Introducción a dominios euclidianos

Facultad de Ciencias UNAM

Introducción

El objetivo de esta sección es introducir y estudiar una generalización del famoso "Algoritmo de la división euclidiano"; el cual es un método para calcular el máximo común divisor de dos enteros. Por si no lo recuerdas, aquí ta:

Supongamos que $a, b \in \mathbb{Z}$ con $a > b > 0$. Nuestro objetivo es encontrar explícitamente a $\text{mcd}\{a, b\}$. Para esto, sean

$$q_0 := \text{máx}\{n \in \mathbb{Z} \mid bn \leq a\} \quad \text{y} \quad r_0 = a - bq_0.$$

Entonces $0 \leq r_0 <^1 b$ y podemos escribir

$$a = bq_0 + r_0 \tag{1}$$

En caso de que $r_0 = 0$, entonces $a = bq_0$, lo cual implica $b|a$ y por lo tanto, $\text{mcd}\{a, b\} = b$ y ya acabamos.

[1] De lo contrario, $a - bq_0 = r_0 \geq b$ y por lo tanto, $a \geq bq_0 + b = b(q_0 + 1)$, contradiciendo nuestra elección de q_0.

En caso de que $r_0 \neq 0$, definimos

$$q_1 := \text{máx}\{n \in \mathbb{Z} \mid r_0 n \leq b\} \quad \text{y} \quad r_1 = b - r_0 q_1.$$

Entonces $0 \leq r_1 <^2 r_0$ y podemos escribir

$$b = q_1 r_0 + r_1. \tag{2}$$

En caso de que $r_1 = 0$, entonces $b = q_1 r_0$ (en particular $r_0 | b$) y ocupando (1) obtenemos

$$a = (q_1 r_0) q_0 + r_0 = r_0(q_1 q_0 + 1).$$

Por lo tanto, $r_0 | a$ y $r_0 | b$, es decir r_0 es divisor común de a y b. Mas aun, como (por definición) $r_0 = a - b q_0$ es una $\mathbb{Z}$-combinación lineal de a y b, entonces todo divisor común de a y b divide a r_0. Por lo tanto, $\text{mcd}\{a, b\} =^3 r_0$.

---

[2] Esto se demuestra de la misma manera en la que demostramos $r_0 < b$.

[3] Recordemos que $\text{mcd}\{m, n\}$ es el único entero tal que (i) es divisor común de m y n y (ii) $d | \text{mcd}\{m, n\}$ para todo d divisor común de m y n.

En caso de que $r_1 \neq 0$, podemos encontrar (de la misma manera que en los casos anteriores) $q_2, r_2 \in \mathbb{Z}_{\geq 0}$ tales que $r_2 < r_1$ y

$$r_0 = q_2 r_1 + r_2.$$

En caso de que $r_2 = 0$, se puede demostrar que $\text{mcd}\{a, b\} = r_1$. Por supuesto, la demostración es muy similar a la que dimos para ver que $\text{mcd}\{a, b\} = r_0$ cuando $r_1 = 0$.

Ahora bien, debería de ser claro que podemos seguir de esta manera, pero parecería que no hay nada que garantice que este procedimiento eventualmente acabe. Al fin y al cabo, dependemos de que exista $N \in \mathbb{Z}_{\geq 0}$ tal que $r_N = 0$; pues en este caso, $\text{mcd}\{a, b\} = r_{N-1}$.[4]

Afortunadamente, *si* podemos garantizar la existencia de semejante N. En efecto, recordemos que la sucesión de las r_i es estrictamente decreciente, es decir, $r_0 > r_1 > r_2 > \cdots$, pero como $r_i \geq 0$ para toda i, entonces la sucesión de las r_i es finita y por lo tanto, existe $N \in \mathbb{Z}$ tal que $r_N = 0$.

[4] Cabe recalcar que si $n = 0$, definimos $r_{-1} = b$.

Por lo tanto, para cualesquiera dos enteros $a, b \in \mathbb{Z}$ con $a > b > 0$, existe $N \in \mathbb{Z}_{\geq 0}$; $q_0, \ldots, q_N \in \mathbb{Z}_{\geq 0}$; $r_0, \ldots, r_{N-1} \in \mathbb{Z}_{\geq 0}$ tales que
$r_0 > r_1 > \cdots > r_{N-2} > r_{N-1}$,

$$\begin{aligned} a &= bq_0 + r_0 \\ b &= r_0 q_1 + r_1 \\ r_0 &= r_1 q_2 + r_2 \\ r_1 &= r_2 q_3 + r_3 \\ &\vdots \\ r_{N-3} &= r_{N-2} q_{N-1} + r_{N-1} \\ r_{N-2} &= r_{N-1} q_N, \end{aligned} \tag{3}$$

y $\text{mcd}\{a, b\} = r_{N-1}$.

Ahora bien, no olvidemos que queremos generalizar este resultado. En otras palabras, dado un anillo arbitrario R, nos gustaría encontrar condiciones suficientes sobre R para que se satisfaga la siguiente condición:

Para todo $a, b \in R$ con $b \neq 0$, existe $N \in \mathbb{Z}_{\geq 0}$; $q_0, \ldots, q_N \in R$; $r_0, \ldots, r_{N-1} \in R$; y una sucesión de ecuaciones como la de (3).

De esta manera, r_{N-1} sera el máximo común divisor de a y b en R. Ahora bien, notemos que

1. Lo que nos permitió construir la sucesión de ecuaciones fue la posibilidad de encontrar para cualesquiera dos elementos x, y con $x \neq 0$, otros dos elementos q, r tales que

$$x = yq + r.$$

   En efecto, con esta hipótesis, podremos empezar con a, b $(b \neq 0)$ para obtener q_0, r_0 que satisfagan $a = bq_0 + r_0$. Luego (en caso de que $r_0 \neq 0$) podremos aplicarle esta hipótesis de nuevo a b, r_0 para obtener q_1, r_1 tales que ... bla, bla, bla.

2. Lo que nos permitió garantizar que la sucesión de ecuaciones eventualmente se acaba (o equivalentemente lo que nos permitió garantizar la existencia de la $N \in \mathbb{Z}_{\geq 0}$), fue que $b > r_0 > r_1 > \cdots$ y que $r_i \geq 0$ para toda i.

   Esto presenta una dificultad porque en un anillo arbitrario, no existe la noción de orden entre sus elementos. Afortunadamente, ya sabemos como darle una noción de orden a un anillo: definimos una norma. Por lo tanto, acabamos de encontrar una condición necesaria para nuestra generalización: vamos a trabajar en anillos con una norma.

Con esto en mente, introducimos las siguiente definición.

Dominio euclidiano

Definición

Supongamos que R es un dominio entero y que N es una norma en R.
Decimos que R es un **dominio euclidiano** (abreviado **DE**) con la norma N si para toda $a, b \in R$, $b \neq 0$, existen $q, r \in R$ tales que

$$a = qb + r \text{ con } r = 0 \text{ o } N(r) < N(b)$$

En este caso a q y r les llamamos el **cociente** y **residuo** (respectivamente) de la división.

Comentario

La razón por la que pedimos una norma y no una campo-norma es que en $\mathbb{R}_{\geq 0}$, *si* existen sucesiones infinitas estrictamente decrecientes. Por lo tanto, no podremos generalizar el argumento que dimos para demostrar la finitud del algoritmo.

La siguiente proposición muestra que nuestra definición de dominio euclidiano cumple lo deseado. Específicamente, que en un dominio euclidiano, cualesquiera dos elementos tienen un máximo común divisor que se puede calcular algorítmicamente.

Como es de esperarse, la demostración es completamente análoga a la demostración del algoritmo de la división euclidiano que dimos en la introducción.

El algoritmo de la división en dominios euclidianos

Proposición 1

Supongamos que R es un dominio euclidiano con la norma N. Si $a, b \in R$ con $b \neq 0$, entonces existe $n \in \mathbb{Z}_{\geq 0}$; $q_0, \ldots, q_n \in \mathbb{Z}_{\geq 0}$; $r_0, \ldots, r_{n-1} \in \mathbb{Z}_{\geq 0}$ tales que

1. $N(r_0) > N(r_1) > \cdots > N(r_{n-2}) > N(r_{n-1}) \geq 0$ y

$$\begin{aligned} a &= bq_0 + r_0 \\ b &= r_0 q_1 + r_1 \\ r_0 &= r_1 q_2 + r_2 \\ &\vdots \\ r_{n-3} &= r_{n-2} q_{n-1} + r_{n-1} \\ r_{n-2} &= r_{n-1} q_n. \end{aligned}$$

2. El ideal generado por a y b coincide con el ideal principal generado por r_{n-1}, es decir, $(a, b) = (r_{n-1})$.

Demostración.

1. Primero aplicas la definición de dominio euclidiano a a, b para obtener la primera ecuación y la desigualdad $N(r_0) < N(b)$, luego aplicas la definición de dominio euclidiano a b, r_0 para obtener la segunda ecuación y $N(r_1) < N(r_0)$, luego aplicas la definición de dominio euclidiano a r_0, r_1 para obtener la tercera ecuación y la desigualdad $N(r_2) < N(r_1)$, luego aplicas la definición de dominio euclidiano a r_0, r_1 para...

   Recordemos que este proceso es finito porque de lo contrario tendríamos una sucesión infinita en $\mathbb{Z}_{\geq 0}$ que es estrictamente decreciente:

   $$0 \leq \cdots N(r_k) < N(r_{k-1}) < \cdots N(r_1) < N(r_0)$$

   lo cual es obviamente imposible. Para ser precisos, la $n \in \mathbb{Z}$ que buscamos es igual a "el numero de ecuaciones que podemos generar usando el procedimiento descrito anteriormente" menos 1.

2. $\subset$) Primero notemos que como $r_{n-2} = r_{n-1}q_n$, entonces $r_{n-1}|r_{n-2}$. Usando esto y la igualdad $r_{n-3} = r_{n-2}q_{n-1} + r_{n-1}$, obtenemos que $r_{n-1}|r_{n-3}$. Siguiendo de esta manera, por inducción es fácil ver que $r_{n-1}|r_0$. Finalmente, (procediendo de la misma manera) tenemos que $r_{n-1}|b$ (usando que $r_{n-1}|r_0$ y la igualdad $b = r_0q_1 + r_1$) y que $r_{n-1}|a$ (usando que $r_{n-1}|a$ y la igualdad $a = bq_0 + r_0$). Por lo tanto, r_{n-1} es divisor común de a y b, y en particular $(a, b) \subset (r_{n-1})$.

   $\supset$) Primero notemos que como $a = bq_0 + r_0$, entonces $r_0 = a - bq_0 \in (a, b)$. Usando esto y la igualdad $b = r_0q_1 + r_1$, también tenemos que $r_1 = b - r_0q_1 \in (r_0, b) \subset (a, b)$. Siguiendo de la misma manera, es fácil ver por inducción que $r_{n-1} \in (a, b)$. Cabe recalcar que para el paso inductivo es mas fácil usar inducción fuerte (es decir suponer $r_i \in (a, b)$ para toda $i \leq k$ y demostrar que $r_{k+1} \in (a, b)$) pues tenemos la siguiente ecuación

$$r_{k+1} = r_{k-1} - q_{k+1}r_k \in (r_{k-1}, r_k) \subset (a, b),$$

   donde la inclusión se cumple porque por hipótesis de inducción $r_i \in (a, b)$ para toda $i \leq k$.

$\mathbb{Z}$ es un dominio euclidiano

Obviamente, $\mathbb{Z}$ con la norma $N(k) = |k|$ es un dominio euclidiano; pero por la manera en la que formulamos la definición de dominio euclidiano, todavía no hemos demostrado esto: El detalle es que en los axiomas de dominios euclidianos arbitrarios garantizábamos la existencia del cociente y el residuo para $a, b \in R$ con $b \neq 0$. Sin embargo, cuando demostramos el algoritmo de la división en $\mathbb{Z}$, supusimos $a > b > 0$. Veamos que este caso implica el resto. Específicamente, veamos que

Si $a, b \in \mathbb{Z}$ *con* $a > b > 0$, *entonces existen* $q_0, r_0 \in \mathbb{Z}$ *tales que*

$$a = bq_0 + r_0 \quad y \quad 0 \leq r_0 < b.$$

implica que

Si $x, y \in \mathbb{Z}$ *con* $y \neq 0$, *entonces existen* $q, r \in \mathbb{Z}$ *tales que*

$$x = yq + r \quad y \quad |r| < |y|.$$

Sean $x, y \in \mathbb{Z}$ con $y \neq 0$ y supongamos sin perdida de generalidad que $|x| \geq |y|$. Si $|x| = |y|$, entonces $q = \pm 1$ y $r = 0$ cumplen lo deseado. Por lo tanto, supongamos que $|x| > |y|$. Procedemos por casos:

Caso 1. $y < 0$.
Caso 1.1. $x > 0$. Entonces como $|x| > |y|$, tenemos que $x > -y > 0$. Poniendo $a := x$, $b := -y$, obtenemos $q_0, r_0 \in \mathbb{Z}$ tales que

$$x = a = bq_0 + r_0 = (-y)q_0 + r_0 = y(-q_0) + r_0 \quad \text{y} \quad r_0 < b = -y = |y|.$$

Por lo tanto, $q := -q_0$ y $r := r_0$ cumplen lo deseado.
Caso 1.2. $x < 0$. Entonces como $|x| > |y|$, tenemos que $-x > -y > 0$. Poniendo $a := -x$, $b := -y$, obtenemos $q_0, r_0 \in \mathbb{Z}$ tales que

$$-x = a = bq_0 + r_0 = (-y)q_0 + r_0 \quad \text{y} \quad r_0 < b = -y = |y|$$

o equivalentemente,

$$x = yq_0 - r_0 \quad \text{y} \quad |-r_0| = r_0 < b = -y = |y|.$$

Por lo tanto, $q := q_0$ y $r := -r_0$ cumplen lo deseado.

Caso 2. $y > 0$. Es completamente análogo.

Un corolario importante del algoritmo de la división

Corolario 2

Supongamos que R es un dominio euclidiano y $a, b \in R$ con $b \neq 0$. Entonces

1. a y b tienen un máximo común divisor d (que podemos calcular algorítmicamente).
2. En un dominio euclidiano *si* se vale la equivalencia

$$d' \text{ es un máximo común divisor de } a \text{ y } b \iff (d') = (a, b).$$

3. Si d' es un máximo común divisor de a y b, entonces d' puede ser escrito como R-combinación lineal de a y b. Específicamente, existen $x, y \in R$ tales que

$$d = ax + by$$

Demostración.

1. Recordemos que en la proposición 1.15.3 vimos que "$(x, y) = (d) \implies d$ es un máximo común divisor de x y y".
2. Antes que nada, recuerda que en la proposición 1.15.3 vimos que en un anillo conmutativo arbitrario, *solo* se vale la implicación

   $$d' \text{ es un máximo común divisor de } a \text{ y } b \impliedby (d') = (a, b).$$

   Ahora bien, recuerda que en la proposición 1.15.3 vimos que d es un máximo común divisor de a y b si y solo si d es generador del ideal mas chico que contiene a (a, b). En particular, todos los mcd's de a y b generan el mismo ideal.

   Usando esto y el hecho de que la r_{n-1} del algoritmo de la división es tal que $(r_{n-1}) = (a, b)$, obtenemos lo deseado.
3. Esto es simplemente consecuencia de que $d' \in (d') = (a, b)$.

□

Cuidado

Supongamos que $a, b \in \mathbb{Z}$ con $a > b > 0$ y sean q_0, r_0 tales que

$$a = bq_0 + r_0 \quad \text{y} \quad r_0 < b$$

Si $r_0 \neq 0$ (o equivalentemente, $b \nmid a$) y definimos $q := q_0 + 1$ y $r := r_0 - b$, entonces

$$bq + r = b(q_0 + 1) + (r_0 - b) = bq_0 + b + r_0 - b = bq_0 + r_0 = a$$

y

$$|r| = |r_0 - b| = -(r_0 - b) = b - r_0 < b = |b|$$

donde la segunda igualdad se cumple porque $r_0 < b$.

En resumen, acabamos de ver que para cualesquiera dos enteros $a, b \in \mathbb{Z}$ con $a > b > 0$ y $b \nmid a$, tenemos dos opciones para el cociente y el residuo.

En general, no hay nada en los axiomas de dominio euclidiano que garantice la unicidad de los cocientes (las q_i), o de los residuos (las r_i), o del máximo común divisor (r_{n-1}).