TEMA 2 ARITMETICA ENTERA Y MODULAR

Denotaremos por $\mathbb{Z} = \{0, 1, -1, 2, -2, \ldots\}$ al conjunto de los numeros enteros. Sobre dicho conjunto hay definidas una operacion suma y una operacion producto.

Propiedades de la suma.

1) Conmutativa: $a+b=b+a$
2) Asociativa: $(a+b)+c = a+(b+c)$.
3) Elemento neutro: $a+0=a$.
4) Elemento inverso: $a+(-a)=0$
5) Cancelativa: $a+c=b+c \Rightarrow a=b$.

Propiedades del producto

1) Conmutativa: $a \cdot b = b \cdot a$
2) Asociativa: $a(b \cdot c) = (ab) \cdot c$
3) Elemento neutro: $a \cdot 1 = a$.
4) Cancelativa por elementos distintos de cero: si $a \cdot c = b \cdot c$ y $c \neq 0$ entonces $a=b$.
5) Distributiva: $a(b+c) = ab+ac$.

Propiedad de la division

Si $a, b \in \mathbb{Z}$ y $b \neq 0$ entonces existen uno unicos $q, r \in \mathbb{Z}$ tq $a = qb+r$ y $0 \leq r < |b|$.

A q y r los llamaremos el cociente y el resto de dividir a entre b y los denotaremos $a \operatorname{div} b$ y $a \bmod b$.

EJEMPLO

1) $123 \operatorname{div} 9 = 13$ y $123 \bmod 9 = 6$

2) $(-123) \operatorname{div} 9 = -14$ y $(-123) \bmod 9 = 3$

$$\begin{array}{r|l} 123 & 9 \\ \cline{2-2} 33 & 13 \\ 6 & \end{array}$$

$123 = 13 \cdot 9 + 6$

$-123 = (-13) \cdot 9 - 6 \Rightarrow -123 = (-13) \cdot 9 - 9 + 9 - 6 =$
$= (-14) \cdot 9 + 3.$

Sean $a, b \in \mathbb{Z}$. Diremos que a divide a b (ó que b es un múltiplo de a) (ó que a es un divisor de b) y lo denotaremos $a|b$, si existe $c \in \mathbb{Z}$ tq $b = a \cdot c$.

EJEMPLO

$2|6$ y $2 \nmid 9$

Sea $p \in \mathbb{Z} \setminus \{1, -1\}$. Diremos que p es primo si sus únicos divisores son $1, -1, p$ y $-p$.

EJEMPLO

$2, -2, 3, -3, 5, -5, 7, -7, 11, -11, \ldots$ son números primos.

Dos numeros enteros son primos relativos si los unicos divisores que tienen en comun son el 1 y el -1.

EJEMPLO

4 y 9 son primos relativos.

TEOREMA DE BEZOUT

Sean $a, b \in \mathbb{Z}$. Entonces a y b son primos relativos si y solo si existen $u, v \in \mathbb{Z}$ tq $au + bv = 1$.

EJERCICIO

Calcular numeros enteros u y v tq $4u + 9v = 1$.

-D-

$u = -2$ y $v = 1$.

TEOREMA FUNDAMENTAL DE LA ARITMETICA

Todo numero entero mayor o igual que 2 se puede poner de forma unica (salvo reordenaciones) como producto de numeros primos positivos.

EJERCICIO

Calcular la descomposicion en primos de 360

-D-

$$\begin{array}{r|l} 360 & 2 \\ 180 & 2 \\ 90 & 2 \\ 45 & 3 \\ 15 & 3 \\ 5 & 5 \\ 1 & \end{array}$$

$$360 = 2^3 \cdot 3^2 \cdot 5$$

COROLARIO

Si $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r}$ es la descomposición en primos de un entero positivo n, entonces $(\alpha_1+1)(\alpha_2+1)\ldots(\alpha_r+1)$ es el número de divisores positivos de n.

EJERCICIO

¿Cuántos divisores tiene el número 360?

-D-

$360 = 2^3 \cdot 3^2 \cdot 5 \Rightarrow 360$ tiene $(3+1)(2+1)(1+1) = 24$ divisores positivos $\Rightarrow 360$ tiene 48 divisores.

Sean $a, b \in \mathbb{Z}$ tq $a \neq 0$ ó $b \neq 0$. Un número entero d diremos que es un máximo común divisor de a y b si verifica lo siguiente:

1) $d|a$ y $d|b$

2) si $c|a$ y $c|b$ entonces $c|d$.

NOTA

Si d es un m.c.d de a y b entonces $-d$ es también un m.c.d de a y b. Denotaremos por m.c.d$\{a,b\}$ al m.c.d de a y b que es positivo.

EJEMPLO

m.c.d$\{6,10\} = 2$ m.c.d$\{6,0\} = 6$.

m.c.d$\{0,0\}$ no tiene sentido m.c.d$\{6,6\} = 6$.

Sean $a, b \in \mathbb{Z}$. Un numero entero m es un minimo comun multiplo de a y b si verifica lo siguiente:

1) $a|m$ y $b|m$

2) si $a|c$ y $b|c$ entonces $m|c$.

NOTA

Si m es un m.c.m. de a y b entonces $-m$ es tambien un m.c.m de a y b. Denotaremos por $m.c.m\{a,b\}$ al m.c.m de a y b que es mayor o igual que cero

EJEMPLO

$m.c.m\{6,10\}=30$, $m.c.m\{0,0\}=0$, $m.c.m\{6,0\}=0$, $m.c.m\{6,6\}=6$.

PROPOSICION

Si $a,b \in \mathbb{Z}\setminus\{0\}$, entonces $m.c.d\{a,b\}=m.c.d\{|a|,|b|\}$ y $m.c.m\{a,b\}=m.c.m\{|a|,|b|\}$.

TEOREMA

Sean $p_1,\dots,p_r$ numeros primos positivos y $\alpha_1,\beta_1,\alpha_2,\beta_2,\dots,\alpha_r,\beta_r \in \mathbb{N}$. Entonces:

1) $m.c.d\{p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}, p_1^{\beta_1}p_2^{\beta_2}\cdots p_r^{\beta_r}\} = p_1^{\min\{\alpha_1,\beta_1\}}p_2^{\min\{\alpha_2,\beta_2\}}\cdots p_r^{\min\{\alpha_r,\beta_r\}}$.

2) $m.c.m\{p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_r^{\alpha_r}, p_1^{\beta_1}p_2^{\beta_2}\cdots p_r^{\beta_r}\} = p_1^{\max\{\alpha_1,\beta_1\}}p_2^{\max\{\alpha_2,\beta_2\}}\cdots p_r^{\max\{\alpha_r,\beta_r\}}$

EJERCICIO

Calcular el m.c.d y el m.c.m de 120 y 231.

-D-

$120 = 2^3 \cdot 3 \cdot 5 \qquad 231 = 3 \cdot 7 \cdot 11.$

$\text{m.c.d}\{120, 231\} = \text{m.c.d}\{2^3 \cdot 3^1 \cdot 5^1 \cdot 7^0 \cdot 11^0, 2^0 \cdot 3^1 \cdot 5^0 \cdot 7^1 \cdot 11^1\} =$

$= 2^0 \cdot 3^1 \cdot 5^0 \cdot 7^0 \cdot 11^0 = 3.$

$\text{m.c.m}\{120, 231\} = \text{m.c.m}\{2^3 \cdot 3^1 \cdot 5^1 \cdot 7^0 \cdot 11^0, 2^0 \cdot 3^1 \cdot 5^0 \cdot 7^1 \cdot 11^1\} =$

$= 2^3 \cdot 3^1 \cdot 5^1 \cdot 7^1 \cdot 11^1 = 9240.$

PROPOSICION

Si a y b son enteros positivos entonces $\text{m.c.d}\{a,b\} \cdot \text{m.c.m}\{a,b\} = ab.$

ALGORITMO DE EUCLIDES

ENTRADA: a y b enteros positivos.

SALIDA: $\text{m.c.d}\{a,b\}$.

$(a_0, a_1) = (a, b)$

Mientras $a_1 \neq 0$

$(a_0, a_1) = (a_1, a_0 \bmod a_1)$

Devuelve a_0.

EJERCICIO

Calcular el m.c.d de 282 y 134.

-D-

$(a_0, a_1) = (282, 134) = (134, 14) = (14, 8) = (8, 6) = (6, 2) = (2, 0)$

$\text{m.c.d}\{282, 134\} = 2.$

ECUACIONES DIOFANTICAS LINEALES

Una ecuacion diofantica lineal es una expresion de la forma $a_1x_1+a_2x_2+\dots+a_nx_n=b$, donde $a_1,a_2,\dots,a_n,b\in\mathbb{Z}$ y $x_1,x_2,\dots,x_n$ son incognitas. Una solucion de dicha ecuacion es una n-tupla $(c_1,c_2,\dots,c_n)\in\mathbb{Z}^n$ tq $a_1c_1+a_2c_2+\dots+a_nc_n=b$.

Teorema de Bezout generalizado

Si $a_1,a_2,\dots,a_n,b\in\mathbb{Z}$ y $d=m.c.d\{a_1,a_2,\dots,a_n\}$, entonces la ecuacion diofantica $a_1x_1+a_2x_2+\dots+a_nx_n=b$ tiene solucion si y solo si $d|b$. Ademas, en dicho caso tiene las mismas soluciones que la ecuacion diofantica

$$\frac{a_1}{d}x_1+\frac{a_2}{d}x_2+\dots+\frac{a_n}{d}x_n=\frac{b}{d}.$$

EJEMPLO

1) La ecuacion $9x-6y+15z=22$ no tiene solucion ya que $m.c.d\{9,6,15\}=3$ y $3\nmid 22$.

2) La ecuacion $6x-14y+12z=10$ tiene solucion ya que $m.c.d\{6,14,12\}=2$ y $2|10$. Ademas tiene las mismas soluciones que la ecuacion $3x-7y+6z=5$.

Ecuaciones lineales diofanticas con dos incognitas

Sean $a,b,c \in \mathbb{Z}$ tq $m.c.d\{a,b\}=1$. Si (x_0,y_0) es una solucion de $ax+by=c$, entonces el conjunto formado por todas las soluciones de la ecuacion es $\{(x_0+b\cdot k,\ y_0-a\cdot k)$ tq $k\in\mathbb{Z}\}$

EJERCICIO

Calcular todas las soluciones de la ecuacion $10x-8y=14$.

-D-

Como $m.c.d\{10,8\}=2$ y $2|14$, entonces la ecuacion tiene solucion y ademas tiene las mismas soluciones que la ecuacion $5x-4y=7$.

Una solucion de la ecuacion es $(3,2)$ y $m.c.d\{5,4\}=1$.

Entonces el conjunto de todas sus soluciones es

$\{(3-4\cdot k,\ 2-5k)$ tq $k\in\mathbb{Z}\}$.

ALGORITMO Extendido de Euclides

Entrada: a y b enteros positivos.

Salida: $s,t,d\in\mathbb{Z}$ tq $d=m.c.d\{a,b\}$ y $as+bt=d$.

$(a_0,a_1)=(a,b)$, $(s_0,s_1)=(1,0)$, $(t_0,t_1)=(0,1)$

Mientras $a_1\neq 0$

$q=a_0 \text{ div } a_1$

$(a_0,a_1)=(a_1,a_0-a_1\cdot q)$, $(s_0,s_1)=(s_1,s_0-s_1 q)$, $(t_0,t_1)=(t_1,t_0-t_1\cdot q)$

Devuelve $d=a_0$, $s=s_0$ y $t=t_0$.

EJERCICIO

Calcular todas las soluciones de la ecuacion $120x-93y=6$.

-D-

$m.c.d\{120,93\}=3$ y $3|6$ por tanto la ecuacion tiene solucion y ademas tiene las mismas soluciones que $40x-31y=2$. Para obtener una solucion de la ecuacion aplicaremos el algoritmo extendido de Euclides a 40 y 31.

$$(a_0,a_1)=(40,31)\overset{q=1}{=}(31,9)\overset{q=3}{=}(9,4)\overset{q=2}{=}(4,1)\overset{q=4}{=}(1,0)$$
$$(s_0,s_1)=(1,0)=(0,1)=(1,-3)=(-3,7)=(7,-)$$
$$(t_0,t_1)=(0,1)=(1,-1)=(-1,4)=(4,-9)=(-9,-)$$

El algoritmo nos proporciona la igualdad $40\cdot 7+31(-9)=1$.

Por tanto $40\cdot 14-31\cdot 18=2$. Por consiguiente $(14,18)$ es una solucion de la ecuacion. En consecuencia el conjunto de todas las soluciones es $\{(14-31\cdot k, 18-40\cdot k) \text{ tq } k\in\mathbb{Z}\}$.

EJERCICIO

Calcular todas las soluciones de la ecuacion diofantica

$$72x+123y=18.$$

ECUACIONES EN CONGRUENCIAS DE GRADO UNO

Sean $a, b, m \in \mathbb{Z}$. Escribiremos $a \equiv b \pmod{m}$, que se lee "a es congruente con b modulo m", si $m \mid a-b$.

EJEMPLO

$5 \equiv 1 \pmod{2}$ $\qquad$ $7 \not\equiv 2 \pmod{3}$

Una ecuacion en congruencias de grado uno es una expresion de la forma $ax \equiv b \pmod{m}$ donde $a, b, m \in \mathbb{Z}$ y x es una incognita. Una solucion para dicha ecuacion es un número entero c tq $ac \equiv b \pmod{m}$.

EJEMPLO

Los numeros enteros $4, 9, 14, -1, -6, -11$ son soluciones de la ecuacion $3x \equiv 2 \pmod{5}$

EJEMPLO

La ecuacion $2x \equiv 1 \pmod{4}$ no tiene solucion ya que $2x$ es par y por tanto $2x-1$ es impar. Por consiguiente $2x-1$ no es multiplo de 4.

Teorema para resolver congruencias

1) La ecuacion $ax \equiv b \pmod{m}$ tiene solucion si y solo si

$m.c.d\{a,m\} \mid b$.

2) Si $d = m.c.d\{a,m\}$ y $d \mid b$, entonces las ecuaciones

$ax \equiv b \pmod{m}$ y $\frac{a}{d}x \equiv \frac{b}{d} \left(\mathrm{mod}\ \frac{m}{d}\right)$ tienen las

mismas soluciones.

3) Si $m.c.d\{a,m\} = 1$ y u es una solucion de $ax \equiv b \pmod{m}$

entonces el conjunto formado por todas las soluciones de

la ecuacion es $\{u + km \text{ tq } k \in \mathbb{Z}\}$.

4) La ecuacion $ax + c \equiv b \pmod{m}$ tiene las mismas

soluciones que $ax \equiv b - c \pmod{m}$

5) La ecuacion $ax \equiv b \pmod{m}$ tiene las mismas

soluciones que $(a \bmod m) \cdot x \equiv (b \bmod m) \pmod{m}$.

6) Si $u, v \in \mathbb{Z}$ y $au + mv = 1$ entonces $bu \bmod m$ es

una solucion de $ax \equiv b \pmod{m}$.

EJERCICIO

Calcular todas las soluciones de la ecuacion. $237x \equiv 191 \pmod 5$.

-D-

Por el punto 5) del Teorema anterior y como $237 \bmod 5 = 2$ y $191 \bmod 5 = 1$, sabemos que la ecuacion $237x \equiv 191 \pmod 5$ tiene las mismas soluciones que $2x \equiv 1 \pmod 5$. Como $m.c.d\{2,5\} = 1$ y $1|1$ entonces sabemos que la ecuacion $2x \equiv 1 \pmod 5$ tiene solucion. Por el punto 6) del Teorema anterior sabemos que existe un entero perteneciente al conjunto $\{0,1,2,3,4\}$ que es solucion de la ecuacion. Probando obtenemos que 3 es una solucion de la ecuacion. Aplicando el punto 3) del Teorema anterior podemos concluir que el conjunto formado por todas las soluciones de la ecuacion es $\{3+5\cdot k \mid k \in \mathbb{Z}\}$.

EJERCICIO

Calcular todas las soluciones de la ecuacion $30x \equiv 20 \pmod{50}$.

-D-

m.c.d$\{30, 50\} = 10$ y $10|20$. Aplicando el punto 1) del Teorema la ecuacion tiene solucion y ademas por el punto 2) tiene las mismas soluciones que la ecuacion $3x \equiv 2 \pmod 5$. Buscamos un entero del conjunto $\{0,1,2,3,4\}$ que sea solucion. Como 4 es una solucion entonces aplicando el punto 3) del Teorema tenemos que el conjunto de todas las soluciones de la ecuacion es $\{4+5k \text{ tq } k \in \mathbb{Z}\}$.

EJERCICIO

Calcular todas las soluciones de la ecuacion $242x \equiv 4 \pmod{392}$

-D-

mcd$\{242, 392\} =$ m.c.d$\{2\cdot 11^2, 2^3 \cdot 7^2\} = 2$

Como $2|4$ la ecuacion tiene solucion y ademas tiene las mismas soluciones que $121x \equiv 2 \pmod{196}$.

Sabemos que la ecuacion tiene una solucion perteneciente al conjunto $\{0,1,\ldots,195\}$. Para calcular dicha solucion utilizaremos el punto 6) del Teorema anterior. Notese que si encontramos $u, v \in \mathbb{Z}$ tq $121u + 196v = 1$ entonces $2\cdot u \bmod 196$ es una solucion.

Para calcular u y v le aplicaremos el algoritmo extendido de Euclides a 121 y 196.

$$(a_0,a_1)=(196,121)\overset{q=1}{=}(121,75)\overset{q=1}{=}(75,46)\overset{q=1}{=}(46,29)\overset{q=1}{=}(29,17)\overset{q=1}{=}(17,12)=\ldots$$
$$(s_0,s_1)=(1,0)=(0,1)=(1,-1)=(-1,2)=(2,-3)=(-3,5)=\ldots$$
$$(t_0,t_1)=(0,1)=(1,-1)=(-1,2)=(2,-3)=(-3,5)=(5,-8)=\ldots$$

$$(a_0,a_1)=(17,12)\overset{q=1}{=}(12,5)\overset{q=2}{=}(5,2)\overset{q=2}{=}(2,1)\overset{q=2}{=}(1,0)$$
$$(s_0,s_1)=(-3,5)=(5,-8)=(-8,21)=(21,-50)=(-50,\ldots)$$
$$(t_0,t_1)=(5,-8)=(-8,13)=(13,-34)=(-34,81)=(81,\ldots)$$

El algoritmo nos proporciona la igualdad

$$196(-50)+121\cdot 81=1$$

Por tanto $2\cdot 81 \bmod 196 = 162$ es una solucion de la ecuacion $121x\equiv 2 \pmod{196}$. Por ~~[illegible]~~ el punto 3) del Teorema tenemos que todas las soluciones de la ecuacion son $\{162+196\cdot k \text{ tq } k\in\mathbb{Z}\}$.

EJERCICIO

¿ Cuantas soluciones tiene la ecuacion $72x\equiv 4 \pmod{242}$ en el intervalo $[1000, 2000]$?

Sistemas de ecuaciones en congruencias

① Resolver el sistema $\left.\begin{array}{l} 4x \equiv 6 \pmod{10} \\ 3x \equiv 1 \pmod{4} \end{array}\right\}$.

-D-

En primer lugar vemos si todas las ecuaciones tienen solucion. En caso de que alguna ecuacion no tenga solucion decimos que el sistema no tiene solucion.

$$\left.\begin{array}{l} 2x \equiv 3 \pmod{5} \\ 3x \equiv 1 \pmod{4} \end{array}\right\}.$$

Resolvemos la primera ecuacion $x = 4 + 5k$.

Ahora le imponemos a $4+5k$ que sea solucion de la segunda ecuacion.

$$3(4+5k) \equiv 1 \pmod{4} \Rightarrow 12 + 15k \equiv 1 \pmod{4}$$

$$\Rightarrow 15k \equiv -11 \pmod{4} \Rightarrow 3k \equiv 1 \pmod{4} \Rightarrow$$

$$\Rightarrow k = 3 + 4\cdot\overline{k}.$$

Por tanto $x = 4+5k$ y $k = 3+4\cdot\overline{k}$. Por consiguiente

$$x = 4+5(3+4\overline{k}) = \boxed{19 + 20\cdot\overline{k}}$$

② Resolver el sistema $\left.\begin{array}{l} 2x \equiv 2 \pmod 4 \\ 6x \equiv 3 \pmod 9 \\ 2x \equiv 3 \pmod 5 \end{array}\right\}$.

-D-

Pasamos al sistema $\left.\begin{array}{l} x \equiv 1 \pmod 2 \\ 2x \equiv 1 \pmod 3 \\ 2x \equiv 3 \pmod 5 \end{array}\right\}$.

Solucion de la primera ecuacion $x = 1+2k$. Sustituimos en la segunda ecuacion $2(1+2k) \equiv 1 \pmod 3 \Rightarrow$

$\Rightarrow 2+4k \equiv 1 \pmod 3 \Rightarrow 4k \equiv -1 \pmod 3 \Rightarrow k \equiv 2 \pmod 3$

$\Rightarrow k = 2+3\bar{k}$. Por tanto $x = 1+2k = 1+2(2+3\bar{k}) =$

$= 5+6\bar{k}$. Sustituimos ahora en la tercera ecuacion

$2(5+6\bar{k}) \equiv 3 \pmod 5 \Rightarrow 10+12\bar{k} \equiv 3 \pmod 5 \Rightarrow$

$\Rightarrow 12\bar{k} \equiv -7 \pmod 5 \Rightarrow 2\bar{k} \equiv 3 \pmod 5 \Rightarrow$

$\Rightarrow \bar{k} = 4+5\cdot\bar{\bar{k}}$. Por tanto $x = 5+6\bar{k} =$

$= 5+6(4+5\bar{\bar{k}}) = \boxed{29+30\bar{\bar{k}}}$

③ Resolver el sistema $\left.\begin{array}{l} 2x \equiv 2 \pmod{4} \\ 3x \equiv 6 \pmod{12} \end{array}\right\}$

-D-

Pasamos al sistema $\left.\begin{array}{l} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{4} \end{array}\right\}$.

Solucion de la primera ecuacion $x = 1 + 2k$. Sustituimos en la segunda $1 + 2k \equiv 2 \pmod{4} \Rightarrow 2k \equiv 1 \pmod{4}$.
Esta ecuacion no tiene solucion y por tanto el sistema no tiene solucion.

④ ¿Cuantos numeros enteros del intervalo $[1000, 2000]$ son pares, al dividirlo entre 7 dan de resto 1 y al multiplicarlo por 3 y dividirlo entre 5 dan de resto 2?

-D-

$$\left.\begin{array}{l} x \equiv 0 \pmod{2} \\ x \equiv 1 \pmod{7} \\ 3x \equiv 2 \pmod{5} \end{array}\right\}$$

$x = 0 + 2k$

$0 + 2k \equiv 1 \pmod{7} \Rightarrow 2k \equiv 1 \pmod{7} \Rightarrow k = 4 + 7\overline{k}$

$x = 0 + 2k = 2(4 + 7\overline{k}) = 8 + 14\overline{k}$

$3(8 + 14\overline{k}) \equiv 2 \pmod{5} \Rightarrow 24 + 42\overline{k} \equiv 2 \pmod{5}$

$\Rightarrow 42\overline{k} \equiv -22 \pmod{5} \Rightarrow 2\overline{k} \equiv 3 \pmod{5} \Rightarrow$

$\Rightarrow \overline{k} = 4 + 5 \cdot \overline{\overline{k}}$

$x = 8 + 14 \cdot \overline{k} = 8 + 14(4 + 5\overline{\overline{k}}) = 64 + 70 \cdot \overline{\overline{k}}$

el conjunto de soluciones del sistema es

$\{64 + 70 \cdot \overline{\overline{k}}$ tq $\overline{\overline{k}} \in \mathbb{Z}\}$. Veamos cuantas de estas

soluciones estan en $[1000, 2000]$.

$1000 \leq 64 + 70 \cdot \overline{\overline{k}} \leq 2000 \Rightarrow 936 \leq 70 \cdot \overline{\overline{k}} \leq 1936 \Rightarrow$

$\Rightarrow \dfrac{936}{70} \leq \overline{\overline{k}} \leq \dfrac{1936}{70} \Rightarrow 13'37 \leq \overline{\overline{k}} \leq 27'65$

$\Rightarrow 14 \leq \overline{\overline{k}} \leq 27$.

Por tanto las soluciones del sistema que estan en $[1000, 2000]$ son aquellas que se obtienen dandole a $\overline{\overline{k}}$ los valores $14, 15, \dots, 27$.

Por tanto la solucion del problema es 14.

El anillo de los enteros modulo un entero positivo.

Dado un entero positivo m, denotaremos por $\mathbb{Z}_m = \{0, 1, \dots, m-1\}$.
En $\mathbb{Z}_m$ definimos una suma y un producto de la siguiente forma: $a \oplus b = (a+b) \bmod m$ y $a \odot b = (ab) \bmod m$.

Ejemplo

En $\mathbb{Z}_7$ tenemos que $4 \oplus 5 = 2$ y $4 \odot 5 = 6$

Propiedades de la operacion $\oplus$

1) Conmutativa: $a \oplus b = b \oplus a$.
2) Asociativa: $a \oplus (b \oplus c) = (a \oplus b) \oplus c$.
3) Elemento neutro: $a \oplus 0 = a$.
4) Elemento inverso: $a \oplus m-a = 0$

NOTA

Al inverso para la operacion $\oplus$ de a lo denotaremos por $-a$.

EJEMPLO

En $\mathbb{Z}_7$ tenemos que $-2 = 5$.

Propiedades de la operación $\odot$

1) Conmutativa: $a \odot b = b \odot a$.
2) Asociativa: $a \odot (b \odot c) = (a \odot b) \odot c$.
3) Elemento neutro: $a \odot 1 = a$.
4) Distributiva: $a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$.

NOTA

En $\mathbb{Z}_m$ hay elementos que tienen inverso para el producto y elementos que no tienen inverso para el producto.

Si $a \in \mathbb{Z}_m$ y a tiene inverso para el producto entonces a dicho inverso lo denotaremos por a^{-1}.

Ejemplo

En $\mathbb{Z}_9$ se tiene que $2 \odot 5 = 1$ por tanto $2^{-1} = 5$.

En $\mathbb{Z}_9$ el 3 no tiene inverso para el producto

A los elementos de $\mathbb{Z}_m$ que tienen inverso para el producto se les llama unidades.

Ejemplo

El conjunto de las unidades de $\mathbb{Z}_9$ es

$\{1, 2, 4, 5, 7, 8\}$

TEOREMA

Un elemento $a \in \mathbb{Z}_m$ tiene inverso para el producto si y solo si $m.c.d\{a,m\}=1$. Además, si $a \cdot u + m \cdot v = 1$ con $u, v \in \mathbb{Z}$, entonces $u \bmod m$ es el inverso para el producto de a.

Ejercicio

Calcular las unidades de $\mathbb{Z}_{15}$

-D-

$\mathcal{U}(\mathbb{Z}_{15}) = \{1,2,4,7,8,11,13,14\}$.

Ejercicio

Calcular el inverso para el producto de 35 en $\mathbb{Z}_{97}$.

-D-

Como $m.c.d\{35,97\}=1$ entonces sabemos que existe 35^{-1} en $\mathbb{Z}_{97}$. Para calcularlo le aplicamos el algoritmo extendido de Euclides a 35 y 97.

$$(a_0,a_1)=(97,35) \overset{q=2}{=} (35,27) \overset{q=1}{=} (27,8) \overset{q=3}{=} (8,3) \overset{q=2}{=} (3,2) \overset{q=1}{=} (2,1) \overset{q=2}{=} (1,0)$$

$$(s_0,s_1)=(1,0)=(0,1)=(1,-1)=(-1,4)=(4,-9)=(-9,13)=(13,m)$$

$$(t_0,t_1)=(0,1)=(1,-2)=(-2,3)=(3,-11)=(-11,25)=(25,-36)=(-36,m)$$

El algoritmo nos proporciona la igualdad $97 \cdot 13 + 35(-36) = 1$.

Aplicando el Teorema anterior obtenemos que

$$35^{-1} = (-36) \bmod 97 = \underline{\underline{61}}$$

Ejercicio

Resuelve en $\mathbb{Z}_9$ la ecuacion $x+7=5x+2$.

-D-

$$x+7=5x+2 \Rightarrow 4x=5 \Rightarrow x=4^{-1}\cdot 5 \Rightarrow x=7\cdot 5 \Rightarrow x=8.$$

Ejercicio

Resuelve en $\mathbb{Z}_{10}$ la ecuacion $8x+5=2x+7$

-D-

$$8x+5=2x+7 \Rightarrow 6x=2$$

Como en $\mathbb{Z}_{10}$ no exite 6^{-1} entonces no puedo proceder como en el ejercicio anterior.

$$6x=2 \Rightarrow 6x\equiv 2 \pmod{10} \Rightarrow 3x\equiv 1 \pmod{5}$$

$$\Rightarrow x=2+5K.$$

La solucion del problema son lo numeros de la forma $2+5K$ que pertenecen a $\{0,1,\dots,9\}=\mathbb{Z}_{10}$.

Por tanto nuestra ecuacion tiene dos soluciones $x=2$ y $x=7$.

Ejercicio

Resuelve en $\mathbb{Z}_{15}$ la ecuacion $9x+14=1+3x$.

-D-

$$9x+14=1+3x \Rightarrow 6x=-13 \Rightarrow 6x=2 \Rightarrow 6x\equiv 2 \pmod{15}$$

Cómo $m.c.d\{6,15\}=3$ y $3\nmid 2$ la ecuacion en congruencias no tiene solucion. Por tanto la ecuacion $9x+14=1+3x$ no tiene solucion en $\mathbb{Z}_{15}$.

EJERCICIO

Calcular 3^{127} en $\mathbb{Z}_{10}$.

-D-

$3^1=3,\ 3^2=9,\ 3^3=7,\ 3^4=1$.

$$\begin{array}{l|l} 127 & 4 \\ \hline 07 & 31 \\ 3 & \end{array} \qquad 127=4\cdot 31+3$$

$$3^{127}=3^{4\cdot 31+3}=(3^4)^{31}\cdot 3^3=1^{31}\cdot 7=7.$$

EJERCICIO

Calcular 3^{127} en $\mathbb{Z}_{15}$.

-D-

$3^1=3,\ 3^2=9,\ 3^3=12,\ 3^4=6,\ 3^5=3,\ 3^6=9$

se repiten cada 4.

$$\begin{array}{l|l} 127 & 4 \\ \hline 07 & 31 \\ 3 & \end{array} \qquad 127=4\cdot 31+3$$

$$3^{127}=3^3=12.$$