

# La aritmética de los relojes

Por Paulo Tirao

# 4.

1. Introducción.
2. La aritmética del reloj.
3. Los enteros módulo  $m$ .
4. La aritmética modular.
5. Aplicaciones a la aritmética entera.
6. Las reglas de divisibilidad.
7. Ecuaciones lineales en la aritmética modular.
8. Residuos cuadráticos.
9. Los códigos de Julio César.

## □ 4.1. Introducción

*El médico:*

Ahora son las 10 de la mañana. Tome la próxima pastilla a las 2 de la tarde, y luego una cada 8 horas.

*El paciente:*

OK. Entonces tomo la próxima a las 2 de la tarde, luego a las ... 2 más 8 ... eso es a las 10 de la noche, otra a las 10 más 8 ... a las 6 de la mañana, después a las 6 más 8 ... 14, ¡ah! de nuevo a las 2 de la tarde. Entonces sigo así: a las 2 de la tarde, a las 10 de la noche y a las 6 de la mañana. Muchas gracias (ver **figura 4.1**). Hasta luego.

¡Qué manera de sumar! ¿Así que  $10 + 8 = 6$ ? ¡Qué bonito! Bueno... Sí, en la aritmética del reloj sí.

No es difícil encontrar otras situaciones donde esta aritmética: la aritmética del reloj, cíclica o modular, aparece naturalmente.

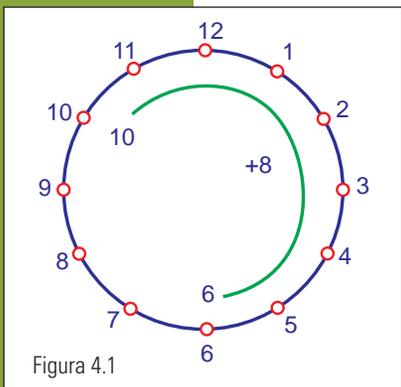
*El médico:*

Bueno, hoy es martes. A ver..., vuelva entonces en 10 días.

*El paciente:*

Muy bien. No hay problema. Hoy es martes, en 10 días será..., perfecto viernes. Estaré desocupado. Muchas gracias.





¡Qué manera de sumar! Así que martes +10 = viernes. ¡Qué bonito! Bueno... Sí, en la aritmética de la semana sí.

Si le ponemos números a los días de la semana, empezando con domingo = 0, lunes = 1, martes = 2, etc., resulta que martes + 10 = 2 + 10, que ya sabemos da viernes = 5. Es decir, en la aritmética de la semana  $2 + 10 = 5$ .

A esta altura también podemos contestar correctamente cuánto es  $2 + 10$  en la aritmética del reloj, y cuánto es  $10 + 8$  en la aritmética de la semana.

#### Recopilando

En la aritmética del reloj

$$10 + 8 = 6$$

$$2 + 10 = 0.$$

En la aritmética de la semana

$$10 + 8 = 4$$

$$2 + 10 = 5.$$

El resultado cambia cuando pasamos de la aritmética del reloj, que tiene 12 horas, a la aritmética de la semana, que tiene 7 días. De hecho, podemos ubicar los días de la semana como las horas de un reloj de 7 horas. Dispuestos así, vemos que la aritmética de la semana y la de este reloj de 7 horas, son muy parecidas.

Como veremos más adelante esta **aritmética cíclica o modular** aparece como herramienta útil en situaciones en las que, quizá, no lo sospechábamos. Sin embargo, esto no sorprende demasiado a un matemático. En efecto, una vez que comprendemos una situación dada, entendemos su estructura y sus leyes, entonces podemos crear una teoría que cobra vida propia. Es frecuente, que no sólo sirva para explicar el fenómeno original que le dio vida, sino que encuentre utilidad en muchas otras situaciones preexistentes, o en situaciones y modelos creados basados en esta teoría.

En este capítulo nos familiarizaremos con estas aritméticas hasta ser capaces de hacer cuentas como sumas, restas y multiplicaciones, de la misma manera que lo hacemos en la aritmética tradicional. Daremos un marco formal y riguroso con ideas matemáticas sencillas, pero fundamentales. Marco que permite que esas ideas se puedan extender y generalizar a otras aritméticas dentro de la matemática.

Más adelante, veremos aplicaciones más sofisticadas como las reglas de divisibilidad.

También incluiremos una sección dedicada a la teoría de códigos. Desde muy temprano en la historia, la aritmética modular estuvo ligada a la construcción de códigos para el envío de mensajes secretos. Se le atribuye a Julio César el invento de uno de los primeros códigos que usaron los ejércitos romanos por largo tiempo de forma efectiva y exitosa. Estos códigos se basan en la aritmética modular.

## □ 4.2. La aritmética del reloj

Todos tenemos alguna experiencia en hacer cuentas con horas o con los días de la semana. Por esto exponemos directamente el tema y en la próxima sección veremos los aspectos formales y más rigurosos.

### La aritmética del reloj de 12 horas

Comencemos repasando la aritmética del reloj usual. Supongamos que queremos sumar 9 más 7. Empezamos sumando “normalmente”. Si

$$\begin{aligned} 9 &= \text{—————} \\ 7 &= \text{—————} \end{aligned}$$

Entonces,  $9 + 7 = \text{—————}$

Ahora, para ver el resultado en el reloj enroscamos esa recta, y vemos que el resultado es  $9+7=4$  (ver **figura 4.2**).

**Regla.** Para sumar dos horas primero se suman normalmente y si este número es más grande que 12, el resultado final es sólo lo que se pasa de 12.

Es decir, se suman las dos horas normalmente, y luego si es necesario se resta una vez 12.

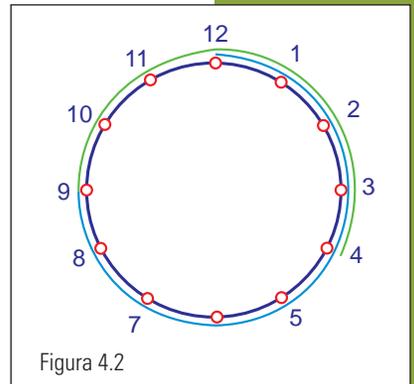
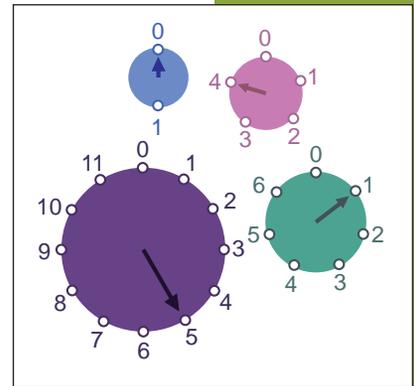


Figura 4.2

$$2 + 8 = 10 \quad 3 + 11 = 2 \quad 5 + 7 = 0 \quad 3 + 8 = 11 \quad 9 + 11 = 8$$

Para evitar confusiones, acordamos que las 12 horas son: **0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10** y **11**, es decir usaremos la hora 0 y no la hora 12.

Antes de continuar, introducimos una nueva notación para indicar que estamos usando la aritmética del reloj, u otra tan rara como ésta, y así evitar lo extraño que resulta por ejemplo la igualdad  $9 + 7 = 4$ .

Intentemos sumar tres o más números en esta aritmética.

**Notación.** Usaremos el símbolo  $\equiv$  para denotar igualdad en esta aritmética. Así  $9 + 7 \equiv 4$  en la aritmética del reloj.

$$\begin{aligned} 2 + 8 + 3 &= (2 + 8) + 3 & 3 + 11 + 4 &= (3 + 11) + 4 & 5 + 7 + 7 &= (5 + 7) + 7 \\ &\equiv 10 + 3 & &\equiv 2 + 4 & &\equiv 0 + 7 \\ &\equiv 1 & &\equiv 6 & &\equiv 7 \end{aligned}$$

La suma de varios sumandos se hace paso a paso, al igual que la suma usual de enteros. Esta suma de varios sumandos también se puede hacer así:

Ejemplos



Ejemplos



**Regla.** Para sumar varios números en la aritmética del reloj, se suman todos los sumandos normalmente, y si este número es más grande o igual que 12, se resta 12 la cantidad de veces necesaria hasta obtener un número entre 0 y 11.

Veamos cómo se resta. Para esto es útil pensar en el reloj y en la resta de horas. Por ejemplo, si ahora son las 4, ¿qué hora era hace 6 horas?

Ejemplos

$$4 - 6 \equiv 10 \quad 9 - 5 \equiv 4 \quad 1 - 4 \equiv 9 \quad 7 - 6 \equiv 1 \quad 2 - 2 \equiv 0$$



La resta se hace normalmente y, si es necesario, se suma 12 para obtener un número entre 0 y 11, y tener así una de las 12 horas posibles.

Volviendo al reloj, podemos decir que la suma se realiza en sentido horario y la resta en sentido antihorario. Si nos abstraemos del reloj, tanto la suma como la resta se hacen de la misma forma.

**Regla.** La suma y resta de varios sumandos en la aritmética del reloj se hace normalmente, y luego se suman o restan múltiplos de 12 hasta obtener un número entre 0 y 11.

Ejemplos

$$6 + 9 - 3 \equiv 0 \quad 4 - 11 + 2 - 1 \equiv 6 \quad 10 + 8 - 7 + 5 \equiv 4 \quad 4 + 11 - 3 - 9 \equiv 3 \quad 1 - 10 + 1 - 3 \equiv 1$$



Hasta aquí un primer acercamiento a la aritmética del reloj. Ahora, podríamos preguntarnos: ¿qué pasaría en un reloj de 8 horas? ¿Y en uno de 10 horas? Por suerte, nada raro.

### La aritmética de otros relojes y la aritmética de la semana

El hecho de que hayamos comenzado con un reloj de 12 horas no es determinante, porque podríamos haber desarrollado una aritmética similar en cualquier otro reloj. No sólo en uno que marque las 24 horas, sino también en relojes que no existen como tales, como por ejemplo uno de 9 horas u otro de 17 horas.

Ejemplos

*En la aritmética de un reloj de 9 horas*

$$6 + 8 \equiv 5 \quad 4 + 11 + 2 \equiv 8 \quad 3 + 4 - 5 \equiv 2 \quad 4 - 7 \equiv 6 \quad 8 + 4 - 6 \equiv 6$$



Ejemplos

*En la aritmética de un reloj de 17 horas*

$$6 + 8 \equiv 14 \quad 4 + 11 + 2 \equiv 0 \quad 3 + 4 - 5 \equiv 2 \quad 4 - 7 \equiv 14 \quad 8 + 4 - 6 \equiv 6$$



En ambos ejemplos usamos el signo  $\equiv$  para denotar igualdad en estas dos aritméticas distintas como lo habíamos usado en la aritmética del reloj de 12 horas. En todos estos casos estaba claro de cuántas horas eran los respectivos relojes, por eso el uso del mismo símbolo no causa ninguna confusión. Si el contexto no es claro usaremos una notación más completa.

**Notación.** Para decir que “ $6 + 8$  es igual a  $5$  en la aritmética de un reloj de 9 horas”, diremos “ $6 + 8$  es congruente a  $5$  módulo  $9$ ”. Y escribiremos “ $6 + 8 \equiv 5 \pmod{9}$ ”.

Otro ejemplo conocido, es el de la *aritmética de la semana*. En esta aritmética sabemos sumar martes + 2 días, domingo + 3, y sabemos restar miércoles - 1. En efecto, sabemos hacer esto porque esta aritmética es la misma que la aritmética de un reloj de 7 horas. Basta convenir en cómo ordenar los días de la semana en un reloj de 7 horas. Convengamos entonces en poner: domingo = 0, lunes = 1, martes = 2, miércoles = 3, jueves = 4, viernes = 5 y sábado = 6.

Entonces:

**Martes + 5 días =  $2 + 5 \equiv 0 \pmod{7}$ .** Entonces, si hoy es martes en cinco días será 0 = domingo.

**Martes + 11 días =  $2 + 11 \equiv 6 \pmod{7}$ .** En once días será 6 = sábado.

4.1 Hacer las siguientes sumas y restas:  $4 + 3 - 2 \pmod{6}$   $10 + 9 - 4 \pmod{11}$

4.2 Calcular  $10 + 6 - 3 + 11$  en las aritméticas módulo 12, 15, 18 y 22.

4.3 Sumar  $10 + 10 + 10 + \dots$ , diez veces en la aritmética módulo 11, 12 y 20.

4.4 Calcular  $1 + 2 + 3 + \dots + 98 + 99 + 100 \pmod{2}$ . Ayuda: en la aritmética módulo 2 hay sólo dos números 0 y 1.

4.5 Calcular  $3 + 3 + \dots + 3 \pmod{9}$ . Ayuda: el resultado depende de la cantidad de sumandos. Más aún hay sólo tres respuestas posibles.

4.6. Demostrar que si  $m$  es impar, entonces  $1 + 2 + 3 + \dots + (m - 1) + m \equiv 0 \pmod{m}$

Para  
resolver



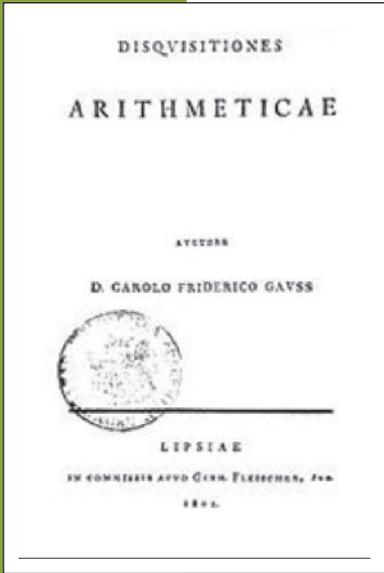
### □ 4.3. Los enteros módulo $m$

En esta sección presentaremos la construcción formal de la aritmética modular, que es el marco adecuado para describir el contenido de la sección anterior. Este marco también permite ampliar nuestras capacidades para definir otras operaciones, por ejemplo: la multiplicación modular.

Karl Friederich Gauss, el príncipe de las matemáticas, concibió y desarrolló sistemáticamente estos conceptos. Una de sus obras maestras, *Disquisitiones Arithmeticae* está dividida en siete secciones, de las cuales varias están dedicadas o relacionadas con la aritmética modular.

- I. Números congruentes en general.
- II. Congruencias de primer grado.





- III. Residuos de potencias.
- IV. Congruencias de segundo grado.
- V. Formas y ecuaciones indeterminadas de segundo grado.
- VI. Varias aplicaciones de las discusiones precedentes.
- VII. Ecuaciones definiendo secciones de un círculo.

### Múltiplos y divisores

Tomemos para empezar el número **5**. Los múltiplos enteros de **5** son: **5, 10, 15, 20, 25, 30, 35, ...** el **0** y también **-5, -10, -15, -20, -25, -30, -35, ...**

Los primeros, resultan de multiplicar **5** por **1, 2, 3, 4, 5, 6, 7**, etc; el **0** es múltiplo de **5** porque  $5 \cdot 0 = 0$ , y los últimos se obtienen multiplicando **5** por **-1, -2, -3, -4, -5, -6, -7**, etc. Recordamos que el conjunto de los números enteros es:

$$\mathbb{Z} = \{\dots -4, -3, -2, -1, 0, \dots 1, 2, 3, 4, \dots\}$$

Formalmente, el conjunto de todos los múltiplo de **5** es:

$$I_5 = \{k \cdot 5 : k \in \mathbb{Z}\}$$

El conjunto de todos los múltiplos de un entero **m** cualquiera es:

$$I_m = \{k \cdot m : k \in \mathbb{Z}\}$$

### Observaciones



- 1) El conjunto de múltiplos de **m** y el conjunto de múltiplo de **-m**, son iguales. Es decir,  $I_m = I_{-m}$
- 2) El conjunto de múltiplos del **0** tiene un sólo elemento, el **0**. El conjunto de múltiplos del **1** es el de todos los enteros. Es decir,  $I_0 = \{0\}$  y  $I_1 = \mathbb{Z}$ .
- 3) Los conjuntos  $I_m$ , con **m** distinto de **0**, son todos *coordinables*, es decir tienen la misma cantidad de elementos. En efecto la función **F** de **Z** en los múltiplos de **m** que le asigna al entero **k** el múltiplo de **m**, **km** es claramente una *biyección*. Es decir, es una asignación biunívoca que asigna a cada entero uno y sólo un múltiplo de **m**, y tal que todo múltiplo es asignado a algún entero. Así podemos referirnos sin ambigüedad al tercer múltiplo de **21**, el **63**, o al séptimo múltiplo de **13**, el **91**.
- 4) Si dibujamos los múltiplos de distintos **m** en la recta, veremos que los dibujos resultan del mismo tipo. De hecho, si lo miráramos desde muy lejos diríamos que son iguales. La única excepción es el caso de los múltiplos del **0**.

Si graficamos los múltiplos de un número dado en la recta (**Figura 4.3**), cualquiera sea el número, el gráfico se ve así:

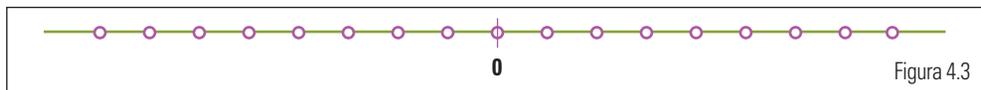


Figura 4.3

De la definición de múltiplos, se sigue que un entero  $r$  es múltiplo de otro  $m$ , si  $r \in I_m$ , es decir si existe un entero  $k$  tal que  $r = km$ . Esta definición alternativa de múltiplo de un número nos permite definir de manera similar el concepto de divisor.

**Definiciones.** Un entero  $r$  es múltiplo de otro  $m$ , si existe un entero  $k$  tal que  $r = km$ .  
Un entero  $s$  es divisor de otro  $m$ , si existe un entero  $k$  tal que  $m = ks$ .

Notar que  $s$  es divisor de  $m$  exactamente cuando  $m \in I_s$ .

El conjunto de múltiplos de un entero fijo  $m$  tiene propiedades respecto de las operaciones de suma y producto de números enteros que hay que destacar. Cuando decimos suma consideramos también la resta como parte de la suma, ya que  $a$  menos  $b$  es lo mismo que  $a$  más  $-b$ .

**Proposición.** Sea  $m$  un entero fijo. entonces:

1. la suma de dos múltiplos de  $m$ , es un múltiplo de  $m$ ,
2. el producto de un múltiplo de  $m$  por un entero cualquiera  $r$ , es un múltiplo de  $m$ .

Es decir, el conjunto  $I_m$  de múltiplos de  $m$  es cerrado para la suma (y la resta) y es absorbente para el producto, ya que basta que un factor esté en  $I_m$  para asegurar que el producto también esté.

**Demostración.** Tomemos dos múltiplos de  $m$ . Supongamos que estos son  $am$  y  $bm$ . Luego, su suma es  $am + bm = (a + b)m$ , que es también múltiplo de  $m$ . Además, el producto de uno de ellos  $am$  y un entero cualquiera  $c$ , es  $(am)c = (ac)m$ , que es múltiplo de  $m$ .

## Los días de la semana

Volvamos a la aritmética de la semana. El siguiente dibujo representa un período de tiempo en el que cada punto es un día. Hemos pintado los domingos color rojo, los lunes de color azul y el resto de los días de la semana de un color distinto cada uno. Así todos los días quedan repartidos en siete subconjuntos, cada uno formado por los puntos de un mismo color (Figura 4.4). Es decir, el primer subconjunto es el de los días domingos, el segundo el de los días lunes, etc.

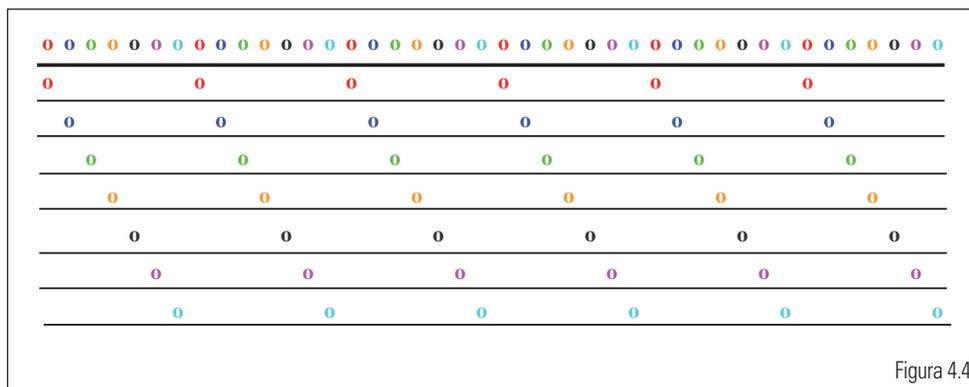


Figura 4.4

Si numeramos los días comenzando con **domingo** = 0, **lunes** = 1 y así hasta **sábado** = 6 entonces, este dibujo muestra una partición del conjunto de todos los enteros en siete subconjuntos. Desde el punto de vista de los múltiplos, los días domingo ó puntos **rojos** del dibujo son exactamente todos los múltiplos de 7; mientras que los días lunes ó puntos **azules** son todos múltiplos de 7 más 1. Los días martes en **verde** son todos dos unidades más grandes que un múltiplo de 7, éstos son 2, 9, 16, 23, 30, etc. Recíprocamente, si estamos en una posición dada para determinar qué día de la semana corresponde basta medir cuánto se pasa de un múltiplo de 7. Si estamos en la posición 67 hacemos:  $67 = 7 \cdot 9 + 4$ , y vemos que estamos en el día 4 de la semana, es decir en miércoles.

## La división entera

Antes de seguir avanzando es necesario recordar qué es la división entera. Es aquella división con resto.

**Demostración:** Si  $m = 0$ , ya está. Basta tomar  $q = 0$  y  $r = 0$  independientemente de  $n$ . Además, esta es la única elección posible. Supongamos

ahora que tanto  $m$  como  $n$  son naturales, es decir mayores que 0. En este caso, consideremos los múltiplos positivos de  $n$ :  $n, 2n, 3n, 4n, \dots$  etc. y seleccionemos sólo los menores o iguales que  $m$ , supongamos que son  $n, 2n, 3n, \dots, qn$ . Entonces,  $m - qn$  es mayor o igual que 0 y menor que  $n$ , de lo contrario el siguiente múltiplo de  $n$ ,  $(q + 1)n$ , sería todavía menor o igual que  $m$ . Así, si tomamos  $r = m - qn$  resulta lo que queremos:  $m = qn + r$  en las condiciones requeridas (ver figura 4.5).

**Conclusión.** El resto de la división de  $m$  por 7, determina el día de la semana (o el color) que le corresponde a  $m$  en este dibujo.

**Teorema.** Dado dos enteros  $m$  y  $n$ ,  $n$  distinto de 0, existen únicos enteros  $q$  y  $r$ , con  $0 \leq r < |n|$  tales que  $m = qn + r$ . El entero  $q$  es el cociente de  $m$  dividido  $n$  y  $r$  es el resto.

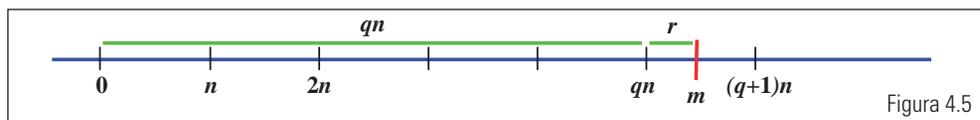


Figura 4.5

Ahora, si el divisor  $n$  es negativo, dividimos  $m$  por  $-n$  que es positivo; así tendremos que  $m = q(-n) + r$ . Pero entonces tenemos que  $m = (-q)n + r$ , es decir el cociente es  $-q$  y el resto el mismo  $r$ .

Si  $m$  es negativo, dividimos  $-m$ , que es positivo, por  $n$  que podemos suponer positivo; así tendremos  $-m = qn + r$ . De aquí resulta  $m = -qn - r$ , con  $-r$  negativo; como  $0 \leq r < n$  tenemos que  $0 < n - r \leq n$ .

Si  $n - r < n$  ponemos  $m = -qn - n + n - r = (-q - 1)n + (n - r)$  y vemos que ésta es la expresión deseada con  $r' = n - r$ . Si, en cambio, es  $n - r = n$ , es decir si  $r = 0$ , no hacemos nada y escribimos  $m = -qn$ .

Finalmente, veamos que  $q$  y  $r$  son únicos en las condiciones exigidas. Supongamos que  $m = qn + r$  y que también  $m = pn + s$ , entonces tendremos  $qn + r = pn + s$ . Entonces,  $qn - pn = s - r$ , pero esto no es posible ya que  $s - r$  es en valor absoluto menor que  $n$ , mientras que  $qn - pn = (q - p)n$  es en valor absoluto siempre mayor que  $n$ , salvo que sea 0. En este caso es  $q = p$ , y luego resulta  $s = r$ .

En la división entera:

- el resto es siempre positivo o  $0$ ;
- el cociente puede ser un entero negativo;
- no hay restricciones sobre el signo de  $m$  y  $n$ . Es decir, podemos dividir un número positivo por uno negativo, uno negativo por uno positivo o uno negativo por otro negativo;
- $n$  es múltiplo de  $m$ , si y sólo si el resto de la división de  $n$  por  $m$  es  $0$ .

Observaciones



Dados dos enteros  $m$  y  $n$  cualesquiera ( $n$  distinto de  $0$ ), dividir  $m$  por  $n$  es encontrar los enteros  $q$  y  $r$  que da el Teorema. Como ambos son únicos, en las condiciones del Teorema, toda vez que se haga la división se obtendrá el mismo resultado. Esto que parece una trivialidad, es una trivialidad. Por lo tanto, cuando dos personas obtengan resultados distintos para una misma división, al menos uno ¡está equivocado!

- La división de  $13$  por  $3$  es:  $13 = 4 \cdot 3 + 1$
- La división de  $13$  por  $-3$  es:  $13 = (-4) \cdot (-3) + 1$
- La división de  $-13$  por  $3$  es:  $-13 = (-5) \cdot 3 + 2$
- La división de  $-13$  por  $-3$  es:  $-13 = 5 \cdot (-3) + 2$

Ejemplo



4.7 Calcular:  $3$  dividido  $13$ ;  $-3$  dividido  $13$ ;  $3$  dividido  $-13$ ;  $-3$  dividido  $-13$ .

4.8 Supongamos  $n$  es un entero distinto de  $0$ . Calcular:  $0$  dividido  $n$ ;  $n$  dividido  $n$ ;  $-n$  dividido  $n$ ;  $n$  dividido  $-n$ ;  $-n$  dividido  $-n$ . Notamos que  $-n$  es el opuesto de  $n$ , que no necesariamente es negativo. El signo de  $-n$  es el opuesto que el de  $n$ . Si  $n = -13$ , entonces  $-n = 13$ .

4.9 Supongamos que  $n$  es un entero distinto de  $0$ . Calcular:  $n$  dividido  $2n$ ;  $-n$  dividido  $2n$ ;  $2n$  dividido  $n$ ;  $-2n$  dividido  $n$ .

Para resolver



## El máximo común divisor

Presentamos a continuación una definición formal de máximo común divisor y enunciamos algunas propiedades básicas que necesitaremos más adelante, y que quizá no resulten tan familiares.

**Definición.** Sean  $a$  y  $b$  enteros no nulos. El máximo común divisor de  $a$  y  $b$  es el mayor natural  $d$  que divide a ambos. Se denota  $d = (a, b)$ .

Algunas observaciones y propiedades elementales sobre esta definición.

- El máximo común divisor es simétrico, es decir  $(a, b) = (b, a)$ .
- Se puede tomar máximo común divisor de enteros positivos y negativos.
- El máximo común divisor de dos enteros es siempre mayor o igual que  $1$ .
- $(1, b) = 1$ , para todo entero  $b$  no nulo.
- $(a, b) = (-a, b)$   
 $= (a, -b)$

$= (-a, -b)$ , para todo par de enteros  $a$  y  $b$ . Recordamos una vez más que  $-a$  es el opuesto de  $a$  y, por lo tanto, no es necesariamente negativo; puede ser  $a = -4$  y así  $-a = 4$ .

## Ejemplos



Calculemos el máximo común divisor de  $21$  y  $-12$ . Comenzamos listando los divisores positivos de cada uno de ellos.

Los divisores positivos de  $21$  son:  $1, 3, 7$  y  $21$ .

Los divisores positivos de  $-12$  son:  $1, 2, 3, 4, 6$  y  $12$ .

Ahora, listamos los divisores positivos comunes; estos son:  $1$  y  $3$ . Por lo tanto, y de acuerdo a la definición, el máximo común divisor de  $21$  y  $-12$  es  $(21, -12) = 3$ .

**Proposición.** Sean  $a$  y  $b$  enteros no nulos. Sea  $d$  un entero positivo que divide a ambos, tal que si  $d'$  es otro divisor común positivo de ambos,  $d'$  divide a  $d$ . Entonces  $d$  es el máximo común divisor de  $a$  y  $b$ .

**Demostración.** Por hipótesis,  $d$  es un divisor natural común. Más aún, como es divisible por cualquier otro divisor común positivo se sigue que es el mayor de éstos. Luego,  $d$  satisface la definición de máximo común divisor.

Continuamos con otro resultado que caracteriza al máximo común divisor de otra manera y que nos será útil más adelante.

**Proposición.** Sean  $a$  y  $b$  enteros no nulos. El máximo común divisor de  $a$  y  $b$  es el menor entero positivo que es combinación lineal entera de  $a$  y  $b$ . Es decir, el menor entero positivo que se puede escribir de la forma  $d = ma + nb$  con  $m$  y  $n$  enteros.

**Demostración.** Veamos primero que  $d$  divide a  $a$  y divide a  $b$ , es decir que es un divisor común de  $a$  y  $b$ . Dividiendo  $a$  por  $d$  tenemos que  $a = qd + r$  con  $r$  positivo y menor que  $d$  o igual a  $0$ . Dividiendo  $b$  por  $d$  tenemos que  $b = pd + s$  con  $s$  positivo y menor que  $d$  o igual a  $0$ .

Supongamos que  $r$  es distinto de  $0$ , entonces  $r = a - qd$  es positivo y menor que  $d$ , y además

$$\begin{aligned} r &= a - qd \\ &= a - q(ma + nb) \\ &= a - qma - qnb \\ &= (1 - qm)a - (qn)b \end{aligned}$$

Así,  $d$  no es el menor entero positivo que se escribe como combinación lineal entera de  $a$  y  $b$ . Luego  $r = 0$  y  $d$  divide a  $a$ . Análogamente, se muestra que  $s = 0$  y  $d$  divide a  $b$ .

Finalmente, si  $d'$  es un natural que divide a  $a$  y  $b$ , entonces divide a  $d$ , pues si  $a = d'e$  y  $b = d'f$ , entonces:

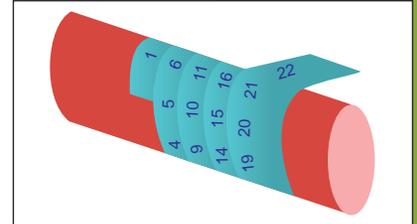
$$\begin{aligned} d &= ma + nb \\ &= m d'e + n d'f \\ &= d'(me + nf) \end{aligned}$$

Ahora, la proposición anterior asegura que  $d$  es el máximo común divisor de  $a$  y  $b$ .

### Los enteros módulo $m$ : $Z_m$

Recordemos el caso de los días de la semana. Pintamos cada día con un color distinto: los domingos de rojo, los lunes de azul, etc. En ese caso el número relevante era el 7. Ahora, en vez de 7 tomaremos cualquier entero  $m$  mayor que 1. Es decir  $m$  puede ser 2, 3, 17, 24 ó 1.245.

Para los días de la semana habíamos partido el conjunto de todos los enteros en los siete subconjuntos de días posibles. El conjunto de todos los días resultó ser la unión disjunta del subconjunto de todos los domingos, unión de todos los lunes, unión de todos los martes, etc.



Ahora, si en vez de 7 tenemos  $m$ , el conjunto de todos los enteros queda partido como unión disjunta de  $m$  subconjuntos: el subconjunto de múltiplos de  $m$ , el subconjunto de múltiplos de  $m$  corrido en 1 o múltiplos de  $m$  más 1, el subconjunto de múltiplos de  $m$  más 2, etc., hasta terminar con el subconjunto de múltiplos de  $m$  más  $m - 1$ .

Supongamos  $m = 5$ . Entonces:

$$Z = \{\dots, -15, -10, -5, 0, 5, 10, 15, 20, \dots\} \cup \{\dots, -14, -9, -4, 1, 6, 11, 16, 21, \dots\} \cup \{\dots, -13, -8, -3, 2, 7, 12, 17, 22, \dots\} \cup \{\dots, -12, -7, -2, 3, 8, 13, 18, 23, \dots\} \cup \{\dots, -11, -6, -1, 4, 9, 14, 19, 24, \dots\}$$

Ejemplo



En general, para un  $m$  cualquiera tendremos, como ya dijimos,  $m$  subconjuntos. El primero es el de los múltiplos de  $m$ , el segundo es el de todos los enteros cuyo resto en la división por  $m$  es 1, el tercero es el de los enteros con resto 2 en la división por  $m$ , y así sucesivamente.

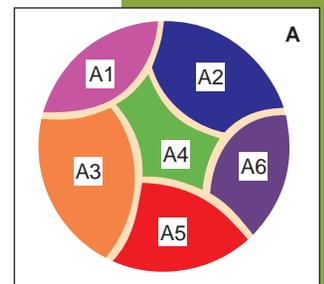
### Particiones y equivalencia

Tener una partición de un conjunto y tener, en ese conjunto, una relación de equivalencia es lo mismo.

**Regla.** El resto de la división por  $m$  decide en qué subconjunto estará un entero dado.

Recordemos

- Una *partición* de un conjunto  $A$  es una familia de subconjuntos  $A_i$  no vacíos y disjuntos, tales que su unión es todo el conjunto. En el dibujo, vemos una partición de  $A$  en seis partes.
- Una *relación de equivalencia* en  $A$ , es una relación binaria reflexiva, simétrica y transitiva.



Dada una partición de  $A$ , definimos la relación  $\sim$  diciendo que  $a \sim b$  si  $a$  y  $b$  están ambos en una misma parte. Es muy fácil verificar que esta relación es reflexiva, simétrica y transitiva.

Recíprocamente, dada una relación de equivalencia  $\sim$  en  $A$ , las partes de  $A$  son las clases de equivalencia de la relación. Es decir, cada parte está formada por todos los elementos relacionados con uno dado.

## La relación de congruencia módulo $m$

**Definición.** Dado un entero  $m > 1$  diremos que dos enteros  $a$  y  $b$  son equivalentes módulo  $m$ , si  $a$  y  $b$  tienen el mismo resto en la división por  $m$ . En este caso escribiremos  $a \equiv b \pmod{m}$ .

Esa definición es equivalente a esta otra.

$$a \equiv b \pmod{m} \text{ si } a - b \text{ es múltiplo de } m.$$

**Demostración.** En efecto, si  $a$  y  $b$  tienen el mismo resto en la división por  $m$ , entonces tenemos que  $a = q_1 m + r$  y que  $b = q_2 m + r$ , luego  $a - b = q_1 m - q_2 m = (q_1 - q_2) m$ . Esto muestra que  $a - b$  es un múltiplo de  $m$ .

Recíprocamente, si  $a$  tiene un resto  $r_1$  en la división por  $m$  y  $b$  tiene resto  $r_2$ , y  $a - b$  es múltiplo de  $m$ , entonces tenemos que  $a = q_1 m + r_1$  y que  $b = q_2 m + r_2$ , luego  $a - b = (q_1 - q_2) m + (r_1 - r_2)$ . Pero como  $a - b$  es múltiplo de  $m$ , entonces  $a - b - (q_1 - q_2) m = (r_1 - r_2)$  es múltiplo de  $m$ , pero esto es sólo posible si  $r_1 - r_2 = 0$  y luego  $r_1 = r_2$  como queríamos.

**Proposición.** La relación  $\equiv \pmod{m}$  es de equivalencia. Las clases de equivalencia están formadas por los enteros con el mismo resto en la división por  $m$ .

**Demostración.** La relación de congruencia módulo  $m$  es claramente reflexiva y simétrica, ya que  $a$  tiene el mismo resto que  $a$  en la división por  $m$  y, si  $a$  tiene el mismo resto que  $b$  entonces  $b$  tiene el mismo resto que  $a$ . Veamos que es transitiva. Sean  $a$  y  $b$  con el mismo resto en la división por  $m$  y sea  $c$  con el mismo resto que  $b$  en la división por  $m$ . Entonces el resto de  $a$  y el resto de  $c$  en la división por  $m$  son iguales.

Con lo que sabemos ahora, podemos afirmar que para el caso de los días de la semana, la partición de todos los días, en días domingo, lunes, martes, etc. es la misma que da la relación de equivalencia  $\equiv \pmod{7}$ .

Llamaremos conjunto de enteros módulo  $m$  al conjunto  $Z_m$ . Este conjunto sólo tiene  $m$  elementos. Cada elemento de este conjunto es un subconjunto infinito de enteros, es toda una clase de equivalencia de la relación  $\equiv \pmod{m}$ .

El conjunto de clases de equivalencia de la relación  $\equiv \pmod{m}$  se denota  $Z_m$ .

Los enteros  $0, 1, 2, 3, \dots, m-1$  pertenecen a clases distintas y, por lo tanto, son un conjunto de representantes de todas las clases. Usualmente elegiremos estos representantes. Como notación

usaremos simplemente  $a$  para referirnos a su clase (esto no causará confusión porque del contexto quedará claro si nos referimos al entero  $a$  o la clase de congruencia de  $a$  módulo  $m$ ). De todas formas, para referirnos a la clase de un entero cualquiera  $a$  también podemos usar  $[a]$ .

Para el caso de los días de la semana, tomar clase es preguntarse qué día de la semana cae un cierto día. Identificar si ese día es lunes o miércoles es determinar su clase de congruencia módulo 7.

Veamos otros casos. Tomemos  $m = 15$  y analicemos qué es  $Z_{15}$ . Sabemos que  $Z_{15}$  es un conjunto con 15 elementos, cada uno de sus elementos es un subconjunto infinito de enteros que tienen un mismo resto en la división por 15. Así los enteros 1, 16, 31 y 46 están en un mismo subconjunto. Esto se resume diciendo que:

$$\begin{aligned} 1 &\equiv 16 \\ &\equiv 31 \\ &\equiv 46 \pmod{15} \end{aligned}$$

Cada uno de estos 15 conjuntos tiene un miembro distinguido. Estos son: 0, 1, 2, ..., 14. Luego, para identificar a qué clase pertenece un entero dado basta decir con cuál de éstos comparte clase. Así, para identificar la clase a la que pertenece el 1.542, basta decir  $1.542 \equiv 12 \pmod{15}$ .

Veamos algunos ejemplos simples. Tomemos los números 247 y -58 y calculemos sus clases de congruencia módulo 2, 3, 5, 9 y 11.

**Aclaración que aclara.** Cuando decimos calcular la clase de congruencia de un entero dado  $a$  módulo un  $m$  dado, debemos encontrar el único de los enteros  $0, 1, 2, \dots, m-1$  que es congruente con  $a$  módulo  $m$ . Esto no es otra cosa que calcular el resto de la división de  $a$  por  $m$ .

$$\begin{array}{ll} 247 \equiv 1 \pmod{2} & -58 \equiv 0 \pmod{2} \\ 247 \equiv 1 \pmod{3} & -58 \equiv 2 \pmod{3} \\ 247 \equiv 2 \pmod{5} & -58 \equiv 2 \pmod{5} \\ 247 \equiv 4 \pmod{9} & -58 \equiv 5 \pmod{9} \\ 247 \equiv 5 \pmod{11} & -58 \equiv 8 \pmod{11} \end{array}$$

4.10 Calcular las clases de congruencia módulo 7 de los siguientes enteros: 13, -18, 1.743.

4.11 Encontrar un número entre 23 y 29 que sea congruente a 1 módulo 5.

Para resolver



## Suma y producto módulo $m$

De la misma forma en que sumamos horas en el reloj de 12 horas y días de la semana podremos sumar enteros módulo  $m$ . Más aun, podremos también multiplicarlos.

Para sumar o multiplicar dos enteros módulo  $m$  se toma un representante de cada uno, se suman o multiplican, y finalmente se considera la clase del resultado.

**Definición.** Dado un entero  $m$  mayor que 1 y dados  $[a]$  y  $[b]$  en  $Z_m$ , definimos la suma de enteros módulo  $m$  por  $[a] + [b] = [a + b]$ , y el producto de enteros módulo  $m$  por  $[a] \cdot [b] = [a \cdot b]$ .

## Ejemplos

$$6 + 5 \equiv 3 \pmod{8}$$

$$6 \cdot 5 \equiv 6 \pmod{8}$$

$$6 + 5 \equiv 1 \pmod{5}$$

$$6 \cdot 5 \equiv 0 \pmod{5}$$

$$6 + 5 \equiv 2 \pmod{3}$$

$$6 \cdot 5 \equiv 0 \pmod{3}$$



## Para resolver

4.12 Decir si es correcto o no:

$$23 \equiv 3 \pmod{8}$$

$$42 \equiv 1 \pmod{7}$$

$$-37 \equiv 1 \pmod{3}$$

4.13 En todos los casos encontrar el menor  $x$  no negativo que verifique la identidad planteada:

$$76 \equiv x \pmod{8}$$

$$83 \equiv x \pmod{7}$$

$$-22 \equiv x \pmod{3}$$

## □ 4.4. La aritmética modular

La suma y el producto de los enteros módulo  $m$  son operaciones heredadas de la suma y el producto de los enteros. Lo mismo sucedió con la aritmética del reloj o la aritmética de la semana. Las propiedades básicas, que listamos a continuación, son heredadas de las correspondientes propiedades de la aritmética de los enteros.

## Propiedades



Sea  $m$  un entero,  $m > 1$ . Entonces, la suma y el producto de enteros módulo  $m$  tienen las siguientes propiedades.

1. La suma es asociativa.
2. La suma es conmutativa.
3. La clase del  $0$ ,  $[0]$ , es el elemento neutro para la suma.
4. Toda clase  $[a]$  tiene un opuesto para la suma  $[m - a]$  que llamamos  $-[a]$ .
5. El producto es asociativo.
6. El producto es conmutativo.
7. La clase del  $1$ ,  $[1]$ , es el elemento neutro o identidad para el producto.
8. El producto es distributivo respecto a la suma.

A modo de ejemplo, veamos cómo se demuestran algunas de esas propiedades.

Para la suma (el resto se deduce de manera análoga):

$$\begin{aligned}
 * \text{ asociatividad de la suma: } & \quad ([a] + [b]) + [c] \equiv [a + b] + [c] \\
 & \quad \equiv [(a + b) + c] \\
 & \quad \equiv [a + (b + c)] \\
 & \quad \equiv [a] + ([b + c])
 \end{aligned}$$

$$* \text{ opuesto para la suma: } [a] + [-a] \equiv [a - a] \equiv [0]. \text{ Además } [m - a] \equiv [-a].$$

Hasta aquí, las analogías con la aritmética de los números enteros. Ahora, veamos que hay algunas diferencias. Por ejemplo, en  $\mathbb{Z}_{12}$ ,  $6 + 6 = 0$ . Esto no pasa en los enteros. Nunca obtenemos  $0$  sumando un mismo número dos veces. En general, en  $\mathbb{Z}_m$  si sumamos  $m$  veces  $1$  obtenemos  $0$ , es decir  $1 + 1 + \dots + 1 = 0$  si hay  $m$  sumandos. Por otro lado, por ejemplo en  $\mathbb{Z}_5$ ,  $4 \cdot 4 = 1$ , es decir  $4$  al cuadrado es  $1$ , y también  $3 \cdot 2 = 1$ . Hay números distintos de la identidad o su opuesto que son inversibles para el producto. En cambio, para el producto de enteros los únicos inversibles son el  $1$  y su opuesto el  $-1$ .

Para los enteros, se puede aprender de memoria las tablas de multiplicar del 2, del 3, etc., hasta la del 10. Pero, como los enteros son infinitos, es imposible saber de memoria todas las tablas de multiplicar. En cambio, para los enteros módulo  $m$ , sólo hay una cantidad finita de tablas que aprender, porque es finita la cantidad de enteros módulo  $m$ .

A continuación, mostramos las tablas de suma y multiplicación completas, es decir para todos los enteros módulo  $m$  juntos, para algunos valores pequeños de  $m$ .

Tablas de suma y multiplicación de  $\mathbb{Z}_m$  para  $m : 2 \dots 8$

$\mathbb{Z}_2$ :

+	0	1
0	0	1
1	1	0

.	0	1
0	0	0
1	0	1

$\mathbb{Z}_3$ :

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

.	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$\mathbb{Z}_4$ :

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

.	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

$\mathbb{Z}_5$ :

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

.	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

$\mathbb{Z}_6$ :

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

.	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

$$Z_7:$$

+	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

.	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

$$Z_8:$$

+	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

.	0	1	2	3	4	5	6	7
0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7
2	0	2	4	6	0	2	4	6
3	0	3	6	1	4	7	2	5
4	0	4	0	4	0	4	0	4
5	0	5	2	7	4	1	6	3
6	0	6	4	2	0	6	4	2
7	0	7	6	5	4	3	2	1

Cada una de estas tablas tiene sus propias regularidades, que se distinguen a simple vista. Además, el conjunto de tablas tiene también otras regularidades que son algo más difíciles de explicitar.

Con las tablas a mano, discutamos sobre estas regularidades.

### Pares y nones

Las tablas de  $Z_2$  no son más que las reglas de sumar y multiplicar pares e impares. En efecto, los enteros pares son exactamente los congruentes a 0 módulo 2, y los impares son exactamente los congruentes a 1 módulo 2. Entonces, **par + par = par**, **par + impar = impar** e **impar + impar = par**. Esto se corresponde con que  $0 + 0 = 0$ ,  $0 + 1 = 1$  y  $1 + 1 = 0$  en  $Z_2$ .

La situación con el producto es análoga. Es decir, **par . par = par**, **par . impar = impar** e **impar . impar = impar**. Esto se corresponde con que  $0 . 0 = 0$ ,  $0 . 1 = 0$  y  $1 . 1 = 1$  en  $Z_2$ .

### Regularidad en la tabla de la suma

Es evidente que en las filas de las tablas de la suma aparecen todos los números ordenados y en forma cíclica. Más aun, entre una fila dada y la próxima, la diferencia es un corrimiento a la derecha en una unidad. Claro, esta última fila se obtiene de la anterior sumando 1.

### Divisores de cero

En todas las tablas de multiplicación tenemos que en la primera fila y en la primera columna son todos ceros, esto es así pues  $0 . a = 0$  y  $a . 0 = 0$  para todo  $a$ . Lo que llama

la atención es que en algunas tablas no hay más ceros que éstos (digamos obligatorios) y en cambio en otras hay más ceros. Por ejemplo, en la tabla de  $Z_4$  vemos que  $2 \cdot 2 = 0$ . Un par de elementos distintos de cero que multiplicados dan cero, se llaman *divisores de cero*. Nos podemos hacer una primera pregunta:

### ¿qué tablas tienen divisores de cero?

Otra pregunta, más fina aún, es:

### ¿cuáles son exactamente todos los divisores de cero que hay en $Z_m$ para cada $m$ ?

Mirando las tablas, observamos que las que corresponden a  $m = 4, 6, y 8$  tienen divisores de cero, mientras que las que corresponden a  $m = 2, 3, 5$  y  $7$  no tienen divisores de cero. Estos últimos son números primos y los primeros son números compuestos. La respuesta a la primera pregunta es:

Supongamos que  $a$  y  $b$  son dos números distintos de  $0$  en  $Z_m$  con  $a \cdot b = 0$ . En primer lugar,

Si  $m$  es primo, entonces  $Z_m$  no tiene divisores de cero.  
Si  $m$  no es primo, entonces  $Z_m$  tiene divisores de cero.

podemos suponer que tanto  $a$  como  $b$  son menores que  $m$ , como lo son los elementos de la tabla. Luego  $a \cdot b = 0$  en  $Z_m$  quiere decir que  $a \cdot b$  es múltiplo de  $m$ , es decir  $a \cdot b = k \cdot m$ . Si  $m$  es primo, se sigue que  $m$  divide a  $a$  o  $m$  divide a  $b$ ; pero como ambos son menores que  $m$  esto no es posible y  $m$  no es primo.

Por otro lado, si  $m$  no es primo, entonces  $m = a \cdot b$  con  $a$  y  $b$  menores que  $m$ , luego en  $Z_m$  tenemos que  $a \cdot b = 0$ . Es decir,  $Z_m$  tiene divisores de cero.

### Unidades

En todas las tablas de multiplicación vemos algunas unidades. En todas vemos al  $1$  y al  $m - 1$  como unidades. Esto es porque siempre  $1 \cdot 1 = 1$ , además siempre  $m - 1 = -1$  en  $Z_m$  y  $-1 \cdot -1 = 1$ . Ahora en varias tablas aparecen más unidades.

### ¿Qué tablas tienen otras unidades?

Para aquellas tablas con otras unidades no triviales, es decir distintas de  $1$  y  $-1$ ,

### ¿cuáles son todas las unidades no triviales?

Si hiciéramos muchas más tablas, veríamos que todas tendrán unidades no triviales. Sólo  $Z_2, Z_3, Z_4,$  y  $Z_6$ , no tienen otras unidades. Esto se puede deducir se la siguiente verdad.

**Un  $a$  en  $Z_m$  es inversible si y sólo si  $(a, m) = 1$ .**

$a$  y  $m$  se dicen *coprimsos* si el máximo común divisor de ellos  $(a, m)$  es  $1$ .

Aclaración

En efecto, si  $a$  es inversible, entonces existe  $b$  tal que  $a b = 1$ , en  $Z_m$ . Es decir,  $a b - 1 = k m$  o, equivalentemente,  $1 = a b - k m$ . Luego, si  $d$  es el máximo común divisor de  $a$  y  $m$ , tanto  $m$  como  $a$  son múltiplos de  $d$ . Así resulta que  $1$  es múltiplo de  $d$ , lo que sólo es posible si  $d = 1$ .

Recíprocamente, si  $a$  y  $m$  son coprimos, entonces  $1 = a t + m s$  (recordemos que siempre el máximo común divisor de dos números se puede escribir como combinación lineal entera de ellos). Tomando clase de congruencia y dado que  $m s$  es  $0$  en  $Z_m$ , resulta que  $1 = a t$  en  $Z_m$ .

## Cuadrados perfectos

Los cuadrados perfectos son aquellos números que aparecen en la diagonal de la tabla de multiplicación; son los resultados de hacer  $a \cdot a = a^2$  para algún  $a$ . El estudio de estos cuadrados perfectos fue, en la historia de la teoría de números, un hito. Más adelante en este capítulo volveremos a esto bajo el título La Reciprocidad Cuadrática.



Para resolver

4.14 Mirando las tablas de multiplicación escritas más arriba, listar los cuadrados perfectos de de cada una de ellas.

4.15 Observar que en todos los casos el producto de unidades es otra unidad. ¿Cómo se explica esto?

## □ 4.5. Aplicaciones a la aritmética entera



La resolución de ecuaciones acaparó, desde tiempos remotos, mucha atención de la ciencia matemática y muchísimos matemáticos han dedicado vidas enteras a su estudio y al desarrollo de métodos para encontrar soluciones a las mismas. Hoy en día, sigue siendo un área de muy vasta de investigación y, a pesar de todos los resultados alcanzados, queda muchísimo por hacer.

Cuando decimos ecuaciones sin más aclaraciones, incluimos todo tipo de ecuaciones, es decir, consideramos aquellas con más de una variable, con coeficientes en distintos conjuntos de números y sistemas de ecuaciones de estos tipos. Además, dada una ecuación o dado un sistema de ecuaciones con coeficientes en cierto conjunto de números podemos buscar soluciones en el mismo conjunto donde viven los coeficientes, o restringir la búsqueda

de soluciones a un conjunto más chico, o permitir soluciones en conjuntos más grandes. Muchas veces, sólo interesan las soluciones reales de una ecuación polinomial, aunque también tenga soluciones complejas; o sólo interesan las soluciones enteras que pueda tener esa misma ecuación. Otras veces, se consideran las soluciones reales o complejas de una ecuación polinomial con coeficientes enteros o racionales.

Repasemos algunos conceptos para ecuaciones polinomiales con una sola variable con coeficientes reales. Por ejemplo:

$$x^2 + 1 = 0; \quad 3x^3 - 2x^2 + 1 = 0; \quad 5x^4 + x^3 - 2x + 3 = 0; \quad ax^2 + bx + c = 0.$$

Sabemos que:

- 1) algunas no tienen ninguna solución real, por ejemplo la primera,
- 2) todas tienen soluciones complejas. Más aún, tienen tantas como su grado, si se cuentan con multiplicidad,
- 3) las de grado impar siempre tienen al menos una solución real,
- 4) para las de grado 2 hay una fórmula para sus 2 soluciones complejas.

Las tres primeras ecuaciones del ejemplo tienen coeficientes enteros. Para éstas, podríamos preguntar si las soluciones son o no enteras. O simplemente, podríamos preguntar si tienen o no soluciones enteras, sin importar que tengan otras soluciones.

### Ecuaciones enteras

La aritmética modular es una herramienta que ayuda a estudiar ecuaciones enteras.

No pretendemos dar ningún método sistemático para tratar estos problemas. Sin embargo, sí queremos reforzar la impresión de que la aritmética modular es una herramienta efectiva en diversos problemas con números enteros.

El principio general es que para estudiar un problema entero puede ser más fácil estudiar las versiones modulares del mismo problema. Cambiamos un problema por muchos problemas similares más fáciles.

Veamos este principio en algunos ejemplos.

¿Tiene la ecuación  $3X + 2Y = 1$  soluciones enteras? Si tiene, ¿cuáles son todas sus soluciones enteras?

Ejemplo



Luego de contemplar esta ecuación y haciendo algunas pruebas podemos ver que  $a = 1$  y  $b = -1$  es solución, pues:

$$3 \cdot 1 + 2 \cdot (-1) = 3 - 2 = 1$$

Quizá sea un poco más difícil darse cuenta de que  $a = 3$  y  $b = -4$  también es solución, pues

$$3 \cdot 3 + 2 \cdot (-4) = 9 - 8 = 1$$

Podríamos continuar buscando, pero ¿hasta cuándo?

Por otro lado, el par  $(0, 0)$  no es solución, ya que si  $X = 0$  e  $Y = 0$ , entonces  $3X + 2Y = 0$  y no  $3X + 2Y = 1$ .

Analicemos esta ecuación bajo algunas congruencias. Como **2** y **3** aparecen en ella, no parece absurdo empezar con **2** y **3**. Supongamos que el par  $(X, Y)$  es solución de la ecuación, entonces tendremos que  $3X + 2Y \equiv 1 \pmod{2}$  y también  $3X + 2Y \equiv 1 \pmod{3}$ .

En el primer caso estaremos analizando cuestiones de paridad. Como  $3X + 2Y \equiv X \pmod{2}$ , pues  $3X \equiv X \pmod{2}$  y  $2Y \equiv 0 \pmod{2}$ , si  $3X + 2Y \equiv 1$ , entonces debe ser  $X \equiv 1 \pmod{2}$ , es decir si hay solución  $X$  debe ser impar.

En el segundo caso, como  $3X + 2Y \equiv -Y \pmod{3}$  debe ser  $-Y \equiv 1 \pmod{3}$ , que es lo mismo que  $Y \equiv -1 \pmod{3}$ .

Resumiendo, si  $(X, Y)$  es solución debe ser  $X = 2n + 1$ , y debe ser  $Y = 3m - 1$ . Reemplazando en la ecuación resulta que :

$$3X + 2Y = 3(2n + 1) + 2(3m - 1) = 1$$

que es lo mismo que  $6n + 3 + 6m - 2 = 1$ , o lo mismo que  $6(n + m) = 0$ . De aquí se deduce que  $m = -n$ . Recíprocamente, si tomamos  $n$  y  $m$  tales que  $m = -n$  y a partir de ellos construimos  $X = 2n + 1$  e  $Y = 3m - 1 = -3n - 1$  éstos serán solución de la ecuación.

Como conclusión, tenemos que la ecuación  $3X + 2Y = 1$  tiene soluciones enteras y todas las soluciones son de la forma  $X = 2n + 1$  e  $Y = -3n - 1$ , donde  $n$  es un entero cualquiera. Podemos explicitar algunas.

Si $n = 0$	$X = 1, Y = -1$	Si $n = -1$	$X = -1, Y = 2$
Si $n = 1$	$X = 3, Y = -4$	Si $n = -2$	$X = -3, Y = 5$
Si $n = 2$	$X = 5, Y = -7$	Si $n = -3$	$X = -5, Y = 8$

## Reglas de divisibilidad

La aritmética modular es particularmente adecuada para estudiar problemas de divisibilidad. Recordemos que un número entero  $n$  es divisible por  $m$ , si y sólo si  $n = 0$  en  $\mathbb{Z}_m$  es decir si  $n$  es congruente a  $0$  módulo  $m$ . Esto nos permitirá deducir y explicar las reglas de divisibilidad que conocemos y además obtener otras.

¿Qué reglas conocemos? Seguramente, las reglas de divisibilidad por **2** y por **5**. Quizá también la de divisibilidad por **3** y alguna más. Comencemos con algunos ejemplos.

### Ejemplos



#### Ejemplos de divisibilidad

1)  $124$  es divisible por  $4$ , pues  $124 = 100 + 20 + 4$   
 $\equiv 0 + 0 + 0$   
 $\equiv 0 \pmod{4}$

2) ¿Para qué valores de  $n$  el número  $3^n + 1$  es divisible por  $4$ ?

- Si  $n = 1$  -----  $3^n + 1 = 4$ , que sí es divisible por 4.
- Si  $n = 2$  -----  $3^n + 1 = 10$ , que no es divisible por 4.
- Si  $n = 3$  -----  $3^n + 1 = 28$ , que sí es divisible por 4.
- Si  $n = 4$  -----  $3^n + 1 = 82$ , que no es divisible por 4.
- Si  $n = 5$  -----  $3^n + 1 = 244$ , que sí es divisible por 4.
- Si  $n = 6$  -----  $3^n + 1 = 730$ , que no es divisible por 4.

Este experimento hace tentador arriesgar que  $3^n + 1$  es divisible por 4 exactamente cuando  $n$  es impar. ¿Podremos probar esto para todo  $n$ ? Sí, podemos.

Primer paso, observamos que  $3 \equiv -1 \pmod{4}$ . Esta es la clave porque entonces  $3^n \equiv (-1)^n \pmod{4}$ , según sea  $n$  par o impar. Finalmente,  $3^n + 1 \equiv (-1)^n + 1 \equiv 2 \pmod{4}$  ó  $0$ , según sea  $n$  par o impar, como queríamos.

## □ 4.6. Las reglas de divisibilidad de los naturales

Las reglas de divisibilidad son reglas prácticas que permiten determinar si un número natural dado es divisible por 2, 3, 5, etc. en términos de sus dígitos decimales. Por ejemplo, un número es divisible por 2, es decir es par si su último dígito es par.

Estas reglas dependen de la escritura del número en base 10. Luego, no sirven para determinar si el número  $124^2 - 11$  expresado así es divisible por 3 o no. Si quisiéramos aplicar la regla de divisibilidad por 3, primero debemos escribir  $124^2 - 11$  como 15.365 para aplicarla luego.

Recordemos algunas de las reglas de divisibilidad más fáciles.

**Divisibilidad por 2:** un número es divisible por 2, si el dígito de las unidades es par, es decir si es 0, 2, 4, 6 u 8.

**Divisibilidad por 5:** un número es divisible por 5, si el dígito de las unidades es divisible por 5, es decir es 0 ó 5.

**Divisibilidad por 3:** un número es divisible por 3, si la suma de sus dígitos es divisible por 3.

**Divisibilidad por 9:** un número es divisible por 9, si la suma de sus dígitos es divisible por 9.

Las dos últimas reglas de divisibilidad, por 3 y por 9, son distintas de las primeras, ya que incluyen determinar si otro número es divisible por 3 ó 9, respectivamente. Sin embargo, estos números son mucho más chicos que los originales, así iterando esta regla llegaremos a un punto en el que podremos determinar si el número en cuestión es divisible por 3 o por 9 por simple inspección. A modo de ejemplo, determinemos si el número

**$A = 123456789123456789123456789123456789123456789123456789123456789$**

es divisible por 3 o no. La suma de sus dígitos es 315, cuyos dígitos suman 9. Como 9 es divisible por 3, entonces 315 también es divisible por 3, luego  $A$  es divisible por 3.

A continuación, deducimos estas reglas y algunas más usando la aritmética modular. Una vez que las hayamos comprendido se podrá enunciar otras reglas de divisibilidad.

## Divisibilidad por 2

Supongamos que queremos determinar si 3.257 es divisible por 2 o no. Esto es lo mismo que determinar si 3.257 es congruente a 0 módulo 2 o no. Por lo tanto, debemos calcular la clase de congruencia de 3.257 módulo 2. Para esto resulta conveniente escribir 3.257 de la siguiente forma:

$$3.257 = 3 \cdot 10^3 + 2 \cdot 10^2 + 5 \cdot 10 + 7.$$

Esto no es más que nuestro sistema decimal.

Ahora, si planteamos lo que necesitamos saber:  $3.257 \equiv X \pmod{2}$ , que es equivalente a plantear  $3.257 = 3 \cdot 10^3 + 2 \cdot 10^2 + 5 \cdot 10 + 7 \equiv X \pmod{2}$ , y dado que  $10 \equiv 0 \pmod{2}$ , resulta que :

$$3.257 = 3 \cdot 10^3 + 2 \cdot 10^2 + 5 \cdot 10 + 7 \equiv 7 \pmod{2}.$$

El que determinar si todo el número  $3.257 = 3 \cdot 10^3 + 2 \cdot 10^2 + 5 \cdot 10 + 7$  es o no divisible por 2 es su último dígito, el 7. En este caso, claro está, 7 no es par y 3.257 tampoco.

Repitamos esto en general. Si en vez de 3.257, tenemos el número  $a_r a_{r-1} \dots a_3 a_2 a_1 a_0$ , también escrito en sistema decimal, donde los  $a$ 's son sus dígitos decimales, tenemos que:

$$a_r a_{r-1} \dots a_3 a_2 a_1 a_0 = a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \dots + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$$

Nuevamente, como  $10 \equiv 0 \pmod{2}$ , resulta que:

$$a_r a_{r-1} \dots a_3 a_2 a_1 a_0 = a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \dots + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \equiv a_0 \pmod{2}.$$

Conclusión:  $a_r a_{r-1} \dots a_3 a_2 a_1 a_0$  es divisible por 2 si su último dígito,  $a_0$ , lo es.

## Divisibilidad por 5

Sea  $A = a_r a_{r-1} \dots a_3 a_2 a_1 a_0$ . Tomando congruencia módulo 5, y dado que  $10 \equiv 0 \pmod{5}$ , tenemos que:

$$a_r a_{r-1} \dots a_3 a_2 a_1 a_0 = a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \dots + a_3 \cdot 10^3 + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \equiv a_0 \pmod{5}.$$

Conclusión:  $a_r a_{r-1} \dots a_3 a_2 a_1 a_0$  es divisible por 5, si su último dígito,  $a_0$ , lo es.

### Divisibilidad por 3

Sea  $A = a_r a_{r-1} \dots a_3 a_2 a_1 a_0$ . Tomando congruencia módulo 3, y dado que  $10 \equiv 1 \pmod{3}$ , tenemos que:

$$\begin{aligned} a_r a_{r-1} \dots a_2 a_1 a_0 &= a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \dots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \\ &\equiv a_r + a_{r-1} + \dots + a_2 + a_1 + a_0 \pmod{3}. \end{aligned}$$

Conclusión:  $a_r a_{r-1} \dots a_3 a_2 a_1 a_0$  es divisible por 3, si la suma de sus dígitos es divisible por 3.

### Divisibilidad por 9

Sea  $A = a_r a_{r-1} \dots a_3 a_2 a_1 a_0$ . Tomando congruencia módulo 9, y dado que  $10 \equiv 1 \pmod{9}$ , tenemos que:

$$\begin{aligned} a_r a_{r-1} \dots a_2 a_1 a_0 &= a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \dots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0 \\ &\equiv a_r + a_{r-1} + \dots + a_2 + a_1 + a_0 \pmod{9}. \end{aligned}$$

Conclusión:  $a_r a_{r-1} \dots a_3 a_2 a_1 a_0$  es divisible por 9, si la suma de sus dígitos es divisible por 9.

### Divisibilidad por 11

Sea  $A = a_r a_{r-1} \dots a_3 a_2 a_1 a_0$ . En este caso, tomando congruencia módulo 11, tenemos una novedad.

Ahora  $10 \equiv -1 \pmod{11}$ , y luego  $10^2 \equiv 1 \pmod{11}$ .

En general,  $10^k \equiv 1 \pmod{11}$  si  $k$  es par y  $10^k \equiv -1 \pmod{11}$  si  $k$  es impar. Entonces, resulta que:

Si  $A = a_r a_{r-1} \dots a_3 a_2 a_1 a_0$ , con  $r$  par, es decir  $A$  tiene un número impar de dígitos, entonces  $a_r a_{r-1} \dots a_2 a_1 a_0 = a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \dots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$

$$\equiv a_r - a_{r-1} + \dots + a_2 - a_1 + a_0 \pmod{11}.$$

Si  $A = a_r a_{r-1} \dots a_3 a_2 a_1 a_0$ , con  $r$  impar, es decir  $A$  tiene un número par de dígitos, entonces  $a_r a_{r-1} \dots a_2 a_1 a_0 = a_r \cdot 10^r + a_{r-1} \cdot 10^{r-1} + \dots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$

$$\equiv -a_r + a_{r-1} - \dots - a_2 + a_1 - a_0 \pmod{11}.$$

Conclusión:  $a_r a_{r-1} \dots a_3 a_2 a_1 a_0$  es divisible por 11, si la suma alternada de sus dígitos es divisible por 11. No importa cómo se realice la suma alternada de los dígitos, es decir no importa empezar con + o con - ya que una suma alternada es la opuesta de la otra suma alternada, y así ambas son divisibles por 11, o ambas no lo son.

---

## □ 4.7. Ecuaciones lineales en la aritmética modular

---

Hasta aquí, hemos aprendido la aritmética elemental de los enteros modulares. Demos un paso hacia adelante y consideremos ecuaciones de grado 1 con una sola incógnita. Esto

resultará más complicado que el estudio de las mismas ecuaciones en los enteros o en los números reales. Sin embargo, daremos una respuesta completa y totalmente satisfactoria.

Recordemos cuál es la situación en el caso de los enteros o de los reales. La ecuación  $3X + 1 = 0$  tiene siempre una solución real, que se obtiene despejando. Si  $3X + 1 = 0$ , entonces  $3X = -1$  y  $X = -1/3$ . Más aún, esta es la única solución real. Si nos preguntamos si esta misma ecuación tiene o no soluciones enteras, basta mirar su única solución real y ver si es o no entera. En este caso como  $-1/3$  no es entero, la ecuación no tiene solución entera.

La ecuación  $AX + B = 0$ , suponiendo  $A$  distinto de  $0$  tiene siempre una solución real, más precisamente  $X = -B/A$ . Más aun, esta solución es única.

¿Qué pasa con este mismo tipo de ecuaciones en el mundo modular?

## Ejemplos

$$2X + 2 \equiv 1 \pmod{4}$$

$$3X + 2 \equiv 1 \pmod{4}$$



Resolver una ecuación es encontrar al menos una solución, si la hay. Explicar claramente que no hay, si no las hay. Finalmente, en el caso de haber soluciones, darlas todas.

Al principio de esta sección consideramos una ecuación y buscábamos soluciones reales o enteras. Los conjuntos en los que buscábamos esas soluciones eran muy grandes, de hecho infinitos.

En cambio, en las ecuaciones del ejemplo buscamos soluciones en un conjunto finito y muy chico. Buscamos soluciones en  $Z_4$  que tiene sólo 4 elementos, entonces podemos probar con todos ellos y ver qué resulta. Evaluamos, operando con la suma y la multiplicación de  $Z_4$  los miembros de la izquierda de cada ecuación en todos los elementos de  $Z_4$ , el 0, el 1, el 2 y el 3.

Con esto es posible resolver estas dos ecuaciones completamente. En la primera tabla vemos que como resultado de la evaluación sólo obtuvimos los números 0 y 2. No obtuvimos el 1. Luego, la primera ecuación del ejemplo no tiene ninguna solución módulo 4. En cambio, en la segunda tabla obtuvimos todos los números posibles, luego la segunda ecuación del ejemplo tiene una solución:  $X = 1$ . Más aún, ésta es única.

	$2X+2$
0	2
1	0
2	2
3	0

	$3X+2$
0	2
1	1
2	0
3	3

Con estas tablas, que usamos para resolver las ecuaciones del ejemplo, también podemos decir algunas cosas más. Si en la primera ecuación en vez del 1 estuviera el 2, la primera tabla indica que la nueva ecuación tiene solución. Más aun, tiene exactamente dos soluciones:  $X = 0$  y  $X = 2$ . En cambio, en la segunda la situación es más uniforme, ya que si cambiamos el 1 por cualquier otro número 0, 2, ó 3, la nueva ecuación también tiene una única solución.

**Resumiendo:** La ecuación  $2X + 2 \equiv C \pmod{4}$  tiene solución sólo para  $C=0$  y  $C=2$ . En estos casos tiene, exactamente, dos soluciones.

La ecuación  $3X + 2 \equiv C \pmod{4}$  tiene solución para todo  $C$ , es decir  $C=0, 1, 2$  ó  $3$ . En todos los casos tiene una única solución.

¿Cuál es la razón de esta diferencia entre el comportamiento de una y otra ecuación?

Parte de la razón está en el coeficiente que acompaña a la incógnita  $X$  y en el  $4$ . En la primera ecuación este coeficiente es  $2$  y en la segunda es  $3$ . ¿Y la diferencia? Bueno, el máximo común divisor entre  $2$  y  $4$  es  $(2, 4) = 2$  y el máximo común divisor de  $3$  y  $4$  es  $(3, 4) = 1$ . Éstas son, justamente, las cantidades de soluciones que hay en uno y otro caso, cuando hay solución.

Antes de seguir, observemos que la ecuación  $2X + 2 \equiv 1 \pmod{4}$  es equivalente a la ecuación  $2X + 1 \equiv 0 \pmod{4}$  porque para pasar de la primera a la segunda basta restar  $1$  a ambos miembros, y para volver de la segunda a la primera basta sumar  $1$  a ambos miembros. Así, ambas tienen las mismas soluciones.

Por lo tanto, basta estudiar las ecuaciones de la forma  $AX + B \equiv 0 \pmod{m}$ . La verdad precisa y completa para estas ecuaciones es la siguiente:

**Proposición:** La ecuación  $AX + B \equiv 0 \pmod{m}$  tiene solución, si y sólo si  $(A, m)$  divide a  $B$ . Cuando hay solución, hay exactamente  $(A, m)$  soluciones distintas.

Ante una ecuación dada, esta verdad nos sirve para determinar si la misma tiene o no solución, y en caso de tener solución, para saber cuántas tiene. Sin embargo, no nos dice cómo encontrar las soluciones.

Veremos cómo encontrar, cuando existen, todas las soluciones. Si bien, esto no reemplaza a la demostración de la Proposición es una parte importante de la misma.

Analicemos un par de ejemplos:

$$\begin{aligned}6X + 2 &\equiv 0 \pmod{15} \\6X + 9 &\equiv 0 \pmod{15}\end{aligned}$$

Ejemplos 

Ambas ecuaciones son muy parecidas  $m = 15$  y  $A = 6$  en ambas. Sólo cambia  $B$ , en un caso es  $B = 2$  y en el otro  $B = 9$ . Tenemos que  $(6, 15) = 3$ . Según la proposición, debemos testear si  $3$  divide o no a  $B$ . Para la primera ecuación resulta que no, porque  $3$  no divide a  $2$ . Para la segunda resulta que sí, porque  $3$  sí divide a  $9$ . Conclusión: la primera ecuación no tiene solución, la segunda sí.

Aunque no es necesario, hagamos una tabla para cada ecuación

	$6X+2$
0	2
1	8
2	14
3	5
4	11
5	2
6	8
7	14
8	5
9	11
10	2
11	8
12	14
13	5
14	11

	$6X+9$
0	9
1	0
2	6
3	12
4	3
5	9
6	0
7	6
8	12
9	3
10	9
11	0
12	6
13	12
14	3

Como predijo la proposición, la primera no tiene solución y la segunda sí. Más aun, la segunda tiene **3** soluciones:  $X = 1, X = 6, X = 11$ . ¿Cómo encontrarlas?

A partir de la ecuación  $6X + 9 \equiv 0 \pmod{15}$  consideramos otra que se obtiene dividiendo todo por el  $(6, 15) = 3$ , para obtener la ecuación  $2X + 3 \equiv 0 \pmod{5}$ . Esta última siempre tiene solución porque el coeficiente de  $X$  y  $m$ , en este caso **2** y **5**, son siempre coprimos, es decir con máximo común divisor igual a **1**. En este caso, esto quiere decir que el **2** es invertible en  $\mathbb{Z}_5$ . En efecto,  $2 \cdot 3 = 1$  en  $\mathbb{Z}_5$ . Luego, la ecuación  $2X + 3 \equiv 0 \pmod{5}$  se resuelve fácilmente. Sumamos  $-3$  para obtener  $2X \equiv -3$ , y multiplicamos por **3**, el inverso de **2** y resulta  $X \equiv -9 \equiv 1 \pmod{5}$ . Esta solución es única módulo **5**. A partir de ésta, podemos encontrar otras módulo **15**, sumando **5** y luego **10**. Así, aparecen las soluciones **1, 6 y 11** que vimos en la tabla.

Hagamos un ejemplo más.

## Ejemplo



Consideremos la ecuación  $4X + 7 \equiv 17 \pmod{18}$ . Procedamos paso a paso.

1. Reemplazamos la ecuación dada por esta otra equivalente  $4X + 8 \equiv 0 \pmod{18}$ . Esto se obtiene de la primera sumando **1** a ambos miembros.
2. Calculamos el máximo común divisor de **4** y **18**. Tenemos  $(4, 18) = 2$ .
3. Observamos que **2** sí divide a **8** y concluimos que la segunda ecuación tiene solución. Como esta es equivalente a la primera, la primera también tiene solución. Más aún, ambas tienen las mismas soluciones.
4. A partir de la segunda ecuación consideramos otra, que se obtiene de ésta dividiendo todos los coeficientes y el **18** por **2**. Así, consideramos la ecuación  $2X + 4 \equiv 0 \pmod{9}$  que es equivalente a la ecuación  $2X \equiv 5 \pmod{9}$ .
5. En ésta última, como **2** es inversible y su inverso es **5**, multiplicamos ambos miembros por **5** para obtener la ecuación equivalente  $X \equiv 7 \pmod{9}$ .
6. Ahora **7** es la única solución de esta última ecuación y **7** es solución de la primera pero no la única.
7. Para obtener las restantes, que sabemos son **2**, sumamos a esta solución **9**. Obtenemos así las dos soluciones de la ecuación original: **7** y **16**.

Resolver completamente las siguientes ecuaciones.

4.16.  $6X + 5 \equiv 14 \pmod{21}$

4.17.  $6X + 5 \equiv 13 \pmod{21}$

Para resolver



## □ 4.8. Residuos cuadráticos

Esta sección es más difícil que las anteriores. Su contenido es elemental, pero profundo. Se incluyó porque es considerado como el inicio de la teoría de números moderna.

Sea  $p$  un primo impar. Un entero  $a$ , coprimo con  $p$ , es un *residuo cuadrático* módulo  $p$ , si existe un  $x$  tal que  $x^2 \equiv a \pmod{p}$ . En caso contrario,  $a$  es un *no-residuo cuadrático* módulo  $p$ .

Dados un primo  $p$ , y un entero cualquiera  $a$ , el símbolo de Legendre está definido como sigue:

$$\left(\frac{a}{p}\right) = \begin{cases} +1, & \text{si } p, a = 1, \text{ y } a \text{ es residuo cuadrático módulo } p \\ 0, & \text{si } p \mid a \\ -1, & \text{si } p, a = 1, \text{ y } a \text{ es no-residuo cuadrático módulo } p \end{cases}$$

Calculemos los cuadrados en  $\mathbb{Z}_p$ , para  $p = 5, 7, 11$ .

	1	2	3	4	5	6	7	8	9	10
$k^2$ módulo 5	1	4	4	1						
$k^2$ módulo 7	1	4	2	2	4	1				
$k^2$ módulo 11	1	4	9	5	3	3	5	9	4	1

Ahora listemos los residuos cuadráticos y los no-residuos cuadráticos para  $p = 5, 7, 11$ , menores que  $p$ .

	Residuos cuadráticos	Residuos no-cuadráticos
$p = 5$	{1,4}	{2,3}
$p = 7$	{1,2,4}	{3,5,6}
$p = 11$	{1,3,4,5,9}	{2,6,7,8,10}

Es notable que para cada uno de estos primos, la cantidad de residuos cuadráticos y la cantidad de no-residuos cuadráticos sea la misma. Si hiciéramos más experimentos, encontraríamos que este fenómeno se repite.

Este resultado dice cuántos residuos hay, pero no cómo encontrarlos, ni determinar si un número dado es

residuo cuadrático o no. El siguiente criterio es una herramienta eficiente, justamente para determinar si un  $a$  dado es residuo cuadrático o no.

**Proposición:** Exactamente la mitad de los enteros  $a$ , con  $0 < a < p-1$ , son residuos cuadráticos módulo  $p$ .

## Criterio de Euler

Sea  $p$  un número primo impar, es decir distinto de  $2$ , y  $a$  un entero cualquiera coprimo con  $p$ , entonces:

$$\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$$

### Ejemplos



¿Es  $2$  residuo cuadrático módulo  $13$ ?

Usemos el criterio de Euler para contestar esta pregunta.

Como  $2^6 = 64 = 13 \cdot 5 - 1$ , entonces  $2^6 \equiv -1 \pmod{13}$ , por lo tanto  $2$  no es residuo cuadrático módulo  $13$  y la ecuación  $x^2 \equiv 2 \pmod{13}$  no tiene solución.

Residuos cuadráticos módulo  $11$ .

Para determinar todos los residuos cuadráticos módulo  $11$  usamos nuevamente el criterio de Euler. Entonces, calculemos  $a^{(11-1)/2} = a^5$  para toda unidad  $a$  de  $\mathbb{Z}_{11}$ .

Tenemos:  $1^5 \equiv 1$ ,  $2^5 \equiv -1$ ,  $3^5 \equiv 1$ ,  $4^5 \equiv 1$ ,  $5^5 \equiv 1$ ,  $6^5 \equiv -1$ ,  $7^5 \equiv -1$ ,  $8^5 \equiv -1$ ,  $9^5 \equiv 1$  y  $10^5 \equiv -1$ . Los residuos cuadráticos módulo  $11$  son entonces  $\{1, 3, 4, 5, 9\}$ .

El papel de los números primos toma enorme relevancia en este tema debido al próximo resultado. El mismo reduce el problema de decidir qué enteros  $m$  son residuos cuadráticos módulo un primo  $p$ , al problema de decidir qué primos  $q$  son residuos cuadráticos módulo  $p$ .

La prueba de este teorema es inmediata a partir del criterio de Euler.

Como dijimos, este teorema permite reducir el cálculo de  $\left(\frac{m}{p}\right)$  para un  $m$  dado, al cálculo de  $\left(\frac{q}{p}\right)$  para los primos  $q$  que dividen a  $m$ .

En efecto si  $m = q_1 \cdot x \cdot \dots \cdot x \cdot q_r$  es la factorización prima de  $m$ , entonces, el teorema aplicado repetidas veces dice que  $\left(\frac{m}{p}\right) = \left(\frac{q_1}{p}\right) \left(\frac{q_2}{p}\right) \dots \left(\frac{q_r}{p}\right)$ .

Luego, para conocer  $\left(\frac{m}{p}\right)$  para cualquier entero  $m$  y cualquier primo impar  $p$ , basta conocer  $\left(\frac{q}{p}\right)$  para todos los primos  $q$  y conocer  $\left(\frac{\pm 1}{p}\right)$ . Comenzamos con lo más fácil.

**Teorema:** Sea  $p$  un primo impar y sean  $a$  y  $b$  enteros coprimos con  $p$ . Entonces

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right)$$

**Teorema:** Para todo primo  $p$  impar, es decir distinto de  $2$ , valen:

a.  $\left(\frac{1}{p}\right) = 1$

$$\text{b. } \left(\frac{-1}{p}\right) = 1, \text{ si } p \equiv 1 \pmod{4} \text{ y } \left(\frac{-1}{p}\right) = -1, \text{ si } p \equiv 3 \pmod{4}$$

$$\text{c. } \left(\frac{2}{p}\right) = 1, \text{ si } p \equiv 1 \text{ o } p \equiv 7 \pmod{8} \text{ y } \left(\frac{2}{p}\right) = -1, \text{ si } p \equiv 3 \text{ o } p \equiv 5 \pmod{8}.$$

## La Ley de Reciprocidad Cuadrática

Cada uno de los matemáticos que se ocuparon de este fenómeno formuló el resultado a su manera. Quizá hoy, la versión más difundida sea la de Legendre. Sin embargo, en ciertos contextos, otras pueden resultar más útiles.

Versión de Legendre.

Sean  $p$  y  $q$  primos impares. Entonces  $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\left(\frac{p-1}{2}\right)\left(\frac{q-1}{2}\right)}$

Este teorema nos da un método muy eficiente para calcular recursivamente  $\left(\frac{p}{q}\right)$ . Veamos cómo funciona.

Ejemplo. Tomemos  $p = 11$  y  $q = 43$  y calculemos  $\left(\frac{11}{43}\right)$ . Por la reciprocidad cuadrática:  $\left(\frac{11}{43}\right)\left(\frac{43}{11}\right) = (-1)^{\left(\frac{11-1}{2}\right)\left(\frac{43-1}{2}\right)} = (-1)^{5 \cdot 21} = -1$ . Además  $\left(\frac{43}{11}\right) = \left(\frac{-1}{11}\right) = -1$ , pues 43 es congruente a  $-1$  módulo 11. Luego,  $\left(\frac{11}{43}\right) = 1$ .

Es decir, existe al menos un entero  $m$ , tal que  $m$  al cuadrado es congruente a **11** módulo **43**.

Calculemos  $\left(\frac{17}{97}\right)$ . Tenemos  $\left(\frac{17}{97}\right) = \left(\frac{97}{17}\right) (-1)^{8 \cdot 48} = \left(\frac{12}{17}\right) = \left(\frac{2}{17}\right) \left(\frac{2}{17}\right) \left(\frac{3}{17}\right) = \left(\frac{17}{3}\right) (-1)^8 = \left(\frac{2}{3}\right) = -1$ . En este ejemplo, hemos usado varias manipulaciones aritméticas sin mencionarlás explícitamente. Por ejemplo, que  $\left(\frac{2}{17}\right) \left(\frac{2}{17}\right) = 1$ , esto es así porque el símbolo de Legendre vale **1** ó **-1** y, por lo tanto, su cuadrado siempre es **1**.

Como conclusión de este cálculo podemos asegurar que no existe ningún entero  $m$ , que al cuadrado sea congruente a **17** módulo **97**.

Ejemplo



4.18 Listar todos los residuos cuadráticos y los no-residuos cuadráticos módulo  $p$ , para  $p = 13, 17$ .

4.19 Decir si las siguientes ecuaciones tienen o no solución.

$$x^2 \equiv -7 \pmod{13}$$

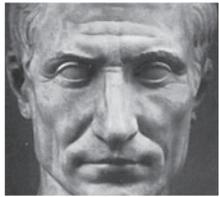
$$5x^2 \equiv 2 \pmod{13}$$

$$x^2 \equiv 9 \pmod{23}$$

4.20 Evaluar los siguientes símbolos de Legendre.  $\left(\frac{11}{29}\right)$   $\left(\frac{23}{61}\right)$

Para resolver





## □ 4.9. Los códigos secretos de Julio César

Ya en la época del Imperio Romano, el envío de mensajes a los ejércitos propios, o a los aliados, sin que fueran interceptados por los enemigos era un problema que desvelaba al emperador. La historia le reconoce a Julio César, entre otros méritos, el de haber inventado un sistema para enviar mensajes que de ser interceptados no podían ser interpretados y sólo podían ser descifrados por sus aliados.

Estos códigos se basan en la aritmética modular con  $m = 26$ , el 26 no es casual, es la cantidad de letras del alfabeto (el 26 corresponde a nuestro alfabeto sin dobles ni ñ, cada uno debe usar la cantidad de letras de su propio alfabeto).

En esta sección describiremos la primera versión de estos códigos y otras modificadas, y aún más sofisticadas.

Una idea elemental para codificar mensajes es la de reemplazar cada letra del mensaje original por otra, según un diccionario dado. Tanto el que envía un mensaje, como el que lo recibe, debe conocer el diccionario. Para mantener los mensajes secretos hay que asegurarse que el enemigo no encuentre el diccionario. Hasta aquí, nada de aritmética modular.



### Ejemplo



Supongamos que en nuestro diccionario secreto para codificar mensajes tenemos los siguientes reemplazos.

$a \rightarrow g,$                        $e \rightarrow j,$   
 $i \rightarrow o,$                        $m \rightarrow r$

Supongamos que recibimos el mensaje secreto Ro rgrg rj rorg  
Para decodificarlo tenemos que usar los reemplazos inversos

$g \rightarrow a,$                        $j \rightarrow e,$   
 $o \rightarrow i,$                        $r \rightarrow m.$

Resultado ... “mi mamá me mima”.

En este juego de enviar mensajes secretos el tiempo es un factor relevante. El enemigo intentará quebrar nuestro código, y es posible que lo logre después de algún tiempo. Es así que el mantener por mucho tiempo un diccionario fijo puede resultar peligroso. A pesar de que hay muchos diccionarios posibles, tantos como permutaciones de las 26 letras del alfabeto (esto es  $26! = 403.291.461.126.605.635.584.000.000$ ) quien intente descubrir uno de estos diccionarios puede ayudarse con algunas verdades del idioma. Por ejemplo, la forma en que se combinan las vocales y las consonantes, de combinaciones prohibidas, de saber qué letras son más frecuentes, etc. Así, con tiempo y luego de interceptar suficiente cantidad de mensajes es posible descubrir el diccionario secreto.

Julio César tuvo la siguiente idea. Propuso considerar el diccionario cíclico que reemplaza a una letra dada por la que está 3 posiciones más adelante, considerando que luego de la z sigue la a. En definitiva propuso considerar un alfabeto cíclico.

Julio César, por alguna razón, eligió el 3. Pero nosotros podríamos, sin más complicaciones, elegir un **m** entre 1 y 25 y reemplazar a cada letra por la que está **m** lugares más adelante en el alfabeto cíclico.

Para ayudar a codificar y decodificar anotamos

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Tomemos **m = 5** y supongamos que el mensaje a codificar es

TU MAMA TE MIMA

T = 20, luego su reemplazo es  $20 + 5 = 25 = Y$   
 U = 21, luego su reemplazo es  $21 + 5 = 26 = Z$   
 M = 13, luego su reemplazo es  $13 + 5 = 18 = R$   
 ....

Así el mensaje codificado es

YZ RFRF YJ RNRF

Ejemplo



El mensaje codificado cambia si cambiamos **m** porque estamos cambiando el diccionario.

Veamos que resulta para diversos valores de **m**.

<b>m</b>	TU	MAMA	TE	MIMA
1	UV	NBNB	UF	NJNB
7	AB	THTH	AL	TPTH
15	IJ	BPBP	IT	BXBP
21	OP	HVHV	OZ	HDHV
25	ST	LZLZ	SD	LHLZ

Entonces, Julio César podía elegir un **m** distinto cada vez que había que codificar un mensaje y enviar junto con el mensaje cifrado la llave, es decir el valor de **m**. Quien recibía el mensaje conocía el sistema y, con el valor de **m**, podía decodificar el mensaje recibido.

*El mensajero murió.*

El mensaje codificado usando **m = 7** se lee: LS TLUZHQLYV TBYPV

Ejemplo



Supongamos que recibimos este mensaje que incluye la llave, en este caso **m = 13**.

No debemos olvidar que estamos con la aritmética módulo 26.

$N = 14$ , luego  $14 - 13 = 1 = A$ , es decir  $N \rightarrow A$

$G = 7$ , luego  $7 - 13 = -6 = 20 = T$ , es decir  $G \rightarrow T$

....

Hagamos algo más sistemático. Recordemos el orden de cada letra en el alfabeto.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Ahora hacemos

Codificado	N	G	N	P	N	E		R	F	G	N		A	B	P	U	R
Orden	14	7	14	16	14	5		18	6	7	14		1	2	16	21	18
-13	1	20	1	3	1	18		5	19	20	1		14	15	3	8	5
decodificado	A	T	A	C	A	R		E	S	T	A		N	O	C	H	E

Codificado	A	B		A	B	F		R	F	C	R	E	N	A
Orden	1	2		1	2	6		18	6	3	18	5	14	1
-13	14	15		14	15	19		5	19	16	5	18	1	14
decodificado	N	O		N	O	S		E	S	P	E	R	A	N

¡ATACAR ESTA NOCHE NO NOS ESPERAN!

En algún momento, quizá los mismos romanos, construyeron un aparato para codificar y decodificar mensajes usando estos sistemas. Este consistía de dos platos redondos montados sobre un eje, ambos con las 26 letras del alfabeto ordenadas en sentido horario. Se acomodan los discos de manera tal que las letras A de ambos coincidan. Luego, haciendo girar uno sobre el otro  $m$  lugares en sentido horario, se lee el diccionario para codificar, mientras que girándolo en sentido antihorario se lee el diccionario para decodificar.

4.21 Codificar el mensaje “Traigan agua y pan”, usando  $m = 6, 11, \text{ y } 19$ .

4.22 Decodificar el mensaje “HGNKEKVCEKQPGU NQ NQITCUVG”, sabiendo que la llave es  $m = 2$ .



Para resolver