Lección nº A Junio, 2021

Apéndice A

$\mathbb{Z}$

En este apéndice estudiaremos las propiedades más importantes de los números enteros, tales como las nociones de divisibilidad, congruencias y ecuaciones diofánticas.

A.1. Divisibilidad

Definición. Sean $a, b \in \mathbb{Z}$. Diremos que a *divide* a b, y lo denotaremos por $a \mid b$ si existe un número entero $k \neq 0$ tal que $b = ka$. También diremos que a es un *divisor* de b o que b es un múltiplo de a. Si a no divide a b escribiremos $a \nmid b$.

Observaciones. (1) Si $a \in \mathbb{Z}$, entonces $1 \mid a$.

(2) Si $a \in \mathbb{Z}$, entonces $a \mid 0$.

(3) La relación de divisibilidad es un *preorden*, es decir, es una relación reflexiva y transitiva: Es claro que $a \mid a$ para todo $a \in \mathbb{Z}$. Si $a, b, c \in \mathbb{Z}$ son tales que $a \mid b$ y $b \mid c$, entonces existen números enteros $k' \neq 0$ y $k'' \neq 0$ tales que $b = k'a$ y $c = k''b$. Si $k = k'k''$, entonces $k \neq 0$ es un número entero y

$$c = k''b = k''(k'a) = ka,$$

de donde $a \mid c$.

(4) Si $a, b \in \mathbb{Z}$ y $|a| < |b|$, entonces $b \nmid a$. En efecto, supongamos que $b \mid a$, entonces podemos escribir $a = bk$ para cierto $k \in \mathbb{Z}$ con $k \neq 0$, de donde $|a| = |b||k| \geq |b|$, lo que contradice que $|a| < |b|$.

(5) Si $a, b \in \mathbb{Z}$, entonces $a \mid b$ y $b \mid a$ si y sólo si $|a| = |b|$.

(6) Si $0 \mid a$ entonces $a = 0$.

(7) Si $a \mid b$ y $a \mid c$, entonces $a \mid bx + cy$ para todo $x, y \in \mathbb{Z}$.

Ejercicio A.1. Demuestre (5), (6) y (7) en las observaciones anteriores.

Teorema A.2 (Algoritmo de división)**.** *Sean $a, b \in \mathbb{Z}$ con $b \neq 0$. Entonces existen únicos $q, r \in \mathbb{Z}$ tales que*

$$a = bq + r \quad y \quad 0 \leq r < |b|.$$

Demostración. Empecemos probando la unicidad: Supongamos que $a = bq + r$ y $a = bq' + r'$ con $0 \leq r, r' < |b|$. Asumamos que $r < r'$. Restando estas dos igualdades obtenemos

$$b(q - q') = r' - r,$$

de donde $b \mid r' - r$. Pero $0 < r' - r \leq r < b$, de modo que $b \nmid r' - r$ por la observación (4) arriba. Esta contradición se produce por suponer que $r < r'$. De manera análoga, la desigualdad $r' < r$ tampoco es posible, de donde $r = r'$. Con esto, tenemos que $bq = bq'$ y como $b \neq 0$, se tiene que $q = q'$.

A continuación, probemos la existencia: Primero asumiremos que $b > 0$. Sea

$$A = \{a - nb \,|\, a - nb \geq 0 \text{ y } n \in \mathbb{Z}\}.$$

Tenemos que $A \subseteq \mathbb{N}$ y además $A \neq \emptyset$. En efecto, si $n = -a^2$, entonces

$$a - nb = a + a^2 b \geq a + a^2 \geq 0,$$

y por ende $a - nb \in A$. Por el *principio de buen ordenamiento* A tiene un elemento mínimo r. Entonces $r \geq 0$ y $r = a - qb$ para cierto $q \in \mathbb{Z}$, de donde

$$a = bq + r \quad \text{y} \quad 0 \leq r.$$

Queda probar que $r < b$ Supongamos que $r \geq b$ y escribamos $r = b + r'$ con $r' \geq 0$, entonces

$$r' = r - b = a - bq - b = a - (q + 1)b \in A$$

y $0 \leq r' < r$, lo que contradice la minimalidad de r. Así $r < b$.

Queda probar el caso cuando $b < 0$. Notemos que en este caso $-b > 0$ y por lo recientemente probado, existen enteros q' y r tales que

$$a = -bq' + r \quad \text{y} \quad 0 \leq r < | - b|.$$

Tomamos $q = -q'$ y de este modo se tiene

$$a = bq + r \quad \text{y} \quad 0 \leq r < |b|.$$

Esto completa la demostración. □

Definición. Un número entero $p > 0$ se dice *primo* si $p \neq 1$ y si $a \mid p$, con $a > 0$, implica que $a = 1$ o $a = p$. Si $p < 0$, p se dice *primo* si $-p$ es primo. Un número entero que no es primo se dice un *número compuesto*.

Dos números enteros a, b se dicen *coprimos* o *primos relativos* si para todo $n \in \mathbb{Z}$ tal que $n > 0$, $n \mid a$ y $n \mid b$ se tiene que $n = 1$. Dicho de otro modo, si el único divisor común positivo de a y b es 1.

Proposición A.3. *Sean $a, b \in \mathbb{Z}$ no ambos iguales a 0. Existe un único número entero $d > 0$ con la siguiente propiedad: $d \mid a$, $d \mid b$ y si $c \mid a$ y $c \mid b$, entonces $c \mid d$.*

Demostración. Probaremos primero la unicidad de d: Supongamos que existen $d, d' > 0$ que son divisores de a y b y que son maximales respecto a la divisibilidad, es decir, que si $c \mid a$ y $c \mid b$, entonces $c \mid d$ y $c \mid d'$. Tomando $c = d'$ obtenemos que $d' \mid d$. Tomando $c = d$ tenemos en cambio que $d \mid d'$. Se sigue entonces que $|d| = |d'|$, como $d, d' > 0$ esto implica que $d = d'$.

Ahora probaremos la existencia: Consideremos el conjunto

$$A = \{ax + by > 0 \,|\, x, y \in \mathbb{Z}\}.$$

El conjunto A es no vacío, pues $a^2 + b^2 \in A$. Así, A tiene un elemento mínimo, al que llamaremos d. Este elemento tiene la forma

$$d = ax + by \tag{A.1}$$

para ciertos $x, y \in \mathbb{Z}$. Si $c \mid a$ y $c \mid b$ entonces $c \mid au + bv$ para todo $u, v \in \mathbb{Z}$ y en particular $c \mid ax + by$, es decir, $c \mid d$. Por ende, sólo queda probar que $d \mid a$ y $d \mid b$. Para esto aplicando el algoritmo de división, existen enteros q, r tales que

$$a = dq + r \quad \text{y} \quad 0 \leq r < d,$$

y por ende, de (A.1) se sigue que

$$a = (ax + by)q + r,$$

de donde, si $r > 0$

$$r = (1 - qx)a + (-qy)b \in A,$$

lo que contradice la minimalidad de d, y por ende se sigue que $r = 0$, de donde $d \mid a$. De manera análoga se tiene que $d \mid b$. □

Definición. Dados dos enteros a, b no ambos iguales a 0, al único número d de la proposición anterior se lo llama el *máximo común divisor* de a y b, y se lo denota por (a, b).

Siendo más detallados: Si $a, b \in \mathbb{Z}$, no ambos iguales a 0, su máximo común divisor $d = (a, b)$ es el único entero positivo que es divisor de a y b y que es múltiplo de todos los divisores de a y b. La demostración de la proposición anterior nos da aún más información sobre el máximo común divisor de dos números enteros:

Teorema A.4 (Identidad de Bézout)**.** *Sean a, b dos números enteros, no ambos iguales a 0 y sea $d > 0$ un número entero. Las siguientes afirmaciones son equivalentes:*

(i) $d = (a, b)$.

(ii) *$d \mid a$, $d \mid b$ y existen números enteros x, y tales que $d = ax + by$. Esta igualdad se denomina la* identidad de Bézout.

Ejercicio A.5. Sean a y b dos números enteros, no ambos iguales a 0 y sea $d = (a, b)$. Pruebe que

$$\{ax + by \,|\, x, y \in \mathbb{Z}\} = d\mathbb{Z},$$

donde $d\mathbb{Z} = \{kd \,|\, k \in \mathbb{Z}\}$ es el conjunto de todos los múltiplos de d.

Corolario A.6. *Sean a, b dos números enteros distintos de 0. Las siguientes afirmaciones son equivalentes:*

(i) *a y b son coprimos.*

(ii) $(a, b) = 1$.

(iii) *Existen enteros* x, y *tales que* $ax + by = 1$.

Demostración. Si a y b son coprimos, su único divisor común positivo es 1 y por lo tanto $(a, b) = 1$. Recíprocamente, supongamos que $(a, b) = 1$. Si c es un divisor de a y b, se tiene que $c \mid (a, b)$, es decir, $c \mid 1$, de donde $c = 1$ o $c = -1$ y por ende a y b son coprimos. Esto prueba la equivalencia de (i) y (ii). La equivalencia de (ii) y (iii) es inmediata del teorema precedente. □

Teorema A.7 (Teorema fundamental de la aritmética)**.** *Sea* $a \in \mathbb{Z}$, $a \neq 0$. *Existen números primos* $p_1, \ldots, p_n$ *(no necesariamente distintos) tales que*

$$a = \varepsilon p_1 p_2 \cdots p_n,$$

con $\varepsilon = \pm 1$. *Más aún, esta descomposición es única, en el sentido de que si* $q_1, \ldots, q_m$ *son número primos tales que*

$$a = \varepsilon' q_1 q_2 \cdots q_m$$

con $\varepsilon' = \pm 1$, *entonces* $n = m$ *y existe una función biyectiva* $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ *tal que* $p_i = q_{\sigma(i)}$ *para todo* $1 \leq i \leq n$.

Para demostrar este teorema, haremos uso del siguiente resultado.

Lema A.8. *Sean* $a, a_1, \ldots, a_n \in \mathbb{Z}$ *y* p *un número primo.*

(1) *Si* $(a, a_i) = 1$ *para* $1 \leq i \leq n$, *entonces* $(a, a_1 a_2 \cdots a_n) = 1$.

(2) *Si* $(a_i, a_j) = 1$ *para todo* $i \neq j$ *y si* $a_i \mid a$ *para todo* $1 \leq i \leq n$, *entonces* $a_1 a_2 \cdots a_n \mid a$.

(3) *Si* $p \mid a_1 a_2 \cdots a_n$, *entonces* $p \mid a_i$ *para algún* $1 \leq i \leq n$.

Demostración. (1) Por el Corolario A.6 podemos escribir $ax_i + a_i y_i = 1$ para ciertos $x_i, y_i \in \mathbb{Z}$, y por ende tenemos que

$$a_1 a_2 \cdots a_n y_1 y_2 \cdots y_n = (1 - ax_1)(1 - ax_2) \cdots (1 - ax_n). \tag{A.2}$$

Probaremos por inducción sobre n que existe un número entero b tal que $(1 - ax_1)(1 - ax_2) \cdots (1 - ax_n) = 1 - ab$. Esto es trivial si $n = 1$, pues basta tomar $b = x_1$. Supongamos el resultado válido para n, así

$$(1 - ax_1) \cdots (1 - ax_n)(1 - ax_{n+1}) = (1 - ab)(1 - ax_{n+1}) = 1 - a(b + x_{n+1} - abx_{n+1}),$$

y como $b + x_{n+1} - abx_{n+1} \in \mathbb{Z}$ se tiene lo deseado. Con esto, si escribimos $y = y_1 \cdots y_n$ en (A.2), tenemos que existe $x \in \mathbb{Z}$ tal que

$$a_1 \cdots a_n y = 1 - ax,$$

es decir

$$ax + (a_1 \cdots a_n)y = 1,$$

lo que por el Corolario A.6 significa que $(a, a_1 \cdots a_n) = 1$.

(2) Procedemos por inducción sobre n. Para $n = 1$ no hay nada que probar. Por hipótesis de inducción tenemos que $a_2 \cdots a_n \mid b$. Existen entonces $k, k' \in \mathbb{Z}$ tales que $a = a_1 k = a_2 \cdots a_n k'$. Además, como $(a_1, a_i) = 1$ para todo $2 \leq i \leq n$, por la parte (1) se tiene que $(a_1, a_2 \cdots a_n) = 1$, de modo que existen $x, y \in \mathbb{Z}$ tales que $a_1 x + a_2 \cdots a_n y = 1$. De este modo tenemos que

$$a = a1 = aa_1 x + aa_2 \cdots a_n y = (a_2 \cdots a_n k')a_1 x + (a_1 k)a_2 \cdots a_n y = a_1 a_2 \cdots a_n (k'x + ky),$$

lo que significa que $a_1 a_2 \cdots a_n \mid a$.

(3) Supongamos que $p \nmid a_i$ para todo $1 \leq i \leq n$. Fijemos i y sea $d = (p, a_i)$. Como $d \mid p$, entonces $d = \pm p$ o $d = 1$, pero $d \mid a_i$ y $p \nmid a_i$, entonces $d \neq \pm p$, de donde $d = 1$. Así $(p, a_i) = 1$ para todo $1 \leq i \leq n$. Por la parte (1) se tiene que $(p, a_1 \ldots a_n) = 1$, de donde $p \nmid a_1 \ldots a_n$. □

Demostración del Teorema A.7. Claramente 1 es un producto (vacío) de números primos. Además, es claro que basta probar el teorema para los números enteros positivos. Supongamos que el resultado es falso, y sea A el conjunto de todos los enteros positivos que *no* se pueden expresar como un producto de números primos. Por nuestra asunción, A es no vacío y $1 \notin A$, de modo que A tiene un elemento mínimo $a \neq 1$. Este número no puede ser primo, y por lo tanto es compuesto, y así existen $a_1, a_2 \in \mathbb{Z}$, que podemos asumir positivos, tales que $a = a_1 a_2$. Como $a_1 < a$ y $a_2 < a$, entonces $a_1, a_2 \notin A$ por la minimalidad de a, y por ende a_1 y a_2 son productos de números primos. Pero esto implica que a también es un producto de números primos y por ende $a \notin A$. Esto es una contradicción.

Ahora, probemos la unicidad.Claramente $\varepsilon = \varepsilon'$, por lo que podemos asumir que

$$p_1 \cdots p_n = q_1 \cdots q_m.$$

Dado que $p_1 \mid p_1 \cdots p_n$, se tiene que $p_1 \mid q_1 \cdots q_m$ y por ende existe $\sigma(1) \in \{1, \ldots, m\}$ tal que $p_1 \mid q_{\sigma(1)}$. Pero como $q_{\sigma(1)}$ es primo, esto implica que $p_1 = q_{\sigma(1)}$. Cancelando estos términos de la igualdad obtenemos

$$p_2 \cdots p_n = q_1 \cdots \widehat{q_{\sigma(1)}} \cdots q_m,$$

donde el símbolo $\widehat{\cdot}$ significa que el número bajo este ha sido removido. La demostración se sigue haciendo inducción sobre n. □

Teorema A.9. *Existen infinitos números primos.*

Demostración. Supongamos que el conjunto de números primos es finito y sean estos $p_1, \ldots, p_n$. Sea $a = p_1 \cdots p_n + 1$. Como $a > 1$, el Teorema Fundamental de la Aritmética implica que a es un producto de números primos y por ende, algún p_i es divisor de a, pero entonces, como $p_i \mid p_1 \cdots p_n$ se sigue que

$$p_i \mid a - p_1 \cdots p_n = 1,$$

lo que es imposible. □

A continuación, presentamos dos ejercicios que proporcionan demostraciones alternativas para el teorema anterior. La primera es una demostración analítica y la segunda una demostración topológica.

Ejercicio A.10. Sea $n \in \mathbb{N}$, con $n \geq 1$ y denotemos por $P[n]$ al conjunto de todos los números primos positivos menores o iguales a n y por P al conjunto de todos los números primos positivos.

(a) Usando series geométricas apropiadas y el teorema fundamental de la aritmética muestre que

$$\prod_{p \in P[n]} \left(1 - \frac{1}{p}\right)^{-1} \geq \sum_{k=1}^{n} \frac{1}{k} > \log(n),$$

donde log es la función logaritmo natural.

(b) Use la serie de Taylor para $\log(1-x)$ alrededor de 0 para probar que

$$\log \prod_{p\in P[n]} \left(1-\frac{1}{p}\right)^{-1} < \sum_{p\in P[n]} \frac{1}{p} + \frac{1}{2}.$$

(c) Deduzca de (a) y (b) que

$$\sum_{p\in P[n]} \frac{1}{p} \geq \log(\log(n)) - \frac{1}{2}$$

y que por ende la serie $\sum_{p\in P} \frac{1}{p}$ es divergente.

(d) Concluya a partir de (c) que existen infinitos números primos.

Ejercicio A.11. Para cada $a, b \in \mathbb{Z}$ con $b > 0$, definimos el conjunto

$$a + b\mathbb{Z} = \{a + bk \mid k \in \mathbb{Z}\}.$$

Esta es la progresión geométrica de diferencia b que pasa por a. Además, como en el ejercicio anterior, sea P el conjunto de números primos positivos.

(a) Muestre que la familia $\{a + b\mathbb{Z} \mid a, b \in \mathbb{Z}, b > 0\}$ es una base para una topología sobre $\mathbb{Z}$ (esta topología se conoce como la *topología de Furstenberg* sobre $\mathbb{Z}$)

(b) Demuestre que todos los abiertos básicos son conjuntos abiertos y cerrados a la vez.

(c) Usando el teorema fundamental de la aritmética, pruebe que

$$\mathbb{Z} \setminus \{1, -1\} = \bigcup_{p\in P} (0 + p\mathbb{Z}),$$

y concluya que $\{1, -1\}$ es abierto en caso de que P sea finito.

(d) Pruebe que la situación descrita en (c) es imposible y, por ende, que P es infinito.

El siguiente ejercicio permite generalizar la definición de máximo común divisor a más de dos números enteros:

Ejercicio A.12. Sean $a, b, c \in \mathbb{Z} \setminus \{0\}$. Demuestre que

(a) $(a, b) = (b, a)$.

(b) $((a, b), c) = (a, (b, c))$.

Con esto, podemos definir el máximo común divisor de $a, b, c \in \mathbb{Z} \setminus \{0\}$ mediante $(a, (b, c))$ y denotarlo por (a, b, c), ya que la parte (b) del ejercicio anterior elimina el riesgo de ambigüedad respecto a la posición de los paréntesis. Más generalmente, si $a_1, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$, definimos recursivamente

$$(a_1, a_2, \ldots, a_n) = ((a_1, \ldots, a_{n-1}), a_n).$$

Ejercicio A.13. Sean $a, b \in \mathbb{Z}$ con $a \neq 0 \neq b$. Pruebe que si $d = (a, b)$, entonces

$$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$$

A.2. El algoritmo euclidiano extendido

La identidad de Bézout presentada en el apartado anterior nos proporciona un criterio útil para determinar si un número dado es el máximo común divisor de dos enteros. Sin embargo el problema de calcular explícitamente el máximo común divisor de dos números enteros no ha sido abordado. En esta sección presentamos un algoritmo que da una respuesta satisfactoria a este problema.

Teorema A.14 (Algoritmo euclidiano)**.** *Sean a, b dos enteros no ambos iguales a 0. Entonces si $q, r \in \mathbb{Z}$ son tales que*

$$a = bq + r \quad y \quad 0 \leq r < |b|,$$

se tiene que

$$(a, b) = (b, r).$$

Demostración. Sea $d = (a, b)$, entonces $d \mid a$ y $d \mid b$, de donde $d \mid a - bq = r$. Supongamos que $c \mid b$ y $c \mid r$, entonces $c \mid bq + r = a$, de donde $c \mid d$. Esto, por definición, significa que $d = (b, r)$. □

El teorema anterior nos provee de un método efectivo para el cálculo del máximo común divisor: Supongamos que $|a| > |b| > 0$. Definamos $r_0 = a$, $r_1 = b$ y $r_2 = r$, donde

$$a = bq + r \quad \text{y} \quad 0 \leq r < |b|.$$

Entonces, por el teorema tenemos que

$$(a, b) = (r_1, r_2).$$

Si $r_2 = 0$, tenemos que $b \mid a$ y por ende $(a, b) = b = r_1$. Si $r_2 \neq 0$ escribimos

$$r_1 = q_2 r_2 + r_3 \quad \text{con} \quad 0 \leq r_3 < r_2,$$

de modo que

$$(a, b) = (r_1, r_2) = (r_2, r_3).$$

Si $r_3 = 0$ entonces $r_2 \mid r_1$ y así $(r_1, r_2) = r_2$. De no ser así continuamos iterando este proceso: Obtenemos una sucesión $(r_n)_{n \geq 0}$ definida recursivamente por

$$r_{n-1} = q_n r_n + r_{n+1} \quad \text{y} \quad 0 \leq r_{n+1} < r_n.$$

En cada etapa tenemos que

$$(a, b) = (r_n, r_{n+1}).$$

El hecho de que (r_n) es estrictamente decreciente, y acotada inferiormente por 0 implica que existe n suficientemente grande tal que $r_{n+1} = 0$ y en consecuencia se tiene que $r_n \mid r_{n-1}$, de donde

$$(a, b) = (r_{n-1}, r_n) = r_n,$$

por lo que este algoritmo efectivamente nos permite calcular el máximo común divisor de dos números enteros.

Ejemplo A.15. Calculemos el máximo común divisor de 93100 y 20691. Escribamos $a = 93100$ y $b = 20691$. Entonces, aplicando el algoritmo euclidiano tenemos

$$\begin{aligned} 93100 &= 4 \cdot 20691 + 10336, & r_1 &= 10336, \\ 20691 &= 2 \cdot 10336 + 19, & r_2 &= 19, \\ 10336 &= 544 \cdot 19 + 0, & r_3 &= 0, \end{aligned}$$

de modo que $(93100, 20691) = 19$.

Si bien el algoritmo anterior nos provee un método efectivo para el cálculo del máximo común divisor, no nos provee, al menos por el momento de un método para el cálculo de un par de números enteros x, y tales que, si $d = (a, b)$,

$$d = ax + by.$$

En lo que sigue, a los números x e y los llamaremos *coeficientes de Bézout* de d.

Exploremos con más detenimiento el algoritmo euclidiano, pero esta vez conservaremos más información que solamente los residuos r_n: Definamos tres sucesiones adicionales (q_n), (x_n) y (y_n) del siguiente modo:

$$x_0 = 1, \quad x_1 = 0, \quad y_0 = 0, \quad y_1 = 1,$$

para cada n escribimos

$$r_{n-1} = r_n q_n + r_{n+1} \quad \text{con} \quad 0 \leq r_{n+1} < r_n,$$

esto caracteriza q_n y r_{n+1}, y entonces definimos

$$x_{n+1} = x_{n-1} - q_n x_n \quad \text{y} \quad y_{n+1} = y_{n-1} - q_n y_n.$$

Con esto, tenemos

Lema A.16. *Para cada n se verifica que*

$$r_n = ax_n + bx_n.$$

Demostración. Procederemos por inducción sobre n. Para $n = 0$ y $n = 1$ tenemos que

$$ax_0 + by_0 = a1 + b0 = a = r_0$$

y

$$ax_1 + by_1 = a0 + b1 = b = r_1,$$

por lo que la igualdad se satisface para $n = 0$ y $n = 1$. Asumiendo el resultado para todo $k \leq n$, con $n \geq 1$, tenemos que

$$\begin{aligned} ax_{n+1} + by_{n+1} &= a(x_{n-1} - q_n x_n) + b(y_{n-1} - q_n y_n) \\ &= (ax_{n-1} + by_{n-1}) - q_n(ax_n by_n) \\ &= r_{n-1} - q_n r_n, \end{aligned}$$

donde hemos usado la hipótesis de inducción para $k = n - 1$ y $k = n$. Ahora, notemos que por definición de q_n y r_n se tiene que $r_{n-1} = q_n r_n + r_{n+1}$, de donde

$$ax_{n+1} + by_{n+1} = r_{n+1},$$

lo que completa la demostración. □

Notemos que ya sabemos que existe n tal que $r_{n+1} = 0$, con lo cual $r_n = (a, b)$. Entonces tenemos que

$$r_n = ax_n + by_n,$$

y hemos probado el siguiente resultado:

Teorema A.17 (Algoritmo euclidiano extendido)**.** *Con las notaciones precedentes, sea n tal que $r_{n+1} = 0$, entonces $(a, b) = r_n$ y*

$$r_n = ax_n + by_n,$$

es decir, x_n y y_n son los coeficientes de Bézout de r_n.

Ejemplo A.18. Sean $a = 93100$ y $b = 20691$ como en el ejemplo anterior. Aplicamos el algoritmo euclidiano extendido y tabulamos los valores obtenidos:

n	x_n	y_n	r_n	q_n
0	1	0	93100	
1	0	1	20691	4
2	1	-4	10336	2
3	-2	9	19	544
4			0	

Con esto tenemos que

$$(93100, 20691) = 19 = 93100(-2) + 20691(9).$$

A.3. Ecuaciones lineales diofánticas

Sean $a, b, c \in \mathbb{Z}$. Cuando $c = (a, b)$, la identidad de Bézout establece que la ecuación

$$ax + by = c \tag{A.3}$$

tiene al menos una solución sobre $\mathbb{Z}$. Dicho de otro modo, existen $x, y \in \mathbb{Z}$ que satisfacen la ecuación. Ahora nos aprestamos a probar un resultado más general. En mente tendremos dos objetivos: Caracterizar (en términos de a, b y c) todas las ecuaciones de la forma A.3 que admiten al menos una solución en el conjunto de números enteros y, conociendo la existencia de soluciones, determinar el conjunto de todas las soluciones enteras de tal ecuación.

Definición. Una ecuación de la forma

$$ax + by = c,$$

donde $a, b, c \in \mathbb{Z}$, se denomina una *ecuación lineal diofántica.*

Teorema A.19. *Sean $a, b, c \in \mathbb{Z}$ con $a, b \neq 0$. Sea $d = (a, b)$. Las siguientes afirmaciones son equivalentes:*

(i) *La ecuación lineal diofántica $ax + by = c$ admite una solución $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$.*

(ii) *$d \mid c$.*

Demostración. Supongamos que $d \mid c$ y escribamos $c = dk$ para cierto $k \in \mathbb{Z}$. Por la identidad de Bézout existen enteros x_1, y_1 tales que $d = ax_1 + by_1$. Multiplicando ambos lados de esta igualdad por k obtenemos $c = dk = a(x_1k) + b(y_1k)$, por lo que, si definimos $x_0 = x_1k$ y $y_0 = y_1k$, tenemos que $c = ax_0 + by_0$ y así la ecuación lineal diofántica $ax + by = c$ admite al menos una solución.

Recíprocamente, supongamos que $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ es una solución de la ecuación lineal diofántica $ax + by = c$. Por el Ejercicio A.5 tenemos que $c = ax_0 + by_0 \in d\mathbb{Z}$, de donde $c = dk$ para cierto $z \in \mathbb{Z}$, lo que implica que $d \mid c$. □

Si exploramos la demostración anterior, vemos que no solo hemos caracterizado la existencia de soluciones enteras de una ecuación lineal diofántica, sino que obtenemos un método efectivo para el cálculo de (al menos) una solución: Con la notación del teorema, podemos usar el algoritmo euclidiano extendido para encontrar $x_1, y_1 \in \mathbb{Z}$ tales que

$$d = ax_1 + by_1,$$

y, entonces

$$x_0 = \frac{cx_1}{d}, \quad y_0 = \frac{cy_1}{d},$$

es una solución de la ecuación. Aquí hemos usado la siguiente notación: Si $a \mid b$, y $a \neq 0$, entonces existe un único entero k tal que $b = ak$, entonces definimos $\dfrac{b}{a} = k$.

Porisma A.20. *Sean $a, b, c \in \mathbb{Z}$ con $a \neq 0 \neq b$. Sea $d = (a, b)$ y supongamos que $d \mid c$. Escribamos $d = ax_1 + by_1$ para ciertos $x_1, y_1 \in \mathbb{Z}$. Entonces el par $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ dado por*

$$x_0 = \frac{cx_1}{d}, \quad y_0 = \frac{cy_1}{d},$$

es una solución de la ecuación diofántica $ax + by = c$.

Ahora que sabemos cómo determinar la existencia de soluciones de una ecuación lineal diofántica y que sabemos además como encontrar una solución, veremos como determinar todas las posibles soluciones.

Teorema A.21. *Sean $a, b, c \in \mathbb{Z}$ con $a, b \neq 0$ y sea $d = (a, b)$. Supongamos que $d \mid c$ y sea $(x_0, y_0) \in \mathbb{Z} \times \mathbb{Z}$ una solución de la ecuación lineal diofántica $ax + by = c$. Entonces el conjunto de todas las soluciones de esta ecuación está dado por*

$$S = \left\{ \left(x_0 + \frac{bk}{d}, y_0 - \frac{ak}{d} \right) \,\middle|\, k \in \mathbb{Z} \right\}.$$

Demostración. Primero probaremos que todos los elementos de S son soluciones de la ecuación $ax + by = c$. En efecto, como (x_0, y_0) es solución tenemos que $ax_0 + by_0 = c$, con lo cual

$$a\left(x_0 + \frac{bk}{d}\right) + b\left(y_0 + \frac{ak}{d}\right) = ax_0 + by_0 + \frac{abk}{d} - \frac{abk}{d} = c.$$

Recíprocamente, sea $(x_1, y_1) \neq (x_0, y_0)$ una solución de la ecuación, es decir, $ax_1 + by_1 = c$. Como $ax_0 + by_0 = c$, al restar estas ecuaciones obtenemos

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

de donde

$$\frac{a}{d}(x_1 - x_0) = -\frac{b}{d}(y_1 - y_0). \tag{A.4}$$

Tenemos entonces que $\frac{b}{d} \mid \frac{a}{d}(x_1 - x_0)$. Sea p un número primo tal que $p \mid \frac{b}{d}$. Notemos que $p \nmid \frac{a}{d}$, pues de ser el caso, podemos escribir $b = dkp$ y $a = dk'p$ para ciertos $k, k' \in \mathbb{Z}$ lo que implica que $dp \mid a$ y $dp \mid a$, de donde $dp \mid d$, lo que es absurdo. De este modo $p \mid (x_1 - x_0)$. Con esto, tenemos que

$$\frac{b}{dp} \mid \frac{x_1 - x_0}{p},$$

y un argumento recursivo sobre el número de primos que aparecen en $\frac{b}{d}$ muestra que $\frac{b}{d} \mid x_1 - x_0$. Así, existe $k \in \mathbb{Z}$ tal que $x_1 - x_0 = \frac{bk}{d}$, es decir

$$x_1 = x_0 + \frac{bk}{d}.$$

Sustituyendo esto en la igualdad (A.4) tenemos que

$$\frac{a}{d}\frac{bk}{d} = -\frac{b}{d}(y_1 - y_0),$$

de donde

$$y_1 = y_0 - \frac{ak}{d},$$

lo que prueba que $(x_1, y_1) \in S$. □

Ejemplo A.22. Consideremos la ecuación lineal diofántica

$$4158x - 1470y = 126.$$

Apliquemos el algoritmo euclidiano extendido para calcular $(4158, -1470)$ y los correspondientes coeficientes de Bézout: Tomamos $a = 4158$ y $b = -1470$ y tabulamos los resultados en la siguiente tabla:

n	x_n	y_n	r_n	q_n
0	1	0	4158	
1	0	1	-1470	-2
2	1	2	1218	-2
3	2	5	966	1
4	-1	-3	252	3
5	5	14	210	1
6	-6	-17	42	5
7			0	

De este modo tenemos que $(1458, -1470) = 42$ y además

$$42 = 4158(-6) + (-1470)(-17).$$

Ahora, notemos que $126 = 3 \cdot 42$, de modo que $42 \mid 126$ y por ende la ecuación lineal diofántica tiene solución. Más aún, una solución está dada por

$$x_0 = 3(-6) = -18, \quad y_0 = 3(-17) = -51.$$

Con esto, el conjunto de soluciones está dado por

$$S = \{(-18 - 35k, -51 - 99k) \,|\, k \in \mathbb{Z}\}.$$

A.4. Congruencias

Fijemos $n \in \mathbb{Z}$, con $n \geq 2$. Definimos $n\mathbb{Z}$ como el conjunto

$$n\mathbb{Z} = \{nk \,|\, k \in \mathbb{Z}\}.$$

Definimos la relación $\sim$ sobre $\mathbb{Z}$ del siguiente modo:

$$a \sim b \Leftrightarrow b - a \in n\mathbb{Z},$$

es decir, $a \sim b$ si y sólo si existe $k \in \mathbb{Z}$ tal que $b - a = nk$. Esta es una relación de equivalencia:

- *Reflexividad:* Si $a \in \mathbb{Z}$ tenemos que $a - a = 0n$, de donde $a \sim a$.
- *Simetría:* Si $a \sim b$, entonces $b - a = nk$ para cierto $k \in \mathbb{Z}$, de donde $a - b = n(-k)$, y como $-k \in \mathbb{Z}$ tenemos que $b \sim a$.
- *Transitividad:* Si $a \sim b$ y $b \sim c$, existen enteros $k_1, k_2 \in \mathbb{Z}$ tales que $b - a = nk_1$ y $c - b = nk_2$. Definiendo $k = k_1 + k_2 \in \mathbb{Z}$ obtenemos

  $$c - a = (c - b) + (b - a) = nk_1 + nk_2 = nk,$$

  por lo que $a \sim c$.

Al conjunto cociente de $\mathbb{Z}$ por la relación de equivalencia $\sim$ lo denotamos por $\mathbb{Z}/n\mathbb{Z}$ (otros autores usan la notación $\mathbb{Z}/n$ o $\mathbb{Z}_n$, esta última usualmente da lugar a confusión porque también se utiliza, cuando $n = p$ es un número primo, para denotar al anillo de enteros p-ádicos). Además escribiremos $a \equiv b \pmod{n}$ en lugar de $a \sim b$ y en este caso diremos que a y b son *congruentes módulo* n. A la clase de equivalencia representada por $a \in \mathbb{Z}$ la denotaremos usualmente por $\overline{a}$ o $[a]$ y, cuando necesitemos hacer énfasis en n, por $[a]_n$.

Proposición A.23. *Sean $a, a', b, b', c \in \mathbb{Z}$. Se verifican las siguientes propiedades:*

(1) *Si $a \equiv a' \pmod{n}$ y $b \equiv b' \pmod{n}$, entonces $a + b \equiv a' + b' \pmod{n}$.*

(2) *Si $a \equiv a' \pmod{n}$ y $b \equiv b' \pmod{n}$, entonces $ab \equiv a'b' \pmod{n}$.*

(3) *Si $ac \equiv bc \pmod{n}$ y $(c, n) = 1$, entonces $a \equiv b \pmod{n}$.*

Demostración. Supongamos que $a \equiv a' \pmod{n}$ y $b \equiv b' \pmod{n}$, entonces podemos escribir $a = a' + kn$ y $b = b' + jn$ para ciertos $k, j \in \mathbb{Z}$, con lo cual

$$a + b = a' + b' + (k + j)n,$$

lo que significa que $a + b \equiv a' + b' \pmod{n}$. Esto prueba (1). De manera análoga, tenemos

$$ab = (a' + kn)(b' + jn) = a'b' + (a'j + kb' + kjn)n,$$

lo que significa que $ab \equiv a'b' \pmod{n}$. Así, hemos probado (2).

Finalmente, supongamos que $ac \equiv bc \pmod{n}$ y que $(c, n) = 1$, entonces podemos escribir $cx + ny = 1$ para ciertos $x, y \in \mathbb{Z}$. Tenemos que $ac = bc + kn$ para cierto $k \in \mathbb{Z}$. Multiplicando esta ecuación por x obtenemos

$$acx = bcx + kxn,$$

y como $cx = 1 - ny$ esto nos da

$$a - any = b - bny + kxn,$$

o, lo que es lo mismo,

$$a = b + (ay - by + kx)n,$$

lo que significa que $a \equiv b \pmod{n}$. □

Gracias a la proposición anterior, podemos definir la suma y multiplicación de dos elementos de $\mathbb{Z}/n\mathbb{Z}$ del siguiente modo:

$$[a] + [b] = [a + b] \quad \text{y} \quad [a][b] = [ab].$$

La proposición implica que estas operaciones están bien definidas (es decir, no dependen de los representantes de las clases de equivalencia escogidos). Más aún, la estructura de anillo conmutativo con unidad de $\mathbb{Z}$ induce en $\mathbb{Z}/n\mathbb{Z}$ una estructura de anillo conmutativo con unidad, donde el neutro para la multiplicación es [1]. Por abuso de lenguaje, usualmente escribiremos $a \in \mathbb{Z}/n\mathbb{Z}$ en lugar de $[a]$.

Proposición A.24. *Para todo entero $n > 1$ se tiene que*

$$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \ldots, [n-1]\},$$

y además $|\mathbb{Z}/n\mathbb{Z}| = n$.

Demostración. Sea $a \in \mathbb{Z}$, entonces $[a] \in \mathbb{Z}/n\mathbb{Z}$. Aplicando el algoritmo de división, podemos escribir

$$a = nq + r \quad \text{con} \quad 0 \leq r < n,$$

de modo que $[a] = [r]$ y $0 \leq r \leq n - 1$, y así

$$\mathbb{Z}/n\mathbb{Z} \subseteq \{[0], [1], \ldots, [n-1]\}.$$

La otra inclusión es trivial. Ahora, para probar que $|\mathbb{Z}/n\mathbb{Z}| = n$, basta probar que las clases $[0], [1], \ldots, [n-1]$ son dos a dos distintas. Para ello, sean $0 \leq i < j \leq n - 1$ y supongamos que $[i] = [j]$. Esto significa que $j = i + kn$ para cierto $k \in \mathbb{Z}$. Dado que $j > 0$ y $i < n$, necesariamente $k \geq 0$. Si $k > 0$, entonces $i + kn \geq n$, de donde $j \geq n$, lo que es absurdo, así $k = 0$ y por ende $i = j$, una contradicción. Así $[i] \neq [j]$. □

Proposición A.25. *Un elemento $[a] \in \mathbb{Z}/n\mathbb{Z}$ es invertible en $\mathbb{Z}/n\mathbb{Z}$ si y sólo si $(a, n) = 1$.*

Demostración. Supongamos que $[a]$ es invertible en $\mathbb{Z}/n\mathbb{Z}$, entonces existe $b \in \mathbb{Z}$ tal que $[1] = [a][b] = [ab]$, lo que significa que $ab - 1 = kn$ para cierto $k \in \mathbb{Z}$, es decir, $ab + (-k)n = 1$. Esto último significa precisamente que $(a, n) = 1$.

Recíprocamente, supongamos que $(a, n) = 1$, y escribamos $ax + ny = 1$, entonces $[a][x] = [1]$, de donde $[a]$ es invertible. □

Corolario A.26. *Si p es un número primo, entonces $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo. En este caso usaremos la notación $\mathbb{F}_p$ en lugar de $\mathbb{Z}/p\mathbb{Z}$.*

Lema A.27. *Sean $u, n \in \mathbb{Z}$ tales que $n > 1$ y $(u, n) = 1$. Entonces la función $\gamma : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ definida por $\gamma([a]) = [ua]$, $[a] \in \mathbb{Z}$ es biyectiva.*

Demostración. Probemos que la función es inyectiva. Para ello, supongamos que $[ua] = [ub]$ para ciertos $[a], [b] \in \mathbb{Z}/n\mathbb{Z}$, esto significa que $ua \equiv ub \pmod{n}$, y como $(u, n) = 1$, esto implica que $a \equiv b \pmod{n}$, es decir, $[a] = [b]$, lo que prueba la inyectividad de γ. Dado que $|\mathbb{Z}/n\mathbb{Z}| = n$, el conjunto $\mathbb{Z}/n\mathbb{Z}$ es finito y por ende γ es además sobreyectiva. □

Teorema A.28 (Teorema pequeño de Fermat)**.** *Sea p un número primo y $a \in \mathbb{Z}$ tal que $a \not\equiv 0 \pmod{p}$. Entonces*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Demostración. Notemos que

$$[a]^{p-1}[1][2]\cdots[p-1] = [a1][a2]\cdots[a(p-1)] = \gamma([1])\gamma([2])\cdots\gamma([p-1]),$$

donde γ es la función definida en el Lema anterior. Dado que $a \not\equiv 0 \pmod{p}$, esta función es biyectiva, y puesto que la multiplicación es conmutativa, tenemos que

$$[a]^{p-1}[1][2]\cdots[p-1] = [1][2]\cdots[p-1],$$

lo que implica que $[a^{p-1}] = [a]^{p-1} = [1]$, es decir,

$$a^{p-1} \equiv 1 \pmod{p}.$$

□

Corolario A.29. *Para todo entero $a \in \mathbb{Z}$ y todo número primo p tenemos que*

$$a^p \equiv a \pmod{p}.$$

Demostración. Si $a \equiv 0 \pmod{p}$ el resultado es trivial. Si $a \not\equiv 0 \pmod{p}$, entonces por el teorema anterior $a^{p-1} \equiv 1 \pmod{p}$, de donde $a^{p-1}a \equiv 1a \pmod{p}$, es decir, $a^p \equiv a \pmod{p}$. □

A.5. La función φ de Euler

Definición. Definimos el conjunto $(\mathbb{Z}/n\mathbb{Z})^\times$ como el conjunto de elementos de $\mathbb{Z}/n\mathbb{Z}$ que son invertibles y lo llamamos el *grupo de unidades* de $\mathbb{Z}/n\mathbb{Z}$.

Recordemos que un elemento $[a]$ es invertible en $\mathbb{Z}/n\mathbb{Z}$ si y sólo si $(a, n) = 1$. Por ende,

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{[a] \in \mathbb{Z}/n\mathbb{Z} \,|\, (a, n) = 1\}.$$

El nombre de *grupo* no es accidental:

Lema A.30. *$(\mathbb{Z}/n\mathbb{Z})^\times$ es un grupo abeliano con la operación de multiplicación heredada de $\mathbb{Z}/n\mathbb{Z}$.*

Demostración. Sean $[a],[b] \in (\mathbb{Z}/n\mathbb{Z})^\times$, entonces existen $[c],[d] \in \mathbb{Z}/n\mathbb{Z}$ tales que $[a][c] = [1] = [b][d]$, de donde

$$([a][b])[cd] = ([a][c])([b][d]) = [1][1] = [1],$$

y así $[a][d] \in (\mathbb{Z}/n\mathbb{Z})^\times$, lo que significa que $(\mathbb{Z}/n\mathbb{Z})^\times$ es cerrado por multiplicación. La multiplicación es claramente asociativa y conmutativa y además $[1] \in (\mathbb{Z}/n\mathbb{Z})^\times$. Si $[a] \in (\mathbb{Z}/n\mathbb{Z})^\times$ entonces $[a]^{-1}[a] = [-1]$, lo que significa que $[a]^{-1} \in (\mathbb{Z}/n\mathbb{Z})^\times$. Así $(\mathbb{Z}/n\mathbb{Z})^\times$ es un grupo abeliano. □

Definición. La *función φ de Euler* es la función $\varphi : \mathbb{Z}^* \to \mathbb{Z}$ definida por

$$\varphi(n) = |(\mathbb{Z}/n\mathbb{Z})^\times \quad \forall n \in \mathbb{Z}^+.$$

Teorema A.31. *Si $(n,m) = 1$ entonces los grupos $\mathbb{Z}/nm\mathbb{Z}$ y $(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$ son isomorfos. Además, también $(\mathbb{Z}/nm\mathbb{Z})^\times$ es isomorfo a $(\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times$.*

Demostración. Consideremos la función $f : \mathbb{Z}/nm\mathbb{Z} \to (\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})$ definida por

$$f([a]_{nm}) = ([a]_n, [a]_m).$$

Esta función está bien definida: Supongamos que $[a]_{nm} = [a']_{nm}$, entonces $a = a' + knm$ para cierto $k \in \mathbb{Z}$. De este modo tenemos que $a = a' + (km)n$, es decir, $[a]_n = [a']_n$ y similarmente $[a]_m = [a']_m$. Ahora, notemos que

$$\begin{aligned} f([a]_{nm} + [b]_{nm}) &= f([a+b]_{nm}) \\ &= ([a+b]_n, [a+b]_m) \\ &= ([a]_n + [b]_n, [a]_m + [b]_m) \\ &= ([a]_n, [a]_m) + ([b]_n, [b]_m) \\ &= f([a]_{nm}) + f([b]_{nm}), \end{aligned}$$

por lo que f es un homomorfismo de grupos. Ahora, supongamos que $f([a]_{nm}) = 0$, es decir, $[a]_n = 0$ y $[a]_m = 0$, lo que implica que $m \mid a$ y $n \mid a$ y como $(m,n) = 1$, esto implica que $mn \mid a$, así $[a]_{mn} = 0$, de donde f es inyectiva. Dado que $|\mathbb{Z}/nm\mathbb{Z}| = mn = |(\mathbb{Z}/n\mathbb{Z}) \times (\mathbb{Z}/m\mathbb{Z})|$, se sigue que f es un isomorfismo de grupos. Más aún, notemos que

$$\begin{aligned} f([a]_{nm}[b]_{nm}) &= f([ab]_{nm}) \\ &= ([ab]_n, [ab]_m) \\ &= ([a]_n[b]_n, [a]_m[b]_m) \\ &= ([a]_n, [a]_m)([b]_n, [b]_m) \\ &= f([a]_{nm})f([b]_{nm}), \end{aligned}$$

por lo que ¡f es un isomorfismo de anillos!

Supongamos que $[a]_{mn} \in (\mathbb{Z}/nm\mathbb{Z})^\times$ y sea $b \in \mathbb{Z}$ tal que $[ab]_{nm} = [1]_{nm}$, entonces (similar a la prueba de que f está bien definida) $[ab]_n = [1]_n$ y $[ab]_m = [1]_m$, de modo que $f([a]_{nm}) \in (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times$. De este modo, la restricción de f a $(\mathbb{Z}/nm\mathbb{Z})^\times$ nos da una función

$$g : (\mathbb{Z}/nm\mathbb{Z})^\times \to (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times.$$

Dado que f es un homomorfismo de anillos, entonces g es un homomorfismo de grupos. Como f es inyectiva, g también es inyectiva. Sin embargo aquí no sabemos si los órdenes de los grupos de salida

y llegada son los mismos, por lo que nos vemos en la obligación de probar que g es sobreyectiva. Sea $([b]_n, [c]_m) \in (\mathbb{Z}/n\mathbb{Z})^\times \times (\mathbb{Z}/m\mathbb{Z})^\times$, como f es sobreyectiva, existe $a \in \mathbb{Z}$ tal que $f([a]_{nm}) = ([b]_n, [c]_m)$. Similarmente, existe $a' \in \mathbb{Z}$ tal que $f([a']_{nm}) = ([b]_n^{-1}, [c]_m^{-1}) = ([b]_n, [c]_m)^{-1}$, y entonces tenemos

$$f([a]_{nm}[a']_{nm}) = f([a]_{nm}(f([a']_{nm}) = ([b]_n, [c]_m)([b]_n, [c]_m)^{-1} = 1,$$

de donde, como f es inyectiva, $[a]_{nm}[a']_{nm} = [1]_{nm}$, lo que implica que $[a]_{nm} \in (\mathbb{Z}/nm\mathbb{Z})^\times$, y por lo tanto $g([a]_{nm}) = ([b]_n, [c]_m)$, lo que prueba que g es sobreyectiva. □

Proposición A.32. *La función φ de Euler verifica las siguientes propiedades:*

(1) $\varphi(p) = p - 1$ *para todo número primo p.*

(2) *Si p es un número primo y $n \geq 1$ es un entero, entonces*

$$\varphi(p^n) = p^{n-1}(p-1) = p^n\left(1 - \frac{1}{p}\right).$$

(3) *Si a, b son coprimos, entonces $\varphi(ab) = \varphi(a)\varphi(b)$.*

Demostración. (1) es evidente del hecho de que $(\mathbb{Z}/p\mathbb{Z})^\times = \mathbb{Z}/p\mathbb{Z} \setminus \{0\}$. Ahora, notemos que el único divisor de p^n distinto de 1 es p, y por ende, para todo número entero a tenemos que $(a, p^n) = 1$ o $p \mid (a, p^n)$. Pero $p \mid (a, p^n)$ si y sólo si $p \mid a$, de modo que

$$\begin{aligned}(\mathbb{Z}/p^n\mathbb{Z})^\times &= \{[a] \in \mathbb{Z}/p^n\mathbb{Z} \,|\, p \nmid a\} \\ &= \mathbb{Z}/p^n\mathbb{Z} \setminus \{[a] \in \mathbb{Z}/p^n\mathbb{Z} \,|\, 0 \leq a < p^n \text{ y } p \mid a\}.\end{aligned}$$

Notemos que los múltiplos de p menores o iguales a p^n son $0, 1p, 2p, \cdots p^{n-1}p$ y por lo tanto

$$|\{[a] \in \mathbb{Z}/p^n\mathbb{Z} \,|\, 0 \leq a < p^n \text{ y } p \mid a\}| = p^{n-1},$$

de modo que

$$\varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1) = p^n\left(1 - \frac{1}{p}\right).$$

Esto prueba (2).

Por el teorema anterior, tenemos que si $(a, b) = 1$, entonces

$$\varphi(ab) = |(\mathbb{Z}/ab\mathbb{Z})^\times| = |(\mathbb{Z}/a\mathbb{Z})^\times \times (\mathbb{Z}/b\mathbb{Z})^\times| = |(\mathbb{Z}/a\mathbb{Z})^\times||(\mathbb{Z}/b\mathbb{Z})^\times| = \varphi(a)\varphi(b).$$

Esto completa la demostración. □

Teorema A.33 (Fórmula de Euler)**.** *Sea $a \in \mathbb{Z}$, con $a > 0$, entonces*

$$\varphi(a) = a \prod_{\substack{p \in P \\ p \mid a}} \left(1 - \frac{1}{p}\right),$$

donde, como es usual, P denota el conjunto de todos los números primos positivos.

Demostración. Por el teorema fundamental de la aritmética podemos escribir

$$a = p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}$$

donde $p_1, \ldots, p_k$ son primos distintos y $n_1, \ldots, n_k \geq 1$ son enteros. De este modo, por la proposición anterior, parte (3), tenemos que

$$\varphi(a) = \varphi(p_1^{n_1})\varphi(p_2^{n_2}) \cdots \varphi(p_k^{n_k}),$$

y usando la parte (2) de la proposición, obtenemos

$$\begin{aligned}
\varphi(a) &= p_1^{n_1}\left(1 - \frac{1}{p_1}\right) p_2^{n_2}\left(1 - \frac{1}{p_2}\right) \cdots p_k^{n_k}\left(1 - \frac{1}{p_k}\right) \\
&= p_1^{n_1} p_2^{n_2} \cdots p_k^{n_k}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right) \\
&= a \prod_{j=1}^{k} \left(1 - \frac{1}{p_j}\right).
\end{aligned}$$

Notemos que $p_1, \ldots, p_k$ son precisamente todos los números primos que dividen a a, de modo que

$$\varphi(a) = a \prod_{\substack{p \in P \\ p \mid a}} \left(1 - \frac{1}{p}\right),$$

como se deseaba. □