Aritmética de los Números Enteros (parte 2)

Pablo L. De Nápoli

Departamento de Matemática
Facultad de Ciencias Exactas y Naturales
Universidad de Buenos Aires

Álgebra I - Segundo cuatrimestre de 2020

Recordamos de la clase anterior: el algoritmo de división

Teorema (Algoritmo de división en $\mathbb{Z}$, teorema 4.3.1 en el apunte)

Dados números enteros $a, b \in \mathbb{Z}$ con $b \neq 0$ existen únicos números enteros $q = q(a,b)$ y $r = r(a,b)$ tales que $a = bq + r$ y $0 \leq r < |b|$.

Parte I

Congruencias

Definición de congruencias

Definición

Sean $a, b \in \mathbb{Z}$ y sea $n \in \mathbb{N}$. Decimos que a y b son congruentes módulo n y lo escribimos

$$a \equiv b \ (mod\ n)$$

cuando $n|b-a$.

Proposición

Otra definición equivalente Sean $a, b \in \mathbb{Z}$ y sea $n \in \mathbb{N}$. Entonces, $a \equiv b$ (mód n) si y sólo si a y b proporcionan el mismo resto cuando los dividimos por n.

Algunos ejemplos:

$$3 \equiv 8 \quad (\text{mód } 5)$$

$$6 \equiv -1 \quad (\text{mód } 7)$$

$$12 \equiv 0 \quad (\text{mód } 3)$$

Prueba de la equivalencia de las definiciones

Demostración.

Dividamos a y b por n, es decir escribamos:

$$a = nq + r \text{ donde } 0 \leq r < n$$

$$b = nq' + r' \text{ donde } 0 \leq r' < n$$

Hemos de demostrar que $a \equiv b \pmod{n}$ si y sólo si $r = r'$.

- Supongamos primero que $r = r'$. Entonces $b - a = nq' - nq = n(q' - q)$. Luego $n|b - a$ o sea $a \equiv b \pmod{n}$.
- Por otra parte, supongamos que $a \equiv b \pmod{n}$. Entonces:

$$b - a = n(q' - q) + r' - r$$

Si suponemos que $r' \geq r$ entonces como $0 \leq r' - r < n$, tenemos que $r' - r$ debe ser el resto (y $q' - q$ el cociente) en la división enterea de $b - a$ por n. Pero entonces en virtud de la unicidad del resto en la división entera, $r' - r = 0$, ya que $n|b - a$.
(Si fuera $r' < r$, la prueba es análoga pues $b \equiv a \pmod{n}$)

La congruencia es una relación de equivalencia

Proposición

La relación de congruencia tiene las siguientes propiedades:

- **Reflexividad**: $a \equiv a \pmod{n}$.
- **Simetría**: *Si* $a \equiv b \pmod{n}$, *entonces* $b \equiv a (mod\ n)$.
- **Transitividad**: *Si* $a \equiv b \pmod{n}$ *y* $b \equiv c \pmod{n}$, *entonces* $a \equiv c \pmod{n}$

Demostración.

1. $$n|a - a = 0 \Rightarrow a \equiv a \pmod{n}$$
2. Si $a \equiv b \pmod{n} \Rightarrow n|b - a \Rightarrow n| - (b - a)$. O sea $n|a - b \Rightarrow b \equiv a \pmod{n}$.
3. Si $a \equiv b \pmod{n} \wedge b \equiv c \pmod{n} \Rightarrow$ $n|b - a \wedge n|c - b \Rightarrow n|(b - a) + (c - b)$, y por lo tanto $n|c - a \Leftrightarrow a \equiv c \pmod{n}$.

Clases de congruencia módulo n

Recordamos que una relación de equivalencia determina una partición de su dominio en clases de equivalencia [teorema 1.2.6 del apunte].
Así, pues la relación de congruencia parte a los enteros en clases de congruencia módulo n. Por ejemplo, hay cuatro clases de congruencia módulo 4 que son

$$\overline{0} = \{\ldots, -16, -8, -4, 0, 4, 8, 12, 16, ...\}$$

$$\overline{1} = \{\ldots, -15, -7, -3, 1, 5, 9, 13, 17, ...\}$$

$$\overline{2} = \{\ldots, -14, -6, -2, 2, 6, 10, 14, 18, ...\}$$

$$\overline{3} = \{\ldots, -13, -5, -1, 3, 7, 11, 15, 19, ...\}$$

En general, habrá n clases de equivalencia módulo n, una por cada posible resto $\{0, 1, 2, \ldots, n-1\}$ de la división entera por n.

Compatiblidad de las congruencias con las operaciones

Proposición

Si $a \equiv b \pmod{n}$ *y* $c \equiv d \pmod{n}$ *entonces se verifican:*

$$a + c \equiv b + d \pmod{n}$$

$$a - c \equiv b - d \pmod{n}$$

$$ac \equiv bd \pmod{n}$$

Ejemplo: de

$$2 \equiv 12 \pmod{10} \wedge 5 \equiv 15 \pmod{10}$$

podemos deducir

$$2 + 5 \equiv 12 + 15 \pmod{10} \text{ o sea } 7 \equiv 27 \pmod{10}$$

$$2 - 5 \equiv 12 - 15 \pmod{n} \text{ o sea } -3 \equiv -3 \pmod{10}$$

$$2 \cdot 5 \equiv 12 \cdot 15 \pmod{n} \text{ o sea } 10 \equiv 180 \pmod{10}$$

Demostración de la compatiblidad con las operaciones

Demostración.

Por hipótesis, $n|b-a$ y $n|d-c$, en consecuencia:

$$n|(b-a)+(d-c) \;\Rightarrow\; n|(b+d)-(a+c)$$

es decir que $a+c \equiv b+d \pmod{n}$, como afirmamos. Por otra parte,

$$n|(b-a)-(d-c) \;\Rightarrow\; n|(b-d)-(a-c)$$

es decir que: $a-c \equiv b-d \pmod{n}$, que es nuestra segunda afirmación.
Por otra parte, como $n|b-a$ y $n|d-c$, podremos escribir:

$$b-a=ne, \quad d-c=nf$$

para ciertos enteros $e, f \in \mathbb{Z}$. Entonces:

$$bd=(a+ne)(c+nf)=ac+nec+naf+n^2ef=ac+n(ec+af+nef)$$

En consecuencia: $ac \equiv bd \pmod{n}$. □

El caso del módulo 2

Cuando $n = 2$, tenemos dos clases de congruencia módulo 2. La clase de los números pares y la de los impares

$$\overline{0} = \{\ldots, -10, -8, -6 - 4, -2, 0, 2, 4, 6, 8, ...\}$$

$$\overline{1} = \{\ldots, -9, -7, -5, -3, -2, -1, 1, 3, 5, 7, 9, 11, 13, ...\}$$

La proposición anterior generaliza reglas que ya conocemos como

$$0 + 0 \equiv 0 \pmod 2 \Rightarrow par + par = par$$

$$0 + 1 \equiv 1 \pmod 2 \Rightarrow par + impar = impar$$

$$1 + 1 \equiv 0 \pmod 2 \Rightarrow impar + impar = par$$

¡No se puede dividir congruencias!

En general no es posible cancelar factores no nulos en las congruencias. Por ejemplo:

$$2 \times 1 \equiv 2 \times 4 \quad (\text{mód } 6)$$

Sin embargo,

$$1 \not\equiv 4 \quad (\text{mód } 6)$$

En consecuencia, en general no se puede dividir congruencias.

Otra propiedades útiles

Corolario

Si $a \equiv b \pmod{n}$, *entonces para todo* $k \in \mathbb{N}_0$ $a^k \equiv b^k \pmod{n}$

Observación

Si $a \equiv b \pmod{n}$ *y* $m|n$ *entonces también tenemos que* $a \equiv b \pmod{m}$.

Demostración.

Por hipótesis $n|b-a$. Como $m|n$, por transitividad deducimos que $m|b-a$, o sea $a \equiv b \pmod{m}$. □

Parte II

Bases de numeración

Bases de numeración

Desde la escuela primaria estamos familiarizados con la representación de enteros en diferentes bases. Por supuesto, lo primero que se aprende es la base decimal (donde tenemos 10 dígitos $0, 1, 2, 3, 4, 5, 6, 7, 8, 9$).

$$1035 = 1 \times 10^4 + 0 \times 10^3 + 3 \times 10^1 + 5 \times 10^0$$

Pero también es posible utilizar otras bases. Por ejemplo, en la base binaria (base 2) tenemos sólo dos dígitos 0 y 1, y por ejemplo el número once se escribe como 1011 en binario, ya que

$$1011_2 = 1 \times 2^3 + 0 \times 2^3 + 1 \times 2^1 + 1 \times 2^0 = 11$$

Es costumbre indicar la base como subíndice, así pues 102_3 quiere decir el número cuyo desarrollo en base 3 es 102 (escribiendo la base en el sistema decimal).

Números en binario y computadoras

La base binaria es muy utilizada en computación, debido a que (como ya vimos) los circuitos de las computadoras digitales almacenan la información en unidades que tienen dos estados posibles

- encendido: convencionalmente representado por 1.
- apagado: convencionalmente representado por 0.

Estas unidades se llaman bits (palabra que procede de la abreviatura de binary digit, dígito binario en inglés)

Usualmente los bits se agrupan en bloques. Un bloque de 8 bits se denomina un byte. Por ejemplo:

0	0	0	0	1	0	1	1

es un byte. Este byte podría representar al número once escrito en binario.

Un byte puede representar un número entre 0 y 255 que corresponde a

1	1	1	1	1	1	1	1

Comprobación: recordamos la suma geométrica

$$2^7 + 2^6 + 2^5 + 2^4 + 2^3 + 2^2 + 2^1 + 2^0 = \frac{2^8 - 1}{2 - 1} = 2^8 - 1 = 256 - 1 = 255.$$

Otras bases importantes en computación: la base octal

En computación también se emplean la base octal (8) y hexadecimal (16) como abreviaturas de la base binaria.

- En la base octal, los dígitos son $\{0, 1, 2, 3, 4, 5, 6, 7\}$. Como $8 = 2^3$ cada dígito octal corresponde a 3 dígitos binarios. Ejemplo: el byte

0	1	1	0	0	0	0	1

representa al número $97 = 2^6 + 2^5 + 1$ en binario (código ASCII de la letra a). Agrupamos sus dígitos de a 3. Entonces

$$01_2 = 1, 100_2 = 4, 001_2 = 1$$

Por lo que el número 97 se escribe como 141 en octal. Comprobación:

$$1 \cdot 8^2 + 4 \cdot 8^1 + 1 \cdot 8^0 = 64 + 32 + 1 = 97$$

Dígitos en la base hexadecimal (16)

Dígito hexadecimal	en binario	equivalente decimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
A	1010	10
B	1011	11
C	1100	12
D	1101	13
E	1110	14
F	1111	15

Como $16 = 2^4$ cada dígito hexadecimal corresponde a 4 dígitos binarios.

Otras bases importantes en computación: la base hexadecimal

Volvamos a mirar el byte

0	1	1	0	0	0	0	1

que representaba al número $97 = 2^6 + 2^5 + 1$ en binario (código ASCII de la letra a).
Ahora agrupamos sus dígitos de a cuatro. Usando la tabla anterior, vemos que en hexadecimal se escribe 61.

Otro ejemplo: ¿qué número representa el hexadecimal? $2F$. En decimal, $2 \cdot 16 + 15 = 47$. En binario

0	0	1	0	1	1	1	1

Un byte puede almacenar un número hexadecimal de 2 dígitos. Entre 00 y FF (=255 en decimal).

¡Los ejemplos anteriores en la computadora!

Ejemplos en Python 3

```
>>> bin(97)
        '0b1100001'
>>> hex(97)
        '0x61'
>>> 0x2F
        47
>>> 0b1110
        14
>>> oct(97)
        '0o141'
```

El algoritmo para escribir un número en una bases de numeración

El algoritmo para expresar un número en una determinada base es bien conocido desde la escuela: consiste en efectuar sucesivas divisiones enteras del número por la base, hasta obtener un cociente nulo.
Por ejemplo: para expresar 11 en la base 2 efectuamos las divisiones:

$$11 = 5 \times 2 + 1$$

$$5 = 2 \times 2 + 1$$

$$2 = 1 \times 2 + 0$$

$$1 = 0 \times 2 + 1$$

Entonces el desarrollo de 11 en base 2 está formado por los sucesivos restos 1, 1, 0 y 1. $11 = 1011_2$. Notemos que los ceros a la izquierda no aportan nada: por ejemplo

$$001011 = 1011$$

Salvo esta ambigüedad, el desarrollo de un número en una base dada, es único.

Un ejemplo en la base hexadecimal

Para escribir 15151 en la base hexadecimal,

$$15151 = 946 \times 16 + 15$$

$$946 = 59 \times 16 + 2$$

$$59 = 3 \times 16 + 11$$

$$3 = 0 \times 16 + 3$$

Entonces

$$15151 = 3 \cdot 16^3 + 11 \cdot 16^2 + 2 \cdot 16^1 + 15 \cdot 16^0$$

o sea que 15151 se escribe en hexadecimal como $3B2F$

En Python 3

```
>>> hex(15151)
'0x3b2f'
```

Enunciado del teorema

Ahora enunciaremos la escritura en bases como un teorema formal:

Teorema

Dada una base $b \geq 2$ entera, siempre es posible escribir a cada entero $n \in \mathbb{N}$ de una única forma como:

$$n = d_k b^k + d_{k-1} b^{k-1} + \ldots + d_2 b^2 + d_1 b^1 + d_0 b^0$$

donde $d_i \in \mathbb{N}_0$ y $0 \leq d_i < b$, y $d_k \neq 0$.

Existencia

Para probar la existencia del desarollo, utilizamos un argumento de inducción completa en n.
Claramente $n = 1$ admite el desarollo $1 = 1 \cdot b^0$.
Si $n > 1$, y suponemos que el teorema es cierto para los números menores que n, efectuamos la división entera de n por b, escribiendo entonces:

$$n = qb + d_0$$

donde $0 \leq d_0 < b$. Pero como $b \geq 2$, el cociente q es menor que n. Entonces por la hipótesis inductiva, n admitirá un desarrollo de la forma:

$$q = d_k b^{k-1} + d_{k-1} b^{k-2} + \ldots + d_3 b^2 + d_2 b^1 + d_1 b^0$$

(para algún k y ciertos d_i con $0 \leq d_i < b$, y $d_k \neq 0$).
Sustituyendo vemos que:

$$n = d_k b^k + d_{k-1} b^{k-1} + \ldots + d_2 b^2 + d_1 b^1 + d_0 b^0$$

En virtud del principio de inducción completa, concluimos que cualquier $n \in \mathbb{N}$ admite algún desarrollo en base b.

Unicidad

Para establecer la unicidad del desarrollo, procedemos también por inducción completa en n.
Claramente el único desarrollo posible de $n = 1$ es $1 = 1 \cdot b^0$ (pues si $d_i \neq 0$ para algún $i > 1$, $n \geq b$. Y entonces debe ser $1 = d_0$).
Supongamos pues, que el número $n > 1$ admitiera dos desarrollos en base b:

$$n = d_k b^k + d_{k-1} b^{k-1} + \ldots + d_2 b^2 + d_1 b^1 + d_0 b^0$$

$$n = d'_j b^j + d'_{k-1} b^{k-1} + \ldots + d'_2 b^2 + d'_1 b^1 + d'_0 b^0$$

donde $0 \leq d_i < b$ y $0 \leq d'_i < b$ para todo i, $d_k \neq 0$, $d'_j \neq 0$; y supongamos que los números menores que n admiten un único desarrollo.

Unicidad (2)

Nuevamente, tenemos que:

$$n = qb + d_0, \quad n = q'b + d_0'$$

donde

$$q = d_k b^{k-1} + d_{k-1} b^{k-2} + \ldots + d_3 b^2 + d_2 b^1 + d_1 b^0$$

$$q' = d_j' b^{j-1} + d_{j-1}' b^{j-2} + \ldots + d_3' b^2 + d_2' b^1 + d_1' b^0$$

Pero entonces, por la unicidad del cociente y del resto en la división entera de n por b, tendremos que $q = q'$ y que $d_0 = d_0'$.

Y entonces como $q < n$, en virtud de la hipótesis de inducción global, los desarrollos de q y q' (que son el mismo número) deben coincidir, es decir que $k = j$ y $d_i = d_i'$ para $1 \leq i \leq k$.

En virtud del principio de inducción completa, esto prueba que cualquier $n \in \mathbb{N}$ admite un único desarrollo en base b.

Bonus Track: lo implementamos usando la recursión

En Python 3

```
def digitos(n,b):
        if n<b:
                return [n]
        else:
                q,r= divmod(n,b)
                d = digitos(q,b)
                d.append(r)
                return d
```

El ejemplo que calculamos antes

```
>>> digitos(15151,16)
        [3, 11, 2, 15]
```

Parte III

Criterios de divisibilidad

Criterio de divisibilidad por 3 o por 9

Proposición

Un número natural (escrito en el sistema decimal) es divisible por 3 (o por 9) si y sólo si la suma de sus dígitos es divisible por 3 (respectivamente por 9).

Demostración.

Sea

$$n = d_k \times 10^k + d_{k-1} \times 10^{k-1} + \ldots + d_2 \times 10^2 + d_1 \times 10 + d_0$$

la escritura de n en decimal, con $0 \leq d_i < 10$. Entonces como

$$10 \equiv 1 \pmod 3 \Rightarrow 10^k \equiv 1 \pmod 3 \text{ para todo } k \geq 1$$

Consecuentemente

$$n \equiv S = d_k + d_{k-1} + \ldots + d_2 + d_1 + d_0 \pmod 3$$

En particular n es congruente con 0 módulo 3, si y sólo sí la suma S de sus cifras lo es. Para la divisibilidad por 9, la demostración es enteramente similar. □

Criterio de divisibilidad por 11

Proposición

Un número natural (escrito en el sistema decimal) es divisible por 11 *si y sólo la diferencia entre la suma de sus cifras de los lugares pares, y la suma de sus cifras de los lugares impares es disible por* 11*.*

Demostración.

Ahora, tenemos que:

$$10 \equiv -1 \pmod{11} \Rightarrow 10^k \equiv (-1)^k \pmod{11} \text{ para todo } k \geq 1$$

Entonces, manteniendo la notación de la prueba anterior, vemos que:

$$n \equiv D = \sum_{j=0}^{k} (-1)^j d_j = \left(\sum_{j \text{ par}} d_j \right) - \left(\sum_{j \text{ impar}} d_j \right) \pmod{11}$$

y n congruente a 0 módulo 11 si y sólo si D lo es. □

Otros criterios de divisibilidad

Ejercicio

Demostrar los criterios de divisibilidad por 4 y por 5, a saber:

1. Un número n es divisible por 5 si y sólo si el dígito de las unidades es 0 o 5.
2. Un número n es divisible por 4 si y sólo si el número formado por el dígito de las decenas y el de las unidades lo es.