es negativo, se tiene que $-|a| \leq a$. Además puesto que b es positivo por hipotesis y no existe enteros entre cero y uno, se tiene que $b \geq 1$, y en consecuencia si múltiplicamos en ambos lados de esta desigualdad por $-|a|$ se tiene que $-|a|ble-|a|$. De estas dos desigualdades se concluye por transitividad que $-|a| \cdot b \leq a$ y por lo tanto, el conjunto de las diferencias $a - bx$ contiene por lo menos un entero **no** negativo e.g.: $a - b(-|a|) \geq 0$. Luego, en base al principio de buena ordenación $S = \{a - bx \geq 0\}$ tiene mínimo que llamaremos $r = a - bq$. Como $r \in S$ se tiene que $r \geq 0$; además si $r \geq b$ podríamos restar b en ambos lados y obtener un entero positivo menor $r - b \in S$, lo cual contradice el hecho de que r es el mínimo de S. Esto es,

$$r = a - qb \ \wedge \ r \geq b \Rightarrow r - b = a - qb - b = a - (q+1)b \geq 0$$

Luego $0 \leq r < b$. [Unicidad] Si suponemos que existen dos expresiones

$$a = qb + r \text{ y } a = q^{'}b + r^{'} \quad \text{con } 0 \leq r < b,\ 0 \leq r^{'} < b$$

Se tiene que $r - r^{'} = (q^{'} - q)b$. Por un lado, $r - r^{'}$ debe ser en valor absoluto menor que b pues se están restando dos números no negativos menores que b; pero a su vez es múltiplo de b, luego tiene que ser CERO, por lo tanto $r = r^{'}$ y por consiguiente $q = q^{'}$. □

Lema 1.10 *Todo subconjunto no vacío de números enteros cerrado para la adición y la sustracción, contiene sólo al cero, o contiene un número entero positivo mínimo del cual son múltiplos todos los demás.*

Prueba: Sea S, un conjunto no vacío cerrado para la adición y para la sustracción, y sea $a \neq 0$ un elemento de S; por definición de S, $a - a = 0 \in S$, por lo tanto $0 - a = -a \in S$. Luego, S contiene tanto a a como a $-a$, uno de los cuales debe ser positivo, luego S contiene un subconjunto no vacío de números enteros positivos, que por el principio de buena ordenación tiene mínimo. Denominemos a dicho mínimo b. Este conjunto S debe contener todos los múltiplos de b. Contiene a $b \cdot 1$; si contiene a $b \cdot k$, entonces contiene a $b \cdot (k+1)$ pues $b \cdot k + b = b \cdot (k+1)$. También contiene a los múltiplos negativos $-n \cdot b = 0 - nb$.

Veamos que S no contiene **no múltiplos** de b. Si $c \in S$ y c no es múltiplo de b, por el algoritmo de Euclides se tendrá que $c = qb + r$, lo cual implicaría que $r = c - qb \in S$, con $0 \leq r < b$. Si $r = 0$, se tiene que $c = qb$, lo cual es una contradicción pues supusimos que c no es múltiplo de b. Si $r \neq 0$, también se tiene una contradicción porque r es estrictamente menor que b y por elección b era el menor entero positivo de S. □

1.5.2. Máximo Común Divisor

Definición 1.5 (Máximo Común Divisor) *Un entero d se llama máximo común divisor de dos números enteros a y b si y sólo si es simultáneamente*

divisor de a y de b y además es múltiplo de cualquier otro divisor común. Lo denotamos por $MCD(a,b) = d$. Simbólicamente:

$$MCD(a,b) = d \Longleftrightarrow d|a \wedge d|b \quad \wedge \quad (c|a \wedge c|b \Rightarrow c|d)$$

Por ejemplo, 4 y -4 son los máximos comunes divisores de 12 y 8. Nótese que todo par de enteros no ambos nulos tienen dos máximos comunes divisores que difieren sólo en el signo. Esto da pie a la siguiente definición.

Definición 1.6 (Máximo Común Divisor Positivo) *Un entero positivo d se llama máximo común divisor de dos números enteros a y b si y sólo si es simultáneamente divisor de a y de b y además es múltiplo de cualquier otro divisor común. Lo denotamos por $(a,b) = d$ Simbólicamente*

$$(a,b) = d \Leftrightarrow d|a \wedge d|b \quad \wedge \quad (c|a \wedge c|b \Rightarrow c|d)$$

Nótese que es prácticamente la misma definición pero para muchos propósito es más cómoda de manipular.

Teorema 1.11 *Dos enteros no ambos nulos a y b tienen un máximo común divisor positivo (a,b). Este puede expresarse como "combinación lineal" de a y b con coeficientes enteros u y w como sigue*

$$(a,b) = ua + wb$$

Prueba: Consideremos el conjunto de los números de la forma $xa + yb$, esto es, consideremos $S = \{xa + yb : x, y \in Z\}$. Este conjunto es cerrado bajo la adición y la sustracción (¡Verifíquelo!), y por lo tanto todos sus elementos son múltiplos de algún entero positivo d que debe ser de la forma $d = ua + wb$ para algún $u, w \in Z$. Falta ver que este número d es, en efecto, el máximo común divisor positivo de a y b. Es divisor de a pues $a \in S$ ya que $a = 1 \cdot a + 0 \cdot b$ y por consiguiente $a = k \cdot d$; por igual razonamiento, d es divisor de b. Además como $d = ua + wb$ se tiene que si $c|a$ y $c|b$, entonces $c|ua + wb$, esto es, $c|d$, por lo tanto d es el máximo común divisor positivo de a y b, o sea, $d = (a,b)$ □

Las siguientes son algunas de las propiedades básicas de la función mcd positivo. Se dejan como ejercicio.

$$\begin{aligned} (a,0) &= |a| \\ (a,b) &= (b,a) \\ (a,b) &= (-a,b) \\ (a,b) &= (|a|,|b|) \\ (ak,a) &= |a| \qquad \forall k \in Z \end{aligned} \tag{1.7}$$

El siguiente teorema, que se basa en el Algoritmo de la División, establece una recurrencia que permite hallar el máximo común divisor positivo de cualquier par de enteros.

Teorema 1.12 (Recursión de Euclides) *Si a y b son enteros positivos tales que $a = bq + r$ con $0 \leq r < b$, entonces $(a,b) = (b,r)$*

Prueba: Como $a = bq+r$ se tiene que si $x|a \wedge x|b$, entonces $x|r$ y en consecuencia todo divisor común de a y b es divisor común de b y r. Además, si $x|b \wedge x|r$, entonces $x|a$, y por lo tanto todo divisor común de b y r, es divisor común de a y b. Luego, el conjunto de los divisores comunes de a y b es igual al conjunto de los divisores comunes de b y r; por consiguiente su máximo es el mismo, esto es: $(a, b) = (b, r)$. □

El Teorema 1.9 se denomina Algoritmo de Euclides porque él permite plantear un procedimiento (algoritmo) para determinar el máximo común divisor de cualquier par de enteros positivos. Realmente aun cuando los dos enteros no sean positivos el algoritmo puede hallar su máximo común divisor considerando los números positivos, porque el valor del máximo común divisor positivo no depende de los signos de los números.

En el siguiente ejemplo se muestra como se usa el algoritmo de Euclides para hallar el máximo común divisor positivo de dos enteros positivos.

Ejemplo 1.1 *Halle el máximo común divisor positivo de los enteros* 210 *y* 33 *y expréselo como combinación lineal de dichos enteros.*

Explicación: Al dividir 210 entre 33 se tiene que el resto es 12 y el cociente es 6, esto es, $210 = 33 \cdot 6 + 12$. Luego, en base al lema anterior se tiene que $(210, 33) = (33, 12)$. Repitiendo el proceso se tiene que $33 = 12 \cdot 2 + 9$ y por lo tanto $(210, 33) = (33, 12) = (12, 9)$. Si repetimos el proceso una vez más se tiene que $12 = 9 \cdot 1 + 3$ y que $(210, 33) = (33, 12) = (12, 9) = (9, 3)$. Finalmente, $9 = 3 \cdot 3 + 0$ y

$$(210, 33) = (33, 12) = (12, 9) = (9, 3) = (3, 0) = 3 \ .$$

Para expresar a 3 como combinación lineal de 120 y de 33 se despeja el último resto no nulo, en este caso el tres y en esta expresión se van sustituyendo los restos anteriores como se muestra a continuación.

$$\begin{aligned} 3 &= 12 - 9 \cdot 1 \\ &= 12 - (33 - 12 \cdot 2) \cdot 1 = -33 + 12 \cdot 3 \\ &= -33 + (210 - 33 \cdot 6) \cdot 3 \\ &= 3(210) - 19(33) \end{aligned}$$

•

El procedimiento usado en la primera parte del ejercicio anterior para hallar el máximo común divisor se puede expresar por medio del siguiente algoritmo. El mismo es recursivo y se basa en el Teorema 1.12. Nota: El resto r, de dividir a a entre b, se denota por $a \bmod b$, y está garantizado por el teorema 1.9

{ Retorna el máximo común divisor positivo de a y b}
mcd(a, b);
si $b = 0$ **retorna** a

de lo contrario retorna $\text{mcd}(b, a \bmod b)$;

El teorema 1.11 establece que el máximo común divisor de dos enteros es el valor de la combinación lineal de dichos enteros que produce el menor entero positivo. A continuación deduciremos un algoritmo que extienda el anterior para obtener los coeficientes que permiten escribir al máximo común divisor positivo de a y b como combinación lineal de a y b. Al ser invocado con a y b debe retornar la terna (d, u, w) donde d es el máximo común divisor positivo de a y b, y u, w son los coeficientes de la combinación lineal. Si $b = 0$, $(a, b) = a$ y por lo tanto $a = 1 \cdot a + 0 \cdot b$, y en consecuencia el algoritmo que buscamos debe devolver la terna $(a, 1, 0)$. De lo contrario se invoca de nuevo al algoritmo con $b, a \bmod b$. Si esta invocación retorna la terna (d', u', w'), dado que $d = d'$ y puesto que

$$\begin{aligned} d' &= bu' + (a \bmod b)w' \\ &= bu' + (a - b\lfloor a/b \rfloor)w' \\ &= aw' + b(u' - \lfloor a/b \rfloor w') \end{aligned} \tag{1.8}$$

Aquí, $\lfloor a/b \rfloor$ representa la división entera (el cociente entero de dividir a entre b, el q del algoritmo de la división) Luego, en este caso el algoritmo debe retornar a w' por u y a $(u' - \lfloor a/b \rfloor w')$ por w. A continuación se muestra el código.

{ Retorna (d, u, w), donde $d = (a, b) = ua + wb$}
mcdExtendido(a, b) :;
si $b = 0$ **retorna** $(a, 1, 0)$;
$(d', u', w') \leftarrow$ mcdExtendido$(b, a \bmod b)$;
$(d, u, w) \leftarrow (d', w', u' - \lfloor a/b \rfloor w')$;
retorna (d, u, w);

Ejercicio 1.4 *Halle el máximo común divisor positivo de los enteros* 2520 *y* 242 *y expréselo como combinación lineal de dichos enteros.*

Si un entero m es múltiplo de a y de b se dice que m es múltiplo común de a y b, por ejemplo, 12 y 24 son múltiplos comunes de 4 y de 6. De manera similar como se define la función máximo común divisor se define la función mínimo común múltiplo.

Definición 1.7 (Mínimo Común Múltiplo) *Dados dos enteros positivos a y b decimos que m es el mínimo común múltiplo de a, b y lo representamos por* $\text{mcm}\,(a, b)$ *si y sólo si $a|m$, $b|m$ y $(\forall z \in Z^+)(a|z \wedge b|z \Rightarrow m|z)$. Esto es,*

$$\text{mcm}\,(a, b) = m \Longleftrightarrow a|m \wedge b|m \wedge (\forall z \in Z^+)(a|z \wedge b|z \Rightarrow m|z)$$

Nótese que $\langle Z^+ \cup \{0\}, | \ \rangle$ es un reticulado acotado con mínimo $\widehat{0} = 1$ y máximo $\widehat{1} = 0$ y que el máximo común divisor positivo y el mínimo común múltiplo de a y b son justamente el $\text{ínf}\,(a, b)$ y el $\sup(a, b)$ en dicho reticulado. Alerta: Las palabras máximo y mínimo en las definiciones de máximo común

divisor y de mínimo común múltiplo se refieren al máximo y al mínimo de la relación "divide a"; no deben confundirse con máximo y mínimo de la relación *menor o igual*. Sin embargo, no se crea conflicto con la idea de máximo o mínimo de la relación $\leq$ porque si $a|b$, se tiene que $a \leq b$.

1.6. Números Primos

Los números primos fueron extensamente estudiados por los matemáticos griegos. Matemáticos de la escuela de Pythagoras (500 a 300 a.c) se interesaron en sus propiedades. Euclides en el Libro IX de los Elementos probó que hay infinitos primos—dicha prueba es uno de los primeros ejemplos de una prueba por absurdo—. También probó el Teorema fundamental de la aritmética que establece que todo número entero se puede descomponer como producto de primos en forma única. Cerca del año 200 a.c. Eratosthenes propuso un algoritmo para hallar primos llamado la criba de Eratosthenes. El hombre parece haberse olvidado de los números primos por cerca de 18 siglos. Los siguientes resultados importantes fueron obtenidos por Fermat en el siglo XVII.

Definición 1.8 (Primo) *Un número entero (positivo)*[1] *p es primo si es distinto de 0 y de ± 1 y es divisible solamente por ± 1 y por $\pm p$.*

Una definición equivalente y más compacta es la siguiente:

Definición 1.9 (Primo) *Un número entero p es primo si y sólo si es positivo y tiene exactamente dos divisores positivo.*

Si un número entero positivo mayor que 1 no es primo, se llama compuesto. Observe que el 1 el 0 y los enteros negativos no son ni primos ni compuestos. A continuación se muestra la lista de los primeros 50 números primos: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107, 109, 113, 127, 131, 137, 139, 149, 151, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, y @229.

Si a divide a un numero compuesto, digamos bc, no tiene por qué dividir a sus factores por separado. Pero si a es primo debe dividir a algunos de sus factores. Esto se establece en el siguiente teorema que es una consecuencia del Teorema 1.11 que asegura la existencia de enteros u y w tales que $(a, b) = ua + wb$.

Teorema 1.13 *Si p es primo y $p|ab$, entonces $p|a$ o $p|b$.*

Prueba: Supongamos que $p \not| a$, como p es primo sus únicos divisores son ± 1 y $\pm p$, como $p \not| a$ los únicos divisores comunes de a y p son ± 1. Luego, 1 es máximo común divisor positivo de p y a, esto es, $(a, p) = 1$, y por consiguiente existen u y w tales que $1 = ua + wp$. Si multiplicamos por b se tiene que $b = uab + wpb$, y además como $p|ab$ se tiene que existe $z \in Z$ tal que $ab = zp$, y por lo tanto

[1] Seguiremos a la mayoría de los matemáticos al considerar la primalidad una propiedad exclusiva de los enteros positivos

$b = uzp + wpb = p(uz + wb)$ y en consecuencia $p|b$. □

Ejercicio 1.5 *Demuestre que si p, q_1 y q_2 son primos positivos y $p|q_1q_2$, entonces $p = q_1$ o $p = q_2$.*

Definición 1.10 (Primos Relativos) *Se dice que dos números enteros a y b son primos entre sí, o que son primos relativos si y sólo si sus únicos divisores comunes son ± 1, esto es, si y sólo si $(a, b) = 1$.*

El siguiente teorema es una generalización del anterior.

Teorema 1.14 *Si $c|ab$ y $(a, c) = 1$, entonces $c|b$.*

Teorema 1.15 *Si $(a, b) = 1$, $a|x$ y $b|x$, entonces $ab|x$.*

Ejercicio 1.6 *Pruebe que para todo $a \in Z$, a y $a + 1$ son primos entre sí.*

1.6.1. Teorema Fundamental de la Aritmética

En esta sección se estudiará el teorema fundamental de la aritmética. Dicho teorema afirma que todo entero no primo se puede descomponer en el producto de factores primos, en forma única salvo por el orden de aparición de los factores. La prueba de este teorema se basa en el segundo principio de inducción matemática de los enteros positivos.

Teorema 1.16 *Todo entero no nulo se puede expresar como el producto de (± 1) por factores primos positivos. Dicha expresión es única, salvo por el orden de los factores.*

Prueba: Consideraremos sólo el caso en que n sea un entero positivo. (¿Por qué?) y lo probaremos por inducción generalizada sobre n. Primero probaremos la existencia de una tal descomposición y luego la unicidad de la misma.
Paso base: si n es 1 se cumple porque 1 es 1 por un producto vacío de factores primos. Paso inductivo: Asumimos que todo entero menor que n se puede descomponer como producto de factores primos y probaremos que n se puede descomponer como producto de factores primos. Por casos: si n es primo, entonces es el producto de un solo primo y si n no es primo, entonces tiene algún divisor positivo mayor que 1 y distinto de n; por consiguiente $n = n_1 \cdot n_2$ con $n_1, n_2 > 1$ Luego, como $1 < n_1, n_2 < n$ se pueden, por hipótesis inductiva, descomponer como producto de primos, digamos: $n_1 = p_1p_2 \cdots p_r$ y $n_2 = q_1q_2 \cdots q_s$, se tiene que $n = p_1p_2 \cdots p_rq_1q_2 \cdots q_s$ que es una descomposición en primos de n. Probemos ahora la unicidad también por inducción sobre n. De nuevo, para n igual a 1 se tiene que se cumple porque el producto de primos es vacío. Si asumimos que la descomposición es única para todo entero positivo menor que n debemos probar que la descomposición es única para n. Su pongamos que $n = p_1p_2 \cdots p_r$ y $n = q_1q_2 \cdots q_s$ son dos descomposiciones en primos de n. Como p_1 divide a n se tiene que p_1 divide a algún q_i, pero además como p_1 es primo

se tiene que $p_1 = q_i$ quedando que $p_2 \cdots p_r = q_1 \cdots q_{i-1} q_{i+1} \cdots q_s$ y como este número es menor que n se tiene que cada p_i debe corresponder a algún q_j y que $r = s$. □

Una consecuencia del teorema anterior es que el Teorema demostrado por Euclides que afirma la existencia de infinitos primos. Ya comentamos que es uno de los ejemplos más antiguos de una prueba por absurdo.

Teorema 1.17 (Euclides) *Existen infinitos números primos positivos.*

Prueba: Supongamos, por absurdo, que hay un número finito de primos y enumerémoslos como sigue: $p_1, p_2, \ldots, p_k$. Consideremos al entero positivo $p_1 p_2 \cdots p_k + 1$. Claramente es mayor que cada uno de los p_i, por lo tanto no es primo—no está en nuestra lista de primos.—Como también es mayor que 1, debe ser compuesto y contener al menos un primo en su descomposición—Teorema Fundamental de la Aritmetica—, esto es, alguno de nuestros primos debe dividirlo. Pero si alguno de nuestros primos, digamos p_i, lo divide, entonces como también divide a $p_1 p_2 \ldots p_k$, se tiene que divide a 1, lo cual es una contradicción. Luego el conjunto de los primos no es finito. □

Nota: Agrupando los primos iguales de la descomposición en primos del entero positivo n se tiene que $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. Esto nos permite hallar una fórmula para contar los divisores del número n porque un divisor de n debe ser forzosamente de la forma $d = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$ con $0 \leq \beta_i \leq \alpha_i$. Justifique esta afirmación.

El teorema anterior proporciona además la base para determinar el mínimo común múltiplo de dos enteros. Se deja como ejercicio.

Ejercicio 1.7 *Demuestre que para todo par de enteros positivos a y b se cumple que $ab = \operatorname{mcd}(a,b) \operatorname{mcm}(a,b)$.*

Ejercicio 1.8 *Halle una fórmula que permita calcular el número de divisores positivos de un número entero n en base a su descomposición en primos.*

Ejercicio 1.9 *Halle una fórmula que permita calcular la suma de los divisores positivos del número entero n.*

1.7. Ejercicios

1. Demuestre que si $a|b \wedge a|c$, entonces $a|(b \pm c)$.

2. Demuestre que a y b son enteros positivos tales que $a|b \wedge b|a$, entonces $a = b$.

3. Use el Algoritmo de Euclides para calcular el máximo común divisor
   a) $(24, 18)$ b) $(7, 35)$ c) $(120, 270)$

4. Exprese el máximo común divisor de los pares de números siguientes como combinación lineal de dichos números. Esto es, escriba en cada caso $(x, y) = sx + ty$, con s y t enteros.
   a) $(36, 9)$ b) $(11, 35)$ c) $(48, 18)$

5. Demostrar que si $a > 0 \wedge x \neq 0$, entonces $(ax, ay) = a(x, y)$

6. Demuestre que si $a|bc \wedge (a, b) = 1$, entonces $a|c$

7. Demuestre que si d es divisor común de b y c, es divisor de cualquier combinación lineal entera de b y c, esto es, que $d|xb+yc$ para todo $x, y \in Z$.

8. Pruebe que para toda terna de enteros a, b, c existen enteros r, s, t tales que el máximo común divisor de a, b, c es igual a $ra + sb + tc$.

9. Demostrar que si $(a, b) = 1 \wedge (a, c) = 1$, entonces $(a, bc) = 1$

10. Probar que todo conjunto de enteros cerrado para la sustracción también es cerrado para la adición.

11. Dé ejemplos de conjuntos de enteros cerrados para la adición pero no para la sustracción.

12. Demuestre que si a es un entero y p es un entero positivo tal que $p|a$, entonces $(a, p) = p$.

13. Dados dos enteros a, b, demuestre que si p es primo y $p|ab$, entonces $p|a \vee p|b$.

14. Pruebe que si $d = (a, b)$ y $a|c \wedge b|c$, entonces $d|c$.

15. Demostrar que si b es un entero positivo **compuesto**, tiene un divisor primo positivo $d \leq \sqrt{b}$.

16. Demuestre que si $a|b$, entonces $|a| \leq |b|$ o $b = 0$, y úselo para demostrar que si $a|b$ y $b|a$, entonces $a = \pm b$.

17. Use el principio de buena ordenación para probar que no existe ningún entero positivo entre los enteros cero y uno.

18. Demuestre que si $a_i \in Z^+$ con $1 \leq i \leq n$ y p es un número primo tal que $p|a_1 a_2 \cdots a_n$, entonces existe algún a_j, con $1 \leq j \leq n$ tal que $p|a_j$.

19. Use el algoritmo de Euclides para calcular el máximo común divisor de las siguientes parejas de números y expréselo como combinación lineal de dichos números. ($(a,b) = wa + zb$) a) 24, 30; b) 240, 125; c) 32, 18.

20. Demuestre que si a y b son enteros positivos y $a > b$, entonces $(a,b) = (b, a-b)$.

21. Dados dos enteros positivos a y b, demuestre que si $p_1, p_2, \ldots, p_k$ es una lista sin repeticiones de todos los primos que aparecen en la descomposición en primos de a y de b, y $a = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ y $b = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}$ con $\alpha_i \geq 0$ y $\beta_i \geq 0$ para todo i, entonces el máximo común divisor positivo entre a y b es $p_1^{\text{mín}(\alpha_1,\beta_1)} \cdots p_k^{\text{mín}(\alpha_k,\beta_k)}$ y su mínimo común múltiplo es $p_1^{\text{máx}(\alpha_1,\beta_1)} \cdots p_k^{\text{máx}(\alpha_k,\beta_k)}$.

22. Usando el resultado del ejercicio anterior y el hecho de que $(a,a) = a$ escriba un algoritmo iterativo que reciba como entrada dos enteros positivos a, b y dé como salida en la variable x el máximo común divisor positivo de a, b. Use una variable auxiliar y para almacenar el valor actual de b. No modifique los valores de entrada. Indique la condición de parada de la y teración.

23. Demuestre que para todo par de números enteros positivos a, b se cumple que $ab = \text{mcd}\,(a,b) \cdot \text{mcm}\,(a,b)$.

24. Use el principio de buena ordenación para probar que $\sqrt{2}$ no es un número racional. Sug.: Considere el conjunto $S = \{x \in Z^+ : x\sqrt{2} \in Z^+\}$.

25. Decimos que un número entero positivo n es perfecto si la suma de sus divisores es $2n$, por ejemplo, 6 es perfecto porque $1 + 2 + 3 + 6 = 12$.
a) Verifique que 28 y 496 son perfectos.
b) Demuestre que si $m \in Z^+$ y $2^m - 1$ es primo, entonces $2^{m-1}(2^m - 1)$ es un entero perfecto. (Sug.: Tal vez necesite $\sum_{i=0}^{n} r^i = \frac{r^{n+1}-1}{r-1}$)

26. Demuestre que un número entero positivo n es un cuadrado perfecto si y sólo si tiene un número impar de divisores positivos.

27. Demuestre que si a, b son dos enteros positivos, el conjunto de números de la forma $sa + tb$, donde s, t son enteros positivos, incluye todos los múltiplos de (a,b) mayores que ab.

28. Cuantos divisores positivos tiene n si $n = p^\alpha$, p es primo y $\alpha \geq 0$

29. Si $A = \{a_1, a_2, a_3, a_4, a_5\}$ es un subconjunto de enteros positivos, demuestre que existe un subconjunto no vacío S de A tal que la suma de los elementos de S es múltiplo de 5.

30. Demuestre que si ab es un entero positivo cuadrado tal que $(a,b) = 1$, entonces a, b son ambos cuadrados. Demuestre que si $a|c$, $b|c$ y $(a,b) = 1$, entonces $ab|c$.

31. Demuestre que si n es un entero positivo, entonces n y $n+1$ son coprimos.

32. Demuestre que para todo $m, n \in Z$ existe $r \in Z$ tal que $m = n + r$.

33. Pruebe que para todo entero k no existe un entero entre k y $k + 1$.

34. Proponga un algoritmo eficiente para hallar el mínimo común multiplo entre dos enteros positivos a y b.