Era el año 1977 y en el bar de Amadeo en Leciñena se contaba el primer problema que os propongo.

En ese bar se jugaba a las cartas, al billar, al futbolín y a las máquinas (buenísmas las de Amadeo). Pero sobretodo se contaban historias y chistes y con bastante frecuencia se proponían problemas de ingenio. Si en el bar coincidían Jose Mª Maico y mi tío el Angel de Barcelona, las risas y el entretenimiento estaban aseguradas. Aquel día el problema iba de puros y ocupó a los del lugar durante bastante rato. En esa época no se decía lo malo que era el tabaco y además los puros eran, para los hombres, artículo de obsequio, de celebración, de conversación, de aparentar y de imagen masculina.

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.

La verdad es que nunca supe los datos exactos del problema propuesto y quizás resultó más difícil que el que os he puesto aquí. Podéis intentar buscar la solución pero por si no os sale, continúo con la historia.

José Mª Maico trabajaba en la gasolinera, yo conducía un Diane 6 para ir a estudiar a la universidad, empezaba segundo de matemáticas. Y está fue mi conversación con el gasolinero.

–¿Es verdad que estudias "pa"lo mismo que Carlos?

–Sí, es verdad.

–¿Pues sabrás lo de "las fánticas"? Me quedé perpleja y le pregunté si quería decir ecuaciones diofánticas.

-Eso será, me contesto con mucho interés. Y continuó..

-Me dijeron un problema de comprar puros que no me salía y lo llevé al bar. Llegó el fulano y el mengano... y todos con papeles y venga todos a pensar y hasta Fernando el de la Eulalia y Roberto el del pintor (estos últimos eran médicos y con fama de muy listos), *y nada, todos se rindieron. Al rato apareció Carlos, dijo no sé qué de las "fánticas", cogió un papel y en poco rato dio la solución, "alucinaus"nos dejó.*

Y va otro problema

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 50.000. ¿Cuántas exactamente?

Un poco de historia Resolver problemas en los que las incógnitas son números enteros ha ocupado a muchos genios durante toda la historia. La teoría de números, que trata los problemas de los números enteros, ha necesitado muchos siglos para llegar a demostrar si algunas ecuaciones con apariencia sencilla tienen o no soluciones enteras. Una ecuación diofántica es una ecuación algebraica, los dos miembros de la igualdad son polinomios, en la que los coeficientes son números enteros y las soluciones que se buscan son también números enteros. El nombre se debe a **Diofanto de Alejandría** que el siglo III , en su obra **Aritmética** estudió interesantes ecuaciones de este tipo. En el siglo XVII llegó a manos de Fermat una nueva edición de la obra de Diofanto y este resolvió y planteó muchos nuevos problemas en la teoría de números que se fueron resolviendo en años sucesivos. Quedó sin demostrar la afirmación de que la ecuación $x^n + y^n = z^n$ con n natural mayor que 2, nunca tiene solución entera. Los intentos para probar esta afirmación, que se pasó a llamar el último teorema de Fermat, han contribuido muchísimo al desarrollo de las matemáticas. Por fin, en 1995 Andrew Wiles consiguió demostrar que el último teorema de Fermat era cierto.

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

Recordemos también la relación de divisibilidad, decimos que $x|y$ cuando existe z tal que $y = xz$, se tiene que si $d|x$, $d|xy$ para todo $y \in \mathbb{Z}$, y si $d|x$ y $d|y$, se tiene que $d|x+y$.

Y también el máximo común divisor: Dados $x, y \in \mathbb{Z}$, 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.

La gran idea de Euclides (325 a.c. Alejandría Si $a = cb + r$ se tiene, por lo dicho antes, que d divide a a y a b si y solo sí divide a b y a r y $\{$divisores de a y $b\} = \{$divisores de b y $r\}$.

Así podemos utilizar el algoritmo de la división para calcular los divisores comunes de a y b haciendo divisiones sucesivas, cada vez dividiendo el divisor anterior por el resto anterior hasta obtener una división con resto cero. El cociente de esa última división es el máximo común divisor de a y b, que denotaremos m.c.d(a, b) (algoritmo de Euclides).

Además, en las divisiones que se han hecho para obtener m.c.d$(a, b) = d$ podemos ir poniendo cada resto en función de los anteriores y se tiene que existen $x, y \in \mathbb{Z}$ tales que $ax + by = d$ (Identidad de Bezout).

Máximo común divisor y algoritmo de Euclides. El máximo común divisor de dos números es el mayor de los divisores comunes. La forma más práctica de calcular el mcd es mediante el algoritmo de Euclides. Veámoslo con un ejemplo, calculando el mcd de 192 y 162.

Q		1	5	2	2	
R	192	162	30	12	$\boxed{6}$	0

Así el mcd$(192, 162) = 6$. Fíjate que la fila **Q** está formada por los cocientes enteros de dos de los números de la fila **R**. Esta fila se forma con los correspondientes restos. El mcd es el último resto no nulo, puesto que se tiene

$$\{\text{divisores de } 192 \text{ y } 162\} = \{\text{divisores de } 162 \text{ y } 30\} = \{\text{divisores de } 30 \text{ y } 12\} =$$

$$\{\text{divisores de } 12 \text{ y } 6\} = \{\text{divisores de } 6\}$$

Y está claro que el divisor más grande de los divisores de 6, es 6.

Identidad de Bezout y algoritmo de Euclides extendido. *Identidad de Bezout:* Si $\text{mcd}(a, b) = d$, entonces existen u y v tales que

$$au + bv = d.$$

Los coeficientes u y v se calculan mediante el algoritmo de Euclides extendido:

Numeramos los números de la fila de los restos del siguiente modo:

$$r_0 = 192 \quad r_1 = 162 \quad r_2 = 30 \quad r_3 = 12 \quad r_4 = 6$$

Vamos a ver que para cada r_i existen u_1, v_i enteros tales que

$$192u_i + 162u_i = r_i$$

Escribiremos estos u_1, v_i debajo del correspondiente resto en una tabla ampliada.

Como $r_0 = 192 = 192 \cdot 1 + 162 \cdot 0$, se tiene evidentemente que $u_0 = 1$ y $v_0 = 0$.

También evidentemente $u_1 = 0$ y $v_1 = 1$.

Para el siguiente resto, que es 30, recodemos que es el resto de dividir los dos restos anteriores, así

$$30 = 192 - 162 \cdot 1$$

y se tiene

$u_2 = 1$ y $v_2 = -1$

Para el siguiente resto, que es 12, recodemos que es el resto de dividir los dos restos anteriores, así

$$12 = 162 - 30 \cdot 5 = 162 - (192 - 162 \cdot 1)5 = 192(-5) + 162 \cdot 6$$

y se tiene

$u_3 = -5$ y $v_3 = 6$

Para el siguiente resto, que es 6, recodemos que es el resto de dividir los dos restos anteriores, así

$$6 = 30 - 12 \cdot 2 = (192 - 162 \cdot 1) - (192(-5) + 162 \cdot 6)2 = 192(1 - (-5)2) + 162(-1 - 6 \cdot 2) = 192(11) + 162(-13)$$

$u_4 = 11$ y $v_4 = -13$ Y como 6 es el máximo común divisor la identidad de Bezout en este caso es

$$6 = 192(11) + 162(-13)$$

Q		1	5	2	2	
R	192	162	30	12	6	0
U	1	0	1	-5	11	
V	0	1	-1	6	-13	

En general, si pensamos en los restos numerados y los cocientes numerados en una tabla

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	$\dots$

Recordar que cada elemento de este cuadro se construye de esta forma:

- q_i es el cociente entero de dividir r_{i-1} por r_i. El resto de esta división es r_{i+1}.
- $r_i = r_{i-2} - r_{i-1}q_{i-1}$

  Si para un r_i ya hemos calculado para los anteriores restos las identidades

  $au_{i-2} + bv_{i-2} = r_{i-2}$,

  $au_{i-1} + bv_{i-1} = r_{i-1}$

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

  Y se tiene que podemos construir la tabla de forma automática con

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

Vamos a comenzar resolviendo ecuaciones lineales con dos incógnitas.

Teorema Sean $a, b, c \in \mathbb{Z}$, la ecuación

$$ax + by = c$$

tiene soluciones enteras si y solo si $d|c$ siendo m.c.d$(a, b) = d$.

Si una solución es (x_0, y_0), el conjunto (infinito) de soluciones enteras es

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

Demostración. Si existe una solución (x_0, y_0), se tiene la iguandad $ax_0 + by_0 = c$ y por ser $d|a$ y $d|b$, se tiene que $d|c$.

Recíprocamente con la identidad de Bezout podemos obtener $\overline{x}, \overline{y} \in \mathbb{Z}$ tales que

$$a\overline{x} + b\overline{y} = d$$

y si $c = c_0 d$ es claro que

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

es solución.

Para ver el conjunto de todas las soluciones, por una parte se tiene

$$a((x_0 + \frac{b}{d}t) + b(y_0 - \frac{a}{d}t) = ax_0 + a\frac{b}{d}t + by_0 - b\frac{a}{d}t) = ax_0 + by_0 = c.$$

Por otra parte si se tienen las igualdades,

$$ax + by = c$$

$$ax_0 + by_0 = c$$

restando se obtiene

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

En nuestra ecuación dividimos por d,

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

y tenemos un 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 por este producto y obtenemos

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

y por tanto

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

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

En general tenemos

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

$$a_1x_1 + \cdots + a_nx_n = b$$

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

Demostración. Si existen enteros $(x_1, \cdots, x_{n-1}, x_n)$ tales que $a_1x_1 + \cdots + a_nx_n = b$ y m.c.d$(a_1, a_2, \cdots, a_n) = d$, se tiene que $d|b$.

Para obtener las soluciones, sea m.c.d$(a_1, a_2, \cdots, a_{n-1}) = r$. Calculamos las soluciones $x = u, y = x_n$ de la ecuación

$$rx + a_ny = b$$

Con cada u obtenido anteriormente, calculamos las soluciones de la ecuación

$$a_1x_1 + \cdots + a_{n-1}x_{n-1} = ru$$

y así obtenemos todas las soluciones $(x_1, \cdots, x_{n-1}, x_n)$ de la ecuación inicial.

NUESTRO PROBLEMA **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. Busca la solución que tenga el máximo número de puros de** 40 **pesetas.**

Planteamos la ecuación

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

Suponiendo que tiene solución y teniendo en cuenta que la ecuación

$15x_1 + 32x_2 = x$ siempre tiene soluciones enteras por ser m.c.d$(15, 32) = 1$, podemos comenzar resolviendo la ecuación

$$x + 40x_3 = 1001$$

y buscando $x > 47$

Para ello no se necesita ni siquiera aplicar lo que hemos comentado del algoritmo de euclides y se tiene las siguientes soluciones enteras.

$$x = 1001 - 40s \quad x_3 = s$$

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

$$1001 - 40s > 47$$

, $0 < s < 24$. Si $s = 23$, se tiene $x = 81$ Así que $80 < x < 962$. Observamos que para obtener x_3, máximo, tiene que ser x mínimo.

Para cada x posible resolvemos

$$15x_1 + 32x_2 = x$$

y ahora sí aplicamos el algoritmo de euclides

Q		2	7	
R	32	15	2	1
U	1	0	1	-7
V	0	1	-2	15

Y obtenemos la igualdad $15 \cdot 15 + 32(-7) = 1$, de dónde deducimos que una solucíon particular es

$$x_1 = 15x, x_2 = -7x$$

y todas las posibles soluciones son:

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

Para no tomar valores de t negativos cambiamos de signo el parámetro

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

y como 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 $x > 32 \cdot 15 = 480$, y $s < (1001 - 480)/40 = 13,025$.

Así tomamos $s = 13$ y obtenemos $x = 481$

Ahora de

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

se obtiene

$$224 < t < 226$$

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

$$x_3 = 13$$

$$x_2 = 8$$

$$x_1 = 15$$

Efectivamente

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

Con $s = 14$ obtendríamos $x = 441$ y $7(441)/15 = 205,8$ y $206,7$, así que podemos tomar $t = 206$ y obtenemos

$$x_3 = 14$$

$$x_2 = 3$$

$$x_1 = 23$$

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

Con $s = 15$ obtendríamos $x = 401$. Entre $7(441)/15 = 187,13$ y $187,9$, no existe valor de t.

Con $s = 16$ obtendríamos $x = 361$. Entre $7(361)/15 = 168,4$ y $169,2$, así que podemos tomar $t = 169$ y obtenemos

$$x_3 = 16$$

$$x_2 = 8$$

$$x_1 = 7$$

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

Con $s = 17$ obtendríamos $x = 321$. Entre $7(321)/15 = 149,8$ y $150,4$, así que podemos tomar $t = 150$ y obtenemos

$$x_3 = 17$$

$$x_2 = 3$$

$$x_1 = 15$$

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

Con $s = 18$ obtendríamos $x = 281$. Entre $7(281)/15 = 131,1$ no existe valor de t.

Con $s = 19$ obtendríamos $x = 241$. Entre $7(241)/15 = 112,4$ no existe valor de t.

Con $s = 20$ obtendríamos $x = 201$. Entre $7(201)/15 = 93,8$ y $94,2$ así que podemos tomar $t = 94$

$$x_3 = 20$$

$$x_2 = 3$$

$$x_1 = 7$$

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

Con $s = 21$ obtendríamos $x = 161$. Entre $7(161)/15 = 75,1$ y $94,2$ no existe valor de t.

Con $s = 22$ obtendríamos $x = 121$. Entre $7(121)/15 = 56,4$ y $56,7$ no existe valor de t.

Con $s = 23$ obtendríamos $x = 81$. Entre $7(81)/15 = 37,8$ y $37,9$ no existe valor de t.

Observamos además que para cada valor de $x_3 < 13$ 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

$$x_3 = 20$$

$$x_2 = 3$$

$$x_1 = 7$$

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 50.000. ¿Cuántas exactamente?

Planteamiento del problema. Vamos a llamar B al botín y se tiene:

$$295x + 73 = B \qquad 162y + 51 = B$$

Y se ha de cumplir que $B - 73$ es múltiplo de 295 y $B - 51$ es múltiplo de 162.

¿Cómo encontrar un tal número? Con el algorítmo de Euclides extendido obtenemos

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	67
V	0	1	-1	2	-9	11	-20	51	-122

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

luego
$1 + 162(122)$ es múltiplo de 295 y $1 - 295(67)$ es múltiplo de 162,
Así $73 + 73 \cdot 162(122)$ es múltiplo de 295 y $51 - 51 \cdot 295(67)$ es múltiplo de 162.

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

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.

Calculamos $\overline{B} = -434757$ que no nos sirve porque es un resultado negativo. Pero es claro que si le sumamos un número que sea a la vez múltiplo de 295 y 162 se tendrá que 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.

Los posibles soluciones son

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

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.