Capítulo 3: El anillo de los números enteros

Miguel Ángel Olalla Acosta
miguelolalla@us.es

Departamento de Álgebra
Universidad de Sevilla

Noviembre de 2017

Contenido

Anillo

Definición (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:* $\forall a, b, c \in R$

$$a \cdot (b + c) = a \cdot b + a \cdot c \quad y \quad (a + b) \cdot c = a \cdot c + b \cdot c.$$

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* $a \in R$*.*

Anillo conmutativo. Anillo unitario

Definición (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** *o* **abeliano**.

Ejemplos de anillos (Ejemplo 3.1.2)

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 el producto de dos enteros $xy = y + \overset{x}{\cdots} + y$ es la suma del número y x veces. Esto no ocurre para $\mathbb{Q}$, $\mathbb{R}$ y $\mathbb{C}$, obviamente.

2.- El conjunto $\mathcal{M}(n)$ de las matrices $n \times n$ sobre $\mathbb{Q}$, $\mathbb{R}$ 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.

Algunas propiedades

Proposición (3.1.4)

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* $a \in A$.

Observación (Nota 3.1.5)

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 de un anillo

Definición (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.

Unidades de un anillo. Ejemplos

Ejemplo (3.1.6)

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* $\mathcal{M}(n)$ *son las matrices invertibles.*
3. *Sea* $\mathbb{Q}[x]$ *el anillo de polinomios en la indeterminada* x *con coeficientes racionales, entonces*

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

El grupo de las unidades. Cuerpos

Proposición (3.1.7)

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

Definición (Cuerpo)

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

Ejemplo (3.1.8)

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

Subanillos

Definición (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 $x \cdot y \in S$.*

Observación (Nota 3.1.9)

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

Ejemplos de subanillos

Ejemplo (3.1.10)

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* $1 \notin \mathbb{Z}2$

Homomorfismo de anillos

Definición (Homomorfismo de anillos)

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

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

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

Ejemplos (3.1.11)

1.- La aplicación identidad de un anillo R, Id_R, es un ismomorfismo 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.

Ejemplos (3.1.11)

3.- Sea R el subanillo de las matrices de la forma

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

Definamos la aplicación

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

por la regla

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

Se comprueba que ϕ es un isomorfismo y $R \cong \mathbb{C}$.

Núcleo e imagen de un homomorfismo

Teorema (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* $\ker(\phi)$ *sabemos que es un subgrupo aditivo de $(R,+)$ que además verifica la siguiente propiedad:*

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

Isomorfismo inverso

Teorema (Isomorfismo inverso)

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

Ideales de un anillo conmutativo

Definición (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 $xy \in I$.

Ejemplos de ideales (Ejemplo 3.1.12)

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 $\ker(\phi)$ 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. Diremos que un ideal de este tipo es un **ideal principal**.

Ejemplos de ideales (Ejemplo 3.1.12)

5.- Se demostrará más adelante 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 $\mathbb{Z}$.

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

Anillo cociente

Teorema (Anillo cociente)

Sean $(R, +, \cdot)$ un anillo conmutativo e $I \subset R$ un ideal. Entonces el conjunto cociente R/I con las operaciones $+$ y $\cdot$ dadas por

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

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

es un anillo conmutativo.

Observación (Nota 3.1.13)

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.
Nótese que el anillo cociente R/I es nulo si y sólo si $I = R$.

Anillo cociente (Ejemplo 3.1.14)

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

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

Anillo cociente (Ejemplo 3.1.14)

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.

Anillo cociente (Ejemplo 3.1.14)

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).

Anillo cociente (Ejemplo 3.1.14)

4.- En el anillo $R = \mathbb{Q}[x]$ 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

Teorema (Factorización canónica)

Todo homomorfismo de anillos conmutativos y unitarios, $f : R \to S$, factoriza como la composición $f = i \circ \bar{f} \circ p$ de un epimorfismo de anillos p, un isomorfismo de anillos $\bar{f}$ y un monomorfismo de anillos i del siguiente modo

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

Aquí p es la proyección natural sobre el cociente e i es la inclusión del subgrupo imagen.

Factorización Canónica

Corolario (3.1.15)

Si $f : R \to S$ es un epimorfismo de anillos entonces la aplicación $\bar{f} : R/\ker(f) \to S$ es un isomorfismo.

Corolario (3.1.16)

Si $f : R \to S$ es un monomorfismo de anillos entonces $\bar{f} : R \to \mathrm{Im}(f)$ es un isomorfismo.

Ejemplo 3.1.17

Ejemplo

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

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

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

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

Definición (Divisor de cero)

Sea R un anillo conmutativo. Se dice que un elemento no nulo $x \in R$ 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 $1 \cdot 0 = 0$.

Ejemplo (3.1.18)

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

Definición (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 (3.1.19)

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 (3.1.20)

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.*

Dominio de integridad y propiedad cancelativa

Teorema (Dominio de integridad y propiedad cancelativa)

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

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

Dominio de Integridad finito

Proposición (3.1.21)

Todo dominio de integridad finito es un cuerpo.

Ejemplo (3.1.22)

Si $p \in \mathbb{Z}$ es primo, el anillo $\mathbb{Z}/\mathbb{Z}p$ es un dominio de integridad finito. Luego es un cuerpo.

Observación (3.1.23)

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

Ideales y unidades

Proposición (3.1.24)

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

Corolario (3.1.25)

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

Corolario (3.1.26)

Un anillo conmutativo y unitario es un cuerpo si y sólo si no tiene ideales propios no nulos.

Ideal maximal

Definición (Ideal maximal)

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

Ejemplo (3.1.27)

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 $\mathbb{Z}p \subset I$ entonces la aplicación

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

es un homomorfismo inyectivo de grupos (de hecho es un monomorfismo de anillos). Entonces $|\mathbb{Z}/I| = |f(\mathbb{Z}/I)|$, como $f(\mathbb{Z}/I) \subset \mathbb{F}_p$ es un subgrupo, su orden divide a $|\mathbb{F}_p| = p$. Al ser p primo debe ser $|\mathbb{Z}/I| = 1$ ó p, luego $I = \mathbb{Z}$ ó $\mathbb{Z}p$.

Ideal primo

Definición (Ideal primo)

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

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

Ideales primos y maximales

Proposición (3.1.28)

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.*

Ideales primos y maximales

Proposición (3.1.29)

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.*

Corolario (3.1.30)

Todo ideal primo maximal de un anillo conmutativo unitario es un ideal primo.

Primo no implica maximal

Ejemplo (3.1.31)

Sea $R = \mathbb{Q}[x, y]$. Sea el ideal $I = Rx$ de los polinomios que son múltiplos de x.
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 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 $\ker(\phi) = I$. Por la factorización canónica 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.

Característica de un dominio de integridad

Proposición (3.1.32)

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 $x \in R$

Definición (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.*

Característica de un dominio de integridad

Ejemplo (3.1.33)

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

Observación (3.1.34)

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 $\mathbb{F}_p[x]$.

Principio de buena ordenación

Teorema (Principio de buena ordenación)

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

El orden de los números enteros

Propiedades del orden de enteros:

Propiedad reflexiva: $a \geq a$.
Propiedad transitiva: si $a \geq b$ y $b \geq c$ entonces $a \geq c$.
Propiedad antisimétrica: si $a \geq b$ y $b \geq a$ entonces $a = b$.
Orden total: dados dos enteros a y b entonces $a \geq b$ o $b \geq a$.
Buen orden: todo conjunto de enteros *acotado inferiormente* posee un mínimo.

Si $a \geq 0$ entonces $a + a \geq a$.
Si $a \geq b$ entonces $a + c \geq b + c$.
Si $a \geq b$ y $c \geq 0$ entonces $a \cdot c \geq b \cdot c$.
Si $a \geq b$ y $c \leq 0$ entonces $a \cdot c \leq b \cdot c$.

Divisibilidad

Si a y b son enteros, ¿Qué significa "a divide a b"?

Definición (Divisibilidad)

Sean a y b dos enteros. Se dirá que a **divide a** *b si existe un entero c tal que $a \cdot c = b$. En este caso se escribe $a|b$.*

Unidades

¿Hay números enteros que dividan a todos los demás?

Sí, el 1 y el -1.
¡Las unidades de $\mathbb{Z}$!

¿Hay alguno más?

No, ¿sabes demostrarlo?

Propiedades de la divisibilidad

1. Propiedad reflexiva: $a|a$
2. Propiedad transitiva: Si $a|b$ y $b|c$ entonces $a|c$.
3. Si $a|b$ y $b|a$ entonces $a = \pm b$.

Observación (3.2.2)

Si a y b son positivos entonces la propiedad 3 es la antisimétrica, es decir, si $a|b$ y $b|a$ entonces $a = b$. Luego la relación de divisibilidad es una **relación de orden** *en el conjunto de los números positivos.*

4. Si $a|b$ y $a|c$ entonces $a|b + c$.
5. Si $a|b$ entonces $a|b \cdot c$.

División euclídea

¿Cómo se dividen dos números enteros, por ejemplo 117586 entre 1532?

$$\begin{array}{r|l} 1\,1\,7\,5\,8\,6 & 1\,5\,3\,2 \\ \cline{2-2} -\,1\,0\,7\,2\,4 & \mathbf{7\,6} \\ \cline{1-1} \quad 1\,0\,3\,4\,6 & \\ -\quad\;\; 9\,1\,9\,2 & \\ \cline{1-1} \quad\;\; \mathbf{1\,1\,5\,4} & \end{array}$$

Entonces $117586 = 76 \cdot 1532 + 1154$.

División euclídea

Teorema (División euclídea)

Sean a y b enteros, $b \neq 0$. Existen unos únicos enteros q y r tales que:

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

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

Subgrupos de $\mathbb{Z}$

Teorema (Subgrupos de $\mathbb{Z}$)

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

Máximo común divisor

¿Qué es el máximo común divisor de dos enteros?

Definición (Máximo común divisor)

Dados dos enteros a y b, diremos que d es un **máximo común divisor** *de a y b, y lo denotaremos por $d = \mathrm{mcd}(a, b)$, si se verifican las siguientes propiedades:*

1. $d|a$ *y* $d|b$.
2. *Si* d' *es un entero 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**.

Máximo común divisor. Propiedades

Observación (3.2.5)

El máximo común divisor de dos enteros, si existe, es único salvo el signo.

Proposición (3.2.6)

Se verifican las siguientes propiedades:

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

Mínimo común múltiplo

¿Qué es el mínimo común múltiplo de dos enteros?

Definición (Mínimo común múltiplo)

Dados dos enteros a y b, diremos que un entero m es un **mínimo común múltiplo** *de a y b, y lo denotaremos por $m = \text{mcm}(a, b)$, si se verifican las siguientes propiedades:*

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

Mínimo común múltiplo. Propiedades

Observación (3.2.7)

El mínimo común múltiplo de dos enteros, si existe, es único salvo el signo.

Proposición (3.2.8)

Se verifican las siguientes propiedades:

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

Máximo común divisor y división euclídea

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, si $r = 0$ es $mcd(a, b) = b$ y si $r \neq 0$

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

Algoritmo de Euclides

Algoritmo (Algoritmo de Euclides)

Sean a y b dos enteros no nulos, $a \geq b$, y efectuemos la división euclídea $a = q \cdot b + r$. Como $r < |b|$, podemos dividir b entre r, y así sucesivamente, obteniendo:

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

Algoritmo de Euclides y existencia del máximo común divisor

Proposición (3.3.2)

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

Teorema (Existencia del máximo común divisor)

Dados dos enteros a, b, *existe el máximo común divisor de a y b,* $\mathrm{mcd}(a, b)$, *que es único salvo el signo.*

Algoritmo de Euclides

Ejemplo (Ejercicio12: Calcular mcd(23532, 1520))

$$\begin{aligned} 23532 &= 15 \cdot 1520 + 732 \\ 1520 &= 2 \cdot 732 + 56 \\ 732 &= 13 \cdot 56 + 4 \\ 56 &= 14 \cdot 4 + 0 \end{aligned}$$

Luego $\text{mcd}(23532, 1520) = 4$

Identidad de Bézout

Observación (3.3.3)

Sean a, b enteros no nulos y sea $d = \text{mcd}(a, b)$. Obsérvese que para cualesquiera enteros γ y δ se verifica que $\gamma a + \delta b$ es un múltiplo de d.

Teorema (Identidad de Bézout)

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

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

A cualquier igualdad de este tipo se le llama **identidad de Bézout**.

Familia infinita de identidades de Bézout

Observación (3.3.4)

Los enteros α y β que aparecen en la identidad de Bézout no son únicos. En efecto, si $\alpha \cdot a + \beta \cdot b = d$ entonces

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

Identidad de Bézout

Ejemplo (Ejercicio 12)

Sabiendo que $\mathrm{mcd}(1520, 23532) = 4$ *escribir una identidad de Bézout usando el algoritmo de Euclides.*

$$\begin{array}{r|l} 23532 = 15 \cdot 1520 + 732 & 732 = 23532 - 15 \cdot 1520 \\ 1520 = 2 \cdot 732 + 56 & 56 = 1520 - 2 \cdot 732 \\ 732 = 13 \cdot 56 + 4 & 4 = 732 - 13 \cdot 56 \\ 56 = 14 \cdot 4 + 0 & \end{array}$$

De donde $4 = 732 - 13 \cdot 56 = 732 - 13 \cdot (1520 - 2 \cdot 732) =$
$(23532 - 15 \cdot 1520) - 13 \cdot (1520 - 2 \cdot (23532 - 15 \cdot 1520)) =$
$(1+13\cdot 2)\cdot 23532+(-15-13-13\cdot 2\cdot 15)\cdot 1520 = 27\cdot 23532+(-418)\cdot 1520$

$$27 \cdot 23532 + (-418) \cdot 1520 = 4.$$

Teorema de Euclides

Teorema (de Euclides)

Sean a, b y c tres enteros no nulos tales que $c|ab$ y $\mathrm{mcd}(a,c)=1$, entonces $c|b$. En particular, si p es un número primo y $p|ab$ entonces $p|a$ o $p|b$.

Máximo común divisor y mínimo común múltiplo

Proposición (3.3.5)

Sean a y b dos enteros no nulos, sea $d = \mathrm{mcd}(a, b)$ y consideremos

$$a' = \frac{a}{d} \text{ y } b' = \frac{b}{d}.$$

Entonces a' y b' son primos entre sí.

Proposición (3.3.6)

Sean a y b dos enteros no nulos y sea $d = \mathrm{mcd}(a, b)$. Entonces

$$\mathrm{mcm}(a, b) = \frac{ab}{d}.$$

Existencia del mínimo común múltiplo

Teorema (Existencia del mínimo común múltiplo)

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

Teorema fundamental de la divisibilidad

Observación (3.3.7)

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

Teorema (fundamental de la divisibilidad)

Todo entero distinto de 0, 1 *y* -1 *se descompone como producto de un número finito de primos. Esta descomposición es única salvo el orden y el signo de los factores primos.*

El conjunto de los números primos es infinito

Teorema (de Euclides sobre la infinitud de los números primos)

El conjunto de los números primos es infinito.

Cálculo de mcd y mcm

Proposición (3.3.9)

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

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

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

Congruencias

¿Qué hora marcará el reloj después de pasar 4, 15, 211, 1203 o 12352 horas?

Después de 15 horas el reloj marca lo mismo que si hubieran pasado 1203 horas. ¿Cómo podemos saber si tras a horas el reloj marcará lo mismo que tras b horas?

Congruencias

Definición (Congruencia)

Sean a, b y m enteros, $m \neq 0$, se dirá que a **es congruente con** *b* **módulo** *m si $a - b$ es divisible por m. Se escribirá $a \equiv b \pmod{m}$.*

Observación (3.4.1)

a y b son congruentes módulo m si y sólo si son congruentes módulo $-m$. Luego podemos suponer siempre, sin pérdida de generalidad, que $m > 0$

Proposición (3.4.2)

$a \equiv b \pmod{m}$ si y sólo si a y b tienen el mismo resto en la división euclídea por m.

Congruencias. Propiedades

Observación (3.4.3)

La relación "ser congruente con" *es precisamente la relación* $\sim_{\mathbb{Z}m}$ *definida en el tema anterior. 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 (3.4.4)

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. $ac \equiv bd \pmod{m}$.

Congruencias y propiedad cancelativa

Observación (3.4.5)

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,

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

Congruencias y propiedad cancelativa

Teorema (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.*

Ecuaciones en congruencias

Proposición (3.4.6)

La ecuación en congruencias

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

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

Ecuaciones en congruencias

Teorema (chino del resto)

Sean $m_1, m_2, \ldots, m_n$ enteros mayores que 1 primos entre sí dos a dos, sean $a_1, a_2, \ldots, a_n$ enteros. El sistema de ecuaciones en 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' también es solución.

Ejemplo 3.4.7

Resolvamos el siguiente sistema de congruencias:

$$x \equiv 1 \pmod 2$$
$$x \equiv 2 \pmod 3$$
$$x \equiv 3 \pmod 5$$

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

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

Por tanto una solución 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.

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

Teorema (Unidades de $\mathbb{Z}/\mathbb{Z}m$)

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

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

Observación (3.5.1)

El conjunto $\mathbb{Z}/\mathbb{Z}p$ 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 $|U_p| = p - 1$.

El teorema de Fermat

Figura: Pierre de Fermat

Teorema ((Pequeño) teorema de Fermat (1640))

Si p es un número primo y no divide a un entero a entonces

$$a^{p-1} \equiv 1 (\mathrm{mod}\, p).$$

La función de Euler

Definición (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,*

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

Propiedades de la función de Euler

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

Teorema (3.5.4)

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

Cálculo de $\phi(n)$

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

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

Observación (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)

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

Teorema de Euler

Figura: Leonhard Euler

Teorema (Teorema de Euler (1736))

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

$$a^{\phi(m)} \equiv 1 (\mathrm{mod}\, m).$$

Teorema de 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

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

$7 \cdot 7 = 49$ 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.