Aritmética I

Leandro Marín

leandro@um.es

Septiembre 2010

Índice

Los Números Enteros

Llamaremos números enteros al conjunto infinito formado por los números positivos y negativos que no tienen parte decimal junto con el cero.
Este conjunto se suele representar mediante la letra $\mathbb{Z}$, por lo tanto $\mathbb{Z} = \{\cdots, -3, -2, -1, 0, 1, 2, 3, \cdots\}$
Dentro de este conjunto existen dos operaciones básicas que son la suma y el producto.

Teorema de la División I

Una de las propiedades básicas que tiene el conjunto de los números enteros es la posibilidad de realizar la división de dos números de forma que obtengamos un cociente y un resto. Formalmente el teorema que nos proporciona este resultado es el siguente:

Theorem

Sean a y b dos números enteros con $b > 1$ a los que llamaremos respectivamente dividendo y divisor. Entonces existen valores enteros q y r, llamados cociente y resto, tales que $a = bq + r$ siendo $0 \leq r < b$. Estos valores son únicos.

Teorema de la División II

- Supongamos $a = 7$ y $b = 3$ en el ejemplo anterior y calculemos el cociente y el resto:

Teorema de la División II

- Supongamos $a = 7$ y $b = 3$ en el ejemplo anterior y calculemos el cociente y el resto:
- Si dividimos 7 entre 3 tocamos a $q = 2$ (cociente) y nos sobra $r = 1$ (resto). Es decir $7 = 3 \cdot 2 + 1$.

Teorema de la División II

- Supongamos $a = 7$ y $b = 3$ en el ejemplo anterior y calculemos el cociente y el resto:
- Si dividimos 7 entre 3 tocamos a $q = 2$ (cociente) y nos sobra $r = 1$ (resto). Es decir $7 = 3 \cdot 2 + 1$.
- Supongamos ahora que dividimos $a = -7$ entre $b = 3$, el cociente y el resto es ...

Teorema de la División II

- Supongamos $a = 7$ y $b = 3$ en el ejemplo anterior y calculemos el cociente y el resto:
- Si dividimos 7 entre 3 tocamos a $q = 2$ (cociente) y nos sobra $r = 1$ (resto). Es decir $7 = 3 \cdot 2 + 1$.
- Supongamos ahora que dividimos $a = -7$ entre $b = 3$, el cociente y el resto es ...
- Si pusiésemos el cociente -2 para ajustar la fórmula tendríamos que tener un resto -1, pero el teorema de la división nos dice que el resto tiene que estar entre 0 y b y por lo tanto ser positivo. Por lo tanto la solución es ...

Teorema de la División II

- Supongamos $a = 7$ y $b = 3$ en el ejemplo anterior y calculemos el cociente y el resto:
- Si dividimos 7 entre 3 tocamos a $q = 2$ (cociente) y nos sobra $r = 1$ (resto). Es decir $7 = 3 \cdot 2 + 1$.
- Supongamos ahora que dividimos $a = -7$ entre $b = 3$, el cociente y el resto es ...
- Si pusiésemos el cociente -2 para ajustar la fórmula tendríamos que tener un resto -1, pero el teorema de la división nos dice que el resto tiene que estar entre 0 y b y por lo tanto ser positivo. Por lo tanto la solución es ...
- Ponemos cociente $q = -3$ y resto 2 con lo que $-7 = 3 \cdot (-3) + 2$.

Dominios Euclídeos

Esta situación que se da en $\mathbb{Z}$ de tener un teorema de la división se produce en otras estructuras algebráicas, que reciben el nombre de dominios euclídeos.
El ejemplo fundamental es $\mathbb{Z}$, pero otro ejemplo muy natural el el conjunto de los polinomios $\mathbb{R}[x]$ en la que tenemos una división tal que el resto siempre tiene grado menor que el divisor.
Todos los algoritmos que se ven en este tema se pueden extender a otros dominios euclídeos, en particular a los polinomios.

Divisibilidad

Un caso particularmente importante es cuando el resto de dividir dos números a y b es 0. En este caso diremos que a es un múltiplo de b o que b es un divisor de a.
Todo número tiene como divisores como mínimo a él mismo y a la unidad, por ejemplo 7 tiene únicamente a esos divisores. Sin embargo 6 tiene como divisores a $1, 2, 3$ y 6.
Un número mayor que 1 diremos que es primo si sus únicos divisores son él mismo y la unidad.

Divisores Comunes

Dados dos números a y b podemos plantearnos cuales son los divisores comunes a ambos. Por ejemplo 12 y 18 tienen como divisores

$$D(12) = \{1, 2, 3, 4, 6, 12\}$$

$$D(18) = \{1, 2, 3, 6, 9, 18\}$$

Los divisores comunes a ambos son

$$D(12) \cap D(18) = \{1, 2, 3, 6\}$$

En el caso particular de un número primo p, puesto que sólo tiene a 1 y a p como divisiores, es muy sencillo calcular sus divisores comunes con cualquier otro número m, serán $\{1\}$ si p no divide a m o $\{1, p\}$ si lo divide.

El Máximo Común Divisor

Llamaremos máximo común divisor al más grande de los divisores comunes a dos números (considerando sólo divisores positivos). Cuando dos números tengan máximo común divisor 1 diremos que son coprimos o primos entre sí.

Theorem

Dados dos números a y b, si d es su máximo común divisor, entonces existen números enteros u y v tal que $a \cdot u + b \cdot v = d$.

El método de calcular todos los divisores de dos números, luego calcular los comunes y posteriormente ver cual es el más grande de ellos es un método muy poco efectivo para el cálculo del máximo común divisor.
El algoritmo que nos permite calcular el máximo común divisor de dos números es el siguiente:

Partimos de dos números a y b de los que queremos calcular el máximo común divisor
while $b \neq 0$ **do**
Calcular r el resto de dividir a entre b
Asignar $a = b$ y $b = r$
end while
El máximo común divisor queda en a

Ejemplo

Calculemos el máximo común divisor de $a = 20$ y $b = 14$

a	b	r
20	14	6
14	6	2
6	2	0
2	0	

Si además de calcular el máximo común divisor necesitamos calcular los coeficientes u y v que nos permiten poner $d = a \cdot v + b \cdot v$ entonces utilizaremos el algoritmo de euclides extendido:

Partimos de dos números a y b de los que queremos calcular el máximo común divisor
Asignamos los valores iniciales $v = 0$ y $t = 1$
while $b \neq 0$ **do**
Calcular q y r el cociente y el resto de dividir a entre b
Asignar $a = b$ y $b = r$
Asignar como nuevos valores de (v, t) los $(t, v - t \cdot q)$ del paso anterior
end while
El máximo común divisor queda en a y en v la que buscamos.
El valor de u se calcula despejando de la ecuación

Ejemplo

Calculemos el máximo común divisor extendido de $a = 20$ y $b = 14$

a	b	r	v	t	q
20	14	6	0	1	1
14	6	2	1	$0 - 1 \cdot 1 = -1$	2
6	2	0	-1	$1 - (-1) \cdot 2 = 3$	3
2	0		3		

El coeficiente u se calcula $2 = 20 \cdot u + 14 \cdot 3$ por lo que $20 \cdot u = 2 - 42 = -40$ y $u = -2$.

Inversos Modulares

Dados b y n dos números enteros con $n > 1$ y tales que el máximo común divisor de b y n sea 1, llamaremos inverso de b módulo n al valor v tal que $b \cdot v - 1$ es un múltiplo de n.
Dicho inverso se puede calcular haciendo $a = n$ y aplicando el algoritmo anterior.
La utilización de los inversos modulares la veremos la próxima semana al estudiar la aritmética modular.

Definición

- Ecuación diofántica: ecuación planteada con coeficientes enteros y de las cual buscamos soluciones enteras.

Definición

- Ecuación diofántica: ecuación planteada con coeficientes enteros y de las cual buscamos soluciones enteras.
- De cuantas formas se pueden conseguir 13 euros con monedas de 2 euros y billetes de 5. Si llamamos respectivamente x e y al número de monedas de 2 euros y el de billetes de 5 euros tendríamos que resolver $2x + 5y = 13$.

Definición

- Ecuación diofántica: ecuación planteada con coeficientes enteros y de las cual buscamos soluciones enteras.
- De cuantas formas se pueden conseguir 13 euros con monedas de 2 euros y billetes de 5. Si llamamos respectivamente x e y al número de monedas de 2 euros y el de billetes de 5 euros tendríamos que resolver $2x + 5y = 13$.
- Una solución del tipo $(x, y) = (6{,}5, 0)$ es incorrecta.

Definición

- Ecuación diofántica: ecuación planteada con coeficientes enteros y de las cual buscamos soluciones enteras.
- De cuantas formas se pueden conseguir 13 euros con monedas de 2 euros y billetes de 5. Si llamamos respectivamente x e y al número de monedas de 2 euros y el de billetes de 5 euros tendríamos que resolver $2x + 5y = 13$.
- Una solución del tipo $(x, y) = (6{,}5, 0)$ es incorrecta.
- Una solución podría ser $(4, 1)$ es decir 4 monedas de 2 euros y 1 billete de 5 euros. Ésto se conoce como una solución particular de la ecuación, que en este caso hemos obtenido de forma intuitiva.

Definición

- Ecuación diofántica: ecuación planteada con coeficientes enteros y de las cual buscamos soluciones enteras.
- De cuantas formas se pueden conseguir 13 euros con monedas de 2 euros y billetes de 5. Si llamamos respectivamente x e y al número de monedas de 2 euros y el de billetes de 5 euros tendríamos que resolver $2x + 5y = 13$.
- Una solución del tipo $(x, y) = (6{,}5, 0)$ es incorrecta.
- Una solución podría ser $(4, 1)$ es decir 4 monedas de 2 euros y 1 billete de 5 euros. Ésto se conoce como una solución particular de la ecuación, que en este caso hemos obtenido de forma intuitiva.
- En este caso es fácil deducir que es la única solución positiva de forma intuitiva, pero podrían interesarnos también soluciones negativas.

Ejemplo de Ecuación Diofántica (I)

Calcular todas las soluciones enteras de la ecuación $23x + 19y = 3$.
Calculamos el máximo común divisor extendido de los coeficientes:

a	b	r	v	t	q
23	19	4	0	1	1
19	4	3	1	-1	4
4	3	1	-1	5	1
3	1	0	5	-6	3
1	0		-6		

El máximo común divisor es 1 y el coeficiente $u = \frac{1-19\cdot(-6)}{23} = 5$.

Ejemplo de Ecuación Diofántica (II)

- El máximo común divisor debe dividir al término independiente (si esto no fuese así la ecuación no tendría solución). Como 1 divide a 3 podemos continuar y multiplicar la expresión $1 = 23 \cdot 5 + 19 \cdot (-6)$ por 3 para obtener una solución particular de la ecuación:

$$3 = 23 \cdot \underbrace{5 \cdot 3}_{x_0} + 19 \cdot \underbrace{(-6) \cdot 3}_{y_0}$$

Ejemplo de Ecuación Diofántica (II)

- El máximo común divisor debe dividir al término independiente (si esto no fuese así la ecuación no tendría solución). Como 1 divide a 3 podemos continuar y multiplicar la expresión $1 = 23 \cdot 5 + 19 \cdot (-6)$ por 3 para obtener una solución particular de la ecuación:

$$3 = 23 \cdot \underbrace{5 \cdot 3}_{x_0} + 19 \cdot \underbrace{(-6) \cdot 3}_{y_0}$$

- Con esta solución particular $(x_0, y_0) = (15, -18)$ planteamos las ecuaciones

$$23x + 19y = 3$$

$$23x_0 + 19y_0 = 3$$

y las restamos, con lo que obtenemos

Ejemplo de Ecuación Diofántica (y III)

- $23(x - x_0) = -19(y - y_0)$ por lo que deducimos que $y - y_0$ es un múltiplo de 23 (digamos $23t$) y por lo tanto $-19 \cdot 23t = 23(x - x_0)$ con lo que $x - x_0 = -19t$.

Ejemplo de Ecuación Diofántica (y III)

- $23(x - x_0) = -19(y - y_0)$ por lo que deducimos que $y - y_0$ es un múltiplo de 23 (digamos $23t$) y por lo tanto $-19 \cdot 23t = 23(x - x_0)$ con lo que $x - x_0 = -19t$.
- La solución general es pues:

$$x = x_0 - 19t = 15 - 19t$$

$$y = y_0 + 23t = -18 + 23t$$

donde t es un número entero cualquiera.

Método General de Resolución

Tenemos la ecuación $ax + by = m$ con $a, b, m \in \mathbb{Z}$.

- Calcular $d = mcd(a, b)$ y u, v tal que $d = au + bv$.

Método General de Resolución

Tenemos la ecuación $ax + by = m$ con $a, b, m \in \mathbb{Z}$.

- Calcular $d = mcd(a, b)$ y u, v tal que $d = au + bv$.
- Si d no divide a m la ecuación no tiene soluciones enteras. Si no poner $m = dh$. Multiplicar $d = au + bv$ por h para obtener una solución particular $m = dh = a\underbrace{(uh)}_{x_0} + b\underbrace{(vh)}_{y_0}$

Método General de Resolución

Tenemos la ecuación $ax + by = m$ con $a, b, m \in \mathbb{Z}$.

- Calcular $d = mcd(a, b)$ y u, v tal que $d = au + bv$.
- Si d no divide a m la ecuación no tiene soluciones enteras. Si no poner $m = dh$. Multiplicar $d = au + bv$ por h para obtener una solución particular $m = dh = a\underbrace{(uh)}_{x_0} + b\underbrace{(vh)}_{y_0}$
- La solución general de la ecuación es

$$x = x_0 - (b/d)t \quad y = y_0 + (a/d)t$$

con $t \in \mathbb{Z}$.

- Un número $p > 1$ es primo si sus únicos divisores son él mismo y la unidad.

- Un número $p > 1$ es primo si sus únicos divisores son él mismo y la unidad.
- El número de primos es infinito.

- Un número $p > 1$ es primo si sus únicos divisores son él mismo y la unidad.
- El número de primos es infinito.
- Los números primos son las piezas básicas con las que podemos construir todos los demás. Los números que son producto de dos o más primos (iguales o distintos) los llamaremos compuestos.

Teorema Fundamental de la Aritmética

Theorem

Dado un número entero $n > 0$ existen primos $p_1 < p_2 < \cdots < p_k$ y exponentes $\alpha_1, \alpha_2, \cdots, \alpha_k$ tales que $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$. Estos primos y exponentes son únicos y esta expresión se conoce como la factorización de n.

Theorem

Un número es compuesto si y sólo si tiene un factor menor o igual que su raiz cuadrada.

Utilizando el teorema anterior, para factorizar un número basta con ir buscando factores primos más pequeños que su raiz cuadrada. Ésto lo podemos hacer de forma recursiva.