Capítulo 7

Congruencias

§7.1. La relación de congruencia

7.1.1. Sea $m_0 \in \mathbb{N}$. Decimos que dos enteros a y b son ***congruentes módulo*** m si $m \mid a - b$ y en ese caso escribimos

$$a \equiv b \mod m.$$

Esto define una relación en el conjunto $\mathbb{Z}$, la relación de ***congruencia módulo*** m.

Proposición. *Sea $m \in \mathbb{N}_0$. La relación de congruencia módulo m en $\mathbb{Z}$ es una relación de equivalencia.*

Demostración. Verifiquemos que esa relación tiene las tres propiedades necesarias.

- Si a es un elemento de $\mathbb{Z}$, entonces sabemos que $m \mid 0 = a - a$, así que $a \equiv a \mod m$.
- Sean a y b dos elementos de $\mathbb{Z}$ tales que $a \equiv b \mod m$, de manera que $m \mid a - b$. De acuerdo a la Proposición 6.1.2(*ii*) tenemos que $m \mid -(a - b) = b - a$ y, por lo tanto, que $b \equiv a \mod m$.
- Sean a, b y c tres elementos de $\mathbb{Z}$ tales que $a \equiv b \mod m$ y $b \equiv c \mod m$, de manera que $m \mid a - b$ y $m \mid b - c$. La Proposición 6.1.5 nos dice que entonces

  $$m \mid (a - b) + (b - c) = a - c$$

  y, en consecuencia, que $a \equiv c \mod m$.

Así, la congruencia módulo m es reflexiva, simétrica y transitiva: esto prueba que es una relación de equivalencia. □

7.1.2. El único entero divisible por 0 es 0 mismo, y esto implica inmediatamente que dos enteros son congruentes módulo 0 exactamente cuando son iguales. En otras palabras, la relación de congruencia módulo 0 es la relación identidad sobre el conjunto $\mathbb{Z}$. Por otro lado, todo entero es divisible por 1, y entonces dos enteros cualesquiera son congruentes módulo 1. La relación de congruencia módulo 1 es, por lo tanto, la relación total en el conjunto $\mathbb{Z}$. En vista de esto, la congruencia módulo uno de estos dos números no es particularmente interesante y nos restringimos en general a considerar módulos mayores que 1.

Por otro lado, es inmediato verificar que si m es un entero negativo la relación de congruencia módulo m coincide con al relación de congruencia módulo $-m$. Es por esta razón que normalmente pedimos que el módulo con el que trabajamos sea no negativo.

7.1.3. La relación de congruencia está estrechamente conectada con el algoritmo de la división:

Proposición. *Sea $m \in \mathbb{N}$. Dos enteros son congruentes módulo m si y solamente si tienen el mismo resto en la división por m.*

Demostración. Sean a y b dos enteros y sean q y r, por un lado, y q' y r', por otro, el cociente y el resto de la división de a y de b por m, de manera que $a = qm + r$, $0 \leq r < m$, $b = q'm + r'$ y $0 \leq r' < m$.

Supongamos primero que $a \equiv b \mod m$, es decir, que $m \mid a - b$. Como m divide a $(q - q')m$ y

$$a - b = (qm + r) - (q'm - r') = (q - q')m + r' - r,$$

vemos que m divide a $r - r'$. Usando el Lema **6.2.2** podemos concluir de esto que $r = r'$ y, por lo tanto, que la condición que da la proposición es necesaria para que a y b sean congruentes módulo m.

Supongamos ahora, para probar que esa condición también es suficiente, que $r = r'$. En ese caso tenemos que

$$a - b = (qm + r) - (q'm + r') = (q - q')m + (r - r') = (q - q')m$$

y es claro que m divide a $a - b$, es decir, que $a \equiv b \mod m$. La proposición queda así probada. □

7.1.4. Usando congruencias, es fácil caracterizar al resto de la división de un número por otro:

Proposición. *Sea $m \in \mathbb{N}$ y sea $a \in \mathbb{Z}$.*

(*i*) *Si r es el resto de dividir a a por m, entonces $a \equiv r \mod m$.*

(*ii*) *Recíprocamente, si s es un elemento de $\{0, \ldots, m-1\}$ tal que $a \equiv s \mod m$, entonces s es el resto de dividir a a por m.*

Estas dos afirmaciones juntas nos dicen que el resto de dividir a a por m es el único elemento

de $\{0, \ldots, m-1\}$ que es congruente con a módulo m.

Demostración. Sea a un entero y sean q y r, respectivamente, el cociente y el resto de dividir a a por m, de manera que, en particular, $a = qm + r$. Se sigue de esta igualdad que $a - r = qm$, así que claramente $m \mid a - r$, esto es, $a \equiv r \mod m$. Esto prueba la primera parte de la proposición.

Para ver la segunda, supongamos que $s \in \{0, \ldots, m-1\}$ es tal que $a \equiv s \mod m$. Como además $a \equiv r \mod m$, como acabamos de probar, vemos que $r \equiv s \mod m$, es decir, que m divide a $r - s$: de acuerdo al Lema 6.2.2, esto implica que $r = s$, esto es, que s es el resto de dividir a a por m. □

7.1.5. La relación de congruencia es compatible con las operaciones aritméticas en el siguiente sentido:

Proposición. *Sea $m \in \mathbb{N}$. Si a, a', b y b' son enteros tales que $a \equiv a' \mod m$ y $b \equiv b' \mod m$, entonces*

$$-a \equiv -a' \mod m,$$
$$a + b \equiv a' + b' \mod m$$

y

$$ab \equiv a'b' \mod m.$$

Demostración. Sean a, a', b, b' enteros tales que $a \equiv a' \mod m$ y $b \equiv b' \mod m$, de manera que m divide a $a - a'$ y a $b - b'$, y hay, por lo tanto, enteros c y d tales que $a - a' = cm$ y $b - b' = dm$. Por un lado, tenemos que

$$(-a) - (-a') = -(a - a') = (-c)m$$

así que m divide a $(-a) - (-a')$ y, en consecuencia, $-a \equiv -a' \mod m$. Por otro,

$$(a + b) - (a' + b') = (a - a') + (b - b') = cm + dm = (c + d)m$$

y

$$\begin{aligned} ab - a'b' &= ab - a'b + a'b - a'b' = (a - a')b + a'(b - b') \\ &= cmb + a'dm = (cb + a'd)m. \end{aligned}$$

Esto nos dice que m divide a $(a + b) - (a' + b')$ y a $ab - a'b'$, es decir, que $a + b \equiv a' + b' \mod m$ y que $ab \equiv a'b' \mod m$, como afirma la proposición. □

7.1.6. La Proposición 7.1.5 nos dice que la relación de congruencia es compatible con la suma y el producto de pares de enteros, pero una inducción más o menos evidente muestra que esto se

extiende a sumas y productos de cualquier número finito de enteros:

Corolario. *Sea $m \in \mathbb{N}$. Si $n \in \mathbb{N}$ y $a_1, \ldots, a_n, b_1, \ldots, b_n \in \mathbb{Z}$ son tales que $a_i \equiv b_i \mod m$ para cada $i \in \{1, \ldots, n\}$, entonces*

$$a_1 + \cdots + a_n \equiv b_1 + \cdots + b_n \mod m$$

y

$$a_1 \cdots a_n \equiv b_1 \cdots b_n \mod m.$$

Demostración. Para cada $n \in \mathbb{N}$ sea $P(n)$ la afirmación

> *si $a_1, \ldots, a_n, b_1, \ldots, b_n$ son enteros tales que $a_i \equiv b_i \mod m$ para cada $i \in \{1, \ldots, n\}$, entonces $a_1 + \cdots + a_n \equiv b_1 + \cdots + b_n \mod m$ y $a_1 \cdots a_n \equiv b_1 \cdots b_n \mod m$.*

Mostraremos que $P(n)$ vale para todo $n \in \mathbb{N}$ y esto claramente probará el corolario. Observemos que la afirmación $P(1)$ vale trivialmente, así que bastará que establezcamos el paso inductivo.

Sea entonces n un elemento cualquiera de $\mathbb{N}$ tal que $n \geq 2$, supongamos que la afirmación $P(n-1)$ vale, y sean $a_1, \ldots, a_n, b_1, \ldots, b_n$ enteros tales que $a_i \equiv b_i \mod m$ para cada $i \in \{1, \ldots, n\}$. En particular, tenemos que $a_i \equiv b_i \mod m$ para cada $i \in \{1, \ldots, n-1\}$ y, por lo tanto, la hipótesis inductiva nos dice que

$$a_1 + \cdots + a_{n-1} \equiv b_1 + \cdots + b_{n-1} \mod m$$

y

$$a_1 \cdots a_{n-1} \equiv b_1 \cdots b_{n-1} \mod m.$$

Como además $a_n \equiv b_n \mod m$, usando la Proposición 7.1.5, tenemos que

$$\begin{aligned} a_1 + \cdots + a_n &= (a_1 + \cdots + a_{n-1}) + a_n \\ &\equiv (b_1 + \cdots + b_{n-1}) + b_n \mod m \\ &= b_1 + \cdots + b_n \end{aligned}$$

y, de manera similar, que

$$\begin{aligned} a_1 \cdots a_n &= (a_1 \cdots a_{n-1}) a_n \\ &\equiv (b_1 \cdots b_{n-1}) b_n \mod m \\ &= b_1 \cdots b_n. \end{aligned}$$

Esto significa que la afirmación $P(n)$ vale y completa la inducción. □

7.1.7. Un caso particular útil del corolario que acabamos de probar es aquel en que consideramos

productos en que todos los factores son iguales:

Corolario. *Sea $m \in \mathbb{N}$. Si a y b son dos enteros tales que $a \equiv b \mod m$ y k es un entero no negativo, entonces $a^k \equiv b^k \mod m$.*

Demostración. Si k es 0 esto es evidente, y si k es positivo esto es un caso particular de la segunda afirmación del Corolario 7.1.6 en el que $a_1 = \cdots = a_k = a$ y $b_1 = \cdots = b_k = b$. □

7.1.8. Como consecuencia de la Proposición 7.1.5 y sus corolarios, cuando tenemos una expresión aritmética construida a partir de enteros usando sumas, productos y potencias y estamos trabajando módulo algún entero positivo m podemos reemplazar esos enteros por otros congruentes. Así, por ejemplo, trabajando módulo 7 es

$$222 + 210^{23} - 297 \cdot 91 \equiv 5 + 0^{23} - 3 \cdot 0 = 5,$$

ya que $222 \equiv 5$, $210 \equiv 91 \equiv 0$ y $297 \equiv 3$. De manera similar, podemos ver que para todo $n \in \mathbb{N}$ el número $10^{3n} + 1$ es divisible por 7 si y solamente si n es impar. En efecto, trabajando módulo 7 tenemos que $10^3 \equiv -1$, así que

$$10^{3n} + 1 = (10^3)^n + 1 \equiv (-1)^n + 1,$$

y esto es 0 si y solamente si n es impar. Observemos que esto nos dice además que cuando n es par el resto de dividir a $10^{3n} + 1$ por 7 es 2.

7.1.9. Veremos muchas aplicaciones de esto en todo lo que sigue, pero mostremos cómo podemos usar los resultados de esta sección para resolver una parte del Ejercicio 6.6.6:

Proposición. *Si a es un entero distinto de 1 y n un entero positivo, entonces $a - 1$ divide a $a^n - 1$.*

Demostración. Sea a un entero distinto de 1 y sea n un entero positivo. Como $|a - 1|$ divide a $a - 1$, trabajando módulo $|a - 1|$ es claro que $a \equiv 1$. De acuerdo al Corolario 7.1.7, entonces, tenemos que $a^n \equiv 1^1 = 1$ y esto significa, precisamente, que $|a - 1|$ divide a $a^n - 1$. La afirmación de la proposición sigue inmediatamente de esto. □

Es importante notar cuál es la diferencia entre esta forma de proceder y la sugerida por el ejercicio 6.6.6. Allí, para ver que $a - 1$ divide a $a^n - 1$ mostramos explícitamente cuál es el cociente — a saber, la suma geométrica $1 + a + \cdots + a^{n-1}$ — mientras que aquí llegamos a la misma conclusión sin necesidad de hacer eso. Es más: el argumento que acabamos de usar no nos da ninguna idea sobre cuál es ese cociente. En la sección siguiente haremos uso de esta misma idea para obtener varios criterios de divisibilidad.

7.1.10. Una última propiedad extremadamente importante y que nos será muy útil más adelante es la siguiente aplicación de la identidad de Bézout.

Proposición. *Sea $m \in \mathbb{N}$ y sea $a \in \mathbb{Z}$. Existe un entero $b \in \mathbb{Z}$ tal que $ab \equiv 1 \mod m$ si y solamente si a es coprimo con m.*

Demostración. Supongamos primero que a y m son coprimos, de manera que existen enteros b y c tales que $ab + mc = 1$. Tenemos entonces que $ab = 1 - mc \equiv 1 \mod m$ y esto muestra que la condición del enunciado es suficiente.

Por otro lado, supongamos que existe un entero b tal que $ab \equiv 1 \mod m$, de manera que m divide a $ab - 1$, esto es, existe $x \in \mathbb{Z}$ tal que $ab - 1 = mx$. Si d un divisor común positivo de a y m, entonces d divide también a $ab - mx = 1$: esto sólo es posible si $d = 1$ y muestra que $\mathsf{mcd}(a, m) = 1$. □

7.1.11. Por ejemplo, como 7 es coprimo con 152, esta proposición nos dice que hay un entero b tal que $7b \cong 1 \mod 152$. Para encontrarlo, usamos el algoritmo de Euclides extendido para encontrar los coeficientes de la identidad de Bézout entre 152 y 7: encontramos fácilmente que $3 \cdot 152 + (-65) \cdot 7 = 1$ y entonces podemos elegir b igual a -65.

Notemos que -65 no es el único entero b con la propiedad de que $7b \equiv 1 \mod 152$. De hecho, si b' es otro entero cualquiera que es congruente con b módulo 152, entonces sabemos que $7b' \equiv 7b \equiv 1 \mod 152$. Nuestro siguiente resultado dice que de esta manera obtenemos todos los enteros con esta propiedad.

Proposición. *Sea $m \in \mathbb{N}$ y sean a y b dos enteros tales que $ab \equiv 1 \mod m$. Un entero c tiene la propiedad de que $ac \equiv 1 \mod m$ si y solamente si es congruente con b módulo m.*

Demostración. Sea c un entero. Si $c \equiv b \mod m$, entonces sabemos que $ac \cong ab \cong 1 \mod m$ y, por lo tanto, la condición que da la proposición es necesaria. Por otro lado, si es $ac \equiv 1 \mod m$, entonces $c = 1c \equiv bac \equiv b1 = 1 \mod m$, así que esa condición también es suficiente. □

7.1.12. Si $m \in \mathbb{N}$ y a es un entero coprimo con m, entonces la Proposición 7.1.10 nos dice que hay enteros b tales que $ab \equiv 1 \mod m$: los llamamos ***inversos módulo m*** de a. Hay, de hecho, muchos, pero la Proposición 7.1.11 nos dice que el conjunto de ellos es una clase de congruencia módulo m: decimos que es «único módulo m».

§7.2. Algunos criterios de divisibilidad

7.2.1. Como $10 \equiv 1 \mod 9$, el Corolario 7.1.7 nos dice que $10^n \equiv 1^n = 1 \mod 9$ para todo $n \in \mathbb{N}$. De esto obtenemos fácilmente el siguiente criterio de divisibilidad por 9:

Proposición. *Sea a un entero positivo. Si $a = (d_k, \ldots, d_0)_{10}$ es la escritura de a en base 10, entonces a es divisible por 9 si y solamente si la suma $d_0 + \cdots + d_k$ de sus dígitos decimales lo es y, de hecho, ambos números tienen el mismo en la división por 9.*

Así, por ejemplo, la suma de los dígitos decimales de 45 261 189 es 36, y la suma de los dígitos decimales de este último número es 9: vemos así que 9 divide a 45 261 189. Esta proposición es el primer ejemplo que da Gauss en su *Disquisitiones Arithmeticae* de una aplicación de la relación de congruencia, y la prueba de damos es exactamente la misma que él da —que reproducimos en la Figura 7.1 en la página siguiente.

Demostración. Sea $(d_k, \cdots, d_0)_{10}$ la escritura decimal de a, de manera que

$$a = d_0 + d_1 \cdot 10 + \cdots + d_k \cdot 10^k.$$

Como observamos arriba, es $10^n \equiv 1 \mod 9$ para todo $n \in \mathbb{N}$, así que gracias a la Proposición 7.1.5 tenemos que $d_i \cdot 10^i \equiv d_1 \cdot 1 = d_1 \mod 9$ para cada $i \in \{0, \ldots, k\}$ y entonces, usando el Corolario 7.1.6, que

$$a = d_0 + d_1 + \cdot 10 + \cdots + d_k \cdot 10^k \equiv d_0 + d_1 + \cdots + d_k \mod 9.$$

Sabemos que a es divisible por 9 si y solamente si $a \equiv 0 \mod 9$ y, de acuerdo a lo que acabamos de probar, esto sucede si y solamente si $d_p + \cdots + d_k \equiv 0 \mod 9$, es decir, si la suma $d_0 + \cdots + d_k$ es divisible por 9. Esto prueba la proposición. □

7.2.2. De manera similar podemos obtener un criterio de divisibilidad por 11:

Proposición. *Sea a un entero positivo y sea $(d_k, \ldots, d_0)_{10}$ la escritura decimal de a. El número a es divisible por 11 si y solamente si 11 divide a la suma alternada de sus dígitos decimales,*

$$d_0 - d_1 + d_2 - d_2 + \cdots + (-1)^k d_k.$$

Por ejemplo, el número 64 320 883 es divisible por 11: en efecto, la suma alternada de sus dígitos decimales es $3 - 8 + 8 - 0 + 2 - 3 + 4 - 6 = 0$, que es divisible por 11.

12.

Theorematibus in hoc capite traditis complura quae in arithmeticis doceri solent innituntur, e. g. regulae ad explorandam divisibilitatem numeri propositi per 9, 11 aut alios numeros. *Secundum modulum* 9 omnes numeri 10 potestates unitati sunt congruae: quare si numerus propositus habet formam $a+10b+100c$ + etc., idem residuum minimum secundum modulum 9 dabit, quod $a+b+c$ + etc. Hinc manifestum est, si figurae singulae numeri decadice expressi sine respectu loci quem occupant addantur, summam hanc numerumque propositum eadem residua minima praebere, adeoque hunc per 9 dividi posse, si illa per 9 sit divisibilis, et contra. Idem etiam de divisore 3 tenendum. Quoniam *secundum modulum* 11, $100 \equiv 1$ erit generaliter $10^{2k} \equiv 1$. $10^{2k+1} \equiv 10 \equiv -1$, et numerus formae $a+10b+100c+$ etc. secundum modulum 11 idem residuum minimum dabit quod $a-b+c$ etc.; unde regula nota protinus derivatur. Ex eodem principio omnia similia praecepta facile deducuntur.

Figura 7.1. El párrafo 12 de las *Disquisitiones Arithmeticae* de Carl Friedrich Gauss, en el que enuncia y prueba nuestra Proposición 7.2.1.

Demostración. Como $10 \equiv -1 \mod 11$, para todo $n \in \mathbb{N}_0$ es $10^n \equiv (-1)^n \mod 11$, así que, como en la prueba de la proposición anterior, tenemos que

$$a = \sum_{i=0}^{k} d_i \cdot 10^n \equiv \sum_{i=0}^{k} d_i \cdot (-1)^n \mod 11.$$

De esto se deduce que 11 divide a a si y solamente si divide a $\sum_{i=0}^{k} d_i \cdot (-1)^n$, que es lo que afirma la proposición. □

7.2.3. El siguiente resultado es similar al de la Proposición 7.2.1, pero ahora tomando los dígitos en bloques de a tres:

Proposición. *Sea $a \in \mathbb{N}$ y sean $(d_k \ldots, d_0)_{10}$ la escritura decimal de a. El número a es divisible por 27 si y solamente si la suma de los números que se obtienen agrupando sus dígitos de a tres desde la derecha,*

$$(d_2, d_1, d_0)_{10} + (d_5, d_4, d_3)_{10} + (d_8, d_7, d_6)_{10} + \cdots,$$

es divisible por 27.

Así, el número 12 492 342 315 es divisible por 27 porque 315 + 342 + 492 + 12 = 1 161 lo es, y esto es así porque 161 + 1 = 162 = 27 · 6 lo es.

Demostración. Sea $l = \lfloor k/3 \rfloor$ y, para cada $i \in \{0, \dots, l\}$, sea $e_i = (d_{3i+2}, d_{3i+1}, d_{3i})_{10}$. Sabemos que $a = (e_l, \dots, e_0)_{1000}$ y la proposición es consecuencia de que

$$a = \sum_{i=0}^{l} e_i \cdot 1000^i \equiv \sum_{i=0}^{l} e_i \mod 27,$$

ya que $1000 \equiv 1 \mod 27$. □

7.2.4. Hay muchos criterios de divisibilidad que miran solamente los últimos dígitos del número. Algunos de ellos son los siguientes:

Proposición. *Sea $a \in \mathbb{N}$ y sea $(d_k, \dots, d_0)_{10}$ la escritura decimal de a.*

(*i*) *El número a es divisible por 2 si y solamente si d_0 es par, y es divisible por 5 si y solamente si $d_0 \in \{0, 5\}$.*

(*ii*) *El número a es divisible por 4 o por 25 si y solamente si el número $(d_1, d_0)_{10}$ lo es.*

Usando esta proposición vemos inmediatamente que 12 326 es divisible por 2, que 101 436 no es divisible por 5, que 874 917 no es divisible por 4 y que 1 927 225 es divisible por 25.

Demostración. Como $10 \equiv 0 \mod 2$ y $10 \equiv 0 \mod 5$, para todo $n \in \mathbb{N}$ se tiene que $10^n \equiv 0 \mod 2$ y $10^n \equiv 0 \mod 5$. Esto implica que

$$a = \sum_{i=0}^{k} d_i \cdot 10^i \equiv d_0$$

tanto módulo 2 como módulo 5. La primera afirmación de la proposición es consecuencia de esto. Por otro lado, como $10^2 \equiv 0$ módulo 4 y módulo 25, tenemos que para cada entero $n \geq 2$ es $10^n = 10^2 \cdot 10^{n-2} \equiv 0 \cdot 10^{n-2} = 0$ tanto módulo 4 como módulo 25 y, por lo tanto,

$$a = \sum_{i=0}^{k} d_i \cdot 10^i \equiv d_0 + d_1 \cdot 10 = (d_1, d_0)_{10}$$

módulo 4 o módulo 25. De esta congruencia se deduce la segunda afirmación de la proposición. □

7.2.5. Un tercer tipo de criterio de divisibilidad puede deducirse usando las mismas ideas.

Proposición. *Sea $a \in \mathbb{N}$ y sea $(d_k, \dots, d_0)_{10}$ la escritura decimal de a. El número a es divisible por 7 si $2(d_k, \dots, d_2)_{10} + (d_1, d_0)_{10}$ lo es.*

El interés de esto es que el número $2(d_k, \dots, d_2)_{10} + (d_1, d_0)_{10}$ es más chico que a y, por lo tanto, que podemos usar el criterio recursivamente. Por ejemplo, para ver que 96 502 es divisible por 7 basta observar que $2 \cdot 965 + 2 = 1\,932$ lo es, y para esto que $2 \cdot 19 + 32 = 70$ lo es.

Demostración. Si $b = (d_k, \dots, d_2)_{10}$ y $c = (d_1, d_0)_{10}$, entonces

$$a = 100b + c \equiv 2b + c \mod 7,$$

ya que $100 \equiv 2 \mod 7$. La proposición es consecuencia de esta congruencia. □

7.2.6. Es natural preguntarse si para todo entero m hay un criterio de divisibilidad por m del estilo de los que vimos.

7.2.7. Proposición. *Sea m un entero positivo. Hay dos enteros positivos N y M tales que para todo $n \in \mathbb{N}$ vale*

$$n \geq N \implies 10^n \equiv 10^{n+M} \mod m.$$

Demostración. Consideremos la sucesión de números

$$r_m(10^0), \quad r_m(10^1), \quad r_m(10^2), \quad r_m(10^3), \quad \dots$$

Todos estos números pertenecen al conjunto $\{0, \dots, m-1\}$ así que no pueden ser distintos: esto nos dice que existen dos enteros u_0 y v_0 tales que $u_0 < v_0$ y $r_m(10^{u_0}) = r_m(10^{v_0})$.

Como consecuencia de esto, el conjunto S de los enteros positivos u tales que existe otro entero v tal que $u < v$ y $r_m(10^u) = r_m(10^v)$ no es vacío, ya que contiene a u_0. Podemos entonces considerar el número $N \coloneqq \min S$. Ahora bien, como N pertenece a S, el conjunto

$$T \coloneqq \{v \in \mathbb{N} : r_m(10^N) = r_m(10^{N+v})\}$$

no es vacío y, otra vez, podemos considerar su elemento mínimo $M \coloneqq \min T$.

Sea ahora n un entero positivo tal que $n \geq N$ y sean q y r el cociente y el resto de dividir a $n - N$ por M, de manera que $n - N = qM + r$ y $0 \leq r < M$. Si $q = 0$, de manera que $n = N + r$, entonces

$$10^{n+M} = 10^{N+M+r} = 10^{N+M}10^r \equiv 10^N 10^r = 10^{N+r} = 10^n \mod m.$$

□

§7.3. Los enteros módulo m

7.3.1. Si $m \in \mathbb{N}$, escribimos $\mathbb{Z}_m$ al conjunto cociente de $\mathbb{Z}$ por la relación de congruencia módulo m y lo llamamos el conjunto de los ***enteros módulo*** m. Es importante recordar que a pesar de este nombre, los elementos de $\mathbb{Z}_m$ no son enteros sino clases de equivalencia, es decir, *conjuntos* de enteros.

7.3.2. Una consecuencia importante de la Proposición 7.1.3 es la determinación de la cantidad de elementos de $\mathbb{Z}_m$:

Proposición. *Sea $m \in \mathbb{N}$. La relación de congruencia módulo m parte a $\mathbb{Z}$ en m clases de equivalencia, que son*

$$[0],\ [1],\ \ldots,\ [m-1].$$

Demostración. Sea $a \in \mathbb{Z}$ y sean $q \in \mathbb{Z}$ y $r \in \{0, \ldots, m-1\}$ el cociente y el resto de la división de a por m. Como $a - r = qm$, tenemos que $a \equiv r \mod m$ y, por lo tanto, que $[a] = [r]$. Esto nos dice que todas las clases de congruencia módulo m aparecen en la lista del enunciado. Para terminar, entonces, bastará que probemos que las m clases allí listadas son distintas dos a dos.

Sean $i, j \in \{0, \ldots, m-1\}$ y supongamos que $[i] = [j]$, de manera que $i \equiv j \mod m$. La Proposición 7.1.3 nos dice entonces que i y j dan el mismo resto al ser divididos por m: como $0 \leq i, j < m$, esto implica que $i = j$ y prueba lo que queríamos. □

7.3.3. La compatibilidad entre la relación de congruencia y las operaciones aritmética que afirma la Proposición 7.1.5 se ve reflejada en el siguiente resultado:

Proposición. *Sea $m \in \mathbb{N}$. Hay funciones $S, P : \mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m$ tales que cada vez que a y b está en $\mathbb{Z}$ se tiene que*

$$S([a],[b]) = [a+b]$$

y

$$P([a],[b]) = [ab].$$

Demostración. Consideremos el subconjunto

$$S = \{(([a],[b]),[a+b]) \in (\mathbb{Z}_m \times \mathbb{Z}_m) \times \mathbb{Z}_m : a, b \in \mathbb{Z}\}$$

del conjunto $(\mathbb{Z}_m \times \mathbb{Z}_m) \times \mathbb{Z}_m$. Se trata, por supuesto, de una relación de $\mathbb{Z}_m \times \mathbb{Z}_m$ a $\mathbb{Z}_m$. Mostremos que se trata, de hecho, de una función.

- Sea $x \in \mathbb{Z}_m \times \mathbb{Z}_m$, de manera que existen α y $\beta \in \mathbb{Z}_m$ tales que $x = (\alpha, \beta)$. Como $\mathbb{Z}_m$ es

el cociente de $\mathbb{Z}$ por la relación de congruencia módulo m, existen enteros a y b tales que $\alpha = [a]$ y $\beta = [b]$ y, de acuerdo a la definición del conjunto S, el par ordenado $(x, [a+b]) = (([a], [b]), [a+b])$ pertenece a S.

- Supongamos, por otro lado, que $x \in \mathbb{Z}_m \times \mathbb{Z}_m$ e y, $y' \in \mathbb{Z}_m$ son tales que los pares ordenados(x, y) y (x, y') están en S. Como recién, existen enteros a, b, c y c' tales que $x = ([a], [b])$, $y = [c]$ e $y' = [c']$.

  Ahora bien, como $(x, y) = (([a], [b]), [c])$ está en S, existen a_1, $b_1 \in \mathbb{Z}$ tales que $[a] = [a_1]$, $[b] = [b_1]$ y $[c] = [a_1 + b_1]$. Esto nos dice que modulo m se tiene que $a \equiv a_1$, $b \equiv b_1$ y $c \equiv a_1 + b_1$ y, por lo tanto, $c \equiv a + b$.

  De manera similar, como $(x, y') = (([a], [b]), [c'])$ está en S, existen a_2, $b_2 \in \mathbb{Z}$ tales que $[a] = [a_2]$, $[b] = [b_2]$ y $[c'] = [a_2 + b_2]$, de manera que $a \equiv a_2$, $b \equiv b_2$ y $c' \equiv a_2 + b_2$: esto implica que $c \equiv a + b$.

  Juntando estas dos cosas, concluimos que $c \equiv c'$ y, como consecuencia de ello, que $y = [c] = [c'] = y'$.

Si a y b son enteros, entonces es claro que $(([a], [b]), [a+b])$ está en S y esto significa, precisamente, que $S([a], [b]) = [a+b]$. Esto muestra que la función S satisface la condición que aparece en el enunciado.

Para ver el resto de la proposición, basta considerar el subconjunto

$$P = \{(([a], [b]), [ab]) \in (\mathbb{Z}_m \times \mathbb{Z}_m) \times \mathbb{Z}_m : a, b \in \mathbb{Z}\}$$

de $(\mathbb{Z}_m \times \mathbb{Z}_m) \times \mathbb{Z}_m$ y mostrar que es también una función $\mathbb{Z}_m \times \mathbb{Z}_m \to \mathbb{Z}_m$ y que satisface la condición del enunciado. Esto puede hacerse de exactamente la misma forma a lo que acabamos de hacer: dejamos los detalles al lector. □

7.3.4. Normalmente escribimos a las funciones S y P que nos da la proposición que acabamos de probar usando los símbolos + y · de suma y producto: si α y β son dos elementos de $\mathbb{Z}_m$, escribimos $\alpha + \beta$ y $\alpha \cdot \beta$ en lugar de $S(\alpha, \beta)$ y $P(\alpha, \beta)$.

Así, si a y b son dos enteros, usando esta notación tenemos que

$$[a] + [b] = [a + b] \tag{1}$$

y

$$[a] \cdot [b] = [a \cdot b].$$

Es importante observar que los símbolos + y · en estas igualdades denotan cosas distintas a la izquierda y a la derecha del signo de igualdad: a la derecha + y · denotan las operaciones usuales entre enteros, mientras que a la izquierda denotan las operaciones que acabamos de definir entre elementos de $\mathbb{Z}_m$. Esto introduce, por supuesto, una ambigüedad en lo que escribimos, pero el contexto es siempre suficiente para resolverla.

7.3.5. Las operaciones de suma y producto que hemos definido en el conjunto $\mathbb{Z}_m$ tienen muchas de las mismas propiedades formales que las usuales de $\mathbb{Z}$:

Proposición. *Sea $m \in \mathbb{N}$.*

(*i*) *Si α, β y γ son elementos de $\mathbb{Z}_n$, entonces*

$$(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma), \qquad (\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma), \tag{2}$$

$$\alpha + \beta = \beta + \alpha, \qquad \alpha \cdot \beta = \beta \cdot \alpha, \tag{3}$$

$$\alpha + [0] = \alpha = [0] + \alpha, \qquad \alpha \cdot [1] = \alpha = [1] \cdot \alpha,$$

y

$$(\alpha + \beta) \cdot \gamma = \alpha \cdot \gamma + \beta \cdot \gamma. \tag{4}$$

(*ii*) *Para cada $\alpha \in \mathbb{Z}_m$, existe $\beta \in \mathbb{Z}_m$ tal que $\alpha + \beta = \beta + \alpha = [0]$. Más aún, si a es un entero tal que $\alpha = [a]$, entonces podemos elegir $\beta = [-a]$.*

Las identidades de (2) nos dicen que las operaciones + y · son asociativa, las de (3) que son conmutativas, las de (3) que las clases $[0]$ y $[1]$ son elementos neutros para ellas, y la de (4) que el producto · se distribuye sobre sumas +. Por otro lado, la segunda parte de la proposición nos dice que todo elemento de $\mathbb{Z}_m$ posee un *opuesto* con respecto a la suma +.

Demostración. Cada una de estas afirmaciones es consecuencia de la correspondiente afirmación sobre las operaciones entre enteros y de la observación de que todo elemento de $\mathbb{Z}_m$ es de la forma $[a]$ para algún $a \in \mathbb{Z}$.

Por ejemplo, si α y β son dos elementos de $\mathbb{Z}_m$, entonces existen enteros a y b tales que $\alpha = [a]$ y $\beta = [b]$ y, por lo tanto,

$$\alpha + \beta = [a] + [b] = [a + b] = [b + a] = [b] + [a] = \beta + \alpha,$$

de manera que la suma en $\mathbb{Z}_m$ es conmutativa. La segunda y la cuarta de estas igualdades son consecuencia directa de la relación (1) y la tercera de la conmutatividad de la suma de enteros. Dejamos al lector la verificación de las demás afirmaciones de la proposición. □

7.3.6. A pesar de esta proposición, que nos dice que las operaciones de suma y producto en $\mathbb{Z}_m$ funcionan en muchos aspectos como las de $\mathbb{Z}$, hay diferencias importantes. Mencionemos las dos que son probablemente las principales:

- En $\mathbb{Z}$ el producto de dos enteros no nulo es siempre no nulo. En $\mathbb{Z}_m$, por otro lado, esto no es siempre cierto. Por ejemplo, si $m = 6$ sabemos que las clase $[2]$ y $[3]$ no son la clase nula $[0]$, pero su producto es $[2] \cdot [3] = [2 \cdot 3] = [6] = [0]$.
- En $\mathbb{Z}$ los dos únicos elementos inversibles son 1 y −1. En $\mathbb{Z}_m$ esto puede no ser cierto. Si

$m = 11$, por ejemplo, la clase $[4]$ es inversible, ya que el producto $[4] \cdot [3] = [12] = [1]$ es la clase unidad $[1]$: esto nos dice que $[4]$ es inversible en $\mathbb{Z}_{11}$ y, sin embargo, $[4]$ no es ni $[1]$ ni $[-1]$.

Con la información que tenemos disponible en este punto podemos caracterizar qué clases de $\mathbb{Z}_m$ son inversibles:

7.3.7. Proposición. *Sea m un entero positivo y sea a un entero. La clase de congruencia $[a]$ es inversible en $\mathbb{Z}_m$ si y solamente si el entero a es coprimo con m.*

Demostración. Si el entero a es coprimo con m, la Proposición 7.1.10 nos dice que hay un entero b tal que $ab \equiv 1 \mod m$ y, por lo tanto, tal que $[a] \cdot [b] = [ab] = [1]$. Recíprocamente, si la clase $[a]$ es inversible en $\mathbb{Z}_m$, entonces hay otra clase β en ese conjunto tal que $[a] \cdot \beta = [1]$. Si b es un entero tal que $\beta = [b]$, esto nos dice que $[ab] = [a] \cdot [b] = [a] \cdot \beta = [1]$, de manera que $ab \equiv 1 \mod m$ y, de acuerdo a la Proposición 7.1.10, entonces a es coprimo con m. □

§7.4. Ejercicios

Algunos criterios de divisibilidad

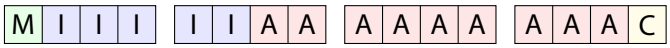
7.4.1. Ejercicio. Sea $a \in \mathbb{N}$ y sean $(d_k \ldots, d_0)_{10}$ la escritura decimal de a. El número a es divisible por 7 si y solamente si la suma alternada de los números que se obtienen agrupando sus dígitos de a tres desde la derecha,

$$(d_2, d_1, d_0)_{10} - (d_5, d_4, d_3)_{10} + (d_8, d_7, d_6)_{10} + \cdots,$$

es divisible por 7. Así, por ejemplo, para ver que 13 476 066 723 es divisible por 7 observamos que $723 - 66 + 476 - 13 = 1\,120$ y que $120 - 1 = 119 = 7 \cdot 17$.

El algoritmo de Luhn

7.4.2. Por lo general, el número de una tarjeta de crédito tiene 16 dígitos y, de acuerdo al estándar ISO/IEC 7812, tiene a siguiente estructura:



- El primer dígito identifica la categoría de entidad que emitió la tarjeta. Por ejemplo, si es un 1 la tarjeta fue emitida por una aerolínea, y si es un 4 o un 5 por un banco.
- Los siguientes cinco dígitos forman un número que identifica al emisor de la tarjeta.
- Los siguientes nueve forman el número de cuenta.
- El último es el llamado ***dígito de control***.

Este último dígito queda determinado por los demás de acuerdo al llamado ***algoritmo de Luhn*** de la siguiente manera. Supongamos que $d_{15} \dots d_2 d_1$ son los quince primeros dígitos del número. Definimos una función $p : \{0, \dots, 9\} \to \{0, \dots, 9\}$ poniendo, para cada $i \in \{0, \dots, 9\}$,

$$p(i) \coloneqq \begin{cases} 0 & \text{si } i = 0; \\ r_9(2i) & \text{si } 0 < i < 9; \\ 9 & \text{si } i = 9. \end{cases}$$

Es fácil tabular los valores de p:

i	0	1	2	3	4	5	6	7	8	9
$p(i)$	0	2	4	6	8	1	3	5	7	9

Si ahora

$$s \coloneqq p(d_1) + d_2 + p(d_3) + d_3 + \cdots + p(d_{13}) + d_{14} + p(d_{15}),$$

entonces el dígito de control d_0 es el resto de dividir por 10 a $-s$. El número completo de la tarjeta es, entonces, $d_{15} \dots, d_2 d_1 d_0$. Por ejemplo, en el número de tarjeta de crédito

```
5204 7400 0990 0014
```
(5)

el número s es

$$p(5) + 2 + p(0) + 4 + p(7) + 4 + p(0) + 0 + p(0) + 9 + p(9) + 0 + p(0) + 0 + p(1) = 36$$

y el resto de dividir a -36 por 10 es 4, que es precisamente el último dígito de (5).

7.4.3. Ejercicio.

(*a*) Muestre que si $d_{15}d_{14}\dots d_1d_0$ es un número de tarjeta de crédito con d_0 calculado a partir del algoritmo de Luhn, entonces

$$d_0 + p(d_1) + d_2 + p(d_3) + d_3 + \cdots + p(d_{13}) + d_{14} + p(d_{15}) \equiv 0 \mod 10.$$

Cuando esta condición se cumple decimos que el número es ***válido***.

(*b*) Pruebe que si $d_{15}d_{14}\dots d_1d_0$ es un número de tarjeta de crédito, entonces un número $d'_{15}d'_{14}\dots d'_1d'_0$ se obtiene de él cambiando cualquier dígito no es válido.

Por ejemplo, como `5204 7400 0990 0014` es un número válido, ninguno de los siguientes números lo es

`1204 7400 0990 0014`, `5604 7400 0990 0014`,
`5294 7400 0990 0014`, `5203 7400 0990 0014`,
`5204 6400 0990 0014`, `5204 7401 0990 0014`.

(*c*) Pruebe que si $d_{15}d_{14}\dots d_1d_0$ es un número de tarjeta de crédito, entonces el número $d'_{15}d'_{14}\dots d'_1d'_0$ se obtiene de él intercambiando dos dígitos contiguos que son distintos entre sí y que no son 0 y 9 no es válido.

Por ejemplo, como `5204 7400 0990 0014` es un número válido, ninguno de los siguientes números lo es

`2504 7400 0990 0014`, `5024 7400 0990 0014`,
`5240 7400 0990 0014`, `5204 7040 0990 0014`,
`5204 7400 0990 0041`, `5207 4400 0990 0014`.

De todas formas, los números

`5204 7400 9090 0014`, `5204 7400 0909 0014`,

que se obtiene intercambiando en el número original un 0 y un 9 contiguos sí son válidos.

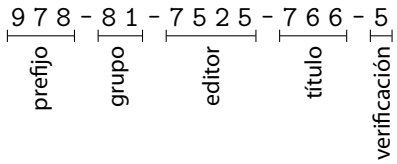
Estos resultados nos dicen que si copiamos mal un número de tarjeta de crédito porque copiamos un dígito mal o porque intercambiamos (casi) cualquier par de dígitos contiguos, podemos darnos cuenta. Esto nos permite reconocer cuándo hubo un error de esos dos tipos, aunque no arreglarlo.

Esta idea es debida a Hans Peter Luhn, que la patentó en 1960 en Estados Unidos [Luh1960]. Hoy pasó al dominio público y está especificada formalmente en el estándar ISO/IEC 7812-1 [IOfS-IEC2017].

Figura 7.2. El código ISBN de un libro y un código de barras que lo representa.

El código ISBN

7.4.4. Normalmente, cuando un libro es publicado el editor contacta a una agencia llamada *International ISBN Agency* y solicita que le asignen un número que lo identifique de manera única, llamado en número ISBN de libro, por las iniciales de *International Standard Book Number*. El formato de estos números fue cambiando desde que fueron creados en 1970. Hoy en día consiste de una tira de 13 dígitos, con el siguiente formato:



Los primeros tres dígitos forman el llamado *prefijo*, que hoy puede ser solamente 978 o 979. Los siguientes dos dígitos dan información sobre el *grupo de registro*, que normalmente está determinado por el país de origen de la publicación o su idioma. Después hay dígitos que identifican el editor de la publicación y al título registrado. Finalmente, el último dígito es el llamado *dígito de verificación*. Frecuentemente las distintas partes del número ISBN se escriben separadas por guiones, como en el ejemplo de arriba, pero no tienen longitudes fijas.

Decimos que un número ISBN $d_{13}d_{12}\cdots d_2d_1$, de manera que cada dígito d_i es un elemento de $\{0,1,\ldots,9\}$, es ***valido*** si

$$d_{12} + 3d_{11} + d_{10} + 3d_9 + d_8 + 3d_7 + d_6 + 3d_5 + d_4 + 3d_3 + d_2 + 3d_1 \equiv 0 \mod 10.$$

Los coeficientes que aparecen aquí son alternadamente 1 y 3.

Ejercicio.

(*a*) Muestre que si $d_{13}\cdots d_2$ los doce dígitos determinados por el prefijo, el grupo de registro, el editor y el título, entonces hay exactamente una forma de elegir un dígito más $d_1 \in \{0,\ldots,9\}$ de manera que $d_{13}\cdots d_2d_1$ sea un número ISBN válido.

(*b*) Pruebe que si $d_{13}\cdots d_2d_1$ es un número ISBN válido, entonces cambiar cualquiera de sus

dígitos por uno distinto, o intercambiar cualquiera de sus pares de dígitos adyacentes que no difieran en 5 resulta en un número que no es válido.

7.4.5. Hasta 2007 se usaba un formato distinto de números ISBN con solamente 10 «dígitos», en el que los nueve primeros son dígitos decimales, es decir, elementos de $\{0, \ldots, 9\}$ y el décimo es un elemento de $\{0, \ldots, 9, 10\}$. Cuando este último dígito es diez, lo escribimos con una letra `X`. Por ejemplo, los siguientes son números ISBN de 10 dígitos:

```
0-8044-2957-X    1-84356-028-3    93-86954-21-4  0-9752298-0-X
```

Como antes, en uno de estos números $d_{10}d_9 \cdots d_2 d_1$ los primeros 9 dígitos $d_{10} \cdots d_2$ se determinan a partir de información como el editor de la publicación y su proveniencia, y el último dígito d_1, llamado *de control*, se determina a partir de los demás, pero en este caso se elige de manera que

$$\sum_{i=1}^{10} (11 - i) d_i \equiv 0 \mod 11.$$

Cuando esta condición se cumple decimos que el número $d_{10}d_9 \cdots d_2 d_1$ es válido.

Ejercicio.

(*a*) Muestre que si $d_{10}d_9 \cdots d_2$ es un número de 9 dígitos decimales hay una única forma de elegir d_1 en $\{0, 1, \ldots, 9, 10\}$ de manera que el número $d_{10}d_9 \cdots d_2 d_1$ sea válido.

(*b*) Muestre que si en un número de estos que es válido cambiamos cualquiera de los dígitos por otro distinto o intercambiamos dos dígitos distintos adyacentes cualesquiera obtenemos un número que no es válido.

Notemos que la segunda parte de este ejercicio nos dice que este método de verificación es mejor que el que describimos arriba para los números ISBN de trece dígitos, ya que permite detectar *cualquier* transposición de dígitos. La razón por que la que este sistema fue abandonado y remplazado por el actual es la necesidad de usar códigos de barra para simplificar la lectura automática de estos números: los códigos de barra normalmente usados solo permiten codificar dígitos decimales.