7 ENTEROS

Después de los booleanos, que permiten hablar de valores de verdad y desarrollar la lógica formal, los números enteros resultan un paso natural en la construcción del edificio de las matemáticas y sus aplicaciones. Aquí se supondrán como entendidos los siguientes conjuntos numéricos:

- Los números *enteros,* denotados usualmente **Z** o **int**: {…,-2,-1-0,1,2,…}.
- Los números *naturales*[1], denotados **N** o **nat**: {0,1,2,3,…}.
- Los enteros *positivos*, denotados aquí $\mathbf{nat}^{+}$: {1,2,3, …}.
- Los enteros negativos, denotados aquí $\mathbf{nat}^{-}$: {-1,-2,-3,…}.

Una comprensión formal de los números enteros comienza por establecer con claridad estos conjuntos numéricos. A manera de ejemplo de cómo sería este enfoque se pueden mencionar los siguientes axiomas, establecidos por Giuseppe Peano en el s. XIX:

Def A (*Axiomas de Peano para* ***nat***)

El conjunto de los *números naturales* **nat**, expresado en términos de 0 y una función sucesor S: **nat** → **nat**, cumple los siguientes axiomas:

a $0 \in \mathbf{nat}$ // 0 es un elemento de **nat**
b $(\forall n{:}\mathbf{nat} \mid : S.n \in \mathbf{nat})$ // si n está en **nat**, su sucesor también lo está
c $(\forall n{:}\mathbf{nat} \mid : S.n \neq 0)$ // el 0 no es sucesor de ningún número natural
d $(\forall n{:}\mathbf{nat} \mid S.n = S.m : n=m)$ // S es 1-1
e $(\forall A{:}2^{\mathbf{nat}} \mid 0 \in A \wedge (\forall n{:}A \mid : S.n \in A) : A = \mathbf{nat})$

□

Estos axiomas caracterizan unívocamente los números naturales y traen a la consciencia propiedades importantes. Una consecuencia de estos axiomas, que resume la esencia los números naturales[2], podría ser:

Teo B (*Formas normales para* **nat**)

$n \in \mathbf{nat} \equiv n=0 \vee (\exists m{:}\mathbf{nat} \mid : n=S.m)$

□

El Teo B proporciona un método para construir cualquier número natural a partir del 0 y la función S. Por ejemplo, se diría 1=S.0, 2=S.1, etc. El axioma **d** afirma que cada uno de estos números es diferente de los demás.

Una representación gráfica de los números naturales tiene la forma:

o bien:

---

[1] En la literatura es usual, también, denominar números naturales a los enteros mayores que 0.

[2] El capturar la 'esencia' quiere decir aquí que, si dos conjuntos cumplen los axiomas, se puede pensar que del uno al otro no hay más que una traducción notacional.

No es difícil demostrar que el axioma **e** es equivalente al siguiente enunciado:

Principio del buen orden: Todo subconjunto no vacío de los naturales tiene un primer elemento o elemento mínimo, con respecto al orden estricto `(`**`nat`**`,<)`**.**

Los *enteros* pueden concebirse como dos copias de los naturales, a una de las cuales se le añade un signo `'-'` y se identifica `-0` con `0`. Su representación gráfica es una recta que crece en las dos direcciones:

Una vez entendidos cómo están constituidos los conjuntos **`nat`** e **`int`**, se pueden definir operaciones básicas sobre ellos, como la suma, la resta, la multiplicación, la división entera, el residuo o módulo, etc.

Por ejemplo, para definir la suma y la multiplicación sobre los naturales se pueden postular los axiomas:

Ax +1: `n + 0 = n`
Ax +2: `n + S.m = S(n+m)`
Ax *1: `n * 0 = 0`
Ax *2: `n * S.m = n*m + n`
Ax <1: `0 < n ≡ (0≠n)`
Ax <2: `S.n < 0 ≡ false`
Ax <3: `S.n < S.m ≡ m < n`

Los axiomas anteriores definen de manera *recursiva* la suma, la multiplicación y la relación de orden estricto <, en el sentido de que se define el valor de la evaluación de una función en términos de los argumentos y de otros valores que se pueden suponer ya entendidos.

Las relaciones así definidas tienen propiedades interesantes (v.gr., asociatividad, conmutatividad, …) y fáciles de mostrar con una técnica llamada *inducción*, cuya corrección se fundamenta en el Axioma **e** de la Definición A. Esta técnica se estudiará más adelante, en el Capítulo 8.

El dominio del discurso en las siguientes secciones será el de los enteros y, ocasionalmente, el de los naturales o el de los enteros positivos.

Ejercicios 7

1 Pruebe el Teorema B.

2 Pruebe que el Principio del Buen Orden es lógicamente equivalente al Axioma e.

3 Muestre que `(`**`nat`**`,<)` es un conjunto bien ordenado.

7.1 DIVISIBILIDAD

Definición A:

```
a divide b      ≡  a|b
                ≡  (∃c|: a*c = b)

a divisor de b  ≡  a|b
```

b *multiplo de* a ≡ a|b

□

Nótese que la definición anterior permite afirmar que:

- x|0
- 0|x ≡ x=0 .

Además, se pueden establecer otros conceptos como, por ejemplo:

par.n ≡ 2|n

impar.n ≡ ¬par.n

7.1.1 Teoremas sobre divisibilidad

El siguiente teorema resume resultados básicos sobre el concepto de ser divisible, fácilmente demostrables a partir de la definición. En general, no se da la demostración, pero en algunos casos se incluye, para resaltar alguna idea importante para tener en cuenta.

Teorema A:

1 a|b ⇒ a|b*c

2 a|b ∧ b|c ⇒ a|c

3 a|b ∧ a|c ⇒ a|(m*b + n*c)

4 c≠0 ⇒ (c*a|c*b ≡ a|b)

5 a|b ∧ b|a ⇒ a = ±b

Dem:

Hip: a*d=b, b*e=a

```
    a*(d*e)
=       ⟨Asociatividad *⟩
    (a*d)*e
=       ⟨Hip: a*d=b⟩
    b*e
=       ⟨Hip: b*e=a ⟩
    a
```

Si a=0, también b=0, y el teorema vale. Si a≠0, entonces d*e=1. Como d,e∈**int**, entonces d=e=±1, y el teorema vale.

6 a|b ∧ a>0 ∧ b>0 ⇒ a≤b

□

La demostración del Teorema A.5 se basa en una propiedad que puede no ser evidente, pero que se entenderá de manera intuitiva. Algo similar se puede decir de lo que afirma la propiedad **6** y de lo que se requiere para demostrarla.

7.1.2 Números primos

Un número *primo* es un número natural mayor que 1 y que solo es divisible por 1 y por él mismo (considerando solo divisores no negativos). Formalmente:

Definición B:
p *primo* ≡ p>1 ∧ (∀d:**nat**| d>0 ∧ d|p : d=1 ∨ d=p)

□

Como los divisores de un número positivo son menores o iguales a él, para decidir si n es primo basta verificar que ¬(d|n), para d=2,3,…,n-1. En realidad, se pueden hacer muchas mejoras a este método si se cae en cuenta, por ejemplo, de que:

- El único primo par es el 2. Si par.n, n>2, entonces n no es primo.
- Si (p*k)|n, también p|n. Por el Teorema A.6, basta revisar la divisibilidad por primos menores que n.
- Si impar.n, n>2 , basta revisar la divisibilidad por los primos impares menores que √n, la raíz cuadrada del número. Si n fuera divisible por p, p>√n, debe existir q tal que p*q=n. Y si q≥√n, se tendría que n=p*q>(√n)*(√n)=n, lo cual es contradictorio. Es decir, debe ser cierto que q<√n.

Ejercicios 7.1

1 Pruebe el Teorema A.

2 Sea **nat**⁺ = **nat**\{0}. Muestre que (**nat**⁺,|) es un orden parcial.

7.2 ALGORITMO DE LA DIVISIÓN

El siguiente teorema, conocido como el *algoritmo de la división*, no es -en realidad- un algoritmo. Es un teorema de existencia, tanto del divisor como del residuo, en una división entera:

Teorema A:
n,d:**int**, d>0 ⇒ (∃q,r| 0≤r<d : n = q*d+r)
Además:

- si n = q*d+r, con 0≤r<d, q y r son únicos
- si ¬(d|n), existen q,r con n = q*d+r, 0<r<d.

Dem:

Sea r = (min k:**int**| 0≤n-k*d: n-k*d). Es claro que r está bien definido porque es el mínimo de un conjunto no vacío de números naturales, el cual debe existir por el principio del buen orden. Sea q el k tal que r = n-k*d, i.e., n = q*d+r.

Obsérvese que r≥0. Si r≥d, entonces n-q*d≥d, de modo que

$$r = n-q*d > n-(q+1)*d \geq 0$$

y r no sería mínimo entre los números de la forma n-k*d, k:**int**. Por tanto, debe tenerse que 0≤r<d.

Si, además, n = q'*d+r', con 0≤r'<d, entonces r'= n-q'*d ≥ n-q*d = r, ya que r es mínimo. Entonces, q'≤q. Si q'<q, debe existir j>0 tal que q'=q+j. Por tanto, 0≤n-(q+j)*d <d. De nuevo, por la minimalidad de r, debería darse que n-(q+j)*d ≥ n-q*d, pero de aquí saldría que j≤0. Es decir, q=q'. Por tanto, r=r' también.

Si ¬(d|n), debe valer r>0.

□

Como q y el r están unívocamente determinados, esto permite definir las funciones parciales ÷ y mod, sobre parejas de **nat**, que los calculen. Se usa la siguiente terminología:

n	: *dividendo*	q = n÷d	: *cociente*
d	: *divisor*	r = n mod d	: *residuo* .

Por ejemplo, 17÷6 = 2, 17 mod 6 = 5, ya que 17 = 2*6 + 5. Se comprueba que 0≤5<6.

Un versión más general permite extender estos conceptos a números enteros y considerar dividendos y divisores negativos. En estos casos:
n,d:**int**, d≠0 ⇒ (∃q,r| 0≤r<|d| : n = q*d+r).

Aquí hay que tener cuidado al calcular cociente y residuo. Por ejemplo, 17÷(-6) = -2, 17 mod (-6) = 5, ya que 17 = (-2)*(-6) + 5. Se comprueba que 0≤5<|-6|.

7.2.1 Un algoritmo para dividir[3]

El Teorema A no es precisamente, un algoritmo. Sin embargo, sí es posible evidenciar la existencia de cociente y residuo mediante un algoritmo que los calcule prácticamente. La siguiente versión, una división basada en restas, puede entenderse como una realización práctica de la demostración del Teorema A, para el caso en que n≥0.

```
// Pre: n≥0 ∧ d>0
q= 0;
r= n;
// Inv: n = q*d+r ∧ 0≤r
// Cota: r
while (r≥d) {
   q= q+1;
   r= r-d;
}
// Pos: n = q*d+r ∧ 0≤r<d
```

Ejercicios 7.2

1 Indique en dónde se usa, en la demostración del Teorema 7.2.A, la hipótesis de que d>0.

2 Si en el algoritmo que se da para construir el cociente y el residuo de una división entera cuestan 1 las asignaciones, ¿cuánto cuesta ejecutar el algoritmo en el caso general?

[3] Esta sección requiere una explicación adicional de la notación algorítmica utilizada, así como de la forma en que los programas se anotan con comentarios que documentan su eventual verificación de corrección.

7.3 DIVISORES Y MÚLTIPLOS COMUNES

Definición A

Se definen las funciones

`mcd: int × int → nat` // *máximo común divisor*
`mcm: int × int → nat` // *mínimo común múltiplo*

así:

`mcd(0,0) = 0`
`mcd(b,c) = (max d:nat| d|b ∧ d|c : d)` , en otro caso

`mcm(0,0) = 0`
`mcm(b,c) = (min m:nat | b|m ∧ c|m : m)` , en otro caso

□

Las funciones `mcd` y `mcm` calculan, respectivamente, el divisor común positivo más grande y el múltiplo común positivo más pequeño, de dos números enteros. En el caso especial de que ambos números sean `0`, las dos funciones tienen `0` como resultado.

Más adelante se verá que siempre se cumplirá que

`mcd(b,c)*mcm(b,c) = b*c`

y, por esta propiedad, se usa prestar atención, en principio, al `mcd`, deduciendo propiedades derivadas de lo anterior para el `mcm`.

El siguiente teorema resume varias de las propiedades importantes del `mcd`. Algunas de ellas son muy sencillas y no se demuestran. Otras se demuestran para mostrar técnicas novedosas que aparecen en esta clase de pruebas.

Teorema B

1 `mcd(b,c) = mcd(c,b)`

2 `(b,c)≠(0,0) ⇒ mcd(b,c) = (min x,y| b*x+c*y>0 : b*x+c*y)`

Dem:

Sea `A = {u| x,y:int ∧ u=b*x+c*y>0}`. Nótese que `nat⊇A≠∅`, porque basta elegir `x=b`, `y=c` para conseguir que `b*x+c*y>0`, ya que `(b,c)≠(0,0)`.

Por el principio del buen orden, `A` tiene un primer elemento. Sea `m = min A = bx`$_0$`+cy`$_0$ y sea `d = mcd(b,c)`.

Si `¬(m|b)`, por el algoritmo de la división existen `q,r`, tales que `b=m*q+r`, con `0<r<m`. Ahora, `r=b-m*q`, de modo que `0<b-(b*x`$_0$`+c*y`$_0$`)*q<m`, o bien `0<b*(1-q*x`$_0$`)+c*(-q*y`$_0$`)<m`, y esto contradice que `m` sea el mínimo de `A`. Entonces `m|b` y, análogamente, `m|c`. Como `d` es máximo divisor común, `m≤d`.

Por otra parte, `d|m` (porque `m` es una combinación lineal entera de `b,c`) y, entonces, `d≤m`.

Así, `m=d`.

3 `mcd(b,c) = d ⇒ (∃x,y|: d=bx+cy)`

Es un corolario del resultado anterior.

□

4 `mcd(b,mcd(c,d)) = mcd(mcd(b,c),d)`

Dem:

Sean $e_1 = mcd(b,mcd(c,d))$, $e_2 = mcd(mcd(b,c),d)$.
$e_2 = bx + cy + dz$, para ciertos x,y,z (por **3**).
Entonces $e_1|b$ y $e_1|mcd(c,d)$. Por transitividad de la divisibilidad, $e_1|c$ y $e_1|d$. Es decir, $e_1|e_2$.
Análogamente, $e_2|e_1$. Es decir, $e_1 = \pm e_2$. Como ambos son no negativos, $e_1 = e_2$.

□

5 $d|c \wedge d|b \Rightarrow d|mcd(b,c)$
Dem:
Como $mcd(b,c) = b*x+c*y$ para ciertos x,y, entonces $d|mcd(b,c)$.

□

6 $mcd(b,b) = |b|$

7 $mcd(b,1) = 1$

8 $mcd(b,0) = |b|$

9 $mcd(b,c) = mcd(|b|,|c|)$

10 $mcd(b,c) = mcd(b,b+c) = mcd(b,b-c)$
Dem:
Si $b=c=0$, el resultado es trivial.
Si b, c no son ambos 0:
Sea $DC(x,y)$el conjunto de los divisores comunes de los enteros x,y.
Sea $d \in DC(b,c)$. Entonces $d|b$ y $d|(b+c)$. Por tanto, $d \in DC(b,b+c)$.
Sea $d \in DC(b,b+c)$. Entonces $d|b$ y $d|((b+c)+(-1)b)$, o bien, $d|b$ y $d|c$. Por tanto, $d \in DC(b,c)$.
Es decir, $DC(b,c)=DC(b,b+c)$.
Entonces: $mcd(b,c) = \max DC(b,c) = \max DC(b,b+c) = mcd(b,b+c)$.
También:
$mcd(b,c) = mcd(b,-c) = mcd(b,b+(-c)) = mcd(b,b-c)$.

11 $d>0 \Rightarrow d*mcd(b,c) = mcd(d*b,d*c)$
Dem:
$mcd(d*b,d*c)$
=
$(\min x,y|\ d*b*x+d*c*y>0:\ d*b*x+d*c*y)$
= $\langle d>0 \rangle$
$d*(\min x,y|\ d*b*x+d*c*y>0:\ b*x+c*y)$
= $\langle d>0 \Rightarrow (d*b*x+d*c*y>0 \equiv b*x+c*y) \rangle$
$d*(\min x,y|\ b*x+c*y>0:\ b*x+c*y)$
=
$d*mcd(b,c)$

12 $d|b \wedge d|c \wedge d>0 \Rightarrow mcd(b/d,c/d) = mcd(b,c)/d$
Si $g = mcd(b,c)$: $mcd(b/g,c/g) = 1$.

13 $d|b*c \wedge mcd(d,c)=1 \Rightarrow d|b$
Dem:
Por 11: $mcd(b*d,b*c) = b*mcd(d,c) = b$. Ahora, $d|b*d$ y $d|b*c$. Entonces $d|mcd(b*d,b*c)$.
Por tanto, $d|b$.

14 $b|m \wedge c|m \Rightarrow mcm(b,c)|m$
Dem:
Por el Algoritmo de la División, existen q,r tales que $m = q*mcm(b,c)+r$, $0 \le r < mcm(b,c)$. Nótese que

`r = m-q*mcm(b,c)`. Como `b|m`, `b|mcm(b,c)`, entonces `b|r`. Análogamente, `c|r`. Entonces `r` es un múltiplo común de b, c que es menor que su mínimo común múltiplo. La única forma de que esto no sea una contradicción es que `r=0`. Por tanto, `mcm(b,c)|m`.

15 $m>0 \Rightarrow mcm(m*b,m*c) = m*mcm(b,c)$

Dem:

Como `mcm(m*b,m*c)` es un múltiplo de `m*b`, y éste es un múltiplo de `m`, entonces `mcm(m*b,m*c)` es un múltiplo de `m`, digamos $m*h_1$. Sea $h_2 = mcm(b,c)$. Entonces: $b|h_2$, $c|h_2$, $m*b|m*h_2$, $m*c|m*h_2$. Por 14, ya que $m*h_2$ es un múltiplo común de `m*b` y `m*c`, debe valer que $m*h_1|m*h_2$. Por tanto, $h_1|h_2$.

Por otra parte, $m*b|m*h_1$, $m*c|m*h_1$, $b|h_1$, $c|h_1$ y entonces $h_2|h_1$.

Entonces: $h_1=h_2$.

16 `mcm(b,c)*mcd(b,c)= b*c`

Dem:

Caso `mcd(b,c)=1` . Sea `m` tal que `mcm(b,c) = m*b`. Entonces `c|m*b`, pero como `mcd(b,c)=1`, por 13 debe darse que `c|m`. Entonces $c \leq m$ y $b*c \leq m*b$. Ahora, `b*c`, siendo un múltiplo común positivo de b y c, debe ser mayor o igual a `mcm(b,c)`. Así que `b*c = m*b = mcm(b,c)`.

Caso `mcd(b,c)=g>1` . Entonces, por 12, `mcd(b/g,c/g)=1`. Aplicando a esta situación el caso anterior, se llega a que `mcm(b/g,c/g)*mcd(b/g,c/g)= (b/g)*(c/g)`. Si se multiplica a ambos lados por g^2 se obtiene el resultado, a partir de 12 y 15.

□

7.3.1 Algoritmo de Euclides

Alrededor de 300 A.C., Euclides describió el algoritmo que lleva su nombre y que sirve para calcular de una manera muy eficiente el máximo común divisor de dos números enteros.

Se presentan dos versiones del método. La versión 1, basada en restas, se entiende de manera fácil y basa su corrección en algunos hechos sencillos del Teorema B. La versión 2, basada en divisiones enteras, es más rápida que la primera, puesto que cada división en la versión 2 resume varias restas de la versión 1.

Versión 1: restas

```
// Pre: b>0 ∧ c>0

x = b;
y = c;

// Inv: x>0 ∧ y>0 ∧ mcd(x,y) = mcd(b,c)
// Cota: x+y

while (x!=y){
   if (x>y){
      x = x-y;
   }
   else y = y-x;
}

// Pos: x = mcd(b,c)
```

Versión 2: divisiones

```
// Pre: b≥0 ∧ c≥0

x = b;
y = c;

// Inv: x≥0 ∧ y≥0 ∧ mcd(x,y) = mcd(b,c)
// Cota: y

while (y!=0){
   int x1 = x;
   x = y;
   y = x1 % x;
}
// Pos: x = mcd(b,c)
```

Es interesante seguir los estados por los que pasan los algoritmos anteriores, para tener una idea de cómo funcionan y qué tan rápido llegan a su resultado.

Ejemplo A

Se quiere calcular `mcd(963,657)`.

Con la versión 1 (restas) del Algoritmo de Euclides se tendrían los siguientes cambios de estado:

Paso	x	y
0	963	657
1	306	657
2	306	351
3	306	45
4	261	45
5	216	45
6	171	45
7	126	45
8	81	45
9	36	45
10	36	9
11	27	9
12	18	9
13	9	9

Con la versión 2 (divisiones) del Algoritmo de Euclides se tendrían los siguientes cambios:

Paso	x	y
0	963	657
1	657	306
2	306	45
3	45	36
4	36	9
5	9	0

Anotar los cambios de estado en la versión 2 sirve para calcular, además, los enteros que sirven para expresar el máximo común divisor como una combinación lineal de los datos iniciales. En rigor, también hay que anotar los cocientes de las divisiones. En el ejemplo:

```
963 = 657*1 + 306
657 = 306*2 + 45
306 = 45*6 + 36
 45 = 36*1 + 9
 36 = 9*4 + 0
```

Entonces:

```
9  = 45 - 36*1
   = 45 - (306 - 45*6)*1
   = -306 + 45*7
   = -306 +(657-306*2)*7
   = 7*657 - 306*15
   = 7*657 -(963-657*1)*15
   = 22*657 - 15*963.
```

□

Ejercicios 7.3

1 Para las siguientes parejas de números `p` y `q`, encuentre `mcd(p,q)` y números `n` y `m` tales que: `mcd(p,q)=n*p + m*q`

- **a** `p=20, q=19`
- **b** `p=121, q=99`
- **c** `p=333, q=153`
- **d** `p=741, q=299`
- **e** `p=975, q=630`

2 Muestre que: $y>0 \Rightarrow mcd(x,y) = mcd(y, x \bmod y)$. Use este resultado para mostrar que el invariante se mantiene en el Algoritmo de Euclides que usa divisiones.

3 En la versión del Algoritmo de Euclides, incluya en el invariante una variable `t` que guarde el valor de la pareja `(x,y)`. Considere el orden lexicográfico sobre $\mathbf{nat}^+ \times \mathbf{nat}^+$ definido a partir del orden estricto $(\mathbf{nat}^+, |)$ (cf. Ejercicio 7.1.2). Muestre que, en cada iteración, `t` cambia a un valor `t'` tal que $t' <_{lex} t$. ¿Cómo puede usarse esta observación para argumentar la terminación del algoritmo?

7.4 MÁS SOBRE PRIMOS

Los números primos tienen gran importancia dentro de la teoría de enteros y de sus aplicaciones. Por ejemplo, el llamado Teorema Fundamental de la Aritmética permite afirmar que todo número natural se puede expresar como un producto de primos. Muchas de las aplicaciones prácticas de los primos se basan en decidir, de manera eficiente, si un número es o no primo y, de manera relacionada, cuando un número no es primo, descubrir cómo puede factorizarse.

El siguiente teorema es básico para mostrar cómo descomponer números naturales en factores primos:

Teorema A

$p \text{ primo}, p|a*b \Rightarrow p|a \vee p|b$

Dem:

Nótese que $p|a*b$. Si $\neg(p|a)$, se tiene que $mcd(a,p)=1$. Por el Teorema 7.3 B.13 , $p|b$.

□

Teorema B (*Teorema Fundamental de la Aritmética*)

Todo $n \in \mathbf{nat}$, $n>1$ es producto de primos. La descomposición es única, si se ordenan:
$n = p_1 \ldots p_r \ , \ p_1 \leq \ldots \leq p_r$

Dem[4]*:*

Sea $A = \{n:\mathbf{nat} \mid n>1 \wedge n \text{ es producto de primos}\} \cup \{0,1\}$. Supóngase que $A^c \neq \emptyset$. Como es un subconjunto **nat**, debe tener un primer elemento n_0. Claramente, n_0 no puede ser 0 ni 1 (porque están en A) ni tampoco 2, ya que 2 es primo y, por tanto, él mismo es un producto de primos. Es decir, todos los números en el intervalo no vacío $2..n_0\text{-}1$ se pueden expresar como productos de primos, porque n_0 es el primero que no lo es.

No es posible que n_0 sea primo, porque, como 2, sería producto de primos. Entonces deben existir p,q que dividen a n_0, tales que $1<p\leq q<n$, i.e., $p*q=n_0$. Pero tanto p como q se pueden expresar como productos de primos, de modo que n_0 también sería un producto de primos. Es decir, n_0 no puede existir, lo que solo es posible si $A^c=\emptyset$, de modo que $A=\mathbf{nat}$.

Si n tiene dos descomposiciones en primos, v.gr.,

$$n = p_1 \ldots p_r = q_1 \ldots q_s$$

razonar de la siguiente manera. Obsérvese que $p_1 | q_1 \ldots q_s$. Si $p_1=q_1$, se puede dividir por p_1 a ambos lados de la ecuación y repetir el argumento con $p_2 \ldots p_r = q_2 \ldots q_s$. Si $p_1 \neq q_1$, también se tiene que $\mathrm{mcd}(p_1,q_1)=1$ y entonces $p_1 | q_2 \ldots q_s$. Se puede continuar hasta encontrar un j, $1<j\leq s$ tal que $p_1=q_j$. Pero entonces se puede dividir por p_1 a ambos lados de la ecuación y continuar el razonamiento, aunque con menos primos. Cuando se acaben los p_i's deben acabarse los q_j's porque, de lo contrario, debería tenerse que 1 se puede expresar como un producto de primos, lo que sería contradictorio. En resumen, hay los mismos primos dentro de los p's que dentro de los q's. Si se ordenan, la representación en factores es única.

□

La descomposición en primos permite considerar una forma de representación de un número natural positivo. Puesto que todo $n \in \mathbf{nat}$, $n>0$, se puede representar unívocamente como

$$n = (*p \mid p \text{ primo}: p^e)$$

se puede usar como representación la secuencia de los exponentes a la que deben elevarse los primos, ordenados ascendentemente, para dar lugar a n. La representación es, en realidad, una sucesión, pero todos los elementos son 0 para los primos mayores que el más grande que divide a n.

Por ejemplo, para $n=220$, se tiene que $220 = 2^2 * 3^0 * 5^1 * 7^0 * 11^1$. Entonces, la secuencia de los exponentes de los primos menores o iguales a 11 es

$$\langle 2,0,1,0,1 \rangle$$

representa a 220, en el sentido de que el conocer esta secuencia permite reconstruir el número n. [Gri1993] usa la notación $\overline{n}$ para denotar la secuencia de exponentes que representa a n, v.gr.,

$\overline{220} = \langle 2,0,1,0,1 \rangle$

---

[4] Se dará una demostración por inducción, una técnica basada en el axioma e de los Axiomas de Peano que se explicará en el siguiente capítulo. Por ahora, se espera que la demostración se comprenda de manera intuitiva.

$\overline{126} = \langle 1,2,0,1 \rangle$

etc.

La representación es especialmente adecuada para multiplicar dos números porque todo lo que hay que hacer es sumar los elementos de las secuencias miembro a miembro, v.gr.,

$\overline{220*126} = \langle 2+1,0+2,1+0,0+1,1+0 \rangle = \langle 3,2,1,1,1 \rangle$

En general, se cumple que:

Teo C:

a $\overline{m*n}_k = \overline{m}_k + \overline{n}_k$

b $m|n \equiv (\forall k|: \overline{m}_k \leq \overline{n}_k)$

c $\overline{mcd(b,c)}_k = \min(\overline{m}_k, \overline{n}_k)$

d $\overline{mcm(b,c)}_k = \max(\overline{m}_k, \overline{n}_k)$

□

Como un Corolario del teorema anterior, usando **a**, **c** y **d** se descubre otra prueba para

$$mcm(b,c)*mcd(b,c) = b*c \ .$$

El siguiente teorema también era conocido por Euclides.

Teorema C
Hay infinitos primos.

Dem:

Si hay finitos primos, sean estos $p_1 \leq \ldots \leq p_r$. El número $n = p_1 \ldots p_r + 1$ no es divisible por ninguno de los r primos en la lista. Como n es un producto de primos, debe ser primo él mismo, de modo que hay una contradicción.

□

Ejercicios 7.4

1 Muestre el Teorema C.

2 Muestre, como se sugiere en el texto, que el Teorema C da otro método para mostrar que $mcm(b,c)*mcd(b,c) = b*c$.

7.5 CONGRUENCIAS

Las ideas de divisibilidad se expresan y manipulan de manera considerablemente simple con el concepto de congruencia, que se enuncia a continuación. Se puede pensar que las congruencias son, esencialmente, una notación conveniente para entender y resolver los problemas de divisibilidad.

Definición A

Sean a,b,m:**int**, $m \neq 0$.

$a =_m b \equiv m|(b-a)$

La notación $a =_m b$ se lee "a es congruente a b módulo m".

□

En la literatura es usual la notación

$$a \equiv b \pmod m$$

pero aquí se prefiere usar el símbolo $=_m$, para no sobrecargar el operador de equivalencia con otro significado.

El siguiente teorema plantea propiedades importantes de las congruencias:

Teorema A

Sean a,b,c,d,m:**int**, $m \neq 0$.

1 $a =_m b \equiv res(a,m)=res(b,m)$

donde $res(x,m)$ es el residuo de dividir x por m.

Dem:

Por el Algoritmo de la división, existen q_1,r_1 y q_2,r_2, tales que

$a = q_1 m + r_1,\ 0 \leq r_1 < m$

$b = q_2 m + r_2,\ 0 \leq r_2 < m$

Entonces:

$b-a = m(q_2-q_1) + (r_2-r_1)$

($\Rightarrow$)

Como $m|(b-a)$ y $m|m(q_2-q_1)$, debe tenerse que $m|(r_2-r_1)$. Ahora, por las restricciones sobre los residuos: $-m<r_2-r_1<m$, de modo que solo puede ser que $r_2-r_1=0$, i.e., $r_1=r_2$.

($\Leftarrow$)

Si $r_1=r_2$, $b-a = m(q_2-q_1)$, de modo que $a =_m b$.

□

2 $a =_m a$

3 $a =_m b \Rightarrow b =_m a$

4 $a =_m b \wedge b =_m c \Rightarrow a =_m c$

5 $a =_m b \Rightarrow a+c =_m b+c$

6 $a =_m b \Rightarrow a*c =_m b*c$

7 $a =_m b \wedge c =_m d \Rightarrow a+c =_m b+d$

8 $a =_m b \wedge c =_m d \Rightarrow a*c =_m b*d$

Dem:

Hip: $m*f=b-a,\ m*e=c-d$

Deben valer:

$m*f*c = b*c - a*c$

$-m*e*b = -b*c + b*d$

Por tanto:

$m(f*c-e*b) = b*d-a*c$

≡

$a*c =_m b*d$

□

Las propiedades 2, 3 y 4 comprueban que $=_m$ es una relación de equivalencia. La clase de equivalencia $[n]_m$ de un número n, por la relación $=_m$, está compuesta por los enteros que, al dividirse por m, dejan residuo igual al que deja n.

Por ejemplo:

$$[12]_7 = \{...,-9,-2,5,12,19,...\}.$$

Las propiedades 5, 6, 7 y 8 reflejan monotonías de las congruencias con respecto a sumas y multiplicaciones a ambos lados.

En el siguiente teorema se incluyen propiedades en las que el módulo puede variar:

Teorema B

Sean a,x,y,d,m,n:**int**; $d,n\neq 0$; $a,m>0$

1 $a*x =_m a*y \equiv x =_{m/mcd(a,m)} y$

Dem:

Si $a*x =_m a*y$, debe existir z tal que $m*z = a*y-a*x$. Por tanto

$$\frac{a}{mcd(a,m)}*(y-x) = \frac{m}{mcd(a,m)}*z$$

Por tanto:

$$\frac{m}{mcd(a,m)} \mid \frac{a}{mcd(a,m)}*(y-x)$$

Ahora, puesto que $mcd(\frac{m}{mcd(a,m)},\frac{a}{mcd(a,m)}) = 1$ (cf. Teorema 7.3 B.12), debe también darse, por el Teorema 7.3 B.13:

$$\frac{m}{mcd(a,m)} \mid (y-x)$$

es decir,

$$x =_{m/mcd(a,m)} y.$$

2 $a*x =_m a*y \wedge mcd(a,m)=1 \Rightarrow x =_m y$

3 $x =_m y \wedge d|m \Rightarrow x =_d y$

4 $x =_m y \wedge x =_n y \equiv x =_{mcm(m,n)} y$

Dem:

($\Rightarrow$) Se tiene que $m|(y-x)$ y $n|(y-x)$. Es decir, $y-x$ es un múltiplo común de m y n, de modo que $mcm(m,n)|(y-x)$, por el Teorema 7.3 B.14. Es decir, $x=_{mcm(m,n)}y$.

($\Leftarrow$) Si $x=_{mcm(m,n)}y$, entonces $x=_m y$ y $x=_n y$, por 3.

□

7.5.1 Aplicaciones a pruebas de divisibilidad

Si n se representa en base 10, se tiene que

$n = (+k|\ 0 \le k < r : d_k * 10^k)$

donde r es el número de dígitos de n y $0 \le d_k < 10$, $0 \le k < r$.

Teorema A

1 $n =_3 (+k|\ 0 \le k < r : d_k)$

Dem:

Nótese que $10 =_3 1$. Usando repetidamente propiedades de las congruencias, se llega a $10^k =_3 1$, para cualquier k, $0 \le k < r$. También: $d_k * 10^k =_3 d_k$, $0 \le k < r$. Por tanto:

$$
\begin{array}{l}
\quad n \\
= \\
\quad (+k|\ 0 \le k < r : d_k * 10^k) \\
=_3 \\
\quad (+k|\ 0 \le k < r : d_k)
\end{array}
$$

2 $n =_9 (+k|\ 0 \le k < r : d_k)$

3 $n =_{11} (+k|\ 0 \le k < r : (-1)^k * d_k)$

□

7.5.2 Teoremas de Fermat / Euler

Los teoremas de Fermat y de Euler enuncian relaciones de congruencia para ciertas potencias de números. En principio parecen curiosidades interesantes pero no muy aplicables. Sin embargo, se pueden aplicar en situaciones prácticas importantes. Aquí se presentan sin demostración.

Teorema A (*de Fermat*)

$p \text{ primo}, \neg(p|a) \Rightarrow a^{p-1} =_p 1$

□

La siguiente definición generaliza el concepto de número primo y es necesario para enunciar el Teorema de Euler.

Definición B

$m,n>0: \quad m \perp n \equiv mcd(m,n)=1$ // m, n son *primos relativos*

$\varphi(n) = (+k|\ 0<k \le n \wedge k \perp n : 1)$ // *función* φ *de Euler*
// No. de primos relativos a n, menores o iguales que n

□

Los primos relativos no tienen factores primos en común.

La función φ se puede calcular, de acuerdo con el siguiente resultado:

Teorema C

$\varphi(n) = n * (*p|\ p|n \wedge primo.p : (1-1/p))$

□

Es decir, para calcular $\varphi(n)$ se multiplica n por los factores $(1-1/p)$, pasando por todos los primos que dividen a n.

Por ejemplo, para calcular $\varphi(20)$, se observa que 20 solo es divisible por los primos 2 y 5. Entonces
$\varphi(20) = 20 * (1-1/2) * (1-1/5) = 8.$

De hecho, los 8 números menores o iguales a 20 que son primos relativos con él son 1, 3, 7, 9, 11, 13, 17, 19.

Cuando p es primo, el Teorema C indica que
$\varphi(p) = p * (1-1/p) = p-1.$

Nótese que, en cualquier caso, $\varphi(n) \geq 1$.

Teorema D (*de Euler*)
$a \perp m \quad \Rightarrow \quad a^{\varphi(m)} =_m 1$

□

7.5.3 Solución de congruencias lineales

Una *congruencia lineal* es una relación de la forma

$$a*x =_m b$$

donde a,b:**int**, $a \neq_m 0$.
Se buscan soluciones para x, en estos casos.

El siguiente análisis resuelve el problema cuando $a \perp m$:

Caso $b=0$:
Hay solución si

$$a*x =_m 0$$

Y, como $a \neq_m 0$, $x =_m 0$ es solución.

Caso $b \neq 0$:
El teorema de Euler permite afirmar que:

$$a*a^{\varphi(m)-1} =_m 1$$

Por tanto, multiplicando por b los dos lados de esta congruencia:

$$a*(a^{\varphi(m)-1}*b) =_m b$$

Es decir, $x =_m a^{\varphi(m)-1}*b$ es solución.

Los cálculos pueden simplificarse si a y b se remplazan por sus residuos módulo m. Para esto, obsérvese que si
$q = a \div m,\ r = a \bmod m,\ s = b \bmod m.$
Entonces:
Ahora:
$a*x =_m b$
$\equiv$
$(q*m+r)*x =_m s$

$\equiv$

$r*x =_m s$

$\Leftarrow$

$x =_m r^{\varphi(m)-1}*s.$

En cualquier caso, se encuentra una solución para la congruencia. Por otra parte, la observación final permite remplazar cálculos dispendiosos por otros –posiblemente- más simples. Nótese que la solución no es única, ya que si x es solución, cualquier y tal que $x =_m$ y también lo será.

En el caso general, puede no ser cierto que $a \perp m$. Las soluciones se enunciaran, sin demostración.

- Si $\neg(mcd(a,m)|b)$ no hay solución.
  Por ejemplo, en la congruencia lineal $6*x =_2 1$, $mcd(6,2)=2$, pero $\neg(2|1)$.
  No hay soluciones (claramente, $6*x$ siempre será par).
- Si $mcd(a,m)|b$, hay $mcd(a,m)$ soluciones diferentes módulo m.
  Por ejemplo, en la congruencia lineal $6*x =_2 12$, $mcd(6,2)=2$, hay 2 soluciones, 0 y 1, que no son congruentes módulo 2.

Ejercicios 7.5

1 Suponga que la expresión decimal de n es de la forma $d_r d_{r-1} \ldots d_0$. Demuestre los siguientes teoremas:

a $n =_9 (+k| 0 \le k < r : d_k)$

b $n =_{11} (+k| 0 \le k < r : (-1)^k * d_k)$

c $n =_5 d_0$

d $n =_2 d_0$

2 Utilice los resultados de **1** para decidir si las siguientes afirmaciones son ciertas o falsas:

a $11|121121$

b $9|123456789$

c $2|1465413$

d $5|1231230$

e $9|364234$

f $9|364239$

g $11|3454$

h $11|204081$

3 Calcule las siguientes expresiones (recuerde que n mod d es el residuo de la división entera n÷d):

a $5^{422} \bmod 7$

b $5^{422} \bmod 8$

c $2^{13574} \bmod 11$

d $252^{12356} \bmod 253$

e $5^{135} \bmod 23$

4 Solucione las siguientes congruencias lineales:

a $9*x =_7 12$

b $4*x =_5 3$

c $7*x =_9 1$

d $8*x =_{11} 10$

e $3*x =_4 2$

f $320*x =_{325} 315$

7.6 ARITMÉTICA MODULAR

La aritmética modular es informalmente, la misma aritmética sobre los enteros, pero calculando sumas y multiplicaciones módulo n para cierto módulo dado. Es decir, cada entero x es remplazado por un número x' en {0,1,...,n-1}, de modo que $x =_n x'$.

Los enteros con la suma son una estructura algebraica $(\mathbf{Z},+,0)$ que cumple las siguientes leyes:
[1] + es una operación cerrada en **Z** (sumar enteros da enteros)
[2] $z+0 = 0+z = z$ (0 es un módulo para +)
[3] + es asociativa
[4] Para cada z existe un elemento w tal que $z+w = w+z = 0$ (hay inversos).

Adicionalmente, se cumple que
[5] + es conmutativa.

Las anteriores propiedades se pueden generalizar a estructuras algebraicas (conjuntos con operaciones) de la forma $(G,\star,e)$, llamadas *grupos.* Un grupo cumple que:
[1] $\star$ es una operación cerrada en G.
[2] $z\star e = e\star z = z$ (e es un módulo para $\star$)
[3] $\star$ es asociativa
[4] Para cada z existe un elemento w tal que $z\star w = w\star z = e$ (hay inversos).

Cuando también se cumple la propiedad
[5] $\star$ es conmutativa.
se dice que el grupo es *conmutativo* o *abeliano*.

Llamando $\mathbf{Z}_n = \{0,1,...,n-1\}$, y $+_n$ a la suma módulo n (definida sobre $\mathbf{Z}_n$), es fácil ver que $(\mathbf{Z}_n,+_n,0)$ es un grupo abeliano.

Si se llama $*_n$ a la multiplicación módulo n, se querría pensar que $(\mathbf{Z}_n,*_n,1)$ fuera un grupo. Pero no lo es, porque 0 no tendría inverso. Sin embargo, si se denota $\mathbf{Z}_p^* = \{1,2,...,p-1\}$, entonces $(\mathbf{Z}_p^*,*_p,1)$ es también un grupo abeliano, siempre que p sea primo (si no, hay dos números q,r en el conjunto, tales que $q*r = p =_p 0$, de modo que la operación $*_p$ no sería cerrada en $\mathbf{Z}_p^*$).

Un estudio más profundo sobre lo que es la aritmética modular y sus aplicaciones requiere ahondar en conceptos algebraicos relativos a la Teoría de Grupos.

Ejercicios 7.6

1 Para $a,b\in\mathbf{Z}_n$ muestre que $a+_n b =_n a+b$.

2 Pruebe que $(\mathbf{Z}_n,+_n,0)$ es un grupo abeliano.

3 Pruebe que $(\mathbf{Z}_p^*,*_p,1)$ es un grupo abeliano, si p es primo.

4 En $(\mathbf{Z}_{13}^*,*_{13},1)$ determine los inversos de cada uno de los elementos en $\mathbf{Z}_{13}^*$.