Algoritmo de Euclides

Paz Jiménez Seral

Departamento de Matemáticas – Universidad de Zaragoza

17 de febrero de 2024

Euclides

Vamos a celebrar una fiesta en casa y queremos gastar 1001 pesetas en puros, exactamente.
Hay puros de 15, 32 y 40 pesetas y queremos que haya al menos uno de cada tipo.
La cuestión es cuántos puros compramos de cada tipo.

Un barco de piratas captura un botín de monedas de oro. Cuando las reparten a partes iguales entre los 295 piratas sobran 73 monedas. Luego en una encarnizada lucha mueren casi la mitad de los piratas, quedando sólo 162. Se vuelve a repartir el botín y ahora sobran sólo 51 monedas. Había muchas monedas pero menos de 50000.
La cuestión es cuántas exactamente.

Puros de 15, 32 y 40 pesetas. Total 1001 pesetas.

$$15x_1 + 32x_2 + 40x_3 = 1001$$

Buscamos soluciones enteras positivas.

Sean $b, a_i \in \mathbb{Z}$ para $i = 1, \cdots, n$, si la ecuación

$$a_1 x_1 + \cdots + a_n x_n = b$$

tiene soluciones enteras, m.c.d$(a_1, a_2, \cdots, a_n) = d$ divide a b.

Recuerda. Gran idea de Euclides (325 a.c. Alejandría)

- A cada a entero le podemos asociar un natural $|a|$
- $a, 0 \neq b \in \mathbb{Z}$, existen unos únicos $c, r \in \mathbb{Z}$ tales que $a = cb + r$ y $|r| < |b|$ (algoritmo de la división).

divisibilidad. $x|y$ cuando existe z tal que $y = xz$

Si $d|x$, $d|xy$ para todo $y \in \mathbb{Z}$, y si $d|x$ y $d|y$, se tiene que $d|x + y$.

máximo común divisor

$x, y \in \mathbb{Z}$, no nulos, existe un único $d \in \mathbb{Z}$, $d > 0$ tal que $d|x$, $d|y$ y si $z|x$ y $z|y$, entonces $z|d$, es el mayor divisor común a x e y.

Gran idea de Euclides

Si $a = cb + r$ se tiene que d divide a a y a b si y solo sí divide a b y a r y

$$\{\text{divisores de } a \text{ y } b\} = \{\text{divisores de } b \text{ y } r\}$$

puros de 15, 32 y 40 pesetas. Total 1001 pesetas.

$$15x_1 + 32x_2 + 40x_3 = 1001$$

$15x_1 + 32x_2 = x$

$$x + 40x_3 = 1001$$

Como m.c.d $(15, 32) = 1$, en principio x puede ser cualquiera pero $x \geq 47$.

$$x = 1001 - 40x_3$$

ahora obligando a soluciones positivas, tenemos $x_3 > 0$ y como

$$1001 - 40x_3 > 47$$

$0 < x_3 < 24$. Así que $80 < x < 962$. Observamos que para obtener x_3, máximo, tiene que ser x mínimo.

$15x_1 + 32x_2 = x$. Euclides $d = ax_1 + bx_2$

Q		q_2	q_3	$\dots$	q_i	$\dots$
R	$r_1 = a$	$r_2 = b$	r_3	$\dots$	r_i	$\dots$
U	$u_1 = 1$	$u_2 = 0$	u_3	$\dots$	u_i	$\dots$
V	$v_1 = 0$	$v_2 = 1$	v_3	$\dots$	v_i	$\dots$

- dividir r_{i-2} por r_{i-1}, cociente q_{i-1} y resto r_i.
- $r_i = r_{i-2} - r_{i-1}q_{i-1}$
- $au_{i-2} + bv_{i-2} = r_{i-2}$ y $au_{i-1} + bv_{i-1} = r_{i-1}$ deducimos

$$\begin{aligned} r_i &= r_{i-2} - r_{i-1}q_{i-1} = \\ &= au_{i-2} + bv_{i-2} - (au_{i-1} + bv_{i-1})q_{i-1} = \\ &= a(u_{i-2} - u_{i-1}q_{i-1}) + b(v_{i-2} - v_{i-1}q_{i-1}) = \\ &= au_i + bv_i. \end{aligned}$$

- $u_i = u_{i-2} - u_{i-1}q_{i-1}$
- $v_i = v_{i-2} - v_{i-1}q_{i-1}$

Resolver $15x_1 + 32x_2 = x$ para cada x

Q		2	7	
R	32	15	2	1
U	1	0	1	$\boxed{-7}$
V	0	1	-2	$\boxed{15}$

Obtenemos $15 \cdot 15 + 32(-7) = 1$, y una solución particular:

$$x_1 = 15x \qquad x_2 = -7x$$

Que no sirve porque buscamos soluciones positivas.

$a, b, c \in \mathbb{Z}$, m.c.d$(a, b) = d$

$$ax + by = c$$

tiene soluciones enteras si y solo si $d|c$

- Si existe solución, por ser $d|a$ y $d|b$, se tiene que $d|c$.
- Si $c = dc_o$, como existen $\overline{x}, \overline{y} \in \mathbb{Z}$ tales que $a\overline{x} + b\overline{y} = d$, se tiene

$$a\overline{x}c_0 + b\overline{y}c_0 = dc_0 = c$$

$$x_0 = \overline{x}c_0 \quad y_0 = \overline{y}c_0$$

es solución

$$\text{soluciones enteras } = \{(x_0 - \frac{b}{d}t, y_0 + \frac{a}{d}t) | t \in \mathbb{Z}\}$$

$$ax + by = c$$
$$ax_0 + by_0 = c$$

restando se obtiene

$$a(x_0 - x) = b(y - y_0)$$

$\frac{a}{d}(x_0 - x) = \frac{b}{d}(y - y_0)$ es multiplo de $\frac{a}{d}$ y $\frac{b}{d}$. Por ser $m.c.d(\frac{a}{d}, \frac{b}{d}) = 1$ es múltiplo de $\frac{a}{d}\frac{b}{d}$. Dividimos

$$\frac{d}{b}(x_0 - x) = \frac{d}{a}(y - y_0) = t \in \mathbb{Z}$$

$$x_0 - x = \frac{tb}{d}, \quad y - y_0 = \frac{ta}{d}$$

luego $x = x_0 - \frac{b}{d}t$, $y = y_0 + \frac{a}{d}t$

Soluciones positivas de $15x_1 + 32x_2 = x$ para cada x

De $15 \cdot 15 + 32(-7) = 1$, todas las posibles soluciones son:

$$x_1 = 15x - 32t \quad x_2 = -7x + 15t$$

solo nos interesan $x_1, x_2 > 0$ obtenemos que

$$7x/15 < t < 15x/32$$

Para que exista un valor entero de t, se tiene

$$\frac{15x}{32} - \frac{7x}{15} = \frac{15 \cdot 15x - 7 \cdot 32x}{32 \cdot 15} = \frac{x}{32 \cdot 15}$$

Para asegurarnos la existencia de t podemos exigir que esa diferencia sea mayor que 1 tamando $x > 32 \cdot 15 = 480$

$$x + 40x_3 = 1001$$

$$x = 1001 - 40x_3$$

tenemos $x_3 > 0$ y como

$$1001 - 40x_3 > 480$$

$x_3 < (1001 - 480)/40 = 13,025$. Así tomamos $x_3 = 13$ y obtenemos $x = 481$
Ahora de

$$7x/15 < t < 15x/32$$

se obtiene

$$224 < t < 226$$

luego $t = 225$ y las soluciones son $x_1 = 481 \cdot 15 - 32 \cdot 225 = 15$,
$x_2 = -7 \cdot 481 + 15 \cdot 225 = 8$

Soluciones positivas de $15x_1 + 32x_2 = 481$ y $481 + 40x_3 = 1001$, $7x/15 < t < 15x/32$

$$15 \cdot 15 + 32 \cdot 8 = 481$$

$$481 + 40 \cdot 13 = 1001$$

$$15 \cdot 15 + 32 \cdot 8 + 40 \cdot 13 = 1001$$

$x_3 < 24$, $x + 40x_3 = 1001$, $x_1 = 15x - 32t \quad x_2 = -7x + 15t$

- $x_3 = 14$, $x = 441$ y $7(441)/15 = 205,8$ y $206,7$, $t = 206$

$$23 \cdot 15 + 3 \cdot 32 + 14 \cdot 40 = 1001$$

- $x_3 = 15$, $x = 401$. $7(441)/15 = 187,13$ y $187,9$, no existe t.
- $x_3 = 16$,$x = 361$. $7(361)/15 = 168,4$ y $169,2$, $t = 169$

$$7 \cdot 15 + 8 \cdot 32 + 16 \cdot 40 = 1001$$

- $x_3 = 17$, $x = 321$. $7(321)/15 = 149,8$ y $150,4$, $t = 150$

$$15 \cdot 15 + 3 \cdot 32 + 17 \cdot 40 = 1001$$

- $x_3 = 18$, $x = 281$. Entre $7(281)/15 = 131,1$ no existe valor de t.
- $x_3 = 19$, $x = 241$. Entre $7(241)/15 = 112,4$ no existe valor de t.
- $x_3 = 20$, $x = 201$. Entre $7(201)/15 = 93,8$ y $94,2$ $t = 94$

$$7 \cdot 15 + 3 \cdot 32 + 20 \cdot 40 = 1001$$

$x_3 < 24,\ x + 40x_3 = 1001,$ $x_1 = 15x - 32t \quad x_2 = -7x + 15t$

- $x_3 = 21$, $x = 161$. $7(161)/15 = 75,1$ y $94,2$ no existe valor de t.
- $x_3 = 22$, $x = 121$. $7(121)/15 = 56,4$ y $56,7$ no existe valor de t.
- $x_3 = 23$, $x = 81$. $7(81)/15 = 37,8$ y $37,9$ no existe valor de t.
- $x_3 < 13$ se tiene $x > 480$ y existe al menos un valor de t que nos da una solución positiva para x_1 y x_2 y que podremos obtener con la fórmula descrita.
  La solución con x_3 máximo es

$$x_3 = 20$$

$$x_2 = 3$$

$$x_1 = 7$$

Universidad Zaragoza

Teorema chino de los restos. $295x + 73 = B \qquad 162y + 51 = B$

$$B = 73 \cdot a + 51 \cdot b$$

de modo que b es múltiplo de 295 y a es múltiplo de 295 más 1
a es múltiplo de 162 y b es múltiplo de 162 más 1.
Total b es múltiplo de 295 y es múltiplo de 162 más 1
a es múltiplo de 162 y a es múltiplo de 295 más 1
Si

$$162\overline{a} + 295\overline{b} = 1$$

$a = 162\overline{a}$ y $b = 295\overline{b}$ verifican las condiciones.

Teorema chino de los restos.
$295x + 73 = B \qquad 162y + 51 = B$

Q		1	1	4	1	1	2	2	
R	295	162	133	29	17	12	5	2	1
U	1	0	1	-1	5	-6	11	-28	$\boxed{67}$
V	0	1	-1	2	-9	11	-20	51	$\boxed{-122}$

$$295 \cdot 67 + 162 \cdot (-122) = 1.$$

$$\overline{B} = -73 \cdot 162(122) + 51 \cdot 295(67)$$

verifica
$\overline{B} - 73 = -73 - 73 \cdot 162(122) + 51 \cdot 295(67)$ es múltiplo de 295 y
$\overline{B} - 51 = -73 \cdot 162(122) + 51 \cdot 295(67) - 51$ es múltiplo de 162 que
son las dos condiciones que buscamos.

Universidad Zaragoza

Calculamos $\overline{B} = -434757$ no nos sirve.
$B = \overline{B} + 295 \cdot 162$ también cumple las dos condiciones (múltiplo de 295 más 73 y múltiplo de 162 más 51).
Además es fácil de ver que si restamos dos posibles soluciones se obtiene un múltiplo de 295 que también es múltiplo de 162.
Soluciones

$$B = -434757 + 295 \cdot 162 \cdot t$$

siendo t un número entero.
Como $295 \cdot 162 = 47790$, el valor de B positivo más pequeño se obtiene con $t = 10$ y es 43143. Además es el único menor de 50000.

Garcias por la atención. Preguntas

Ya has visto que esto ha sido la base para las explicaciones.
Si encuentras erratas, o si hay algo que no entiendes, o simplemente si me quieres preguntar cualquier cosa, ahí va mi dirección

paz@unizar.es