La aritmética modular (parte 2)
Algoritmo de Euclides

6 de septiembre de 2012

Índice

1. Algoritmo de Euclides **1**

2. Identidad de Bézout **3**

1. Algoritmo de Euclides

Sean a y b dos números enteros con $a > b > 0$. Consideremos la siguiente propiedad:

Propiedad 1. Si $a, b \in \mathbb{Z}$, con $b \neq 0$. Entonces $mcd(a, b) = mcd(b, r)$, donde r es el resto de la división euclídea de a entre b.

Para entender lo que dice esta propiedad, pongamos el siguiente ejemplo: si tomamos $a = 20$ y $b = 6$, y efectuamos la división euclídea, observaremos que el cociente es 3 y el resto es $r = 2$. La propiedad nos dice que el mcd entre a y b es el mismo que el mcd entre b y r, es decir, $mcd(20, 6) = mcd(6, 2)$.

La propiedad anterior es la base de un algoritmo de suma importancia, el *algoritmo de Euclides*, que permite calcular de forma muy sencilla el máximo común divisor entre dos números enteros. Detallamos, a continuación, los pasos de este algoritmo:

Algoritmo de Euclides:

Como $mcd(a,b) = mcd(|a|,|b|)$ podemos suponer sin pérdida de generalidad que a y b son positivos.

- Calculamos la división euclídea de a entre b ($a = q_1 \cdot b + r_1$).
  Si $r_1 = 0$, entonces b divide a a y $mcd(a,b) = b$.
  $\hookrightarrow$ Si $r_1 \neq 0$,
  - Calculamos la división euclídea de b entre r_1 ($b = q_2 \cdot r_1 + r_2$).
    $\hookrightarrow$ Si $r_2 = 0$, entonces r_1 divide a b y aplicando el lema anterior, $mcd(a,b) = mcd(b,r_1) = r_1$.
    $\hookrightarrow$ Si $r_2 \neq 0$,
    - Calculamos de nuevo la división euclídea del divisor de la división anterior entre el resto ($r_1 = q_3 \cdot r_2 + r_3$)...

Como $b > r_1 > r_2 > \cdots > r_n \geq 0$, llegará un momento en el que alguno de los restos r_k será nulo y el proceso finalizará. Aplicando el lema anterior se deduce que $mcd(a,b)$ es el último resto no nulo del algoritmo de Euclides.

Veamos un ejemplo. Supongamos que queremos calcular $mcd(689,234)$ aplicando el algoritmo de Euclides. Lo que haremos es efectuar primero la división y, después, en cada paso, hacer la división ente *el divisor* y el *resto* de la división anterior. Pararemos cuando obtengamos una división exacta. El mcd será el *último resto no nulo obtenido*:

1. Dividimos $a = 689$ entre $b = 234$: $\begin{array}{rl} 689 & |\underline{234} \\ 221 & \ \ 2 \end{array}$
2. Dividimos el divisor entre el resto: $\begin{array}{rl} 234 & |\underline{221} \\ 13 & \ \ 1 \end{array}$
3. Dividimos el nuevo divisor entre el nuevo resto: $\begin{array}{rl} 221 & |\underline{13} \\ 0 & \ 17 \end{array}$

El último resto no nulo es el 13. Por tanto, $mcd(689,234) = 13$.

<u>**Observación**</u>:

Como el producto del mcd por el mínimo común múltiplo de dos números es igual al producto de ambos números se tiene que $mcd(689,234) \cdot mcm(689,234) = 689 \cdot 234$. De esta manera podemos calcular también el mínimo común múltiplo de 689 y 234:

$$mcm(689,234) = 689 \cdot 234/13 = 12402.$$

Veamos otro ejemplo. Calculemos ahora $mcd(54321, 50)$:

$$\begin{array}{ll} 54321 & |\underline{50} \\ \quad 21 & 1056 \end{array} \qquad \begin{array}{ll} 50 & |\underline{21} \\ 8 & \ 2 \end{array} \qquad \begin{array}{ll} 21 & |\underline{8} \\ 5 & \ 2 \end{array}$$

$$\begin{array}{ll} 8 & |\underline{5} \\ 3 & \ 1 \end{array} \qquad \begin{array}{ll} 5 & |\underline{3} \\ 2 & \ 1 \end{array} \qquad \begin{array}{ll} 3 & |\underline{2} \\ {\color{red}1} & \ 1 \end{array} \qquad \begin{array}{ll} 2 & |\underline{1} \\ 0 & \ 2 \end{array}$$

Como el último resto no nulo es ${\color{red}1}$ se tiene que $mcd(54321, 50) = 1$, luego 54321 y 50 son primos entre sí.

Además su mínimo común múltiplo es:

$$mcm(54321, 50) = 54321 \cdot 50/mcd(54321, 50) = 2716050.$$

Ejercicio 1. Calcula el mcd y el mcm de los siguientes pares de enteros, usando el Algoritmo de Euclides:

(a) 29341, 1739.

(b) 10285, 9009.

2. Identidad de Bézout

El Algoritmo de Euclides permite demostrar un teorema muy importante de la Teoría de Números, la *Identidad de Bézout*, que afirma que el máximo común divisor de dos números enteros puede expresarse como combinación lineal de ellos:

Teorema 1. Para cualquier par de números enteros a, b, existen otros dos números enteros x, y tales que $mcd(a, b) = x \cdot a + y \cdot b$.

Una expresión del estilo $mcd(a, b) = x \cdot a + y \cdot b$ se denomina una *identidad de Bézout*. Para calcular una identidad de Bézout aplicaremos el Algoritmo de Euclides a a y a b (en caso de ser a ó b negativos tomaríamos el valor absoluto) pero, en cada paso, después de realizar cada división, estableceremos la igualdad DIVIDENDO=DIVISOR · COCIENTE + RESTO y *despejaremos el resto* en función de DIVIDENDO y DIVISOR. Sustituiremos este resto por esta expresión en todos los pasos siguientes de manera que, en cada paso, escribamos el resto como combinación lineal de a y b.

Veamos un ejemplo. Calcularemos una identidad de Bézout para los enteros 250 y 111:

$$\begin{array}{l|l} 250 & \underline{111} \\ 28 & \ 2 \end{array} \qquad 250 = 2\cdot 111 + 28 \Rightarrow 28 = 250 - 2\cdot 111$$

$$\begin{array}{l|l} 111 & \underline{28} \\ 27 & \ 3 \end{array} \qquad \begin{aligned} 111 = 3\cdot 28 + 27 \Rightarrow 27 &= 111 - 3\cdot 28 \\ &= 111 - 3\cdot(250 - 2\cdot 111) \\ &= -3\cdot 250 + 7\cdot 111 \end{aligned}$$

$$\begin{array}{l|l} 28 & \underline{27} \\ 1 & \ 1 \end{array} \qquad \begin{aligned} 28 = 1\cdot 27 + 1 \Rightarrow 1 &= 28 - 1\cdot 27 \\ &= (250 - 2\cdot 111) - 1\cdot(-3\cdot 250 + 7\cdot 111) \\ &= 4\cdot 250 - 9\cdot 111 \end{aligned}$$

$$\begin{array}{l|l} 27 & \underline{1} \\ \mathbf{0} & 27 \end{array} \qquad \textbf{resto nulo} \Rightarrow \boxed{\text{mcd(250,111)} = 1}$$

$x = 4$ e $y = -9$ verifican la Identidad de Bézout: $1 = 4\cdot 250 + (-9)\cdot 111$

Ejercicio 2. Calcula una identidad de Bézout para los enteros $a = 7300$ y $b = 1316$.