Apéndice A
Divisibilidad en $\mathbb{Z}$

Todo número compuesto es medido por algún número primo.
Todo número o bien es número primo o es medido por algún número primo.

Euclides, "Elementos", Libro VII

Cualquier número compuesto puede resolverse en factores primos de una manera única.

Gauss, "Disquisitiones Arithmeticae", §16

Este apéndice contiene un breve resumen de la teoría de números elemental que necesitamos en el curso, específicamente los resultados básicos relacionados con la divisibilidad de números enteros. Algunos otros temas, como la aritmética módulo n, hacen parte del texto principal. El lector interesado puede consultar, por ejemplo, el libro de texto [IR1990].

A.0 Subgrupos de $\mathbb{Z}$

Ya que nuestro curso está dedicado a la teoría de grupos, algunas demostraciones de abajo usan la noción de grupo abeliano. Solamente para facilitar la lectura y no dejar la impresión de que en nuestra exposición hay argumentos circulares, revisemos toda la teoría de grupos necesaria.

Recordemos que un **subgrupo** $A \subset \mathbb{Z}$ es un subconjunto de números enteros que satisface las siguientes condiciones:

1) $0 \in A$,

2) para cualesquiera $a, b \in A$ tenemos $a + b \in A$,

3) para cualquier $a \in A$ tenemos $-a \in A$.

A.0.1. Observación. *Si A y B son dos subgrupos de $\mathbb{Z}$, entonces su intersección $A \cap B$ es también un subgrupo.*

Para $a_1, \ldots, a_n \in \mathbb{Z}$ el **subgrupo generado** por $a_1, \ldots, a_n$ es el subconjunto $\langle a_1, \ldots, a_n \rangle \subseteq \mathbb{Z}$ que satisface una de las siguientes condiciones equivalentes.

1) $\langle a_1, \ldots, a_n \rangle$ es el mínimo subgrupo de $\mathbb{Z}$ que contiene todos los números $a_1, \ldots, a_n$,

2) $\langle a_1, \ldots, a_n \rangle$ es el conjunto de las combinaciones $\mathbb{Z}$-lineales de $a_1, \ldots, a_n$:

$$\langle a_1, \ldots, a_n \rangle = \Big\{ \sum_i n_i a_i \;\Big|\; n_i \in \mathbb{Z} \Big\}.$$

Nos van a interesar dos casos particulares: los subgrupos generados por un número $d \in \mathbb{Z}$:

$$\langle d \rangle = \{ md \mid m \in \mathbb{Z} \}$$

y subgrupos generados por dos números:

$$\langle a, b \rangle = \{ ma + nb \mid m, n \in \mathbb{Z} \}.$$

A.1 División con resto

A.1.1. Teorema (Euclides). *Sean $a, b \in \mathbb{Z}$ dos números enteros, con $b \neq 0$. Entonces, existen $q, r \in \mathbb{Z}$ tales que*

$$a = qb + r, \quad 0 \leq r < |b|.$$

Demostración. Para el conjunto

$$\{ a - xb \mid x \in \mathbb{Z} \}$$

sea

$$r = a - qb$$

su mínimo elemento tal que $r \geq 0$ (este existe, puesto que $b \neq 0$). Supongamos que $r \geq |b|$. Si $b > 0$, tenemos

$$0 \leq r - b = a - qb - b = a - (q+1)\, b < r.$$

De la misma manera, si $b < 0$, entonces

$$0 \leq r + b = a - qb + b = a - (q-1)\, b < r.$$

En ambos casos se produce un elemento $a - (q \pm 1)\, b$, lo que contradice nuestra elección de r. Podemos concluir que $r < |b|$. ■

El resultado que acabamos de describir se llama la **división con resto** de a por b. He aquí una de sus consecuencias importantes.

A.1.2. Proposición. *Todo subgrupo de $\mathbb{Z}$ es de la forma $\langle d \rangle$ para algún $d \in \mathbb{Z}$. En particular, para cualesquiera $a, b \in \mathbb{Z}$ se tiene*

1) $\langle a, b \rangle = \langle d \rangle$ para algún $d \in \mathbb{Z}$,

2) $\langle a \rangle \cap \langle b \rangle = \langle d \rangle$ para algún $d \in \mathbb{Z}$.

Demostración. Sea $A \subseteq \mathbb{Z}$ un subgrupo. Si $A = 0$, entonces $A = \langle 0 \rangle$ y enunciado es trivial. Luego, si $A \neq 0$, entonces A contiene números no nulos. Para cada $x \in A$ también $-x \in A$, así que A contiene números positivos. Sea entonces

$$d := \text{mín}\{ x \in A \mid x > 0 \}.$$

Está claro que $\langle d \rangle \subseteq A$. Para ver la otra inclusión, consideremos un elemento arbitrario $c \in A$. La división con resto por d nos da

$$c = qd + r, \quad 0 \leq r < d.$$

Luego, puesto que $c, d \in A$, tenemos también $r = c - qd \in A$. Por nuestra elección de d, podemos descartar el caso $0 < r < d$. Entonces, $r = 0$ y $c = qd \in \langle d \rangle$. ■

A.2 Divisibilidad y los números primos

A.2.1. Definición. Para dos números enteros $d, n \in \mathbb{Z}$ se dice que d **divide a** n y se escribe "$d \mid n$" si $n = mx$ para algún $m \in \mathbb{Z}$. En este caso también se dice que d es un **divisor** de n o que n es **divisible por** d. Cuando d no divide a n, se escribe "$d \nmid n$".

Notamos que en términos de subgrupos de $\mathbb{Z}$,

$$d \mid n \iff \langle n \rangle \subseteq \langle d \rangle.$$

El lector puede comprobar las siguientes propiedades de la relación de divisibilidad.

0) $a \mid 0$ para todo[*] $a \in \mathbb{Z}$. Esto caracteriza a 0 de modo único. Tenemos $0 \mid a$ solamente para $a = 0$.

1) $a \mid a$ y $\pm 1 \mid a$ para todo $a \in \mathbb{Z}$.

2) Si $a \mid b$ y $b \mid a$, entonces $a = \pm b$.

3) Si $a \mid b$ y $b \mid c$, entonces $a \mid c$.

4) Si $a \mid b$, entonces $a \mid bc$ para cualquier $c \in \mathbb{Z}$.

5) Si $a \mid b$ y $a \mid c$, entonces $a \mid (b + c)$.

A.2.2. Definición. Se dice que un número entero positivo $p > 0$ es **primo** si $p \neq 1$ y los únicos divisores de p son ± 1 y $\pm p$.

En otras palabras, p es primo si y solamente si para $m, n > 0$, si tenemos $p = mn$, entonces o bien $m = p$, $n = 1$ o bien $m = 1$, $n = p$. Los primeros números primos son

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, ...

Por ejemplo, $57 = 3 \cdot 19$ no es primo.

A.2.3. Proposición. *Todo entero no nulo puede ser expresado como*

$$n = \pm p_1^{k_1} \, p_2^{k_2} \cdots p_\ell^{k_\ell}$$

donde p_i son primos diferentes.

Demostración. Sin pérdida de generalidad, podemos considerar el caso de $n > 0$. Sería suficiente ver que n es un producto de primos y juntando múltiplos iguales, se obtiene la expresión de arriba.

Para $n = 1$ tenemos $n = p^0$ para cualquier primo p. Luego, se puede proceder por inducción. Supongamos que el resultado se cumple para todos los números positivos $< n$. Si n es primo, no hay que demostrar nada. Si n no es primo, entonces $n = ab$ donde $a < n$ y $b < n$. Por la hipótesis de inducción, a y b son productos de números primos, y por lo tanto n lo es. ■

En este caso la palabra "primo" es un sinónimo de "primero" y refiere precisamente al hecho de que todo número entero sea un producto de primos. No se trata de ninguna relación de parentesco entre los números.

A.2.4. Teorema (Euclides). *Hay un número infinito de primos.*

[*] Algunas fuentes insisten que $0 \nmid 0$, pero la relación $0 \mid 0$ no tiene nada de malo. De hecho $0 \in \langle d \rangle$ para cualquier $d \in \mathbb{Z}$, en particular para $d = 0$.

Demostración. Consideremos los primeros n números primos

$$p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ p_4 = 7,\ p_5 = 11,\ \ldots,\ p_n.$$

Luego, el número

$$N := p_1 p_2 \cdots p_n + 1$$

no es divisible por ningún primo entre $p_1, \ldots, p_n$. Sin embargo, N tiene que ser un producto de primos, así que es necesariamente divisible por algún primo p tal que $p_n < p \leq N$. ■

A.3 El máximo común divisor

A.3.1. Definición. Para dos números enteros $a, b \in \mathbb{Z}$ su **máximo común divisor** (**mcd**) es un número $d := \text{mcd}(a, b)$ caracterizado por las siguientes propiedades:

1) $d \mid a$ y $d \mid b$,

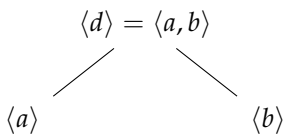
2) si d' es otro número tal que $d' \mid a$ y $d' \mid b$, entonces $d' \mid d$.

Las condiciones de arriba pueden ser escritas como

1) $\langle a \rangle \subseteq \langle d \rangle$ y $\langle b \rangle \subseteq \langle d \rangle$,

2) si $\langle a \rangle \subseteq \langle d' \rangle$ y $\langle b \rangle \subseteq \langle d' \rangle$, entonces $\langle d \rangle \subseteq \langle d' \rangle$.

El subgrupo mínimo de $\mathbb{Z}$ que contiene a $\langle a \rangle$ y $\langle b \rangle$ es $\langle a, b \rangle$. Gracias a A.1.2, sabemos que $\langle a, b \rangle = \langle d \rangle$ para algún $d \in \mathbb{Z}$.



Esto nos lleva al siguiente resultado.

A.3.2. Proposición. *El mcd siempre existe: tenemos*

$$\langle a, b \rangle = \langle d \rangle \quad \textit{donde } d = \text{mcd}(a, b).$$

En particular, se cumple

$$ax + by = \text{mcd}(a, b) \quad \textit{para algunos } x, y \in \mathbb{Z}$$

y $\text{mcd}(a, b)$ *es el mínimo número posible que puede ser representado como una combinación* $\mathbb{Z}$*-lineal de* a *y* b*.*

La última expresión se conoce como la **identidad de Bézout**. Aquí los coeficientes x e y no son únicos. Por ejemplo,

$$2 \cdot (-1) + 3 \cdot 1 = 2 \cdot (-4) + 3 \cdot 3 = 2 \cdot 2 + 3 \cdot (-1) = \cdots = 1.$$

He aquí algunas observaciones respecto a $\text{mcd}(a, b)$.

1) La definición de $d := \text{mcd}(a, b)$ caracteriza a d *salvo signo*. De hecho, si d y d' satisfacen las condiciones de $\text{mcd}(a, b)$, entonces $d \mid d'$ y $d' \mid d$ (o la condición equivalente $\langle d \rangle = \langle d' \rangle$) implica que $d' = \pm d$. Normalmente se escoge $d > 0$, pero estrictamente hablando, todas las identidades con $\text{mcd}(a, b)$ pueden ser interpretadas salvo signo.

2) La definición de $\mathrm{mcd}(a,b)$ es visiblemente simétrica en a y b, así que

$$\mathrm{mcd}(a,b) = \mathrm{mcd}(b,a).$$

3) Para todo $a \in \mathbb{Z}$ se tiene

$$\mathrm{mcd}(a,0) = a.$$

En particular*,

$$\mathrm{mcd}(0,0) = 0.$$

Esto nada más significa que cualquier número divide a 0, o de manera equivalente, que $\langle 0\rangle \subseteq \langle a\rangle$ para todo $a \in \mathbb{Z}$, y también para $a = 0$.

A.3.3. Definición. Si $\mathrm{mcd}(a,b) = 1$, se dice que a y b son **coprimos**.

Si a y b son coprimos, entonces $\langle a,b\rangle = \langle 1\rangle = \mathbb{Z}$, y en particular tenemos

$$ax + by = 1 \quad \text{para algunos } x, y \in \mathbb{Z}.$$

A.3.4. Observación. *Si $a \mid bc$ donde a y b son coprimos, entonces $a \mid c$.*

Demostración. Tenemos

$$ax + by = 1$$

para algunos $x, y \in \mathbb{Z}$. Luego,

$$axc + byc = c,$$

y la expresión a la izquierda es divisible por a. ■

A.3.5. Corolario. *Si p es primo y $p \mid bc$, entonces $p \mid b$ o $p \mid c$.*

Muy a menudo se usa el contrapuesto: si $p \nmid b$ y $p \nmid c$, entonces $p \nmid bc$.

Demostración. Ya que los únicos divisores de p son ± 1 y $\pm p$, tenemos dos casos posibles. En el primer caso, $\mathrm{mcd}(p,b) = 1$ y luego $p \mid c$ por el resultado precedente. En el segundo caso, $\mathrm{mcd}(p,b) = p$, lo que significa que $p \mid b$. ■

A.4 El mínimo común múltiplo

A.4.1. Definición. Para dos números enteros $a, b \in \mathbb{Z}$ su **mínimo común múltiplo (mcm)** es un número $m := \mathrm{mcm}(a,b)$ caracterizado por las siguientes propiedades:

1) $a \mid m$ y $b \mid m$,

2) si m' es otro número tal que $a \mid m'$ y $b \mid m'$, entonces $m \mid m'$.

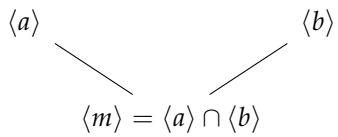
Las condiciones de arriba pueden ser escritas como

1) $\langle m\rangle \subseteq \langle a\rangle$ y $\langle m\rangle \subseteq \langle b\rangle$,

2) si m' es otro número tal que $\langle m'\rangle \subseteq \langle a\rangle$ y $\langle m'\rangle \subseteq \langle b\rangle$, entonces $\langle m'\rangle \subseteq \langle m\rangle$.

*Algunas fuentes insisten que $\mathrm{mcd}(0,0)$ no está definido, pero como vemos, es lógico poner $\mathrm{mcd}(0,0) = 0$.

El subgrupo máximo de $\mathbb{Z}$ que contiene a $\langle a\rangle$ y $\langle b\rangle$ es su intersección $\langle a\rangle \cap \langle b\rangle$. Gracias a A.1.2 sabemos que es también de la forma $\langle m\rangle$ para algún $m \in \mathbb{Z}$.



A.4.2. Proposición. *El mcm siempre existe: tenemos*

$$\langle a\rangle \cap \langle b\rangle = \langle m\rangle \quad \textit{donde } m = \operatorname{mcm}(a,b).$$

Tenemos las siguientes propiedades.

1) La definición caracteriza a $\operatorname{mcm}(a,b)$ de modo único salvo signo.

2) Para cualesquiera $a, b \in \mathbb{Z}$ se tiene

$$\operatorname{mcm}(a,b) = \operatorname{mcm}(b,a).$$

3) Para todo a se cumple

$$\operatorname{mcm}(a,0) = a.$$

En particular,

$$\operatorname{mcm}(0,0) = 0.$$

(De hecho, $0 \mid m$ implica que $m = 0$.)

A.4.3. Proposición. *Para cualesquiera $a, b \in \mathbb{Z}$ tenemos*

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

En particular,

$$\operatorname{mcm}(a,b) = ab \textit{ si y solamente si } a \textit{ y } b \textit{ son coprimos.}$$

Demostración. El caso de $a = b = 0$ es trivial y podemos descartarlo. Sea $d := \operatorname{mcd}(a,b)$ y $m := ab/d$. Vamos a ver que $m = \operatorname{mcm}(a,b)$.

Primero, puesto que $d \mid a$ y $d \mid b$, podemos escribir

$$a = da', \quad b = db'.$$

Luego,

$$m = da'b' = ab' = ba',$$

así que $a \mid m$ y $b \mid m$.

Ahora notemos que

$$d = \operatorname{mcd}(a,b) = \operatorname{mcd}(da', db') = d \cdot \operatorname{mcd}(a', b'),$$

así que

$$\operatorname{mcd}(a', b') = 1$$

y los números a' y b' son coprimos.

Sea m' otro número tal que $a \mid m'$ y $b \mid m'$. Queremos ver que $m \mid m'$. Escribamos

$$m' = ax = by.$$

Luego,

$$m'b' = ab'x = mx, \quad m'a' = ba'y = my,$$

lo que nos da $m \mid m'b'$ y $m \mid m'a'$ y por lo tanto

$$m \mid \mathrm{mcd}(m'b', m'a') = m' \cdot \mathrm{mcd}(a', b') = m'.$$

■

Note que la última proposición nos dice básicamente que la existencia de $\mathrm{mcd}(a, b)$ es equivalente a la existencia de $\mathrm{mcm}(a, b)$.

También se pueden definir mcd y mcm de n números. El lector puede generalizar de manera evidente las definiciones A.3.1 y A.4.1 y ver que estas generalizaciones son equivalentes a

1) $\langle a_1, \ldots, a_n \rangle = \langle d \rangle$ para $d = \mathrm{mcd}(a_1, \ldots, a_n)$,

2) $\langle a_1 \rangle \cap \cdots \cap \langle a_n \rangle = \langle m \rangle$ para $m = \mathrm{mcm}(a_1, \ldots, a_n)$.

Además, se puede ver que las operaciones $\mathrm{mcd}(-,-)$ y $\mathrm{mcm}(-,-)$ son asociativas y por lo tanto la definición generalizada se reduce al caso binario:

1) $\mathrm{mcd}(\mathrm{mcd}(a, b), c) = \mathrm{mcd}(a, \mathrm{mcd}(b, c)) = \mathrm{mcd}(a, b, c)$,

2) $\mathrm{mcm}(\mathrm{mcm}(a, b), c) = \mathrm{mcm}(a, \mathrm{mcm}(b, c)) = \mathrm{mcm}(a, b, c)$,

A.5 El teorema fundamental de la aritmética

A.5.1. Definición. Sea p un número primo fijo. Para un número entero no nulo n su **valuación p-ádica** es el número natural máximo k tal que p^k divide a n:

$$v_p(n) := \max\{k \mid p^k \mid n\}.$$

(Para $n = 0$ normalmente se pone $v_p(0) = +\infty$, pero no vamos a necesitar esta convención.)

Notamos que $v_p(n) = 0$ si y solamente si $p \nmid n$. La valuación p-ádica se caracteriza por

$$n = p^{v_p(n)}\, n',$$

donde $p \nmid n'$ (véase A.3.5).

A.5.2. Lema. *Para cualesquiera $m, n \in \mathbb{Z}$ se cumple*

$$v_p(mn) = v_p(m) + v_p(n).$$

Demostración. Tenemos

$$m = p^{v_p(m)}\, m', \quad n = p^{v_p(n)}\, n',$$

donde $p \nmid m'$ y $p \nmid n'$. Luego,

$$mn = p^{v_p(m)+v_p(n)}\, m'n',$$

donde $p \nmid (m'n')$, así que $v_p(mn) = v_p(m) + v_p(n)$. ■

A.5.3. Teorema. *Todo número entero entero no nulo puede ser representado de modo único como*

$$n = \pm p_1^{k_1}\, p_2^{k_2} \cdots p_\ell^{k_\ell}$$

donde p_i son algunos primos diferentes. A saber, tenemos $k_i = v_{p_i}(n)$.

(La unicidad se entiende salvo permutaciones de los factores $p_i^{k_i}$.)

Demostración. Ya hemos notado en A.2.3 que todo entero no nulo es un producto de primos; la parte interesante es la unicidad. Dada una expresión

$$n = \pm p_1^{k_1} p_2^{k_2} \cdots p_\ell^{k_\ell},$$

para todo primo p podemos calcular la valuación p-ádica correspondiente:

$$v_p(n) = v_p(p_1^{k_1}) + v_p(p_2^{k_2}) + \cdots + v_p(p_\ell^{k_\ell}).$$

Aquí

$$v_p(p_i^{k_i}) = \begin{cases} k_i, & p = p_i, \\ 0, & p \neq p_i. \end{cases}$$

Entonces, $k_i = v_{p_i}(n)$. ■

Entonces, podemos escribir

$$n = \pm \prod_{p \text{ primo}} p^{v_p(n)},$$

donde el producto es sobre todos los números primos, pero $v_p(n) \neq 0$ solamente para un número finito de p.

El último resultado se conoce como el **teorema fundamental de la aritmética**. Su primera demostración completa fue publicada por Gauss en el tratado "Disquisitiones Arithmeticae".

Notamos que

$$\operatorname{mcd}(m,n) = \prod_{p \text{ primo}} p^{\min\{v_p(m), v_p(n)\}}$$

y

$$\operatorname{mcm}(m,n) = \prod_{p \text{ primo}} p^{\max\{v_p(m), v_p(n)\}}.$$

Estas fórmulas no ayudan mucho para grandes valores de m y n. En práctica se usa el **algoritmo de Euclides** basado en la división con resto repetida (es algo parecido a nuestra demostración de A.1.2).

A.6 Generalizaciones

Las definiciones A.3.1 y A.4.1 de mcd y mcm tienen sentido en cualquier dominio de integridad R. En este caso $\operatorname{mcm}(a,b)$ y $\operatorname{mcd}(a,b)$ están definidos salvo un múltiplo $u \in R^\times$. Para $R = \mathbb{Z}$ tenemos $\mathbb{Z}^\times = \{\pm 1\}$. Sin embargo, la existencia de $\operatorname{mcm}(a,b)$ y $\operatorname{mcd}(a,b)$ no está garantizada en general.

Un dominio de integridad donde se puede definir un análogo de la división con resto se llama un **dominio euclidiano**; en este caso mcd y mcm siempre existen gracias a los mismos argumentos que vimos arriba (solo hay que reemplazar los subgrupos $A \subseteq \mathbb{Z}$ por **ideales** $I \subseteq R$). Un ejemplo típico de dominios euclidianos, excepto $\mathbb{Z}$, es el anillo de polinomios $k[X]$ sobre un cuerpo k: para $f, g \in k[X]$, $g \neq 0$ existen $q, r \in k[X]$ tales que $f = qg + r$ donde $-\infty \leq \deg r < \deg g$.

Un dominio de integridad donde se cumple la factorización única (un análogo del teorema fundamental de la aritmética) se llama un **dominio factorización única**. Un típico ejemplo es el anillo de polinomios $k[X_1, \ldots, X_n]$ en n variables sobre un cuerpo k. Todos los dominios euclidianos son dominios de factorización única.

Todo esto se estudiará en la continuación de nuestro curso.

Bibliografía

[IR1990] Kenneth Ireland and Michael Rosen, *A classical introduction to modern number theory*, second ed., Graduate Texts in Mathematics, vol. 84, Springer-Verlag, New York, 1990. MR1070716
https://doi.org/10.1007/978-1-4757-2103-4