Profesor: Martín Matamala
Auxiliares: Bastián Espinoza, José Palacios
MA3101: Elementos de Álgebra

División, Bezout, etc.

09 de Octubre de 2016

Presentamos aqui el algoritmo de la división, la identidad de Bezout y algunas aplicaciones.

ξ El algoritmo de la división en $\mathbb{Z}_+$ es muy sencillo. Para dividir n por k encuentre el mayor q tal que $qk < n$. q lo llamamos cociente y $r := n - qk$ el resto. Estos números están únicamente determinados por las relaciones $r = n - qk,\ r < n$. Se extiende de manera natural a $\mathbb{Z}$, y con las mismas propiedades de unicidad.

Prop. Dados $n, m \in \mathbb{Z},\ mcd(n, m) = 1$, existen enteros α, β tales que $\alpha n + \beta m = 1$.
Presentamos dos pruebas (que son esencialmente la misma):

Dem1. La idea es crear un algoritmo que genere una sucesión decreciente de la forma $|x_1 n + y_1 m| > |x_2 n + y_2 m| > \ldots$. Pongamos $n_0 = n,\ m_0 = m$ y busquemos q_0, r_0 tales que $n_0 = q_0 m_0 + r_0,\ |r_0| < |m_0|$. Para $k \geq 0,\ r_k \neq 0$, definamos $n_{k+1} = m_k,\ m_{k+1} = r_k$ y busquemos q_{k+1}, r_{k+1} tales que $n_{k+1} = q_{k+1} m_{k+1} + r_{k+1},\ |r_{k+1}| < |m_{k+1}|$. La última desigualdad se puede reescribir como $|r_{k+1}| < |r_k|$, y notemos también que cada $n_k,\ m_k$ y r_k es çombinación lineal"de n y m. Sea s el entero tal que $r_s = 0$. Tenemos $n_s = q_s m_s$. Ahora, la obervación crucial es que $mcd(n, m) = mcd(n_k, m_k)$, para todo $k \leq s$. (En efecto: $n_k = q_k m_k + r_k$ implica $mcd(n_k, m_k) = mcd(m_k, r_k)$). Tenemos: $r_s = 0 \Rightarrow n_s = q_s m_s \Rightarrow m_s = mcd(n_s, m_s) = mcd(n, m) = 1$. Como dijimos, m_s es combinación lineal de n y m.

Dem2.
La propiedad se sigue de los casos $n, m \geq 0$. Hagamos inducción en $k := n + m$. El caso base es trivial. Si es cierto cuando $n + m \leq k$, probemosla para $n + m = k + 1$. Sin pérdida de generalidad podemos suponer $n > m$. Elijamos $q, r \in \mathbb{Z}_+$ tales que $n = qm + r,\ 0 < r < m$. Como $mcd(r, m) = 1$ y $r + m < n + m = k + 1$, podemos usar la hipótesis de inducción para encontrar α, β tales que $\alpha r + \beta m = 1$.

Corolario: Bezout. Sean $n, m \in \mathbb{Z}$. Existen $\alpha,\ \beta \in \mathbb{Z}$ tales que $\alpha n + \beta m = mcd(n, m)$.
Dem. Propuesta.

Una forma típica de su uso es:
Prop Sean p, q enteros positivos coprimos. $\mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$ (como grupos aditivos).
Dem. Tenemos que mostrar que $(1, 1) \in \mathbb{Z}_p \times \mathbb{Z}_q$ es generador. Usemos la notación $n(x, y) := (nx, ny)$. Sean $\alpha,\ \beta \in \mathbb{Z}$ tales que $\alpha p + \beta q = 1$. Dado $(a, b) \in \mathbb{Z}_p \times \mathbb{Z}_q$, $(\alpha p b + \beta q a)(1, 1) = (a, b)$. Los detalles se dejan al lector.

Prop. Los elementos invertibles de $(\mathbb{Z}_n, \cdot)$ son precisamente los enteros coprimos con n.
Dem. Sea $m \in \mathbb{Z}$. Existen $\alpha,\ \beta$ tales que $\alpha n + \beta m = mcd(n, m)$, lo que implica $\beta m \equiv_n mcd(n, m)$. Si $mcd(n, m) \equiv_n 1$, entonces m es invertible. Si $mcd(n, m) \not\equiv_n 1$, entonces existe $k \not\equiv_n 0$ tal que $mdc(n, m)k = n$, por lo que $k\beta m \equiv_k mcd(n, m)k \equiv_n 0$. Así, m no es invertible por ser divisor de 0.

ξ La división de polinomios se verá en clases. De todos modos dejamos escrito algo.
Prop. Sean $f, g \in \mathbb{R}[X],\ g \neq 0$. Existen $q, r \in \mathbb{R}[X]$ tales que $f = qg + r,\ gr(r) < gr(g)$.
Dem. Por inducción en $n := gr(f)$. El caso base se deja al lector. Supongamos que es cierto para números menores a n. Si $gr(g) > gr(f)$, entonces $q = 0,\ r = f$ satisfacen las condiciones. Si $gr(g) \leq gr(f)$, entonces existe $\alpha \in \mathbb{R}$ no nulo tal que $h := f - \alpha x^{gr(f) - gr(g)} g$ tiene grado menor que f. Usamos la hipótesis de inducción al dividir h por g y, reordenando los términos, concluimos.

Corolario. Bezout. Sean $f, g \in \mathbb{R}[X]$. Existen $\alpha, \beta \in \mathbb{R}[X]$ tales que $\alpha f + \beta g = mcd(f, g)$.
Dem. Idéntica al caso entero. La ventaja de esta demostración frente a la casi-definición teórica es que nos da un algoritmo para encontrar α y β.