Capítulo 3

El anillo de los números enteros

3.1 Introducción: anillos e ideales

Anillos y cuerpos

Un anillo es un conjunto con dos operaciones binarias internas, llamadas *suma* y *producto*, que satisfacen ciertas propiedades:

Anillo

Un **anillo** es una terna $(R, +, \cdot)$ donde R es un conjunto y $+$ y $\cdot$ son operaciones internas binarias sobre R, llamadas *suma* y *producto* respectivamente, tales que se satisfacen las siguientes propiedades:

1. El par $(R, +)$ es un grupo abeliano, cuyo elemento neutro llamaremos "cero" y lo notaremos por 0.
2. La operación $\cdot$ es *asociativa*: $\forall a, b, c \in R$ es $a \cdot (b \cdot c) = (a \cdot b) \cdot c$.
3. La operación $\cdot$ es *distributiva* a derecha y a izquierda respecto de $+$, es decir: $\forall a, b, c \in R$

$$a \cdot (b + c) = a \cdot b + a \cdot c \text{ y } (a + b) \cdot c = a \cdot c + b \cdot c.$$

4. La operación $\cdot$ tiene un elemento neutro, que llamaremos "uno" y lo notaremos por 1: $1 \cdot a = a = a \cdot 1$ para todo $a \in R$.

UNIVERSIDAD DE SEVILLA

Conmutatividad de la suma y elemento 1

Es un hecho curioso y poco conocido que la conmutatividad del grupo aditivo $(R, +)$ es de hecho una consecuencia de la existencia de un elemento neutro para el producto, el elemento 1.
En efecto, dados $a, b \in R$, podemos desarrollar la expresión $(1 + 1) \cdot (a + b)$ de dos formas aplicando las propiedades distributivas a derecha y a izquierda:

$$(1 + 1) \cdot (a + b) = 1 \cdot (a + b) + 1 \cdot (a + b) = a + b + a + b,$$

$$(1 + 1) \cdot (a + b) = (1 + 1) \cdot a + (1 + 1) \cdot b = a + a + b + b.$$

De donde $a + b + a + b = a + a + b + b$. Sumando el opuesto de a a la izquierda y el opuesto de b a la derecha se tiene $b + a = a + b$. Por tanto, la existencia de "uno" implica que la operación $+$ es conmutativa.

Anillo conmutativo

Sea $(R, +, \cdot)$ un anillo. Si además la operación producto es *conmutativa* ($\forall a, b \in R \; a \cdot b = b \cdot a$) se dice que el anillo es **conmutativo**.

Notación por yuxtaposición

Como viene siendo habitual, en adelante notaremos la operación producto $\cdot$ mediante la yuxtaposición de los correspondientes elementos.
En adelante diremos "sea R un anillo" en lugar de "sea $(R, +, \cdot)$ un anillo", dando por conocidas la operación suma y producto siempre que no haya confusión.

Ejemplo 3.1.1.

1. Los conjuntos de números $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son anillos conmutativos. La estructura de anillo de $\mathbb{Z}$ viene determinada por su estructura de grupo, puesto que

UNIVERSIDAD DE SEVILLA

el producto de dos enteros xy es la suma del número y tantas veces como indique x, si $x \geq 0$ ($xy = y + \overset{x}{\cdots} + y$), o bien la suma del número $-y$ tantas veces como indique $-x$, si $x \leq 0$ ($xy = (-y) + \overset{-x}{\cdots} + (-y)$). Esto no ocurre para $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$, obviamente.

2. El conjunto $\mathscr{M}(n)$ de las matrices $n \times n$ sobre $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ o $\mathbb{C}$ es un anillo con respecto a la suma y al producto de matrices. Este anillo **no es conmutativo**.

3. Si A es un anillo conmutativo, el conjunto $A[x_1, \ldots, x_n]$ de los polinomios en n indeterminadas con coeficientes en A es también un anillo conmutativo.

Proposición 3.1.2. *En un anillo A se verifican las siguientes propiedades:*

1) $0 \cdot a = 0 = a \cdot 0$ *para todo* $a \in A$.

2) $(-1) \cdot a = -a = a \cdot (-1)$ *para todo* $a \in A$.

PRUEBA: 1) Como $0 \cdot a = (0+0) \cdot a = 0 \cdot a + 0 \cdot a$, deducimos que $0 \cdot a = 0$. La otra igualdad es análoga.

2) Como $0 = 0 \cdot a = (1 + (-1)) \cdot a = 1 \cdot a + (-1) \cdot a = a + (-1) \cdot a$, deducimos que $(-1) \cdot a = -a$. La otra igualdad es análoga. □

Anillo nulo

Un anillo R se dice que es *nulo* si tiene un único elemento, en cuyo caso $1 = 0$. Recíprocamente, si en un anillo R se tiene $1 = 0$, entonces R será un anillo nulo, pues para todo elemento $a \in R$ de verificará $a = 1 \cdot a = 0 \cdot a = 0$.

Unidades

Sea R un anillo. Se dice que un elemento $x \in R$ es una **unidad** en R si tiene un inverso multiplicativo, es decir, si existe un elemento $y \in R$ tal que $xy = yx = 1$. En tal caso, el elemento y es único y se llamará el *inverso* de x y de denotará por x^{-1}.
Notaremos por R^* al subconjunto de las unidades de R.

Ejemplo 3.1.3.

UNIVERSIDAD DE SEVILLA

1. Las unidades de $\mathbb{Z}$ son 1 y -1, es decir, $\mathbb{Z}^* = \{1, -1\}$. Sin embargo $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$ y $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$.

2. Las unidades de $\mathscr{M}(n)$ son las matrices invertibles.

3. Sea $\mathbb{Q}[x]$ el anillo de polinomios en la indeterminada x con coeficientes racionales, entonces

$$\mathbb{Q}[x]^* = \mathbb{Q}^* = \mathbb{Q} \setminus \{0\}.$$

Proposición 3.1.4. *Si R es un anillo, el conjunto R^* de las unidades de R es un grupo para el producto del anillo.*

PRUEBA: El *elemento neutro* del producto es 1, que pertenece a R^* pues su inverso es él mismo. Si $x \in R^*$ su simétrico x^{-1} también pertenece a R^*, pues el *simétrico* de x^{-1} es el propio x. Si $x, y \in R^*$ entonces poseen inversos multiplicativos, pongamos x^{-1} e y^{-1} respectivamente, y se tiene que $y^{-1}x^{-1}$ es el inverso multiplicativo de xy, luego la operación producto es *interna* en R^*. Sabemos que el producto verifica la *propiedad asociativa* en todo R, en particular también será asociativo en R^*.

Por tanto $(R^*, \cdot)$ es grupo. □

Cuerpo

Un **cuerpo** es un anillo conmutativo R tal que $1 \neq 0$ y todo elemento distinto de cero es una unidad, i.e. $R^* = R \setminus \{0\}$.

Ejemplo 3.1.5. $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son cuerpos.

UNIVERSIDAD SEVILLA

Subanillos

Subanillo

Sea $(R, +, \cdot)$ un anillo y sea $S \subset R$ un subconjunto. Decimos que S es un **subanillo** de R si se verifican las siguientes propiedades:

(i) S es un subgrupo (aditivo) de $(R, +)$, es decir:

-) $0 \in S$.

-) Si $x, y \in S$, entonces $x - y \in S$.

(ii) $1 \in S$.

(iii) Si $x, y \in S$, entonces $x \cdot y \in S$.

Si S es un asubanillo de $(R, +, \cdot)$, entonces S es un anillo con las operaciones $+$ y $\cdot$.

Veamos algunos ejemplos.

Ejemplo 3.1.6.

1. $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ es una cadena de subanillos. De hecho $\mathbb{Q}$ y $\mathbb{R}$ son **subcuerpos** de $\mathbb{C}$ (cuerpos dentro de un cuerpo).

2. El subconjunto
$$S = \frac{1}{2} \cdot \mathbb{Z} = \left\{ \frac{m}{2} \mid m \in \mathbb{Z} \right\} \subset \mathbb{Q}$$
es un subgrupo aditivo de $\mathbb{Q}$, pero no es un subanillo al no ser cerrado para el producto, pues
$$\frac{1}{2} \cdot \frac{1}{2} = \frac{1}{4} \notin S.$$

3. El conjunto $\mathbb{Z}2 = \{2n \mid n \in \mathbb{Z}\} \subset \mathbb{Z}$ es un subgrupo aditivo de $\mathbb{Z}$ y es cerrado para el producto, pero no es subanillo porque $1 \notin \mathbb{Z}2$

UNIVERSIDAD DE SEVILLA

Homomorfismos de anillos

De manera análoga a lo que se hizo con los grupos, podemos introducir el concepto de homomorfismo de anillo, que será una aplicación compatible con la suma (homomorfismo de grupos) y con el producto.

Homomorfismo de anillos

Sean R y S dos anillos. Una aplicación $f\colon R \to S$ se dice que es un **homomorfismo de anillos** si para todo par de elementos $x, y \in R$ se verifica que

$$f(x+y) = f(x) + f(y),\ f(xy) = f(x)f(y) \text{ y } f(1_R) = 1_S.$$

Si f es un homomorfismo sobreyectivo se dice **epimorfismo**, si es un homomorfismo inyectivo se dice **monomorfismo** y si es un homomorfismo biyectivo se dice **isomorfismo**. Si existe un isomorfismo entre dos anillos R y S, se dice que ambos anillos son **isomorfos** y se escribe $R \cong S$.

Ejemplo 3.1.7.

1. La aplicación identidad de un anillo R, Id_R, es un isomomorfismo de anillos.

2. Si S es un subanillo del anillo R, entonces la inclusión $i : S \longrightarrow R$ es un homomorfismo de anillos. Como i es in yectiva, de hecho es un monomorfismo de anillos.

3. Sea R el conjunto de las matrices de la forma

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}, \text{ con } a, b \in \mathbb{R}.$$

   Es fácil comprobar que R es un subanillo del anillo de la matrices $\mathscr{M}_2(\mathbb{R})$ cuadradas de orden 2 con coeficientes en $\mathbb{R}$. Definamos la aplicación

$$\phi\colon R \to \mathbb{C}$$

   por la regla

$$\phi \begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a + ib \in \mathbb{C}.$$

UNIVERSIDAD SEVILLA

Se comprueba que ϕ es un homomorfismo, pues es compatible con el producto:

$$\phi\left(\begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix}\begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix}\right) = \phi\begin{pmatrix} a_1a_2 - b_1b_2 & a_1b_2 + a_2b_1 \\ -a_1b_2 - a_2b_1 & a_1a_2 - b_1b_2 \end{pmatrix} =$$

$$= a_1a_2 - b_1b_2 + i(a_1b_2 + a_2b_1) = (a_1 + ib_1)(a_2 + ib_2) =$$

$$= \phi\begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix}\phi\begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix},$$

con la suma:

$$\phi\left(\begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix}\right) = \phi\begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ -b_1 - b_2 & a_1 + a_2 \end{pmatrix} =$$

$$= a_1 + a_2 + i(b_1 + b_2) = (a_1 + ib_1) + (a_2 + ib_2) =$$

$$= \phi\begin{pmatrix} a_1 & b_1 \\ -b_1 & a_1 \end{pmatrix} + \phi\begin{pmatrix} a_2 & b_2 \\ -b_2 & a_2 \end{pmatrix},$$

y transforma la unidad de R en la unidad de $\mathbb{C}$:

$$\phi(I) = \phi\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1.$$

Es inmediato comprobar que ϕ es sobreyectiva. Para ver que es inyectiva, como ϕ es un homomorfismo de grupos, podemos calcular el $\mathrm{Ker}(\phi)$. En efecto,

$$\phi\begin{pmatrix} a & b \\ -b & a \end{pmatrix} = a + ib = 0 \Leftarrow a = 0 = b.$$

Luego

$$\mathrm{Ker}(\phi) = \left\{\begin{pmatrix} 0 & 0 \\ -0 & 0 \end{pmatrix}\right\}$$

y ϕ es inyectiva. Por tanto ϕ es un isomomorfismo de anillos y $R \cong \mathbb{C}$.

Núcleo e imagen de un homomorfismo

Sean R y S anillos conmutativos. Sea $\phi\colon R \to S$ un homomorfirmos de anillos. Entonces $\mathrm{Im}(\phi)$ es un subanillo de S y $\mathrm{Ker}(\phi)$ sabemos que es un subgrupo aditivo de $(R, +)$ que además verifica la siguiente propiedad:

$$\forall x \in R,\ \forall y \in \mathrm{Ker}(\phi) \text{ se tiene } x \cdot y \in \mathrm{Ker}(\phi).$$

UNIVERSIDAD DE SEVILLA

PRUEBA: Sabemos que $\mathrm{Im}(\phi)$ es un subgrupo (aditivo) de $(S,+)$. Sean $y_1, y_2 \in \mathrm{Im}(\phi)$: existen $x_1, x_2 \in R$ tales que $\phi(x_1) = y_1$ y $\phi(x_2) = y_2$. Por ser ϕ homomorfismo $y_1y_2 = \phi(x_1)\phi(x_2) = \phi(x_1x_2)$, luego $y_1y_2 \in \mathrm{Im}(\phi)$. Además, $1_S = \phi(1_R) \in \mathrm{Im}(\phi)$. Por tanto, $\mathrm{Im}(\phi)$ es un subanillo de S.

Ya sabemos que $\mathrm{Ker}(\phi) \subset R$ es un subgrupo aditivo.

Sean $x \in R$ e $y \in \mathrm{Ker}(\phi)$. Entonces $\phi(xy) = \phi(x)\phi(y) = \phi(x)0 = 0$, luego $xy \in \mathrm{Ker}(\phi)$. □

Isomorfismo inverso

Si $\phi\colon R \to S$ es un isomorfismo de anillos, entonces también lo es $\phi^{-1}\colon S \to R$.

PRUEBA: Sabemos que ϕ^{-1} es isomorfismo de grupos aditivos. Veamos entonces que es compatible con el producto. Sean $y_1, y_2 \in S$, se verifica

$$\phi\left(\phi^{-1}(y_1y_2)\right) = y_1y_2,$$

$$\phi\left(\phi^{-1}(y_1)\phi^{-1}(y_2)\right) = \phi\left(\phi^{-1}(y_1)\right)\phi\left(\phi^{-1}(y_2)\right) = y_1y_2.$$

Luego $\phi\left(\phi^{-1}(y_1y_2)\right) = \phi\left(\phi^{-1}(y_1)\phi^{-1}(y_2)\right)$, como ϕ es inyectiva se sigue que $\phi^{-1}(y_1y_2) = \phi^{-1}(y_1)\phi^{-1}(y_2)$.

Además, $\phi^{-1}(1_S) = \phi^{-1}(\phi(1_R)) = 1_R$.

Por tanto ϕ^{-1} es isomorfismo de anillos. □

Ideales

Nota 3.1.8. **A partir de este momento, todos los anillos que consideremos serán conmutativos.**

Ideal de un anillo (conmutativo)

Sea $(R,+,\cdot)$ un anillo (conmutativo) y sea $I \subset R$ un subconjunto. Decimos que I es un ideal de R si I es un subgrupo de $(R,+)$ y para todo $x \in R, y \in I$ se verifica que $xy \in I$.

Veamos algunos ejemplos

Ejemplo 3.1.9.

1. Si R es un anillo conmutativo, los subgrupos triviales $\{0\}$ y R son ideales de R. Llamaremos **ideales propios** de R a los no triviales.

2. Un ideal I de un anillo R es el total, si y sólo si $1 \in I$.

3. Si $\phi : R \to S$ es un homomorfismo de anillos, entonces $\mathrm{Ker}(\phi)$ es un ideal de R.

4. Sea R un anillo conmutativo y $x \in R$ un elemento. Sea el subconjunto

$$Rx = \{rx \mid r \in R\}$$

de los "múltiplos" de x en R. Entonces Rx es un ideal de R, que llamaremos *el ideal de R generado por x*. Diremos que un ideal de este tipo es un **ideal principal**

5. Se demostrará más adelante (ver página 124) que los subgrupos de $(\mathbb{Z}, +)$ son de la forma $\mathbb{Z}n$ con $n \geq 0$ (nótese que $\mathbb{Z}n = \mathbb{Z}(-n)$). Por tanto cada $\mathbb{Z}n$ coincide con el ideal generado por n y por tanto también es un ideal de $\mathbb{Z}$. Así pues, todos los subgrupos de $(\mathbb{Z}, +)$ son ideales del anillo $\mathbb{Z}$.

   Esto es debido a que en el anillo $\mathbb{Z}$, el producto viene determinado por la suma.

6. Por otro lado, $\mathbb{Z}$ es un subanillo de $\mathbb{Q}$ pero no un ideal pues el elemento $\frac{1}{2} \cdot 1 \notin \mathbb{Z}$.

UNIVERSIDAD DE SEVILLA

Anillos cociente

El grupo R/I

Sean R un anillo (conmutativo) e I un ideal de R. Como el grupo $(R,+)$ es abeliano, el subgrupo I de $(R,+)$ es normal. Sabemos entonces (tema 2, grupos cocientes) que la operación

$$(x+I)+(y+I)=(x+y)+I\ \forall x,y\in R$$

está bien definida y dota de estructura de grupo (también abeliano) al cociente R/I.
Recordemos que el cociente de grupos viene definido por la relación de equivalencia en R

$$x_1\sim_I x_2 \iff x_1-x_2\in I.$$

Las clases de equivalencia de esta relación son los conjuntos $x+I$, luego

$$x_1+I=x_2+I\iff x_1-x_2\in I.$$

El producto en R/I

En el grupo cociente R/I la operación

$$(x+I)(y+I)=(xy)+I\ \forall x,y\in R$$

está bien definida.

PRUEBA: Sean $x_1,x_2,y_1,y_2\in R$ tales que $x_1+I=x_2+I$ y $y_1+I=y_2+I$, tenemos que probar que la operación no depende de los representantes elegidos en cada clase, es decir, que $x_1y_1+I=x_2y_2+I$. Lo cual ocurre si y sólo si $x_1y_1-x_2y_2\in I$.

$$x_1y_1-x_2y_2=x_1y_1-x_2y_1+x_2y_1-x_2y_2=(x_1-x_2)y_1+x_2(y_1-y_2).$$

Como $x_1+I=x_2+I$, se tiene que $x_1-x_2\in I$. Al ser I ideal, también tenemos que $(x_1-x_2)y_1\in I$. Análogamente $x_2(y_1-y_2)\in I$. Luego $x_1y_1-x_2y_2\in I$. □

Una vez definidas las operaciones suma y producto, dejamos como ejercicio comprobar que $(R/I, +, \cdot)$ es un anillo conmutativo. Nótese el elemento cero de R/I es la clase $0 + I = I$ y que el elemento uno de R/I es la clase $1 + I$.

Anillo cociente

Sean $(R, +, \cdot)$ un anillo conmutativo e $I \subset R$ un ideal. Entonces el conjunto cociente R/I con las operaciones $+$ y $\cdot$ previamente definidas es de nuevo un anillo conmutativo, que llamaremos *anillo cociente* de R por I.

Nota 3.1.10. Si I es un ideal del anillo R, la proyección natural $p : R \longrightarrow R/I$ es un epimorfismo de anillos cuyo núcleo es el ideal I.

Potr otro lado, nótese que el anillo cociente R/I es nulo si y sólo si $I = R$.

Ejemplo 3.1.11.

1. En el anillo $\mathbb{Z}$ los ideales $\mathbb{Z}n$ con $n \geq 1$ producen anillos cocientes finitos de n elementos:

$$\frac{\mathbb{Z}}{\mathbb{Z}n} = \{0 + \mathbb{Z}n, 1 + \mathbb{Z}n, \ldots, (n-1) + \mathbb{Z}n\} = \left\{\overline{0}, \overline{1}, \ldots, \overline{n-1}\right\}.$$

2. Para $n = 2$, estas son las tablas de las operaciones en $\frac{\mathbb{Z}}{\mathbb{Z}2}$:

$+$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$

$\cdot$	$\overline{0}$	$\overline{1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$

Por tanto comprobamos que $\frac{\mathbb{Z}}{\mathbb{Z}2}$ es un cuerpo.

3. Para $n = 3$, estas son las tablas de las operaciones en $\frac{\mathbb{Z}}{\mathbb{Z}3}$:

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{0}$	$\overline{1}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{1}$

Por tanto comprobamos que $\frac{\mathbb{Z}}{\mathbb{Z}3}$ es un cuerpo (todos sus elementos no nulos son unidades).

UNIVERSIDAD SEVILLA

4. En el anillo $R = \mathbb{Q}[x]$ de los polinomios en la indeterminada x con coeficientes racionales, consideramos el ideal $I = \mathbb{Q}[x] \cdot (x^2 - 2)$.

   Dado que $x^2 + I = 2 + I$, es fácil comprobar que en cada clase del conjunto cociente R/I podemos encontrar un representante de grado menor o igual que 1, de donde

$$\frac{\mathbb{Q}[x]}{\mathbb{Q}[x] \cdot (x^2 - 2)} = \{(ax + b) + I \mid a, b \in \mathbb{Q}\}.$$

   Además, cada elemento no nulo $(ax + b) + I$ posee un inverso multiplicativo, luego el anillo cociente R/I es un cuerpo. Dejamos como ejercicio la demostración de este hecho.

Factorización canónica

Hay un teorema de factorización canónica para homomorfismos de anillos.

Factorización canónica

Todo homomorfismo de anillos conmutativos, $f\colon R \to S$, factoriza de manera única como la composición $f = i \circ \bar{f} \circ p$:

$$\begin{array}{ccc} R & \xrightarrow{\ f\ } & S \\ {\scriptstyle p}\downarrow & & \uparrow{\scriptstyle i} \\ R/\operatorname{Ker}(f) & \xrightarrow[\bar{f}]{\cong} & \operatorname{Im}(f) \end{array}$$

donde p es la proyección natural (que es un epimorfismo de anillos), i es la inclusión (que es un monomorfismo de anillos), y $\bar{f}$ es un isomorfismo de anillos.

PRUEBA: La factorización es la misma que la de una aplicación cualquiera. Ya sabemos que p e i son homomorfismos de anillos. Sabemos también que p es sobreyectiva, i es inyectiva y que $\bar{f}$, definida por $\bar{f}(x + \operatorname{Ker}(f)) = f(x)$, es biyectiva. Por último, también sabemos que $\bar{f}$ es un homomorfismo de grupos aditivos. Es evidente que $\bar{f}(1_{R/\operatorname{Ker}(f)}) = \bar{f}(1_R + \operatorname{Ker}(f)) = f(1_R) = 1_S$. Falta ver que $\bar{f}$ es compatible con el producto. Por comodidad, llamaremos $I = \operatorname{Ker}(f)$.

Al ser f un homomorfismo de anillos se tiene:

$$\begin{aligned}\bar{f}((x_1+I)(x_2+I)) &= \bar{f}((x_1x_2)+I)\\ &= f(x_1x_2)\\ &= f(x_1)f(x_2)\\ &= \bar{f}(x_1+I)\bar{f}(x_2+I).\end{aligned}$$

Luego $\bar{f}$ es también un homomorfismo de anillos. □

Corolario 3.1.12. *Si $f\colon R \to S$ es un epimorfismo de anillos entonces la aplicación $\bar{f}\colon R/\operatorname{Ker}(f) \to S$ es un isomorfismo.*

Corolario 3.1.13. *Si $f\colon R \to S$ es un monomorfismo de anillos entonces $\bar{f}\colon R \to \operatorname{Im}(f)$ es un isomorfismo.*

Divisores de cero. Dominios de integridad

Ejemplo 3.1.14. Estudiemos el anillo cociente $\frac{\mathbb{Z}}{\mathbb{Z}4}$. Las tablas de sus operaciones son:

+	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

·	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{0}$	$\overline{2}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

.

Observamos pues que las unidades de $\frac{\mathbb{Z}}{\mathbb{Z}4}$ son $\overline{1}$ y $\overline{3}$. Observamos también que, aún siendo $\overline{2} \neq \overline{0}$, se tiene que $\overline{2}\cdot\overline{2} = \overline{0}$.

Divisor de cero

Sea R un anillo (conmutativo). Se dice que un elemento $x \in R$ es un **divisor de cero** si existe un elemento no nulo $y \in R$ tal que $xy = 0$.

En un anillo no nulo, el 0 siempre es un divisor de cero, pues $1 \cdot 0 = 0$.

UNIVERSIDAD DE SEVILLA

Ejemplo 3.1.15. En el anillo $\mathbb{Z}/\mathbb{Z}4$, el elemento $2+\mathbb{Z}4$ es un divisor de cero, pues $(2+\mathbb{Z}4)(2+\mathbb{Z}4) = 0+\mathbb{Z}4$.

Asimismo, en el anillo $\mathbb{Z}/\mathbb{Z}6$ el elemento $2+\mathbb{Z}6$ es un divisor de cero, pues

$$(2+\mathbb{Z}6)(3+\mathbb{Z}6) = 6+\mathbb{Z}6 = 0+\mathbb{Z}6.$$

Dominio de Integridad

Un **dominio de integridad** (DDI) es un anillo conmutativo no nulo ($1 \neq 0$) cuyo único divisor de cero es el 0.

Proposición 3.1.16. *Sea R un anillo no nulo. Las siguientes propiedades son equivalentes:*

(a) R es un DDI.

(b) Si $r, s \in R$, $rs = 0 \Longrightarrow r = 0$ ó $s = 0$.

Ejemplo 3.1.17.

1. Los anillos $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$ son dominios de integridad.
2. Los anillos cociente $\mathbb{Z}/\mathbb{Z}n$ con $n > 0$ son dominio de integridad si y sólo si n es un número primo[1].

Dominio de integridad y propiedad cancelativa

Sea R un anillo conmutativo. Entonces R es un dominio de integridad si y sólo si se satisface en R la *propiedad cancelativa*, es decir,

$$xy = xz \wedge x \neq 0 \Rightarrow y = z.$$

PRUEBA: Si R es un dominio de integridad, supongamos que $xy = xz$ con $x \neq 0$. Entonces

$$xy = xz \Rightarrow xy - xz = 0 \Rightarrow x(y-z) = 0 \overset{x\neq 0}{\Longrightarrow} y - z = 0 \Rightarrow y = z.$$

[1]Esto se demostrará más adelante.

UNIVERSIDAD SEVILLA

Recíprocamente, si se verifica la propiedad cancelativa, sea $x \in R$, $x \neq 0$ tal que existe $y \in R$ con $xy = 0$. Entonces

$$0 = xy = x0 \Rightarrow y = 0.$$

Luego R no tiene divisores de cero. □

Proposición 3.1.18. *Todo dominio de integridad finito es un cuerpo.*

PRUEBA: Sea R un dominio de integridad finito, sea $x \in R$ un elemento no nulo. Vamos a probar que x es una unidad.

Consideremos la aplicación $f\colon R \to R$ dada por $f(y) = xy$.

Veamos que f es inyectiva. Si $f(y) = f(z)$ entonces $xy = xz$. por la propiedad cancelativa $y = z$. Luego f es inyectiva.

Como R es finito cualquier aplicación inyectiva $f\colon R \to R$ es también sobreyectiva (y por tanto biyectiva). Así que existe $y \in R$ tal que $f(y) = 1$. Es decir,

$$xy = f(y) = 1.$$

Luego todo elemento no nulo $x \in R$ tiene inverso multiplicativo. Por tanto R es un cuerpo. □

Ejemplo 3.1.19. Si $p \in Z$ es primo, el anillo $\mathbb{Z}/\mathbb{Z}p$ es un dominio de integridad, pues dados $\overline{m}, \overline{n} \in \mathbb{Z}/\mathbb{Z}p$, si $\overline{m} \cdots \overline{n} = \overline{0}$, entonces $\overline{mn} = \overline{0}$ y por tanto $mn \in \mathbb{Z}p$. Ahora bien, si el número primo p divide a mn, tiene que dividir a m o a n y por tanto $\overline{m} = \overline{0}$ ó $\overline{n} = \overline{0}$. Como $\mathbb{Z}/\mathbb{Z}p$ es finito, deducimos que es un cuerpo.

Cuerpos finitos

En adelante notaremos por $\mathbb{F}_p$ al cuerpo $\mathbb{Z}/\mathbb{Z}p$, con p número primo.

Proposición 3.1.20. *Sea R un anillo conmutativo. Entonces el conjunto de las* no unidades *de R ($R \setminus R^*$) es igual a la unión de todos los* ideales propios *de R.*

PRUEBA: Si x no es una unidad en R entonces $Rx = \{yx \mid y \in R\}$ es un ideal propio de R que contiene a x, pues $1 \notin Rx$.

Recíprocamente, si una unidad $y \in R$ perteneciera a un ideal $I \subset R$ entonces para cualquier $x \in R$ tendríamos que $x = (xy^{-1})y \in I$, de donde $I = R$. Luego ninguna unidad puede pertenecer a un ideal propio de R. □

Acabamos de demostrar lo siguiente:

UNIVERSIDAD DE SEVILLA

Corolario 3.1.21. *Si un ideal $I \subset R$ contiene una unidad en R entonces $I = R$.*

Corolario 3.1.22. *Un anillo conmutativo no nulo es un cuerpo si y sólo si no tiene ideales propios no nulos.*

Ideales primos y maximales

Ideal maximal

Sea R un anillo (conmutativo). Decimos que un ideal propio $I \subset R$, $I \neq R$, es **maximal** si los únicos ideales que lo contienen son el propio I y R.

Ejemplo 3.1.23. El ideal $\mathbb{Z}p \subset \mathbb{Z}$ con p primo es un ideal maximal. En efecto, si $I \subset \mathbb{Z}$ es un ideal tal que $\mathbb{Z}p \subset I$, como sabemos que I ha de ser de la forma $\mathbb{Z}n$ para algún natural n, se tendrá que $\mathbb{Z}p \subset \mathbb{Z}n$, lo que implica que $p \in \mathbb{Z}n$, es decir, que n divide a p. Como p es primo, o bien $n = 1$, en cuyo caso $I = \mathbb{Z}n = \mathbb{Z}$, o bien $n = p$, en cuyo caso $I = \mathbb{Z}_n = Zp$.

Otra manera de probar lo anterior es la siguiente: si $I \subset \mathbb{Z}$ es un ideal con $I \neq \mathbb{Z}$ tal que $\mathbb{Z}p \subset I$, entonces la aplicación

$$\begin{array}{rccc} f\colon & \mathbb{F}_p = \mathbb{Z}/\mathbb{Z}p & \to & \mathbb{Z}/I \\ & n + I & \mapsto & f(n + \mathbb{Z}p) = n + I \end{array}$$

está bien definida y es un homomorfismo sobreyectivo de grupos (es un epimorfismo). Entonces $|\mathbb{Z}/\mathbb{Z}p| = |\mathbb{Z}/I||\operatorname{Ker}(f)|$, y como $\operatorname{Ker}(f) \neq \mathbb{F}_p$ (porque $f(1 + \mathbb{Z}p) = 1 + I \neq 0 + I$), se debe tener $|, \operatorname{Ker}(f)| = 1$, o lo que es lo mismo, $\operatorname{Ker}(f) = \{0\}$, de donde f también es inyectiva (y por tanto biyectiva), lo que implica que $I = \mathbb{Z}p$.

Ideal primo

Sea R un anillo (conmutativo). Decimos que un ideal propio I de R es un **ideal primo** si satisface la siguiente propiedad:

$$x, y \in R,\ xy \in I \Rightarrow x \in I \text{ ó } y \in I.$$

UNIVERSIDAD SEVILLA

Proposición 3.1.24. *Sea R un anillo. Las propiedades siguientes son equivalentes:*

(a) R es un DDI.

(b) El ideal $\{0\}$ de R es un ideal primo.

Asimismo, las propiedades siguientes también son equivalentes:

(a') R es un cuerpo.

(b') El ideal $\{0\}$ de R es un ideal maximal.

Proposición 3.1.25. *Sean R un anillo conmutativo e $I \subset R$ un ideal propio de R. Entonces:*

1. *I es un ideal primo de R si y sólo si el anillo R/I es un dominio de integridad.*

2. *I es un ideal maximal de R si y solo si el anillo R/I es un cuerpo.*

PRUEBA:

1. Supongamos que I es un ideal primo. Sean $x, y \in R$ tales que $(x+I)(y+I) = 0+I$, entonces

$$0+I = (x+I)(y+I) = xy+I \Leftrightarrow xy \in I \Rightarrow x \in I \ \vee \ y \in I \Rightarrow$$

$$\Rightarrow x+I = 0+I \ \vee \ y+I = 0+I.$$

   Luego R/I no tiene divisores de cero.

   Recíprocamente, si R/I es un dominio de integridad, sean $x, y \in R$ tales que $xy \in I$. Entonces:

$$xy \in I \Rightarrow 0+I = xy+I = (x+I)(y+I) \Rightarrow x+I = 0+I \vee y+I = 0+I \Rightarrow$$

$$\Rightarrow x \in I \ \vee \ y \in I.$$

   Luego I es un ideal primo.

2. Supongamos que $I \subset R$ es un ideal maximal. Sea la proyección $p\colon R \to R/I$ dada por $p(x) = x+I$, que sabemos que es un homomorfismo de anillos. Si $J \subset R/I$ es un ideal, dejamos como ejercicio comprobar que $p^{-1}(J)$ es un ideal de R que contiene a I, luego debe ser $p^{-1}(J) = I$ o $p^{-1}(J) = R$. En el primer caso $J = \{0+I\}$ y en el segundo $J = R/I$.

UNIVERSIDAD DE SEVILLA

Luego los únicos ideales de R/I son los triviales y, por tanto, R/I es un cuerpo.

Recíprocamente, si R/I es un cuerpo sea $J \subset R$ un ideal tal que $I \subsetneq J$. Sea $x \in J \backslash I$, como $x \notin I$ entonces $x+I \neq 0+I$ y $x+I$ tiene un inverso en R/I. Sea $y \in R$ tal que $(x+I)(y+I) = 1+I$. Como $(x+I)(y+I) = xy+I$, se tiene que $1 \in xy+I \subset J$. Luego $J = R$ concluyendo que I es maximal.

□

Como todo cuerpo es dominio de integridad (porque toda unidad no es divisor de cero), tenemos el siguiente corolario.

Corolario 3.1.26. *Todo ideal maximal de un anillo conmutativo (no nulo) es un ideal primo.*

El recíproco no es cierto.

Ejemplo 3.1.27. Sea $R = \mathbb{Q}[x, y]$ el anillo de polinomios en dos variables con coeficientes racionales. Sea el ideal $I = Rx$ de los polinomios que son múltiplos de x. El ideal I no es máximal, pues está contenido en el ideal

$$J = \{g(x, y) \in R \mid \text{el término independiente de } g(x, y) \text{ es nulo}\}.$$

Veamos que I es un ideal primo que no es maximal.

Consideremos la aplicación $\phi\colon R \to \mathbb{Q}[y]$ dada por $\phi(f(x, y)) = f(0, y)$. Se comprueba fácilmente que $\phi(f + g) = \phi(f) + \phi(g)$, $\phi(fg) = \phi(f)\phi(g)$ y que $\phi(1) = 1$. Además ϕ es sobreyectiva. Luego ϕ es un homomorfismo sobreyectivo de anillos.

Como $f(0, y) = 0$ si y sólo si $f(x, y)$ es un múltiplo de x, se tiene que $\mathrm{Ker}(\phi) = I$. Por el corolario 3.1.12 es $R/I \cong \mathbb{Q}[y]$. Como $\mathbb{Q}[y]$ es un dominio de integridad que no es un cuerpo, I es ideal primo que no es maximal.

La característica de un dominio de integridad

Proposición 3.1.28. *Sea R un dominio de integridad y sea $S = \langle 1 \rangle$ el subgrupo aditivo de R generado por 1. Si S es un grupo finito de orden p entonces p es primo y $px = x + \overset{p}{\cdots} + x = 0$ para todo $x \in R$*

PRUEBA: Supongamos que $p = p_1p_2$. Como el orden de 1 es p, se tiene que

$$0 = p1 = (p_1p_2)1 = (p_11)(p_21).$$

Al ser R un dominio de integridad, debe ser $p_11 = 0$ o $p_21 = 0$, en cuyo caso p, el orden de 1, divide a p_1 o a p_2. Luego de los dos factores de p uno es él mismo y el otro 1. Es decir, p es primo.

UNIVERSIDAD SEVILLA

Por otro lado, si $x \in R$, se tiene

$$px = (p1)x = (1+ \overset{p}{\cdots} +1)x = 0x = 0.$$

□

Característica de un dominio de integridad

Sea R un dominio de integridad. Si el orden de $S = \langle 1 \rangle$ es un número primo $p > 0$, diremos que R tiene **característica** p. Si por el contrario el orden de 1 es infinito diremos R tiene **característica** 0.

Ejemplo 3.1.29. $\mathbb{F}_p$ y $\mathbb{F}_p[x]$ tienen característica p. Sin embargo $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{R}[x]$ tienen característica 0.

Dominios de integridad finitos

Si R es un dominio de integridad finito entonces existe un primo $p > 0$ tal que R tiene característica p. El recíproco no es cierto, existen dominios de integridad infinitos con característica positiva, por ejemplo $\mathbb{F}_p[x]$.

3.2 Divisibilidad en $\mathbb{Z}$

Hemos visto que el conjunto $\mathbb{Z}$ de los números enteros, con la suma y el producto, es un dominio de integridad. Aunque esta estructura esté fuertemente ligada a la de grupo con la suma. Enunciamos a continuación una propiedad de los números enteros que usaremos más adelante:

Principio de la buena ordenación

Todo subconjunto no vacío de $\mathbb{Z}$ acotado inferiormente posee un mínimo.

Desarrollamos brevemente la teoría clásica de la divisibilidad sobre los números enteros.

UNIVERSIDAD DE SEVILLA

Divisibilidad

Sean a, b dos enteros. Se dirá que a **divide a** b si existe $c \in \mathbb{Z}$ tal que $ac = b$. En este caso se escribe $a|b$. También se dice que b es **divisible** por a.

Nota 3.2.1. Dos elementos especiales de $\mathbb{Z}$ son 1 y -1. Para empezar, obviamente dividen a todos los números enteros. Pero además son los únicos enteros con esta propiedad.

Supongamos que $a \in \mathbb{Z}$ es otro entero con esta propiedad. Entonces debe dividir a 1, luego existe b tal que $ab = 1$. Entonces, o bien a, b son positivos o son negativos. Si son negativos, se pone $(-a)(-b) = 1$, con lo que se puede suponer que ambos son positivos.

En este caso, si fuese a ó b mayor que 1 (por ejemplo a), sería $a > 1$ y $b > 0$ (luego $b \geq 1$) sería $ab > 1 \cdot b = b \geq 1$, luego $ab > 1$, lo que no puede ser. Así, $a = b = 1$, luego desde el principio $a = \pm 1$, $b = \pm 1$.

Recordemos que 1 y -1 son las unidades del anillo $\mathbb{Z}$.

Propiedades de la relación de divisibilidad

1. Propiedad reflexiva: $a|a$. En efecto, $a = 1 \cdot a$.
2. Propiedad transitiva: Si $a|b$ y $b|c$ entonces $a|c$. En efecto, existen d, d' tales que $b = ad$ y $c = bd'$, luego $c = add'$ lo que implica que $a|c$.
3. Si $a|b$ y $b|a$ entonces $a = \pm b$. En efecto, existen c, c' tales que $b = ac$ y $a = bc'$. Así $a = acc'$, luego $a - acc' = a(1 - cc') = 0$. Si $a = 0$ entonces $b = 0$, si no por definición de divisibilidad, es $1 - cc' = 0$ luego $cc' = 1$, de donde $c' = \pm 1$ y así $a = \pm b$.

Por consiguiente, si nos restringimos a enteros positivos, la divisibilidad es una relación de orden parcial porque la propiedad 3) anterior es la propiedad antisimétrica: $a|b$ y $b|a \Longrightarrow a = b$.

UNIVERSIDAD SEVILLA

La divisibilidad es compatible con las operaciones aritméticas

En concreto:

1. Si $a|b$ y $a|c$ entonces $a|(b \pm c)$. En efecto, existen $d, d' \in \mathbb{Z}$ tales que $b = ad$ y $c = ad'$. Así

$$b \pm c = ad \pm ad' = a(d \pm d')\,,$$

luego $a|(b \pm c)$.

2. Si $a|b$ entonces $a|bc$, $\forall c \in \mathbb{Z}$. En efecto, existe $d \in \mathbb{Z}$ tal que $b = ad$. Así $bc = adc$, luego $a|bc$.

Veamos ahora uno de los resultados más importantes de este tema:

División euclídea

Sean $a, b \in \mathbb{Z}$, $b \neq 0$. Existen unos enteros únicos $q, r \in \mathbb{Z}$ tales que:

1. $a = qb + r$
2. $0 \leq r < |b|$

Al entero q se le llama el **cociente** de la división y a r el **resto**.

PRUEBA: La existencia se puede demostrar usando el principio de buena ordenación. En efecto: sea $S = \{a - bx \mid x \in \mathbb{Z} \text{ y } a - bx \geq 0\}$. S es no vacío y está acotado inferiormente, luego posee un mínimo. Sea $r = a - bq \geq 0$ dicho mínimo. Falta ver que $r < |b|$. En caso contrario, $r = |b| + r'$, $0 \leq r' < r$. Sustituyendo se tiene que $r' = a - b(q \pm 1) \in S$, en contra de ser r el mínimo.

Probemos ahora la unicidad. Supongamos que existen $q', r' \in \mathbb{Z}$ tales que $a = q'b + r', 0 \leq r < |b|$. Si $q \geq q'$, restando obtenemos que $0 \leq (q - q')b = r' - r < |b|$, igualdad que sólo se puede dar si $q = q'$ y $r = r'$. □

Podemos dar una nueva definición de divisibilidad

Divisibilidad y resto

Sean a, b dos enteros, $b \neq 0$. Se dirá que b divide a a si el resto de la división de a por b es cero.

Ahora ya estamos en condiciones de demostrar que todos los subgrupos de $\mathbb{Z}$ son los *ideales principales* $\mathbb{Z}m$ con $m \in \mathbb{Z}$.

Subgrupos de $\mathbb{Z}$

Sea $H \subset \mathbb{Z}$ un subgrupo, existe $m \in \mathbb{Z}$, $m \geq 0$, tal que $H = \mathbb{Z}m$.

PRUEBA: Si $H = \{0\}$ entonces $H = \mathbb{Z}0$.

Si $H \neq \{0\}$, sea $m \in H$ el mínimo de los elementos de H mayores que 0. Veamos que todo elemento de H es un múltiplo de m.

Sea $n \in H$, dividiendo n entre m

$$n = qm + r \text{ con } 0 \leq r < m.$$

Como $r = n - qm$ y $n, m \in H$, entonces $r \in H$. Pero m es el mínimo entero positivo que pertenece H, luego debe ser $r = 0$ y, por tanto, $n = qm \in \mathbb{Z}m$. Es decir, $H \subset \mathbb{Z}m$.

Por otro lado, como $m \in H$, es evidente que $\mathbb{Z}m \subset H$.

Concluyendo que $H = \mathbb{Z}m$, □

Máximo común divisor

Dados dos enteros a y b, diremos que d es **un máximo común divisor** de a y b y denotaremos $d = \textbf{mcd}(a, b)$, si se verifica:

1. $d|a$ y $d|b$.
2. Si d' es tal que $d'|a$ y $d'|b$ entonces $d'|d$.

Si 1 es un máximo común divisor de a y b, se dice que a y b son **primos entre sí**.

UNIVERSIDAD SEVILLA

Unicidad del máximo común divisor

Demostraremos más adelante la existencia de máximo común divisor para cualquier par de enteros a y b. Si d y d' son dos máximos comunes divisores de a y b, entonces debe verificarse que $d|d'$ y $d'|d$, luego $d' = \pm d$. Es decir, el máximo común divisor, si existe, **es único salvo el signo**.

Proposición 3.2.2. *Se verifican las siguientes propiedades:*

1. $\mathrm{mcd}(a, b) = b \Leftrightarrow b|a$.
2. $\mathrm{mcd}(a, b) = \mathrm{mcd}(-a, b) = \mathrm{mcd}(a, -b) = \mathrm{mcd}(-a, -b)$.
3. $\mathrm{mcd}(a, b) = \mathrm{mcd}(b, a)$.

Mínimo común múltiplo

Sean a y b enteros. Diremos que m es un **mínimo común múltiplo** de a y b y denotaremos $m = \mathbf{mcm}(a, b)$, si se verifica:

1. $a|m$ y $b|m$.
2. Si m' es tal que $a|m'$ y $b|m'$ entonces $m|m'$.

Unicidad del mínimo común múltiplo

También demostraremos más adelante la existencia de mínimo común múltiplo para cualquier par de enteros a y b. Si m y m' son dos mínimos comunes múltiplos de a y b, entonces debe verificarse que $m|m'$ y $m'|m$, luego $m' = \pm m$. Es decir, el mínimo común múltiplo, si existe, **es único salvo el signo**.

Proposición 3.2.3. *Se verifican las siguientes propiedades:*

1. $\mathrm{mcm}(a, b) = b \Leftrightarrow a|b$.
2. $\mathrm{mcm}(a, b) = \mathrm{mcm}(-a, b) = \mathrm{mcm}(a, -b) = \mathrm{mcm}(-a, -b)$.
3. $\mathrm{mcm}(a, b) = \mathrm{mcm}(b, a)$.

UNIVERSIDAD DE SEVILLA

3.3 Algoritmo de Euclides. Identidad de Bézout

Veamos un procedimiento, el algoritmo de Euclides, para el cálculo del máximo común divisor.

Proposición 3.3.1. *Sean $a, b \in \mathbb{Z}$ no nulos, pongamos $|a| \geq |b|$, y efectuemos la división euclídea $a = qb + r$. Entonces*

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

PRUEBA: Si $r = 0$ es $a = qb$, luego $\text{mcd}(a, b) = b = \text{mcd}(b, 0)$. Si $r \neq 0$, sean

$$d = \text{mcd}(a, b), \quad d' = \text{mcd}(b, r)\ ;$$

entonces $d|r = a - qb$, luego $d|d'$. Por otra parte, $d'|a = qb + r$, luego $d'|d$ y así $d' = \pm d$. □

Algoritmo de Euclides

El resultado anterior nos permite describir el **Algoritmo de Euclides:** Sean a, b enteros no nulos, pongamos $|a| \geq |b|$, y efectuemos la división euclídea $a = qb + r$. Como $r < |b|$, podemos dividir b entre r, y así sucesivamente, obteniendo:

$$\begin{array}{lcll} a & = & qb + r & 0 \leq r < |b| \\ b & = & q_0 r + r_1 & 0 \leq r_1 < r \\ r & = & q_1 r_1 + r_2 & 0 \leq r_2 < r_1 \\ r_1 & = & q_2 r_2 + r_3 & 0 \leq r_3 < r_2 \\ & \vdots & & \\ r_{n-1} & = & q_n r_n + r_{n+1} & 0 \leq r_{n+1} < r_n \\ r_n & = & q_{n+1} r_{n+1} + 0 & r_{n+2} = 0 \end{array}$$

Pues al ser los restos enteros mayores o iguales que cero cada vez más pequeños, debemos obtener alguno, r_{n+2}, que sea nulo.

Proposición 3.3.2. *En la situación anterior se tiene que $mcd(a, b) = r_{n+1}$. Es decir, el máximo común divisor de a y b es el último resto no nulo al aplicar sucesivamente el algoritmo de división.*

PRUEBA: Por la proposición anterior se tiene que:

$$\text{mcd}(a, b) = \text{mcd}(b, r) = \text{mcd}(r, r_1) = \cdots = \text{mcd}(r_{n-1}, r_n) =$$

UNIVERSIDAD DE SEVILLA

$$= \text{mcd}(r_n, r_{n+1}) = r_{n+1},$$

lo cual demuestra el resultado. □

Con este algoritmo hemos demostrado la existencia del máximo común divisor.

Existencia del máximo común divisor

Dados dos enteros no nulos a y b, existe el máximo común divisor de a y b, $\text{mcd}(a, b)$, que es único salvo el signo.

mcd(a, b) divide a $\gamma a + \delta b$

Sean a, b enteros y sea $d = \text{mcd}(a, b)$. Obsérvese que para cualesquiera enteros γ, δ se verifica que $\gamma a + \delta b$ es un múltiplo de d.

Asociada al máximo común divisor está la identidad de Bézout, cuya existencia teórica viene afirmada por el siguiente teorema:

Identidad de Bézout

Sean a, b enteros no nulos y sea $d = \text{mcd}(a, b)$. Existen enteros α, β tales que

$$\alpha a + \beta b = d.$$

PRUEBA: Demostramos la existencia de manera no constructiva. Sea el subgrupo de $\mathbb{Z}$ generado por a y b:

$$S = \langle a, b \rangle = \{n \in \mathbb{Z} \mid n = xa + yb,\ x, y \in \mathbb{Z}\}.$$

Sabemos (Subgrupos de $\mathbb{Z}$, página 124) que existe $n_0 > 0$ tal que $S = \mathbb{Z}n_0$. Vamos a demostrar que $n_0 = d$, lo haremos probando que $d|n_0$ y $n_0|d$.

Como $n_0 \in S$, existen $\alpha, \beta \in \mathbb{Z}$ tales que

$$n_0 = \alpha a + \beta b.$$

UNIVERSIDAD SEVILLA

Por definición $d|a$ y $d|b$ luego $d|n_0$.

Para ver que $n_0|d$, demostraremos que $n_0|a$ y $n_0|b$. Vamos a probar que $n_0|a$, la otra relación se prueba de forma análoga. Por la división euclídea podemos escribir $a = qn_0 + r$ con $0 \leq r < n_0$. Entonces,

$$r = a - qn_0 = a - q(\alpha a + \beta b) = (1 - q\alpha)a + (-q\beta)b.$$

Por la minimalidad de n_0 en $S = \mathbb{Z}n_0$ tiene que ser $r = 0$, luego $n_0|a$. □

No unicidad de la Identidad de Bézout

Los enteros α y β que aparecen en la identidad de Bézout no son únicos. En efecto: para cualesquiera α, β tales que $\alpha a + \beta b = d$, es

$$(\alpha - kb)a + (\beta + ka)b = d, \quad \forall k \in \mathbb{Z}\,.$$

La identidad de Bézout nos permite probar el siguiente teorema:

Teorema de Euclides

Sean a, b, c enteros tales que $c|ab$ y $\text{mcd}(c, a) = 1$; entonces $c|b$. En particular, si p es primo, $p|ab$ y p no divide a a, entonces $p|b$.

PRUEBA: Evidentemente, la segunda afirmación es consecuencia de la primera; demostremos ésta. Por la identidad de Bézout, $1 = \alpha a + \beta c$. Multiplicando por b esta expresión, se tiene que $b = \alpha ab + \beta cb$. Como $c|ab$ y $c|cb$, se tiene que $c|b$. □

Proposición 3.3.3. *Sean $a, b \in \mathbb{Z}$ no nulos,*

$$d = mcd(a, b), \quad a' = \frac{a}{d}, \quad b' = \frac{b}{d}\,.$$

Entonces a', b' son primos entre sí.

PRUEBA: Si a' y b' no son primos entre sí, entonces existe $d' \in \mathbb{Z}$, $\pm 1 \neq d'$, tal que $d'|a'$ y $d'|b'$. Luego $dd'|a'd = a$, $dd'|b'd = b$ y dd' no divide a d, lo que no es posible. □

Ahora podemos redefinir el mínimo común múltiplo usando el máximo común divisor.

UNIVERSIDAD DE SEVILLA

Proposición 3.3.4. *Sean $a, b \in \mathbb{Z}$ no nulos, $d = mcd(a, b)$. Se verifica que $mcm(a, b) = ab/d$.*

PRUEBA: Sean

$$m = ab/d, \quad a' = a/d, \quad b' = b/d.$$

Se tiene que $m = a'b = ab'$, luego es múltiplo de a y b. Sea $m' \in \mathbb{Z}$ múltiplo de a y b, $m' = aa'' = bb''$. Dividiendo esta última igualdad por d obtenemos $a'a'' = b'b''$ y, por el teorema de Euclides, $a'|b''$, es decir, $b'' = a'c$. Sustituyendo $m' = ba'c = mc$, luego m es el mínimo común múltiplo de a y b. □

Esto prueba la existencia del mínimo común múltiplo.

Existencia del mínimo común múltiplo

Dados dos enteros a, b, existe el mínimo común múltiplo de a y b, $\mathrm{mcm}(a, b)$, que es único salvo el signo.

Número primo

En todas estas notas llamamos números primos a aquellos enteros $p \neq 0, \pm 1$ que son divisibles únicamente por $\pm p$ y ± 1.

El siguiente resultado nos permitirá trabajar con los enteros a través de sus factores primos.

Teorema fundamental de la divisibilidad

Todo entero distinto de 0 y ± 1 se descompone en producto finito de números primos. Esta descomposición es única salvo orden y producto por ± 1.

PRUEBA: Vamos primero a demostrar la existencia de la descomposición. Sea $n \neq 0, \pm 1$ un entero fijo, y vamos a demostrar que n se descompone en producto de primos. Podemos suponer que $n > 0$ porque, si lo demostramos en este caso y

UNIVERSIDAD DE SEVILLA

$n = p_1 \cdots p_r$, entonces $-n = (-1) \cdot p_1 \cdots p_r$, lo que demuestra el resultado para los enteros negativos.

La existencia de la descomposición se prueba por inducción a partir de $n = 2$. El número $n = 2$ es primo. Supongamos que $n > 2$ y que todos los números menores que n se descomponen en producto finito de primos. Si n es primo hemos terminado: es producto de un primo (él mismo). Si no lo es, se descompone en producto $n = n_1 n_2$ de dos enteros positivos estrictamente menores que n. Al aplicar a n_1 y n_2 la hipótesis de inducción, vemos que n se descompone en producto finito de primos.

Para demostrar la unicidad (salvo orden y producto por unidades), basta considerar enteros positivos n por la misma razón que antes. Además, basta ver que no puede haber dos descomposiciones distintas de un mismo número positivo en producto de primos positivos. Vamos a operar por reducción al absurdo. Supongamos que hay números que admiten dos descomposiciones distintas en producto de primos positivos:

$$n = p_1 \cdots p_r = q_1 \cdots q_s.$$

Supongamos que $r \leq s$. Tenemos $p_1 | n = q_1 \cdots q_s$, luego $p_1 | q_i$, para algún i, con $1 \leq i \leq s$, de donde $p_1 = q_i$, al ser q_i primo. Podemos suponer $i = 1$. Dividiendo por p_1 se tiene que $p_2 \cdots p_r = q_2 \cdots q_s$. Repitiendo el razonamiento para $p_2, \ldots, p_r$, llegamos a $1 = q_{r+1} \cdots q_s$. Luego $r = s$ y $p_i = q_i, \quad i = 1, \ldots, r$. □

Teorema (Euclides)

El conjunto de los primos es infinito.

PRUEBA: Supongamos que no, es decir, que el conjunto de los primos fuese finito, y sean $p_1, \ldots, p_r$ todos los primos. Sea $n = p_1 \cdots p_r + 1$. Por la factorización única, n debe ser divisible por algún p_i, lo que implicaría que $p_i | 1$ y eso es imposible. □

Nota 3.3.5. Veremos otra forma de ver el máximo común divisor y el mínimo común múltiplo en función de los factores primos. La factorización única de un entero positivo n la escribiremos usualmente en la forma

$$n = \prod_{p>0 \text{ primo}} p^{\nu_n(p)}$$

donde todos los $\nu_n(p)$ son cero salvo un número finito. La factorización se puede extender a enteros $n < 0$ poniendo

$$n = (-1) \prod_{p>0 \text{ primo}} p^{\nu_{-n}(p)}.$$

Considerando sólo números primos positivos, como hemos hecho antes.

No es difícil comprobar la veracidad de la siguiente proposición, que nos da las definiciones de *máximo común divisor* y *mínimo común múltiplo* tal y como se trabajan en *secundaria*.

Proposición 3.3.6. *Sean*

$$a = \pm \prod_{p>0 \text{ primo}} p^{\nu_a(p)}, \quad b = \pm \prod_{p>0 \text{ primo}} p^{\nu_b(p)}$$

las descomposiciones de dos enteros a y b en producto de primos. Consideremos

$$d = \prod_{p>0 \text{ primo}} p^{\min(\nu_a(p),\nu_b(p))} \text{ y } m = \prod_{p>0 \text{ primo}} p^{\max(\nu_a(p),\nu_b(p))}.$$

Entonces $d = \mathrm{mcd}(a, b)$ y $m = \mathrm{mcm}(a, b)$.

3.4 Congruencias

La divisibilidad nos conduce naturalmente a la noción de congruencia de módulo $m \in \mathbb{Z} \setminus \{0\}$.

Congruencia

Dados enteros dos a, b y un entero no nulo m, se dirá que a **es congruente con** b **módulo** si $a - b$ es divisible por m. En este caso se escribirá $a \equiv b \pmod m$.

Se puede suponer $m > 0$

De la división euclídea se deduce que siempre se puede suponer positivo el módulo m de la congruencia. En efecto, si $m < 0$ y $a \equiv b \pmod m$ es $a - b = km$, luego $a - b = (-k)(-m)$ y por tanto $a \equiv b \pmod{-m}$. Esto es lo que haremos de ahora en adelante.

UNIVERSIDAD SEVILLA

Una propiedad fundamental de las congruencias es la siguiente:

Proposición 3.4.1. *Sean $a, b \in \mathbb{Z}$. Entonces $a \equiv b \pmod{m}$ si y sólo si a y b dan el mismo resto en la división euclídea por m.*

PRUEBA: En efecto, si $a \equiv b \pmod{m}$, entonces $m|(b-a)$. Sean $a = qm+r$ $b = q'm + r'$,$0 \leq r, r' < m$, entonces $a - b = (q - q')m + (r - r')$, igualdad que sólo es posible cuando $r' - r = 0$ ya que $|r' - r| < m$. Recíprocamente, si $a = qm + r$, $b = q'm + r$ es $a - b = (q - q')m$, luego $a \equiv b \pmod{m}$. □

Relación "ser congruente con"

La relación *"ser congruente con"* es precisamente la relación $\sim_{\mathbb{Z}m}$ definida en el tema anterior (Página 89). Luego es una relación de equivalencia y el conjunto cociente es el anillo $\mathbb{Z}/\mathbb{Z}m$.
En consecuencia las congruencias son compatibles con la suma y el producto.

Proposición 3.4.2. *Sea $m > 0$ un entero. Sean $a, b, c, d \in \mathbb{Z}$ tales que $a \equiv b \pmod{m}$ y $c \equiv d \pmod{m}$. Se verifican las siguientes propiedades:*

1. $a + c \equiv b + d \pmod{m}$.
2. $ac \equiv bd \pmod{m}$.

Nota 3.4.3 (Propiedad cancelativa). De cara a resolver ecuaciones en congruencias será necesario saber en qué condiciones se puede aplicar la propiedad cancelativa. Es decir, se trata de ver cuándo se verifica que

$$ax \equiv bx \pmod{m} \Longrightarrow a \equiv b \pmod{m}.$$

Si m es un número primo entonces $\mathbb{Z}/\mathbb{Z}m$ es un dominio de integridad (de hecho es un cuerpo) y se satisface la propiedad cancelativa.

Si m no es primo, en general no se satisface la propiedad cancelativa. Por ejemplo,

$$2 \cdot 2 \equiv 0 \cdot 2 \pmod{4} \quad \text{y} \quad 2 \not\equiv 0 \pmod{4}.$$

UNIVERSIDAD SEVILLA

Congruencias y propiedad cancelativa

Sean $x, m \in \mathbb{Z}$, $m > 0$, se verifica la propiedad

$$\forall a, b \in \mathbb{Z},\ ax \equiv bx \pmod{m} \Longrightarrow a \equiv b \pmod{m}$$

si y sólo si x y m son primos entre si.

PRUEBA: Si $1 < d = \text{mcd}(x, m)$, $x = x'd$, $m = m'd$, entonces $m'x \equiv 0 \cdot x \pmod{m}$ pero $m' \not\equiv 0 \pmod{m}$ porque $0 < m' < m$.

Recíprocamente, si $\text{mcd}(x, m) = 1$, sea $ax \equiv bx \pmod{m}$. Por la identidad de Bézout existen $\alpha, \beta \in \mathbb{Z}$ tales que $\alpha x + \beta m = 1$. Así, $a = \alpha a x + \beta a m$, $b = \alpha b x + \beta b m$, luego

$$a - b = \alpha(ax - bx) + \beta(a - b)m,$$

que es múltiplo de m. Por tanto, $a \equiv b \pmod{m}$. □

Veamos ahora qué ocurre con la ecuación $ax = b,\ a, b \in \mathbb{Z}$. Sabemos que la ecuación anterior tiene solución entera si y sólo si $a|b$ y su solución es $x = \frac{b}{a} \in \mathbb{Z}$. En el caso de las congruencias tenemos

Proposición 3.4.4. *La ecuación en congruencias*

$$ax \equiv b \pmod{m}$$

tiene solución si y sólo si $d = mcd(a, m)$ *divide a* b.

PRUEBA: Supongamos que $d|b$, $b = dc$. La identidad de Bézout nos dice que $d = \alpha a + \beta m$, luego $b = dc = \alpha a c + \beta m c$. Como $mc \equiv 0 \pmod{m}$, se tiene que $\alpha a c \equiv b \pmod{m}$, es decir, αc es solución de la ecuación.

Para la implicación contraria supongamos que x_0 es una solución de la ecuación en congruencias. Es decir $ax_0 - b = km$, luego $d|ax_0 - km = b$. □

UNIVERSIDAD DE SEVILLA

Teorema chino del resto

Sean $m_1, m_2, \ldots, m_n$ enteros, mayores que 1, primos entre sí dos a dos, $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. El sistema de congruencias:

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \\ &\vdots \\ x &\equiv a_n \pmod{m_n} \end{aligned}$$

tiene solución. Además, si x y x' son dos soluciones, entonces $x \equiv x' \pmod{M}$, donde $M = m_1 m_2 \cdots m_n$. Recíprocamente, si x es una solución y $x' \equiv x \pmod{M}$, entonces x' es solución.

PRUEBA: Denotemos $M_i = M/m_i$, $\forall i = 1, \ldots, n$. Es claro que

$$\text{mcd}(m_i, M_i) = 1, \quad \forall i = 1, \ldots, n,$$

luego, por la identidad de Bézout, existen $\alpha_i, \beta_i \in \mathbb{Z}$ verificando

$$1 = \alpha_i m_i + \beta_i M_i, \quad i = 1, \ldots, n.$$

Tomemos $x = a_1\beta_1 M_1 + a_2\beta_2 M_2 + \cdots + a_n\beta_n M_n$ y comprobemos que x es solución. Para ello tendremos que comprobar que $x \equiv a_i \pmod{m_i}$, para todo i, o, equivalentemente, que $x - a_i \equiv 0 \pmod{m_i}$, para todo i. Usando la identidad de Bézout correspondiente, tenemos $a_i = a_i\alpha_i m_i + a_i\beta_i M_i$. Entonces,

$$\begin{aligned} x - a_i &= a_1\beta_1 M_1 + \cdots + a_n\beta_n M_n - a_i\alpha_i m_i - a_i\beta_i M_i = \\ &= a_1\beta_1 M_1 + \cdots + a_{i-1}\beta_{i-1} M_{i-1} + a_{i+1}\beta_{i+1} M_{i+1} + \cdots + a_n\beta_n M_n - a_i\alpha_i m_i, \end{aligned}$$

y, al ser todos los sumandos múltiplos de m_i, es $x - a_i \equiv 0 \pmod{m_i}$.

Dejamos como ejercicio la demostración de la última parte del enunciado. □

Ejemplo 3.4.5. Resolvamos el siguiente sistema de congruencias:

$$\begin{aligned} x &\equiv 1 \pmod{2} \\ x &\equiv 2 \pmod{3} \\ x &\equiv 3 \pmod{5} \end{aligned}$$

Siguiendo la notación de la demostración anterior, en nuestro caso tenemos $m_1 = 2, m_2 = 3, m_3 = 5$, $M = 30, M_1 = 15, M_2 = 10$ y $M_3 = 6$. Por la identidad de Bezout tenemos

UNIVERSIDAD SEVILLA

$$\text{mcd}(m_1, M_1) = 1, 1 = (-7) \cdot 2 + 1 \cdot 15, \text{ luego } \beta_1 = 1.$$
$$\text{mcd}(m_2, M_2) = 1, 1 = (-3) \cdot 3 + 1 \cdot 10, \text{ luego } \beta_2 = 1.$$
$$\text{mcd}(m_3, M_3) = 1, 1 = (-1) \cdot 5 + 1 \cdot 6, \text{ luego } \beta_3 = 1.$$

Por tanto una solución del sistema es

$$x = a_1\beta_1 M_1 + a_2\beta_2 M_2 + a_3\beta_3 M_3 = 53.$$

Las soluciones son los enteros congruentes con 53 módulo 30.

3.5 Los teoremas de Fermat y Euler



Figura 3.1: Pierre de Fermat

Terminamos este tema probando dos teoremas muy importantes, debidos a Fermat (1640) y a Euler (1736). Aunque el teorema de Euler es una generalización del pequeño teorema de Fermat, enunciamos este último como un teorema y no como un corolario por razones históricas: el de Fermat es casi un siglo anterior al de Euler.

Unidades de $\mathbb{Z}/\mathbb{Z}m$

El grupo de las unidades del anillo $\mathbb{Z}/\mathbb{Z}m$ es

$$U_m = \{a + \mathbb{Z}m \mid \text{mcd}(a, m) = 1, 0 \leq a < m\}.$$

UNIVERSIDAD DE SEVILLA

PRUEBA: Supongamos que $a + \mathbb{Z}m$ es unidad. Entonces existe $b + \mathbb{Z}m$ tal que $(a + \mathbb{Z}m)(b + \mathbb{Z}m) = 1 + \mathbb{Z}m$, luego $ab - 1 = qm$, y $ab - qm = 1$, por tanto a y m son primos entre sí.

Recíprocamente, supongamos que $\text{mcd}(a, m) = 1$. Por la identidad de Bezout existen enteros r, s con $ra + sm = 1$. Luego $1 + \mathbb{Z}m = (ra + sm) + \mathbb{Z}m = (ra + \mathbb{Z}m) + (sm + \mathbb{Z}m) = (a + \mathbb{Z}m)(r + \mathbb{Z}m)$. Es decir, $a + \mathbb{Z}m$ es una unidad. □

Nota 3.5.1. El anillo $\mathbb{Z}/\mathbb{Z}p$ es un cuerpo si y sólo si p es primo. De hecho

$$U_p = \{1 + \mathbb{Z}p, \ldots (p-1) + \mathbb{Z}p\}$$

y $|U_p| = p - 1$.

(Pequeño) Teorema de Fermat (1640)

Si p es primo y no divide a $a \in \mathbb{Z}$, entonces $a^{p-1} \equiv 1 \pmod{p}$.

PRUEBA: Si p no divide a a entonces $a + \mathbb{Z}p \in U_p$. Como el orden del grupo U_p es $p - 1$, por el teorema de Lagrange, se tiene

$$(a + \mathbb{Z}p)^{p-1} = 1 + \mathbb{Z}p.$$

Es decir, $a^{p-1} \equiv 1 \pmod{p}$. □

El teorema de Euler generalizará este resultado a enteros no primos. Antes hemos de dar la definición de la función indicatriz de Euler, que asocia a cada entero m la cantidad de unidades de $\mathbb{Z}/\mathbb{Z}m$.

Función ϕ o indicatriz de Euler

A la cantidad de números enteros $a, 1 \leq a \leq m$, que son primos con m se le denota por $\phi(m)$, la **función ϕ o indicatriz de Euler**. Es decir,

$$\phi(m) = |U_m|.$$

Nota 3.5.2. Sea $p \in \mathbb{N}$, p es primo si y sólo si $\phi(p) = p - 1$.

Proposición 3.5.3. *Sea $p \in \mathbb{N}$ primo, entonces $\phi(p^r) = (p-1)p^{r-1}$.*

PRUEBA: Se trata de contar los números entre 1 y p^r que son primos con p^r. Como p es primo, son los números que no son múltiplos de p. Vamos a contar los que sí son múltiplos de p y restárselos a p^r. Los múltiplos de p son

$$\{p, 2p, \ldots, p^r = p^{r-1}p\},$$

es decir, hay p^{r-1} múltiplos de p. Luego

$$\phi(p^r) = p^r - p^{r-1} = (p-1)p^{r-1}.$$

□

Teorema 3.5.4. *Sean m y n dos enteros primos entre si, entonces $\phi(mn) = \phi(m)\phi(n)$.*

PRUEBA: Se trata demostrar que hay tantos elementos en U_{mn} como en $U_m \times U_n$. Vamos a establecer una aplicación biyectiva entre ambos conjuntos. Sea

$$\begin{array}{rcl} f\colon U_{mn} & \to & U_m \times U_n \\ x + \mathbb{Z}mn & \mapsto & (x + \mathbb{Z}m, x + \mathbb{Z}n). \end{array}$$

Como m y n son primos entre sí, si $x + \mathbb{Z}mn \in U_{mn}$ entonces $\mathrm{mcd}(x, mn) = 1$, luego $\mathrm{mcd}(x, m) = \mathrm{mcd}(x, n) = 1$. Es decir, $(x + \mathbb{Z}m, x + \mathbb{Z}n) \in U_m \times U_n$

Además hay que comprobar que f es una aplicación (está bien definida), es decir, que no depende de la elección del representante de la clase $x + \mathbb{Z}mn$. Si $x + \mathbb{Z}mn = y + \mathbb{Z}mn$ ¿es $(x + \mathbb{Z}m, x + \mathbb{Z}n) = (y + \mathbb{Z}m, y + \mathbb{Z}n)$?

$$x + \mathbb{Z}mn = y + \mathbb{Z}mn \Leftrightarrow mn|(x-y) \overset{\mathrm{mcd}(m,n)=1}{\Longleftrightarrow}$$

$$\Leftrightarrow \left\{ \begin{array}{l} m|(x-y) \Leftrightarrow x + \mathbb{Z}m = y + \mathbb{Z}m \\ n|(x-y) \Leftrightarrow x + \mathbb{Z}n = y + \mathbb{Z}n \end{array} \right\} \Leftrightarrow (x+\mathbb{Z}m, x+\mathbb{Z}n) = (y+\mathbb{Z}m, y+\mathbb{Z}n).$$

De la expresión anterior se deduce que f es inyectiva, pues si $x + \mathbb{Z}mn$ e $y + \mathbb{Z}mn$ son tales que $f(x + \mathbb{Z}mn) = f(y + \mathbb{Z}mn)$, es decir,

$$(x + \mathbb{Z}m, x + \mathbb{Z}n) = (y + \mathbb{Z}m, y + \mathbb{Z}n),$$

se obtiene que $x + \mathbb{Z}mn = y + \mathbb{Z}mn$.

Por último, veamos que f es sobreyectiva. Sea $(a + \mathbb{Z}m, b + \mathbb{Z}n) \in U_m \times U_n$ ¿existe $x + \mathbb{Z}mn \in U_{mn}$ tal que $f(x + \mathbb{Z}mn) = (a + \mathbb{Z}m, b + \mathbb{Z}n)$? Como $\mathrm{mcd}(m, n) = 1$, aplicando el *teorema chino del resto* existe algún entero x tal que $x \equiv a \pmod m$ y $x \equiv b \pmod n$. Sabemos que $x + \mathbb{Z}m = a + \mathbb{Z}m$ es unidad en $\mathbb{Z}/\mathbb{Z}m$ y que $x + \mathbb{Z}n = b + \mathbb{Z}n$ es unidad en $\mathbb{Z}/\mathbb{Z}n$ de donde se deduce, por

UNIVERSIDAD DE SEVILLA

ser m y n primos entre sí, que $x + \mathbb{Z}mn$ es una unidad en $\mathbb{Z}/\mathbb{Z}mn$. Luego f es sobreyectiva, pues

$$f(x + \mathbb{Z}mn) = (x + \mathbb{Z}m, x + \mathbb{Z}n) = (a + \mathbb{Z}m, b + \mathbb{Z}n).$$

Por tanto, hay tantos elementos en U_{mn} como en $U_m \times U_n$. Luego $\phi(mn) = \phi(m)\phi(n)$. □

Corolario 3.5.5. *Sea n un entero y $n = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$ su descomposición en factores primos, entonces*

$$\phi(n) = (p_1 - 1) \cdots (p_r - 1) p_1^{n_1 - 1} \cdots p_r^{n_r - 1}.$$

PRUEBA:

$$\phi(n) = \phi(p_1^{n_1} \cdots p_r^{n_r}) = \phi(p_1^{n_1}) \cdots \phi(p_r^{n_r}) = (p_1 - 1)p_1^{n_r - 1} \cdots (p_r - 1)p_r^{n_r - 1} =$$
$$= (p_1 - 1) \cdots (p_r - 1) p_1^{n_1 - 1} \cdots p_r^{n_r - 1}.$$

□

Nota 3.5.6. Si n es un entero y $n = p_1^{n_1} p_2^{n_2} \cdots p_r^{n_r}$ es su descomposición en factores primos, entonces

$$\phi(n) = (p_1 - 1) \cdots (p_r - 1) p_1^{n_1 - 1} \cdots p_r^{n_r - 1} = n \left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right).$$

Ejemplo 3.5.7. Vamos a calcular $\phi(360)$. Como $360 = 2^3 3^2 5$, entonces

$$\phi(360) = \phi(2^3)\phi(3^2)\phi(5) = (2 - 1)2^2(3 - 1)3(5 - 1) = 96.$$

Teorema de Euler (1736)

Sea $a + \mathbb{Z}m$ una unidad en $\mathbb{Z}/\mathbb{Z}m$. Entonces

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

PRUEBA: La demostración es análoga a la del teorema de Fermat. Si $a + \mathbb{Z}m \in U_m$, como $|U_m| = \phi(m)$, por el teorema de Lagrange

$$(a + \mathbb{Z}m)^{\phi(m)} = 1 + \mathbb{Z}m.$$

Luego $a^{\phi(m)} \equiv 1 \pmod{m}$. □



Figura 3.2: Leonhard Euler

Ejemplo 3.5.8. Calcular el resto de dividir 62347^{5827} entre 20. Como $62347 = 3117 \cdot 20 + 7$, entonces $62347^{5827} \equiv 7^{5827} \pmod{20}$. Además 7 es primo con 20, luego podemos aplicar el teorema de Euler. Por un lado $\phi(20) = 8$, por otro, si dividimos 5827 entre 8 se obtiene $5827 = 728 \cdot 8 + 3$. Por el teorema de Euler $7^8 \equiv 1 \pmod{20}$, luego

$$7^{5827} = (7^8)^{728}7^3 \equiv 7^3 \text{ (mod } m).$$

$7 \cdot 7 = 49$ y $49 \equiv 9 \pmod{20}$. Luego $7^3 \equiv 9 \cdot 7 \pmod{20}$ y $63 \equiv 3 \pmod{20}$. De donde el resto de dividir 62347^{5827} entre 20 es 3.

UNIVERSIDAD SEVILLA