Ecuaciones lineales diofantinas aplicadas a programas lineales enteros

Iñaki Sebastián Liendo Infante

10 de junio de 2025

Índice general

Capítulo 1

Prerrequisitos

En los siguientes capítulos usaremos extensivamente resultados básicos de teoría de números y de programación lineal, por lo que es provechoso recopilarlos en las siguientes secciones. En particular, va se destaca la importancia de las ecuaciones lineales diofantinas para la construcción de nuestro algoritmo. En este capítulo consideramos pertinente no incluir demostraciones, pues los enunciados son mostrados en cualquier clase de álgebra superior o de programación lineal, por ejemplo. La referencia principal para la sección de teoría de números es [Lav14]. Finalmente, a lo largo de este capítulo tanto como de esta tesis excluimos al cero del conjunto de los números naturales.

1.1. Teoría de Números

1.1.1. Máximo común divisor y mínimo común múltiplo

En primer lugar, introducimos el símbolo de relación "|" para indicar divisibilidad. Dados dos enteros a, b, decimos que b divide a a (y escribimos $b \mid a$) si existe un entero k tal que $a = k \cdot b$. Así también, denotamos el conjunto de divisores de a como

$$D(a) \coloneqq \{b \in \mathbb{Z} : b \mid a\}.$$

Si a es distinto de cero, encontramos que $D(a)$ es finito, puesto que si $b \mid a$, entonces $|b| \leq |a|$, lo cual implica que $|D(a)| \leq 2|a|$. En caso de que a sea nulo, obtenemos $D(a) = \mathbb{Z}$. Observemos también que $\{-1, 1\} \subseteq D(a)$ para todo entero a.

Definición 1.1. *Sean $a_1, \ldots, a_n$ enteros no todos iguales a cero, entonces definimos su máximo común divisor d como el elemento maximal del conjunto $\bigcap_{i=1}^{n} D(a_i)$, y escribimos $d = \operatorname{mcd}\{a_1, \ldots, a_n\}$. Si $\operatorname{mcd}\{a_1, \ldots, a_n\} = 1$, entonces decimos que $a_1, \ldots, a_n$ son coprimos.*

Puesto que $a_i \neq 0$ para alguna i en la definición anterior, encontramos que el conjunto $\bigcap_{i=1}^{n} D(a_i)$ es finito y, como también es no vacío, en efecto existe un elemento maximal. Es decir, el máximo común divisor d siempre está bien definido.

Observación. No porque una colección de enteros sea coprima ($\operatorname{mcd}\{a_1, \ldots, a_n\} = 1$) se sigue que estos enteros sean coprimos a pares ($\operatorname{mcd}\{a_i, a_j\} = 1$ para todo i, j). Por ejemplo, los enteros $1, 3, 3$ son coprimos pero evidentemente $3, 3$ no lo son.

Definición 1.2. *Decimos que $c \in \mathbb{Z}$ es una combinación lineal entera de un conjunto de enteros $a_1, \ldots, a_n$ si existen enteros $x_1, \ldots, x_n$ tales que $c = a_1x_1 + \cdots + a_nx_n$.*

El siguiente teorema, a pesar de su simpleza, es central para los resultados obtenidos en esta tesis.

Teorema 1.3. *Sea d un entero y sean $a_1, \ldots, a_n$ una colección de enteros no todos iguales a cero. Entonces $d = \text{mcd}\{a_1, \ldots, a_n\}$ si y solo si d es la mínima combinación lineal entera positiva de $a_1, \ldots, a_n$.*

Corolario 1.4. *Si $d = \text{mcd}\{a_1, \ldots, a_n\}$, entonces $\text{mcd}\left\{\frac{a_1}{d}, \ldots, \frac{a_n}{d}\right\} = 1$.*

Además del máximo común divisor, requeriremos al mínimo común múltiplo, empero en menor medida. Sea a un entero y denotamos el conjunto de sus múltiplos como

$$M(a) \coloneqq \{x \in \mathbb{Z} : a \mid x\}.$$

Si a es nulo, entoncees $M(a) = \{0\}$. En caso contrario encontramos que $M(a)$ es un conjunto infinito. Ánalogamente a la Definición 1.1, definimos al mínimo común múltiplo m de una colección de enteros $a_1, \ldots, a_n \in \mathbb{Z} \setminus \{0\}$ como el elemento minimal de $\mathbb{N} \cap \bigcap_{i=1}^{n} M(a_i)$. Escribimos $m = \text{mcm}\{a_1, \ldots, a_n\}$. Para observar que está bien definido, basta mencionar que el producto $|a_1 \cdots a_n|$ es un elemento de la intersección y por lo tanto esta no es vacía.

1.1.2. Ecuaciones lineales diofantinas

Sea $c \in \mathbb{Z}$ y sean $a_1, \ldots, a_n$ enteros. Una ecuación lineal diofantina es una ecuación donde queremos encontrar enteros $x_1, \ldots, x_n$ que satisfagan

$$a_1x_1 + \cdots + a_nx_n = c.$$

Será de nuestro interés en las siguientes secciones resolver iterativamente este tipo de ecuaciones. Por el momento basta mencionar que podemos enfocarnos en el caso $n = 2$ sin ninguna pérdida de generalidad. Los siguientes resultados abordan el problema de determinar existencia y unicidad para las ecuaciones lineales diofantinas, así como la construcción de sus soluciones.

Teorema 1.5 (Existencia)**.** *Sean $a, b \in \mathbb{Z}$, no ambos cero. La ecuación $ax + by = c$ tiene solución si y solo si $\text{mcd}\{a, b\} \mid c$.*

Para construir el conjunto de soluciones a una ecuación lineal diofantina, encontramos primero una solución particular.

Definición 1.6. *Sea $d \coloneqq \text{mcd}\{a, b\}$ y sean x', y' enteros tales que $ax' + by' = d$ (c.f. 1.3). Decimos entonces que x', y' son coeficientes de Bézout asociados a a, b, respectivamente.*

Observación. Los coeficientes de Bézout asociados a un par de enteros no son únicos. en efecto, si x', y' son coeficientes de Bézout de a, b, entonces $x' + b$, $y' - a$ también lo son:

$$a(x' + b) + b(y' - a) = ax' + by' + ab - ab = ax' + by' = d.$$

Para fines de esta tesis basta la existencia de estos coeficientes, por lo que decimos de manera indistinta "los coeficientes de Bézout" y "una elección de coeficientes de Bézout".

Definamos $d \coloneqq \text{mcd}\{a, b\}$ y supongamos que la ecuación $ax + by = c$ tiene solución. Entonces $d \mid c$, por lo que existe $c' \in \mathbb{Z}$ tal que $c = c' \cdot d$. Sean x', y' los coeficientes de Bézout asociados a a, b respectivamente. Entonces

$$a(c' \cdot x') + b(c' \cdot y') = c'(ax' + by') = c'd = c,$$

por lo que $c' \cdot x', c' \cdot y'$ es una ecuación particular a la ecuación $ax + by = c$.

Teorema 1.7 (Construcción)**.** *Sea (x_0, y_0) una solución particular de la ecuación lineal diofantina $ax + by = c$. Entonces todas las soluciones de la ecuación están dadas por*

$$\begin{cases} x = x_0 + \frac{b}{d}t, \\ y = y_0 - \frac{a}{d}t, \end{cases} \tag{1.1}$$

donde $d \coloneqq \text{mcd}\{a, b\}$ y $t \in \mathbb{Z}$.

1.2. Programación lineal

Capítulo 2

El algoritmo

2.1. Fase 1: una restricción particular

2.2. Fase 2: múltiples restricciones junto con la particular

2.2.1. Estrategias alternativas para el problema de factibilidad

2.3. Fase 3: el caso general

Bibliografía

[Lav14] Carmen Gómez Laveaga. *Álgebra Superior: Curso completo*. Programa Universitario del Libro de Texto. Facultad de Ciencias, Universidad Nacional Autónoma de México, Ciudad de México, México, primera edición edition, 2014. Primera reimpresión: julio de 2015.