Pontificia Universidad Católica de Chile
Departamento de Ciencia de la Computación
IIC2283 - Diseño y Análisis de Algoritmos

Ayudantía 13 - Teoría de Números

Septiembre de 2025

Caetano Borges, Manuel Villablanca

---

1. Algoritmo Extendido de Euclides

Use el Algoritmo Extendido de Euclides para calcular el inverso de a módulo b y viceversa para

1. $a = 74, b = 383$
2. $a = 254, b = 32$

Solución

1. Ejecutamos el algoritmo extendido de euclides hasta llegar a $r_k = 0$ (notar que las sucesiones son las mismas que las definidas en clase, agregando $q_{k+1} = \lfloor \frac{r_{k-1}}{r_k} \rfloor$):

k	1	2	3	4	5	6	7
q_k	$-$	5	5	1	2	4	$-$
r_k	383	74	13	9	4	1	0
s_k	0	1	-5	26	-31	88	-383
t_k	1	0	1	-5	6	-17	74

   Cuando aparece $r_6 = 1$ leemos la combinación de Bézout:

$$1 = s_6 \cdot a + t_6 \cdot b = 88 \cdot 74 + (-17) \cdot 383.$$

   Por tanto:

$$74^{-1} \text{ mód } 383 \equiv s_6 \equiv 88 \pmod{383}, \qquad 383^{-1} \text{ mód } 74 \equiv t_6 \equiv -17 \equiv 57 \pmod{74}.$$

2. Como ambos numeros son pares, es facil notar que $MCD(a, b) \geq 2 > 1$, por lo que a no tendra inverso en modulo b y viceversa.

2. Perros 🐕 y gatos 🐈

1. Sean $a, b, c \in \mathbb{Z}$. Demuestre que la ecuación $ax + by = c$ tiene al menos una solución si y solo si $gcd(a, b)|c$.

2. Un grupo de perros y gatos gastaron \$100 en una tienda de juguetes para mascotas. Sabiendo que cada perro gastó \$8, y que cada gato gastó \$5, ¿puedes encontrar cuantos perros y cuantos gatos hay en el grupo?

Solución

1. $\Longrightarrow$:
   Llamemos (x_0, y_0) a la solucion de la ecuacion tal que $ax_0 + by_0 = c$. Luego llamemos $MCD(a, b) = d$. Por definicion de MCD, se cumple que $d|a \wedge d|b$, por definicion de divisor, luego $\exists k_1, k_2 \; a = k_1 \cdot d \wedge b = k_2 \cdot d$. Reemplazemos esto en la ecuacion, teniendo: $k_1 dx_0 + k_2 dy_0 = c$, factorizando por d tenemos: $d(k_1 x_0 + k_2 y_0) = c$, es decir si tomamos $k' = (k_1 x_0 + k_2 y_0)$ podemos decir que $\exists k', d \cdot k' = c$, lo que por definicion significa que $d|c$.
   $\Longleftarrow$:
   Aplicando la identidad de Bezout tenemos: $MCD(a, b) = d = ax + by$, luego, dado que $d|c$, tambien $ax + by|c$, es decir $c = k(ax + by) = axk + byk$. Luego si tomamos $x' = xk$ y $y' = yk$, tenemos que $ax' + by' = c$, por ende (x', y') es una solucion de la ecuacion y asi la ecuacion tiene al menos una solucion.

2. Para resolver el problema deberemos modelar la ecuacion diofantica correspondiente y encontrar si esta tiene soluciones con x e y positivos.
   La ecuacion sera $8x + 5y = 100$, donde $d = MCD(8, 5) = 1|100$, por lo que esta tendra solucion.
   Si aplicamos el algoritmo extendido de euclides llegaremos a que $d = 1, x_g = 2, y_g = -3$. Asi podemos sacar nuestra solucion inicial donde $x_0 = \frac{2 \cdot 100}{1}, y_0 = \frac{-3 \cdot 100}{1}$. asi llegamos a nuestra solucion inicial $(200, -300)$. Sabemos que nuestras soluciones son de la forma $x = 200 - 5k$ e $y = -300 + 8k$, por lo que solo hace falta buscar todos los k tales que $x > 0, y > 0$. Para esto hay 2 valores posibles de k. siendo $k = 38$ y $k = 39$, siendo nuestras soluciones $(10, 4)$ y $(5, 12)$.
   Dado que tenemos 2 soluciones posibles para el problema, no podemos decir con certeza cual es la cantidad de perros y de gatos que habian en el grupo.

3. Alice, Bob y Euclides

Alice y Bob son capaces de producir exactamente A y B dispositivos idénticos (de algún tipo) por día, respectivamente. Los empleados de la empresa para la que trabajan pueden tomarse ciertos días (arbitrarios) para descansar, en los que producen 0 dispositivos. Después de exactamente D días de trabajo, logran una producción de P dispositivos. Sea $d_A \leq D$ la cantidad total de días en los que Alice ha trabajado, y sea $d_B \leq D$ la cantidad total de días en los que Bob ha trabajado. La empresa no registra la asistencia de sus empleados, por lo que se desconocen los valores d_A y d_B.

A la jefa de Alice y Bob le llega el rumor de que durante un período dado de D días, uno de sus empleados no ha trabajado en absoluto para producir los P dispositivos. Antes de comenzar a investigar, necesita saber si los resultados obtenidos avalan esta hipótesis. Escriba un algoritmo eficiente tal que dados los parámetros A, B, P y D, retorne alguna de las siguientes alternativas:

- El nombre del empleado que no ha producido nada en el período indicado de D días.
- `AMBOS_PRODUCEN` si ambos han producido al menos 1 dispositivo de los P obtenidos en el período.
- `NO_SE_PUEDE` si en base a los parámetros de entrada no es posible tener una conclusión.

Solución

Modelamos el problema como una ecuación diofantina:

$$Ad_a + Bd_b = P$$

con el dominio de ambas variables en $[0, D]$.

Algorithm 1 Diofantina(A, B, P, D)

if $P \mod \gcd(A, B) \neq 0$ **then**
    return `NO_SE_PUEDE`
end if
$(g, x_g, y_g) \leftarrow \text{EuclidesExtendido}(A, B)$
$x_0 \leftarrow x_g \cdot \frac{P}{g}$
$y_0 \leftarrow y_g \cdot \frac{P}{g}$
$m \leftarrow \left\lceil \text{máx}\{-(D - y_0)\frac{g}{A}, (0 - x_0)\frac{g}{B}\} \right\rceil$
$M \leftarrow \left\lfloor \text{mín}\{-(0 - y_0)\frac{g}{A}, (D - x_0)\frac{g}{B}\} \right\rfloor$
if $m > M$ **then**
    return `NO_SE_PUEDE`
end if
`Alice_zero` $\leftarrow$ `false`
`Bob_zero` $\leftarrow$ `false`
`Alice_nonzero` $\leftarrow$ `false`
`Bob_nonzero` $\leftarrow$ `false`
for $k \leftarrow m$ **to** M **do**
    $x \leftarrow x_0 + k\frac{B}{g}$
    $y \leftarrow y_0 - k\frac{A}{g}$
    if $x = 0$ **then**
        `Alice_zero` $\leftarrow$ `true`
    else
        `Alice_nonzero` $\leftarrow$ `true`
    end if
    if $y = 0$ **then**
        `Bob_zero` $\leftarrow$ `true`
    else
        `Bob_nonzero` $\leftarrow$ `true`
    end if
end for
if `Alice_zero` $\wedge \neg$`Alice_nonzero` **then**
    return `Alice`
else if `Bob_zero` $\wedge \neg$`Bob_nonzero` **then**
    return `Bob`
else if $\neg$`Alice_zero` $\wedge \neg$`Bob_zero` **then**
    return `AMBOS_PRODUCEN`
end if
return `NO_SE_PUEDE`