Taller - teoría de Números

1) ¿Existen enteros a y b tal que $a+b=544$ y cuyo máximo común divisor es 11?

Se tiene:

$$a+b=544$$
$$mcd(a,b)=11$$

$\therefore\ 11 \mid a$ y $11 \mid b \Rightarrow 11 \mid a+b$

$11 \mid 544$?

Por propiedad: Si $a, b, c \in \mathbb{Z}$ y $c \mid a \wedge c \mid b$, entonces $c \mid (ax+by)$

$544 = K \cdot 11 \Rightarrow 544 = \underbrace{49}_{K} \cdot 11 + \underbrace{5}_{\text{residuo}}$

$\therefore\ 11 \nmid a+b \Rightarrow 11 \nmid 544$

R/ No existen enteros a y b que satisfagan las condiciones

2) Encuentre una regla de divisibilidad para 8 y 16

- Para 8: Un número es divisible por 8 si los últimos 3 dígitos son un número que sea divisible entre 8

Así, por ejemplo:

$10 \equiv 2 \pmod 8$

$10^3 \equiv 2^3 \equiv 0 \pmod 8$

$\Rightarrow$ Para todo $K \geq 3$

$$10^K \equiv 10^3 \cdot 10^{K-3} \equiv 0 \cdot 10^{K-3} \equiv 0 \pmod 8$$

Luego, $n \equiv a_0 + 10a_1 + 10^2 a_2 \pmod 8$

$$\therefore\ 8 \mid n$$

$\Rightarrow n \equiv 0 \pmod 8$ si y solo si

$$a_0 + 10a_1 + 10^2 a_2 \equiv 0 \pmod 8$$
$$\Downarrow$$
número formado por los últimos tres dígitos

- Para 16: Un número es divisible entre 16 si el número formado por sus cuatro últimas cifras es múltiplo de 16

Así tenemos:

$10^2 \equiv 4 \pmod{16}$
$10^2 \equiv 2^2 \pmod{16}$
$10^3 \equiv 2^3 \pmod{16}$

$10^4 \equiv 2^4 \equiv 0 \pmod{16}$

$\Rightarrow$ Para todo $k \geq 4$

$$10^k \equiv 10^4 \cdot 10^{k-4} \equiv 0 \cdot 10^{k-4} \equiv 0 \pmod{16}$$

Luego, $n \equiv a_0 + 10a_1 + 10^2 a_2 + 10^3 a_3 \pmod{16}$

$$\therefore \quad 16 \mid n$$

$\Rightarrow$ $n \equiv 0 \pmod{16}$ si y solo si

$$a_0 + 10a_1 + 10^2 a_2 + 10^3 a_3 \equiv 0 \pmod{16}$$

$$\Downarrow$$

número formado por los últimos 4 dígitos

3) Si p es un número primo y $a^2 \equiv b^2 \pmod{p}$, pruebe que $a \equiv \pm b$

Como $a^2 \equiv b^2 \pmod{p}$ podemos restar b^2 a ambos lados

$$\Rightarrow a^2 - b^2 \equiv 0 \pmod{p}$$
$$(a-b)(a+b) \equiv 0 \pmod{p}$$

Como p es primo, esto implica que:

$$a - b \equiv 0 \pmod{p} \quad ó \quad a + b \equiv 0 \pmod{p}$$
$$a - (-b) \equiv 0 \pmod{p}$$

Como $(a-b)$ y $(a-(-b))$ son divisibles por p

$\Rightarrow a \equiv b \pmod p$ ó $a \equiv -b \pmod p$

$\therefore \underline{a \equiv \pm b}$ cuando se tiene:

$$a^2 \equiv b^2 \pmod p$$

y p es primo

4) Encuentre el resto cuando 19^{19} es dividido entre 5

$19^4 \equiv 1 \bmod 5$	$\underline{19 \equiv 4 \bmod 5}$
$19^8 \equiv 1 \bmod 5$	$19^2 \equiv 16 \bmod 5$
$19^{12} \equiv 1 \bmod 5$	$\underline{19^2 \equiv 1 \bmod 5}$
$\underline{19^{16} \equiv 1 \bmod 5}$	

$$19^{16} \cdot 19^2 \cdot 19 \equiv 1 \cdot 1 \cdot 4 \bmod 5$$

$$19^{19} \equiv \boxed{4} \bmod 5$$

R/El resto es 4

5) Encuentre los últimos dos dígitos de 7^{7^7}

$$7^{7^7} = 7^{49}$$

tenemos:

- $7^1 = 7$
- $7^2 = 49$
- $7^3 = 343$
- $7^4 = 2401$
- $7^5 = 16807$
- $7^6 = 117649$
- $7^7 = 823543$
- $7^8 = 5764801$

$\Rightarrow$ Se tiene un ciclo cada 4 potencias donde se repiten los últimos 2 dígitos

Luego, si partimos del último termino de un ciclo y contamos desde ahí:

$$7^4 \Rightarrow 7^8 \Rightarrow 7^{12} \Rightarrow 7^{16} \Rightarrow 7^{20} \Rightarrow 7^{24} \Rightarrow 7^{28}$$
$$\Rightarrow 7^{32} \Rightarrow 7^{36} \Rightarrow 7^{40} \Rightarrow 7^{44} \Rightarrow 7^{48} \cdot 7^1$$

Como falta 1 en el exponente, significa que se suma una potencia en el ciclo que vuelve a iniciar.

R/ $\therefore$ Los últimos dos dígitos son 07

6) Encuentre $\phi(n)$ para $n = 35$, $n = 100$, $n = 51200$

- $n = 35$

$$35 = 7 \cdot 5$$

$$\phi(35) = \phi(7) \cdot \phi(5)$$
$$\phi(35) = 6 \cdot 4$$
$$\boxed{\phi(35) = 24}$$

$\cdot\, n = 100$ $\qquad 100 = 2^2 \cdot 5^2$

$$\phi(100) = \phi(2^2) \cdot \phi(5^2)$$
$$\phi(100) = 2^2 - 2 \cdot 5^2 - 5$$
$$\phi(100) = 2 \cdot 20$$
$$\boxed{\phi(100) = 40}$$

$\cdot\, n = 51\,200$ $\qquad 51\,200 = 2^{11} \cdot 5^2$

$$\phi(51\,200) = \phi(2^{11}) \cdot \phi(5^2)$$
$$\phi(51\,200) = 2^{11} - 2^{10} \cdot 5^2 - 5$$
$$\phi(51200) = 2048 - 1024 \cdot 25 - 5$$
$$\phi(51200) = 1024 \cdot 20$$
$$\boxed{\phi(51200) = 20480}$$

7) Usted le pregunta a un robot que quiere comer. El responde "48 879". Sabiendo que el robot piensa en hexadecimal pero habla el decimal, ¿qué le debería dar de comer?

Dividimos en 16 para pasar a base hexadecimal

$$48\,879 = 3054 \cdot 16 + \underline{15}$$
$$3\,054 = 190 \cdot 16 + \underline{14}$$
$$190 = \underline{11} \cdot 16 + \underline{14}$$

$\Rightarrow$ En hexadecimal sería 11 14 14 15

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
									A	B	C	D	E	F	

$\therefore\ 48\,879_{10} = BEEF_{16}$

R/ Deberia darle de comer "BEEF" (Carne de res) al robot

8) ¿65 314 638 792 es divisible por 24?

Sabemos que $24 = 8 \cdot 3$
además el $mcm(8,3) = 24$

$\therefore$ Si 8 y 3 dividen a 65 314 638 792, 24 también lo divide

Para 8, el número formado por las últimas 3 cifras debe ser múltiplo de 8

$65\,314\,638\,\underbrace{792}$

$792 = 99 \cdot 8 + \emptyset$

$$\begin{array}{r|l} 792 & 8 \\ \hline 72 & 99 \\ \emptyset & \end{array}$$

$\Longrightarrow 8 \mid 65\,314\,638\,792$

Para 3, la suma de todos los dígitos debe ser divisible entre 3

$6+5+3+1+4+6+3+8+7+9+2 = 54$
$5+4 = 9$
$9 = 3 \cdot 3 + 0$

$\Rightarrow 3 \mid 65\,314\,638\,792$

R/ $\therefore$ 65 314 638 792 Si es divisible por 24

9) Pruebe que $n^p - n$ es divisible por p si p es un número primo

Si $n^p - n$ es divisible por p

$$\Rightarrow n^p - n \equiv 0 \pmod{p}$$
$$n(n^{p-1} - 1) \equiv 0 \pmod{p}$$

Por el pequeño teorema de Fermat tenemos que:

$$n^{p-1} \equiv 1 \pmod{p}$$
$$n^{p-1} - 1 \equiv 0 \pmod{p}$$

Luego, si tuvieramos $n \equiv x \pmod{p}$

$$n(n^{p-1} - 1) \equiv x \cdot 0 \pmod{p}$$
$$n(n^{p-1} - 1) \equiv 0 \pmod{p}$$

$$\boxed{n^p - 1 \equiv 0 \pmod{p}} \quad \text{QED}$$

10) Encuentre los enteros x y y tal que
$314x + 159y = 1$

$$314 = 1 \cdot 159 + 155$$
$$159 = 1 \cdot 155 + 4$$

$$
\begin{aligned}
\underline{155} &= 38 \cdot \underline{4} + \underline{3} \\
\underline{4} &= 1 \cdot \underline{3} + 1 \\
\underline{3} &= 3 \cdot 1 + 0
\end{aligned}
$$

Reemplazo hacia atrás

$$
\begin{aligned}
1 &= 4 - 1 \cdot 3 \\
1 &= 4 - 1(155 - 38 \cdot 4) \\
1 &= 39 \cdot 4 - 155 \\
1 &= 39(159 - 1 \cdot 155) - 155 \\
1 &= 39 \cdot 159 - 40 \cdot 155 \\
1 &= 39 \cdot 159 - 40(314 - 159) \\
1 &= \underbrace{79}_{y} \cdot 159 - \underbrace{40}_{x} \cdot 314
\end{aligned}
$$

$$
\boxed{\begin{aligned} x &= -40 \\ y &= 79 \end{aligned}}
$$

11) Pruebe o controvierta la siguiente afirmación
si $a^2 \equiv b^2 \pmod m$ entonces $a \equiv b \pmod m$
ó $a \equiv -b \pmod m$

Tal como se probó previamente, esta afirmación sólo se cumple si m es un número primo, en caso contrario podemos ver un contraejemplo

Ej: $a = 9$ $b = 7$ y $m = 16$

$$9^2 \equiv 7^2 \pmod{16}$$

$$\underbrace{9 \equiv 7 \pmod{16}}_{\text{Falso}} \qquad \underbrace{9 \equiv -7 \pmod{16}}_{\text{Falso}}$$

12) Encuentre todos los enteros positivos tales que $1066 \equiv 1776 \pmod{m}$

tenemos que $1776 - 1066 \equiv 0 \pmod{m}$
$$710 \equiv 0 \pmod{m}$$

de modo que m van a ser todos los divisores de 710

710	2
355	5
71	71
1	

$\Rightarrow$ divisores: 1, 2, 5, 71, 10, 142, 355, 710

R/ Los enteros positivos que satisfacen la condición son 1, 2, 5, 71, 10, 142, 355 y 710

13) Muestre que la diferencia de dos cubos consecutivos nunca es divisible por 5

Cubo 1 : n^3
Cubo 2 : $(n+1)^3$

$$\Rightarrow n^3 - (n+1)^3 \equiv 0 \pmod{5} \ ?$$
$$\cancel{n^3} - (\cancel{n^3} + 3n^2 + 3n + 1) \equiv 0 \pmod{5}$$
$$-3n^2 - 3n - 1 \equiv 0 \pmod{5}$$

Luego, verificamos el modulo 5 con cada término, teniendo en cuenta que los residuos pueden ser 0, 1, 2, 3, 4

- $n \equiv 0 \mod 5 \Rightarrow -3n^2 - 3n - 1 \equiv 4 \pmod 5$
- $n \equiv 1 \mod 5 \Rightarrow -3n^2 - 3n - 1 \equiv 3 \pmod 5$
- $n \equiv 2 \mod 5 \Rightarrow -3n^2 - 3n - 1 \equiv 1 \pmod 5$
- $n \equiv 3 \mod 5 \Rightarrow -3n^2 - 3n - 1 \equiv 3 \pmod 5$
- $n \equiv 4 \mod 5 \Rightarrow -3n^2 - 3n - 1 \equiv 4 \pmod 5$

En ninguno de los casos 5 divide a la expresión $\therefore$ la diferencia de dos cubos consecutivos nunca es divisible por 5

14) Encuentre un entero positivo n talque $3^2 \mid n$, $4^2 \mid n+1$, $5^2 \mid n+2$

Tenemos $\begin{cases} n \equiv 0 \pmod{3^2} \\ n+1 \equiv 0 \pmod{4^2} \\ n+2 \equiv 0 \pmod{5^2} \end{cases}$

$$\Rightarrow \begin{cases} n \equiv 0 \pmod 9 \\ n+1 \equiv 0 \pmod{16} \\ n+2 \equiv 0 \pmod{25} \end{cases}$$

Así, obtenemos el sistema de ecuaciones:

$$\begin{cases} n = 9a \\ n = 16b - 1 \\ n = 25c - 2 \end{cases}$$

Reemplazando: $\begin{cases} 9a = 16b - 1 \\ 9a = 25c - 2 \end{cases}$

$\Rightarrow \begin{cases} 9a \equiv -1 \pmod{16} \\ 9a \equiv -2 \pmod{25} \end{cases}$

Por el teorema del resto chino se tiene una única solución única modulo $m = 16 \cdot 25$
$\Rightarrow m = 400$

Y encontrando una solución para modulo 16 y modulo 25 tenemos:

$\begin{cases} a \equiv 11 \pmod{16} \\ a \equiv 23 \pmod{25} \end{cases} \Longrightarrow \begin{cases} a = 11 + 16v \\ a = 23 + 25w \end{cases}$

Así,

$$n = 9a = 9(11 + 16v) = 9(23 + 25w)$$
$$99 + 144v = 207 + 225w$$

$\Rightarrow \begin{cases} n \equiv 99 + 144v \\ n \equiv 207 + 225w \end{cases} \qquad \begin{cases} v \equiv 7 \pmod{16} \\ w \equiv 3 \pmod{25} \end{cases}$

Utilizando el teorema del resto chino podemos escribir n como:

$$n \equiv 99 + 144 \cdot 7 \cdot 3 \pmod{400}$$
$$n \equiv 3123 \pmod{400}$$

$\therefore\ n = 3123 + 400K$ para algún entero K

R/ Una posible solución es 3123

15) ¿Cuál es el último dígito de 7^{355}?

tenemos:

- $7^1 = 7$
- $7^2 = 49$
- $7^3 = 343$
- $7^4 = 2401$
- $7^5 = 16807$
- $7^6 = 117649$
- $7^7 = 823543$
- $7^8 = 5764801$

$\Rightarrow$ Se tiene un ciclo cada 4 potencias donde se repite el último dígito

Luego, si partimos del último termino de un ciclo y contamos desde ahí:

$$7^4 \Rightarrow 7^8 \Rightarrow 7^{16} \Rightarrow 7^{32} \Rightarrow 7^{64} \Rightarrow 7^{128}$$
$$\Rightarrow 7^{256} \Rightarrow 7^{320} \Rightarrow 7^{352} \Rightarrow 7^{352} \cdot 7^3$$

Como falta 3 en el exponente, significa que la potencia 7^{355} toma la tercera posición en el ciclo

R/ $\therefore$ el último dígito de 7^{355} es 3

16) Muestre que $3K + 4$ y $4K + 5$ no tienen un factor común más grande que 1

Por contradicción se parte del supuesto de que tienen un factor común d más grande que 1

Así, $\begin{cases} 3K+4 = ad \\ 4K+5 = bd \end{cases}$ donde $a, b \in \mathbb{Z}$

despejamos K,

$$\begin{cases} K = \dfrac{ad-4}{3} \\ K = \dfrac{bd-5}{4} \end{cases}$$

$$\Rightarrow \frac{ad-4}{3} = \frac{bd-5}{4}$$

$$4(ad-4) = 3(bd-5)$$

$$4ad - 16 = 3bd - 15$$

$$4ad - 3bd = 1$$

Así obtenemos una ecuación de la forma de la identidad de Bezout donde el factor común es 1, pero d también es factor común de $4ad - 3bd$. Sin embargo, esto es imposible porque el factor común entre 1 y cualquier otro entero es 1

Así, la suposición de que $3k+4$ y $4k+5$ tienen un factor común d más grande que 1 <u>Es Falsa</u>