ARITMÉTICA MODULAR II

En primer lugar vamos a introducir las ecuaciones diofánticas lineales y posteriormente veremos las ecuaciones lineales en congruencias.

ECUACIONES DIOFÁNTICAS LINEALES

Ejercicio 1 En un mueble, se nos ha roto una pata de 4 centímetros de altura. Para equilibrarlo provisionalmente, disponemos de varios discos de madera, unos de 5 mm de grosor y otros de 3 mm. ¿Cuántos discos de cada clase usaremos?

Ejercicio 2 Una bufanda cuesta 19 rupias, pero el comprador no tiene más que 25 billetes de tres rupias; y la cajera, sólo de cinco. ¿Puede en estas condiciones abonarse el importe de la compra? ¿De cuantas formas?

Ejercicio 3 (propuesto) Resuelve de dos formas el caso en que el comprador no tenga más que billetes de 5 rupias y la cajera, sólo de 3. Una, a partir del ejercicio anterior dando sentido a los valores negativos; y dos, haciéndolo de nuevo en este caso.

Llamamos ***ecuaciones diofánticas*** a aquellas en las que sólo intervienen números enteros. Para resolverlas, aparte de las operaciones algebraicas habituales (sustituir, despejar, reducir, etc.) tendremos en cuenta cuestiones de divisibilidad, que las incógnitas son números enteros; y en la mayoría de los casos, que son números no negativos (positivos incluido el cero). Por ejemplo, si en la resolución de una ecuación diofántica llegamos a que un número n de personas cumple que $n \leq 8{,}75$ y que $n \geq 6{,}25$, sólo puede ser $n = 7$.

• Las *ecuaciones diofánticas lineales* $a'x + b'y = c'$ admiten solución si y sólo si el mcd(a′,b′) divide a c′. En cuyo caso dividiendo entre el mcd llegamos a la ecuación $ax + by = c$, siendo el mcd(a,b) = 1.
La cual tiene infinitas soluciones, siendo la solución general: $x = x_0 + bt$

$y = y_0 - at$ con $t \in Z$;

con (x_0, y_0) una solución particular.

Ejercicio 4 Elías con 1 euro compra sellos de 1, 4 y 12 céntimos. ¿Cuántos ha comprado de cada clase si en total ha adquirido 40 sellos?

Cálculo de la solución particular

La solución particular se puede obtener a ojo o por el algoritmo de Euclides extendido (o del mínimo resto extendido) aplicado a la ecuación: ax + by = 1 y luego multiplicando la solución por c.

Ejemplo 1: 12x + 23y = 7 no tiene solución particular sencilla, pero sí la tiene 12x + 23y = 1 (la (2, –1)); que multiplicada por 7 da (14, –7).

Ejemplo 2: 144x + 46y = –4. El mcd(144, 46) = 2 que divide a –4. Y la ecuación se reduce a: 72x + 23y = –2.
Aquí no se ve a ojo la solución particular. Luego para calcularla utilizaremos el algoritmo de Euclides extendido (o del mínimo resto extendido) aplicado a 72x + 23y = 1 y luego multiplicando por –2:
dividiendo sucesivamente: 72 = 3·23 + 3 y 23 = 8·3 – 1;
despejando los restos: 1 = 8·3 – 23 y 3 = 72 – 3·23;
y sustituyendo sucesivamente: 1 = 8·3 – 23 = 8(72 – 3·23) – 23 = 8·72 – 25·23;
con lo que hemos obtenemos 1 como combinación lineal de 72 y 23, siendo (8, –25) una solución de 72x + 23y = 1. Multiplicando por –2 obtenemos la solución particular (–16, 50).

EL ALGORITMO DE EUCLIDES EXTENDIDO

El algoritmo de Euclides
Si a = b·c + r, mcd(a, b) = mcd(b, r) y haciendo las divisiones sucesivas se llega al mcd.
Ej: mcd(112,70) = (haciendo las divisiones sucesivas) = 14

El algoritmo del mínimo resto
El algoritmo de Euclides se puede hacer más corto si cuando r > b/2 se hace la división por exceso (en cada una de las divisiones sucesivas)
Ej. Con el algoritmo de Euclides y con el algoritmo del mínimo resto, respectivamente:
mcd(21, 13) = mcd(13, 8) = mcd(8, 5) = mcd(5, 3) = mcd(3, 2) = mcd(2, 1) = 1
mcd(21, 13) = mcd(13, 5) = mcd(5, 2) = mcd(2, 1) = 1

El algoritmo de Euclides extendido (o del mínimo resto extendido)
El algoritmo de Euclides extendido permite, además de encontrar un máximo común divisor de dos números enteros *a* y *b*, expresarlo como la mínima combinación lineal de esos números, es decir, encontrar números enteros *s* y *t* tales que mcd(*a*,*b*) = *as* + *bt*. Lo cual se hace despejando los restos de cada ecuación obtenida de las sucesivas divisiones y sustituyendo el resto de la última ecuación en la penúltima, y la penúltima en la antepenúltima y así sucesivamente hasta llegar a la primera ecuación, y en cada paso expresar cada resto como combinación lineal.
Ejemplo:
mcd(21,13) = 1 luego vamos a obtener dos números enteros *x* e *y* tales que 21x + 13y = 1:
21= 2·13–5, 13=3·5–2 y 5= 2·2+1; despejando los restos:
1=5–2·2, 2=3·5–13 y 5= 2·13–21; y sustituyendo sucesivamente:
1= 5–2·2 = 5–2(3·5–13)= –5·5+2·13 = –5(2·13–21) +2·13 = –8·13+5·21, luego x = 5 e y = –8.

CONGRUENCIAS

Se dice que dos enteros a y b son *congruentes* módulo m si la diferencia de a y b es divisible por m, y se emplea la notación: a ≡ b mod m. Esta definición equivale a decir que a y b dan el mismo resto al ser divididos por m.

Propiedades

i) Si dos números son congruentes con un tercero son congruentes entre sí.

ii) $a \equiv 0 \mod m$ quiere decir que *a* es múltiplo de *m*.

iii) *Si* $a \equiv b$ *y* $c \equiv d$; entonces $a + c \equiv b + d$; $a - c \equiv b - d$ y $ac \equiv bd$ *(todas mod m).*

iv) $a \equiv b \mod m \Rightarrow na \equiv nb \mod m$. Es decir, podemos multiplicar sin problemas en congruencias.

v) *Si* $na \equiv nb \mod m$ *y n es primo con m; entonces* $a \equiv b \mod m$. Es decir, podemos dividir sin problemas en congruencias por números primos con el que indica la congruencia. Por ejemplo, $14 \equiv 4 \mod 5 \Rightarrow 7 \equiv 2 \mod 5$ (por ser 2 primo con 5)

- Sin embargo, si el número por el que dividimos no es primo con el que indica la congruencia la propiedad anterior no es cierta.

  Por ejemplo, $14 \equiv 4 \mod 10$; pero sin embargo 7 y 2 no son congruentes entre sí, módulo 10 (al no ser 2 primo con 10).

Pero existe otra propiedad que permite dividir en este caso:

vi) *Si* $na \equiv nb \mod m$ *y d es el mcd(n, m); entonces* $a \equiv b \mod (m/d)$:

Así, $14 \equiv 4 \mod 10 \Rightarrow 7 \equiv 2 \mod 5$

Otro ejemplo que puede ayudar a aclarar esta propiedad es el siguiente:

$28 \equiv 8 \mod 10 \Rightarrow 7 \equiv 2 \mod (10/2) = \mod 5$ (al ser el mcd(4,10) = 2).

Otra forma de proceder, si hay problemas con esta propiedad, es pasando a ecuaciones diofánticas y utilizando la propiedad v: $28 \equiv 8 \mod 10 \Rightarrow 28 = 8 + 10y$, que se puede simplificar entre 2, quedando: $14 = 4 + 5y \Rightarrow 14 \equiv 4 \mod 5$ y, por la propiedad v, entonces $7 \equiv 2 \mod 5$.

vii) *Si* $a \equiv b \mod m \Rightarrow a^n \equiv b^n \mod m$. El recíproco no tiene por qué ser cierto.

Por ejemplo: $7^2 \equiv 5^2 \mod 3$ y sin embargo 7 y 5 no son congruentes modulo3.

viii) Para calcular una potencia, a^n, módulo *m*, podemos poner un número congruente con la base, *a*, pero no del exponente.

La congruencia lineal

La ecuación en congruencias: $ax \equiv c \mod b$ tiene soluciones si y sólo si d = mcd(a, b) divide a c (elemental convirtiéndola en la ecuación diofántica: ax = c + by). En tal caso, el número de soluciones de la ecuación es precisamente d. Si a es primo con b, la solución es única.

Ejemplos: $2x \equiv 1 \mod 6$ no tiene soluciones

$2x \equiv 1 \mod 7$ tiene la solución única $x \equiv 4 \mod 7$

$2x \equiv 4 \mod 8 \Rightarrow x \equiv 2 \mod 4$ o lo que es lo mismo $x \equiv 2$ y $x \equiv 6 \mod 8$

Para resolver las ecuaciones en congruencias podemos utilizar dos métodos, que se pueden incluso mezclar:

1º) Utilizando las propiedades de congruencias:

Ejemplo 1: Para resolver $5x \equiv 3 \mod 7$; como $0 \equiv 7 \mod 7$, sumando queda $5x \equiv 10 \mod 7$; ahora se puede dividir por 5, y resulta la solución única $x \equiv 2 \mod 7$.

Ejemplo 2: $12x \equiv 8 \bmod 20 \Rightarrow 3x \equiv 2 \bmod 5$ (al ser el mcd(4,20) = 4) $\Rightarrow$ sumando 10 al segundo miembro, $3x \equiv 12 \bmod 5 \Rightarrow x \equiv 4 \bmod 5$. Luego la solución es $x \equiv 4 \bmod 5$ o lo que es lo mismo: $x \equiv 4, 9, 14, 19 \bmod 20$.

2º) Convirtiéndolas en ecuaciones diofánticas:
Ejemplo 1: $5x \equiv 3 \bmod 7 \Rightarrow 5x \equiv 3 + 7y$; y hay que resolver la ecuación diofántica: $5x - 7y = 3$; cuya solución es: $x = 2 + 7t$
$y = 1 + 5t$ con $t \in Z$.
Luego la solución de la ecuación en congruencias es $x \equiv 2 \bmod 7$.
Ejemplo 2: $12x \equiv 8 \bmod 20 \Rightarrow 12x = 8 + 20y \Rightarrow 3x = 2 + 5y$ y hay que resolver la ecuación diofántica: $3x - 5y = 2$; cuya solución es: $x = 4 + 5t$
$y = 2 + 3t$
Luego la solución es $x \equiv 4 \bmod 5$ o lo que es lo mismo: $x \equiv 4, 9, 14, 19 \bmod 20$.

Congruencias simultáneas

Se trata de resolver las congruencias simultáneas: $x \equiv 2 \bmod 13$
$x \equiv 3 \bmod 5$
Entonces, se elige la ecuación de módulo mayor: $x \equiv 2 \bmod 13 \Rightarrow x = 2 + 13y$; siendo $y \in Z$. Y se sustituye en la otra ecuación: $2 + 13y \equiv 3 \bmod 5 \Rightarrow 13y \equiv 1 \bmod 5 \Rightarrow y = 2 + 5t$ (se ve directamente o si no resolviendo la ecuación diofántica). Entonces $x = 28 + 65t$ es la solución de las congruencias simultáneas.

Ejercicios de aplicación

1) Resuelve las siguientes ecuaciones en congruencias:
   a) $2x \equiv 1 \bmod 17$ b) $3x \equiv 6 \bmod 18$ c) $40x \equiv 777 \bmod 1777$
   d) $3x \equiv 1 \bmod 19$ e) $4x \equiv 6 \bmod 18$ f) $20x \equiv 984 \bmod 1984$

2) Halla todos los números menores que 1.000, que sean múltiplos de 28, y que divididos por 15 den resto 9.

3) Una mujer tiene un cesto de manzanas. Haciendo grupos de 3 sobran 2 y haciendo grupos de 4 sobran 3. Halla el número de manzanas que contiene el cesto sabiendo que tiene aproximadamente 100.

4) Halla un número que al dividirse por 10 da de resto 9, al dividirse por 9 da de resto 8 y así sucesivamente hasta que al dividirse por dos deje residuo 1.

5) Encuentra dos múltiplos de 7 que dejen resto 1 cuando se divide por 2, 3, 4, 5 ó 6.

6) *La banda*

El director de una banda bastante grande de músicos de un pueblo de Palencia estaba desesperado. Hiciese como hiciese la formación de sus músicos para desfilar, siempre le sobraba uno que se llamaba Cano y tocaba los platillos.

Si colocaba a los músicos de 4 en fondo, le sobraba uno, el pobre Cano que tenía que ir solo al final; si formaban en columna de a tres, el problema seguía siendo el mismo: Cano y sus platillos otra vez solos al final. Incluso cuando la banda desfilaba de dos en dos ocurría igual.

Luisa, la mujer de Cano, que era una gran observadora, propuso al director que los colocase de 5 en fondo. Este le hizo caso y, ¡sorpresa!, todas las filas quedaron completas, ya no sobraba el pobre Cano. ¿Cuántos músicos tenía la banda, si sabemos que tenía más de 30 pero menos de 100?

7) *El cocinero chino*

Diecisiete piratas se reparten un botín de n monedas de oro. Acordaron partes iguales y, si hubiese un resto, se lo darían al cocinero chino. Después del reparto el chino recibió 3 monedas. Pero en la borrachera nocturna 6 piratas murieron acuchillados (en la riña acostumbrada en esos casos). Al otro día los sobrevivientes se vuelven a repartir las monedas y al cocinero le tocaron 4 monedas. Posteriormente, en un naufragio, sólo se salvó el botín, el cocinero y 6 piratas. Así que se vuelven a repartir y le tocaron 5 monedas al cocinero. Encuentra el número n de monedas con que se quedó el cocinero (como mínimo) después de envenenar a los piratas.

8) *El calendario*

¿En qué día de la semana caerá el 18 de febrero de 2.222?

9) *Potencias*

a) Halla el dígito de las unidades de 7^{2000} y de 7^{345}

b) Estudia el dígito de las unidades de cualquier potencia.

c) Halla el resto de dividir $23^{84.292}$ entre 7

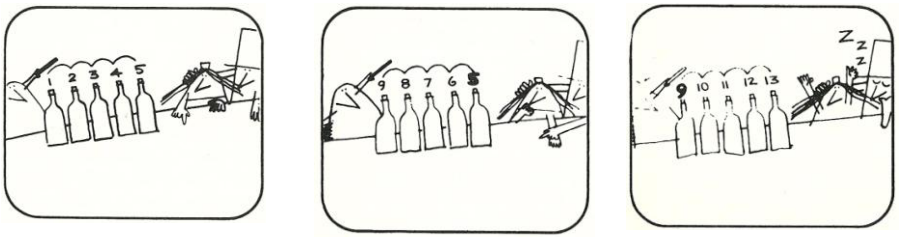
d) Prueba que $30^{99} + 61^{101}$ es divisible entre 31.

e) Prueba que $43^{101} + 23^{101}$ es divisible entre 66.

10) *A vueltas con las botellas*

Para terminar la fiesta de año nuevo, un grupo de amigos deciden abrir una botella de cava. Tienen cinco botellas, pero no se ponen de acuerdo en cual abrir, hasta que uno de ellos dice:

- Ya se como haremos, pondremos las botellas en hilera, e iré contando adelante y atrás por un método que yo se: unos, dos, tres,… y así hasta la que haga el número 2010.



- ¿Sabrías decir que botella eligieron?
- Intenta dar un método general (válido para cualquier número), para saber en que botella terminará la cuenta.
- ¿Qué botella eligen si cuentan hasta 76453829763?

11) *Las jarras*

a) Mide 6 litros con un grifo y dos jarras de 7 y 5 litros.
b) ¿Será posible medir cualquier cantidad con las dos jarras de 7 y 5 litros?
c) Mide 1 litro con un grifo y dos jarras de 9 y 6 litros.
d) ¿Cuándo será imposible obtener una cantidad con dos jarras dadas?
e) Mide 1 litro con un grifo y dos jarras de 9 y 7 litros.