Congruencias en el anillo de los enteros

01. Definición de congruencia en los enteros:

Dos números enteros, *a* y *b*, se dicen *congruentes módulo m*, si se obtiene el mismo resto al dividir cada uno de ellos por *m*. Caso contrario se dice que son *incongruentes modulo m*.

La relación de congruencia *módulo m* en el anillo de los enteros puede en definitiva definirse por la condición:

$$aR_m b \leftrightarrow resto(a/m) = resto(b/m)$$

Representaremos a la relación de congruencia en la forma:

$$a \equiv b (\mathrm{mod}\ m)$$

indicando con ello que los números enteros a y b son congruentes módulo m, es decir, dan el mismo resto al dividirlos por m.

Ejemplo:

Si m=5, podemos encontrar todos los números que, al dividirlos por 5, dan:

- resto 0: $[0]_5 = \{0,5,10,15,...\}$
- resto 1: $[1]_5 = \{1,6,11,16,...\}$
- resto 2: $[2]_5 = \{2,7,12,17,...\}$
- resto 3: $[3]_5 = \{3,8,13,18,...\}$
- resto 4: $[4]_5 = \{4,9,14,19,...\}$

La relación de congruencia es trivialmente una relación reflexiva, simétrica y transitiva, esto es, se trata de una relación de equivalencia:

- Reflexiva:

$$a \equiv a (\mathrm{mod}\ m)$$

- Simétrica:

$$a \equiv b (\mathrm{mod}\ m) \rightarrow b \equiv a (\mathrm{mod}\ m)$$

- Transitiva:

$$\left.\begin{array}{l} a \equiv b (\mathrm{mod}\ m) \\ b \equiv c (\mathrm{mod}\ m) \end{array}\right\} \rightarrow a \equiv c (\mathrm{mod}\ m)$$

en donde cada clase está formada por los infinitos números enteros que dan el mismo resto al dividirlos por m. Estas clases se llaman *clases de restos módulo m*.

Clases de restos módulo m: $[0]_m,[1]_m,...,[m-1]_m$.

Ejemplo:

Clases de restos módulo 7: $[0]_7,[1]_7,[2]_7,[3]_7,[4]_7,[5]_7,[6]_7$

El conjunto cociente del anillo *Z* por la relación de equivalencia antedicha es el conjunto formado por todas las clases de equivalencia, es decir, el conjunto de todas las clases de restos módulo m:

$$Z/Z_m \equiv Z/(m) = \{[0]_m,[1]_m,...,[m-1]_m\}$$

Se cumple que si dos números enteros son congruentes módulo *m*, entonces su diferencia es un múltiplo de *m*:

$$a \equiv b(\text{mod } m) \rightarrow \left.\begin{array}{l} a = q.m+r \\ b = p.m+r \end{array}\right\} \rightarrow a-b=(q-p).m \rightarrow a-b \in (m)$$

Llamando *(m)* al ideal de los múltiplos de *m*.

La relación de congruencia es por tanto compatible con la suma y multiplicación en el anillo de los enteros, por lo que el conjunto cociente de las clases de equivalencia puede estructurarse como un anillo.

El conjunto cociente Z/Z_m, de Z por la relación de equivalencia, que se representa generalmente por $Z/(m)$, se denomina *anillo de las clases de resto módulo m*.

Si *m* es primo entonces el ideal *(m)* será maximal, con lo que el anillo cociente $Z/(m)$ será un anillo de integridad finito, es decir, un cuerpo.

02. Algunas propiedades elementales:

a) Si $a \equiv q.m+r \rightarrow a \equiv r(\text{mod } m)$.
   Es obvio, pues al dividir a por m se obtiene resto r, lo mismo que al dividir r por m.
b) Si $a \in (m) \rightarrow a \equiv 0(\text{mod } m)$
   También es inmediato, por la propiedad anterior, ya que el resto es cero en ambos casos.
c) Si el número *a* es primo con *m*, entonces todo numero congruente con *a* módulo *m* es también primo con *m*: $a \vee m = 1 \wedge a \equiv b(\text{mod } m) \rightarrow b \vee m = 1$.
   En efecto, pues
   Si $a \vee m = 1 \rightarrow \exists A, M \in Z / Aa+Mm=1 \rightarrow Aa+Mm=1 \wedge a-b \in (m) \rightarrow$
   $\rightarrow Aa-Ab \in (m) \rightarrow (1-Mm))-Ab=Km \rightarrow 1=Ab+(M-K)m \rightarrow b \vee m = 1$
d) Si es $f(x)=a_0+a_1x+...+a_nx^n \in Z[x], a \equiv b(\text{mod } m) \rightarrow f(a) \equiv f(b)(\text{mod } m)$
   Efectivamente, ya que la relación de congruencia es estable con respecto a las operaciones de suma y multiplicación en el anillo de los enteros.

e) Si $a \equiv b(\text{mod } m) \wedge h \mid a \wedge h \mid b \wedge h \vee m = d \rightarrow \frac{a}{h} \equiv \frac{b}{h}(\text{mod } \frac{m}{d})$, es decir, si a y b son congruentes modulo *m*, y el entero *h* divide *a* y a *b*, entonces los cocientes de ambos son congruentes módulo *m/d*, siendo *d* el máximo común divisor de *m* y *h*.
Demostración:
$a \equiv b(\text{mod } m) \rightarrow a - b = a'.h - b'.h = (a' - b').h = (a' - b').h'.d \in (m) \rightarrow$
$\rightarrow (a' - b').h'.d = k.m \rightarrow (a' - b').h'.d = k.m'.d \rightarrow (a' - b').h' = k.m' \wedge h' \vee m' = 1$
con lo que $a' - b' = k'.m' \rightarrow a' - b' \in (m') \rightarrow \frac{a}{h} - \frac{b}{h} \in \left(\frac{m}{d}\right) \rightarrow \frac{a}{h} \equiv \frac{b}{h}\left(\text{mod } \frac{m}{d}\right)$

f) Si $a.h \equiv b.k(\text{mod } m) \wedge h \equiv k(\text{mod } m) \wedge h \vee m = 1 \rightarrow a \equiv b(\text{mod } m)$
Demostración:
$h \equiv k(\text{mod } m) \rightarrow h - k \in (m) \rightarrow a(h - k) = ah - ak \in (m) \rightarrow ah \equiv ak(\text{mod } m)$
análogamente se obtiene que $bh \equiv bk(\text{mod } m)$.
$a.h \equiv b.k(\text{mod } m) \wedge bh \equiv bk(\text{mod } m) \rightarrow a.h \equiv b.h(\text{mod } m) \wedge h \vee m = 1 \rightarrow$
$\rightarrow \frac{ah}{h} \equiv \frac{bh}{h}(\text{mod } \frac{m}{1}) \rightarrow a \equiv b(\text{mod } m)$

03. Números incongruentes:

Un conjunto de *h* números enteros, $a_1, a_2, \ldots, a_h$, se denomina *sistema de números incongruentes módulo m*, si al dividir cada uno de ellos por *m*, se obtiene resto distinto.
Un sistema de *h* números incongruentes módulo *m* se dice *completo* si $h = m$.

Ejemplos:

- El conjunto $\{10, 26, 48\}$ es un sistema de números incongruentes módulo 5.
- El conjunto $\{10, 26, 47, 98, 109\}$ es un sistema *completo* de números incongruentes módulo 5. Cualquier otro número entero será congruente módulo 5 con alguno de los números enteros que figuran en el sistema completo.
- Cualquiera que sea el número entero *m*, el conjunto *0,1,2,…,m-1* es un sistema completo de números incongruentes módulo *m*.

Teorema: Dado el conjunto $a_1, a_2, \ldots, a_h$ de números incongruentes módulo *m*, si cada uno de ellos se multiplica por un número *n*, coprimo con *m*, y se le suma un entero *q* cualquiera, entonces el conjunto $na_1 + q, na_2 + q, \ldots, na_h + q$ es un sistema de números incongruentes módulo m.
Demostración: Si suponemos lo contrario llegaríamos a una contradicción. Así, supongamos que dos de estos números, $na_i + q$ y $na_j + q$, son congruentes modulo m, o sea, que dan el mismo resto *r* al dividirlos por *m*:

$$\left.\begin{array}{l} na_i + q = m.A_i + r \\ na_j + q = m.A_j + r \end{array}\right\} \rightarrow (na_i + q) - (na_j + q) \in (m) \rightarrow n(a_i - a_j) \in (m)$$, y como el número n es primo con m, será $a_i - a_j \in (m)$, contra la hipótesis de que a_i, a_j eran incongruentes módulo m.

Podemos utilizar este resultado para probar de forma elemental la congruencia conocida como *Pequeño Teorema de Fermat.*

Teorema (Pequeño Teorema de Fermat): Si el número entero *p* es primo y si *n* no es un múltiplo de *p*, entonces se verifica que *n* elevado a *p-1* es congruente con *1* módulo *p*:

$$p\ primo \wedge n \notin (p) \rightarrow n^{p-1} \equiv 1 (\text{mod } p)$$

Demostración:
El conjunto de *p* números enteros $\{0,1,2,...,p-1\}$ es un sistema completo de números incongruentes módulo *p*. Todos dan resto diferente al dividirlos por *p*.
Por el teorema anterior, también será un sistema de números incongruentes módulo *p* el conjunto $\{n.0, n1, n2, ..., n(p-1)\}$ (se han multiplicado por *n*, coprimo con *p*, y se les ha sumado $q = 0$).
Si consideramos la secuencia $n1, n2, ..., n(p-1)$ se tiene que si *k* es uno de los números $1, 2, ..., (p-1)$ entonces k no es divisible por p, y como n tampoco lo es, sabemos por el Lema de Euclides que *nk* tampoco es divisible por *p*, por lo que *nk* da, al dividirlo por *p*, el mismo resto que alguno de los números de la secuencia $1, 2, ..., (p-1)$. Como todos son distintos se tiene que el producto de los elementos de la secuencia $n1, n2, ..., n(p-1)$ es congruente con el producto de los elementos de la secuencia $1, 2, ..., (p-1)$:

$$n1.n2.....n(p-1) \equiv 1.2.....(p-1) (\text{mod } p),$$

o bien

$$n^{p-1}.1.2.....(p-1) \equiv 1.2.....(p-1) (\text{mod } p)$$

y por la propiedad f) del apartado anterior:

$$n^{p-1} \equiv 1 (\text{mod } p)$$

04. Los restos potenciales:

Sea un numero entero positivo *p*. Se denominan *restos potenciales de p modulo m* a los restos que se obtienen al dividir por *m* las sucesivas potencias de *p*.

En el estudio de los restos potenciales de *p* módulo *m*, podemos considerar los tres casos siguientes:

1) Que en la descomposición en factores primos de *p* aparezcan todos los factores primos de la descomposición de *m*.
2) Que en la descomposición en factores primos de *p* no aparezca ninguno de los factores primos que figuran en la descomposición de *m*.

3) Que en la descomposición en factores primos de *p* aparezcan factores que figuran en la descomposición de *m* y otros que no figuran en dicha descomposición.

Veamos cada uno de los tres casos:

1) El caso en el que *p* y *m* tienen los mismos factores primos:

$$p = a_1^{\varphi_1}.a_2^{\varphi_2}...., a_k^{\varphi_k}$$

$$m = a_1^{\varphi_1'}.a_2^{\varphi_2'}.....a_k^{\varphi_k'}$$

Podemos considerar dos situaciones:

1.1) Que todos los exponentes φ_i' de la descomposición de *m* sean menores o iguales que los correspondientes φ_i en la factorización de *p*:

$$\varphi_i' \le \varphi_i, i = 1, 2, ..., k$$

En este caso es obvio que la división de p^ϕ por *m* es exacta, cualquiera que sea el exponente entero $\phi > 0$.

$$\frac{p^\phi}{m} = \frac{(a_1^{\varphi_1}.a_2^{\varphi_2}...., a_k^{\varphi_k})^\phi}{a_1^{\varphi_1'}.a_2^{\varphi_2'}.....a_k^{\varphi_k'}} = a_1^{\phi\varphi_1-\varphi_1'}.a_2^{\phi\varphi_2-\varphi_2'}...., a_k^{\phi\varphi_k-\varphi_k'} \in Z$$

En definitiva, en este caso todos los restos potenciales son nulos.

1.2) Que alguno/s de los exponentes φ_i' de la descomposición de *m* sea/n mayor/es que el/los correspondientes φ_i en la descomposición de *p*:

$$\exists \varphi_j' / \varphi_j' > \varphi_j$$

En este caso bastaría hallar el mínimo entero h tal que $\varphi_j' \le \varphi_j.h$, con lo cual se verificará que $\varphi_i' \le \varphi_i.h, i = 1, 2, ..., k$, y estaríamos en la situación anterior

$$p^h = a_1^{\varphi_1.h}.a_2^{\varphi_2.h}...., a_k^{\varphi_k.h}$$

$$m = a_1^{\varphi_1'}.a_2^{\varphi_2'}.....a_k^{\varphi_k'}$$

Con lo que la división de $\left(p^h\right)^\phi$ por *m* es exacta, cualquiera que sea el exponente entero $\phi > 0$.

$$\frac{\left(p^h\right)^\phi}{m} = \frac{p^{h\phi}}{m} = \frac{(a_1^{\varphi_1}.a_2^{\varphi_2}...., a_k^{\varphi_k})^{h\phi}}{a_1^{\varphi_1'}.a_2^{\varphi_2'}.....a_k^{\varphi_k'}} = a_1^{h\phi\varphi_1-\varphi_1'}.a_2^{h\phi\varphi_2-\varphi_2'}...., a_k^{h\phi\varphi_k-\varphi_k'} \in Z$$

Resumiendo, p^h es la menor potencia de p cuyo resto potencial es nulo, no siendo nulo el resto potencial correspondiente a $p^1, ..., p^{h-1}$.

Veamos un par de ejemplos de este caso:

Ejemplo 1:

Determinar los restos potenciales de *p=5400* modulo *m=450.*

$$p = 2^3.3^3.5^2$$

$$m = 2.3^2.5^2$$

$$\forall \phi \in Z^+, p^\phi = 2^{3\phi}.3^{3\phi}.5^{2\phi} \rightarrow \frac{p^\phi}{m} = \frac{2^{3\phi}.3^{3\phi}.5^{2\phi}}{2.3^2.5^2} = 2^{3\phi-1}.3^{3\phi-2}.5^{2\phi-2} \in Z$$

La división es exacta, por lo que los restos potenciales son nulos, $\forall \phi \in Z^+$.

Ejemplo 2:

Determinar los restos potenciales de *p=600* modulo *m=450.*

$$p = 2^3.3.5^2$$
$$m = 2.3^2.5^2$$

h=2 es el mínimo entero positivo tal que $2 \le 2^{3h}, 3^2 \le 3^h, 5^2 \le 5^{2h}$, por lo que

$$\forall \phi \in Z^+ / \phi > 1,\ p^\phi = 2^{3\phi}.3^{3\phi}.5^{2\phi} \rightarrow \frac{p^\phi}{m} = \frac{2^{3\phi}.3^{3\phi}.5^{2\phi}}{2.3^2.5^2} = 2^{3\phi-1}.3^{3\phi-2}.5^{2\phi-2} \in Z^+$$

La división es exacta, los restos potenciales son nulos, $\forall \phi \in Z^+ / \phi > 1$.

Si es $\phi = 1$ la división no es exacta, y el resto potencial es 150:

$$\frac{P^1}{m} = \frac{600}{450} \rightarrow \text{Resto} = 150$$

2) El caso en el que ninguno de los factores primos de *p* figura entre los factores primos de *m*:

Si no existen factores primos comunes en la descomposición de *p* y de *m*, ello indica que su MCD es la unidad: $p \vee m = 1$. Lo mismo ocurrirá con las potencias de *p*, $p^\phi, \forall \phi \in Z^+$.

Es decir, todos los restos potenciales serán no nulos, y como solamente pueden existir m restos potenciales, $0,1,...,m-1$, tendrá que haber restos potenciales repetidos.

Supongamos que sea $p^{\phi+\phi'}$ la potencia de exponente más pequeño que da el mismo resto potencial que p^ϕ. Será, entonces:

$$p^{\phi+\phi'} \equiv p^\phi \pmod m$$

de lo cual:

$$p^{\phi+\phi'} - p^\phi = \dot{m} \rightarrow p^\phi \left[p^{\phi'} - 1 \right] = \dot{m}$$

como p^ϕ no es múltiplo de m, será $p^{\phi'} - 1 = \dot{m}$, es decir $p^{\phi'} \equiv 1 \pmod m$.

A ϕ' se le denomina *gaussiano de p con respecto a m*, cumpliendo:

$$p^{\phi'} \equiv 1 \pmod m$$
$$p^{\phi'+1} \equiv p \pmod m$$
$$p^{\phi'+2} \equiv p^2 \pmod m$$
$$\ldots\ \ldots\ \ldots$$
$$p^{\phi'+\phi} \equiv p^\phi \pmod m$$

Así, pues, los restos potenciales son todos diferentes, volviéndose a repetir la secuencia a partir de la potencia $p^{\phi'}$, y así, sucesivamente.

Ejemplo:

Determinemos los restos potenciales de 35, modulo 6.

Se trata de los números sin factores primos comunes

$$p = 5.7$$
$$m = 2.3$$

Como el gaussiano ϕ' ha de verificar que:

$$p^{\phi'} - 1 = \dot{m} \rightarrow 35^{\phi'} - 1 = \dot{6}$$

probamos con las primeras potencias de 35:

$35^0 - 1 = 0,\ 35^1 - 1 = 34 \neq \dot{6},\ 35^2 - 1 = 1225 - 1 = 1224 = \dot{6}, \ldots$

Aparece el primer múltiplo de m para $\phi' = 2$. El gaussiano es 2.

Hallamos los restos potenciales de las potencias de exponente inferior al

gaussiano ($p^0, p^1, p^2, ..., p^{\phi'-1}$). En nuestro caso:

$$35^0, 35^1 \rightarrow restos: \ 1, 5$$

como la secuencia de restos se repite a partir de $p^{\phi'}$, los restos potenciales son 1, 5, 1, 5, 1, 5, ...

$$\text{Restos potenciales de } p^x = \begin{cases} 1, & x = \dot{2} \\ 5, & x = \dot{2}+1 \end{cases}$$

3) El caso en que en la descomposición en factores primos de *p* aparezcan factores que figuran en la descomposición de *m* y otros que no figuran en dicha descomposición:
Supongamos que m tiene en su descomposición en factores primos algunos de ellos que también figuran en la descomposición de p y otros que no figuran en dicha descomposición.
En este caso p no será divisible por m, y tampoco la será cualquier potencia de p, $p^{\phi}, \forall \phi \in Z^+$, por lo que los restos potenciales son distintos de cero, con lo que habrán restos repetidos, ya que solo pueden haber los m restos potenciales $0, 1, ..., m-1$.
Podemos descomponer *m* en un producto de dos factores, *m´* y *m"*, en donde *m´* estaría formado por aquellas potencias de factores primos que están en la descomposición de *p*, y *m"* estaría formado por aquellas potencias de factores primos que no están en la descomposición de *p*. Obviamente, $m' \vee m'' = 1$.
Llamemos $p^{\varphi+\varphi'}$ a la potencia de exponente más pequeño que da el mismo resto potencial que p^{φ}. Se tiene que $p^{\varphi+\varphi'} \equiv p^{\varphi} (\mathrm{mod}\, m)$, de lo cual

$$p^{\varphi+\varphi'} - p^{\varphi} = \dot{m} \rightarrow p^{\varphi}\left[p^{\varphi'} - 1 \right] = \dot{m} = m'.\dot{m}''$$

si *m´* no divide a $p^{\varphi'} - 1$, entonces divide a p^{φ}, $p^{\varphi} = \dot{m}'$, por lo que es $p^{\varphi'} - 1 = \dot{m}'' \rightarrow p^{\varphi'} \equiv 1 (\mathrm{mod}\, m)$, y φ es el primer valor tal que $p^{\varphi} = \dot{m}'$. p^{φ} es la primera potencia cuyo resto se repite (los restos de las potencias inferiores, $p^0, p^1, ..., p^{\varphi-1}$, no vuelven a aparecer) y φ' es el gaussiano de p respecto de m.
Ejemplo:
Determinemos los restos potenciales de 45, modulo 6.
Se trata de los números con algún factor primo común

$$p = 3^2.5$$
$$m = 2.3$$

llamemos $m' = 3$, $m'' = 2$. El gaussiano φ' verifica $p^{\varphi'} - 1 = \dot{m}'' \rightarrow 45^{\varphi'} - 1 = \dot{2}$, probamos las primeras potencias de 45:

$$45^0 - 1 \notin \dot{2}, \ 45^1 - 1 = 44 = \dot{2}, \ ...$$

Aparece el primer múltiplo de m" para $\varphi' = 1$. El gaussiano es 1.
Hallamos los restos potenciales de las potencias de exponente inferior al gaussiano ($p^0, p^1, p^2, ..., p^{\phi'-1}$), que son aquellas cuyos restos potenciales no vuelve a aparecer. En nuestro caso:

$$45^0 \rightarrow resto: 1$$

Las potencias siguientes repiten el mismo resto, 3, al ser el gaussiano igual a

la unidad.
Los restos potenciales, en definitiva, son 1,3,3,3,3,…

El estudio de los restos potenciales nos permite fundamentar los criterios clásicos de divisibilidad, apoyándonos en teoremas prácticamente inmediatos, como el resultado siguiente.

Teorema: La condición necesaria y suficiente para que la suma siguiente

$$S = a_0 + a_1 p + a_2 p^2 + \ldots + a_k p^k$$

sea divisible por *m*, es que lo sea la suma

$$a_0 + a_1 r_1 + a_2 r_2 + \ldots + a_k r_k$$

donde es $r_j, j = 1,2,\ldots,k$ el resto potencial de $p^j, j = 1,2,\ldots,k$ modulo *m*.
Demostración:
Es consecuencia inmediata de ser:

$$a_0 + a_1 p + a_2 p^2 + \ldots + a_k p^k \equiv a_0 + a_1 r_1 + a_2 r_2 + \ldots + a_k r_k \pmod{m}$$

05. Ecuaciones en congruencias:
Son ecuaciones del tipo

$$a_0 + a_1 x + a_2 x^2 + \ldots + a_h x^h \equiv b_0 + b_1 x + b_2 x^2 + \ldots + b_k x^k \pmod{m}$$

Si una solución es x=q, entonces también es solución todo entero p congruente con q módulo m: $p \equiv q \pmod{m}$

En realidad, todos los números congruentes, p,q,…,l,… que son solución de la ecuación, se consideran la misma solución. Para encontrar las soluciones que son distintas habría que encontrar todos los números incongruentes que la verifican. Bastará probar con el sistema completo $\{0,1,2,\ldots,m-1\}$. Si ninguno de estos números verifica la ecuación, entonces no hay solución.

Las ecuaciones en congruencias más elementales son la lineal y la cuadrática:

$$ax \equiv c \pmod{m} \qquad ax^2 \equiv c \pmod{m}$$

En realidad, una ecuación en congruencias es una ecuación diofántica con una incógnita más:

$$ax \equiv c \pmod{m} \rightarrow ax - c = \dot{m} \rightarrow ax - c = my \rightarrow ax - my = c$$

$$ax^2 \equiv c \pmod{m} \rightarrow ax^2 - c = \dot{m} \rightarrow ax^2 - c = my \rightarrow ax^2 - my = c$$

Ejemplos:

1) Soluciones de la ecuación de congruencias $3x \equiv 2 \pmod{2}$.

Probamos con el sistema completo de números incongruentes modulo 2 $\{0,1\}$:

El 0 verifica la ecuación pues $0 \equiv 2(\mathrm{mod}\,2)$, y por tanto la solución está formada por el 2 y todos los números congruentes con 2 modulo 2, esto es, por todos los números pares.
El 1 no verifica la ecuación, pues no se verifica $3.1 \equiv 2(\mathrm{mod}\,2)$.
La ecuación diofántica equivalente es $3x-2y=2$, cuya solución viene dada por $(2k, 3k-1),\ k=0,1,2,...$

2) Soluciones de la ecuación de congruencias $3x^2 \equiv 2(\mathrm{mod}\,5)$.

Probamos el sistema completo de números incongruentes modulo 5 $\{0,1,2,3,4\}$:
El 0 no verifica la ecuación: $0 \equiv 2(\mathrm{mod}\,5)$ falso
El 1 no verifica la ecuación: $3 \equiv 2(\mathrm{mod}\,5)$ falso
El 2 si verifica la ecuación: $12 \equiv 2(\mathrm{mod}\,5)$ cierto
El 3 si verifica la ecuación: $27 \equiv 2(\mathrm{mod}\,5)$ cierto
El 4 no verifica la ecuación: $48 \equiv 2(\mathrm{mod}\,5)$ falso
Una solución es 2 y los números congruentes con 2 modulo 5: $5k+2, k=0,1,2,...$
Otra solución es 3 y los números congruentes con 3 modulo 5: $5k+3, k=0,1,2,...$
La ecuación diofántica equivalente es $3x^2-5y=2$, cuyas dos soluciones vienen dadas por $(5k+2, 15k^2+12k+2)$ y $(5k+3, 15k^2+18k+2)$, $k=0,1,2,...$

Bibliografía:

- Birkkhoff-Mc Lane; Algebra Moderna. Editorial Vicens Vives. Barcelona, 1980.
- Bourbaki; Algebra. Editorial Hermann. Paris, 1962.
- Godement, R.; Algebra. Editorial Tecnos. Madrid, 1978
- Mathworld; Modular arithmetic.
  http://mathworld.wolfram.com/ModularArithmetic.html
- Mathworld; Fermat's Little Theorem.
  http://mathworld.wolfram.com/FermatsLittleTheorem.html
- Rey Pastor, J.- Castro, B.; Elementos de Análisis Matemático. Editorial Saeta. Madrid, 1962