Taller teoría de números

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

Si usamos la propiedad de:

$$a = a' \cdot mcd(a,b)$$
$$b = b' \cdot mcd(a,b)$$

$$mcd(a',b') = 1$$

tenemos que:

$$a' \cdot 11 + b' \cdot 11 = 544$$
$$11(a'+b') = 544$$
$$a'+b' = \frac{544}{11}$$

• Como 11 es un factor en el lado izquierdo, también debe serlo en el lado derecho pero 544 no es divisible por 11.

Ya que no existen enteros a' y b' cuyo máximo común divisor sea 1 y sumados sean $544/11$, no hay solución

2) Encuentre una regla de divisibilidad para 8 y para 16

regla para 8

Calculando los restos potenciales de 10 modulo 8 tenemos:

$$10^0 \equiv 1 \pmod 8$$
$$10^1 \equiv 2 \pmod 8$$
$$10^2 \equiv 4 \pmod 8$$

Entonces un número de la forma $a = a_k 10^k + a_{k-1} 10^{k-1} + \dots + a_1 10 + a_0$ sera divisible por 8 si:

$$a \equiv 4a_2 + 2a_1 + a_0 \pmod 8$$

regla para 16

restos potenciales de 10 modulo 16:

$$10^0 \equiv 1 \pmod{16}$$
$$10^1 \equiv 10 \pmod{16}$$
$$10^2 \equiv 4 \pmod{16}$$
$$10^3 \equiv 8 \pmod{16}$$

Entonces un número a_{10} sera divisible por 16 si:

$$a \equiv 8a_3 + 4a_2 + 10a_2 + a_0$$

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

$$a^2 \equiv b^2 \pmod{p} \implies p \mid a^2 - b^2 \implies a^2 - b^2 = k.p$$

Factorizando, tenemos que:

$$(a-b)(a+b) = k.p$$

y como p es primo:

$$p \mid a-b \quad o \quad p \mid a+b$$

esto, es equivalente a decir:

$$a \equiv -b \pmod{p} \qquad a \equiv b \pmod{p}$$

4) Encuentre el resto cuándo 19^{19} es dividido por 5

por el pequeño teorema de Fermat $\rightarrow$ $19^4 \equiv 1 \pmod{5}$

$19^{19} \equiv (19^4)^4 . 19^3 \pmod{5}$

$19^{19} \equiv 1 \cdot (-1)^3 \pmod{5}$

$19^{19} \equiv 1 . 4 \pmod{5}$

$19^{19} \equiv 4 \pmod{5}$

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

restos potenciales de 7 módulo 10

$7^0 \equiv 1 \pmod{10}$
$7^1 \equiv 7 \pmod{10}$
$7^2 \equiv 9 \pmod{10}$
$7^3 \equiv 3 \pmod{10}$

entonces $(7^7)^7 \equiv 3^7 \pmod{10}$

$\equiv 3^6 . 3 \pmod{10}$

$\equiv (3^2)^3 . 3 \pmod{10}$

$\equiv 9^3 . 3 \pmod{10}$

$\equiv 9^2 . 9 . 3 \pmod{10}$

- $81 \equiv 1 \pmod{10}$
- $9 \equiv 9 \pmod{10}$
- $3 \equiv 3 \pmod{10}$

$$(7^7)^7 \equiv 27 \pmod{10}$$

$(7^7)^7 \equiv 7 \pmod{10} \rightarrow$ los últimos dos dígitos son 0 y 7

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

Factorizacion prima de 35

$$\begin{array}{r|l} 35 & 5 \\ 7 & 7 \\ 1 & \end{array}$$

$$\begin{aligned} 35 &= 7 \cdot 5 \\ \phi(35) &= \phi(7) \cdot \phi(5) \\ &= (7^1 - 7^0)(5^1 - 5^0) \\ &= 6 \cdot 4 \\ &= \boxed{24} \end{aligned}$$

Factorización prima de 100

$$\begin{array}{r|l} 100 & 2 \\ 50 & 2 \\ 25 & 5 \\ 5 & 5 \\ 1 & \end{array}$$

$$\begin{aligned} \phi(100) &= \phi(2^2)\,\phi(5^2) \\ &= (2^2 - 2^1)(5^2 - 5^1) \\ &= 2 \cdot 20 \\ &= \boxed{40} \end{aligned}$$

Factorización prima de 51 200

$$\begin{array}{r|l} 51200 & 2 \\ 25600 & 2 \\ 12800 & 2 \\ 6400 & 2 \\ 3200 & 2 \\ 1600 & 2 \\ 800 & 2 \\ 400 & 2 \\ 200 & 2 \\ 100 & 2 \\ 50 & 2 \\ 25 & 5 \\ 5 & 5 \\ 1 & \end{array}$$

$$\begin{aligned} \phi(51200) &= \phi(2^{11}) \cdot \phi(5^2) \\ &= (2^{11} - 2^{10})(5^2 - 5^1) \\ &= 1024 \cdot 20 \\ &= \boxed{20.480} \end{aligned}$$

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, que le debería dar de comer?

expansión en base 16 del entero 48.879.

$48.879 = 3054 \cdot 16 + \underline{15}$

$3054 = 16 \cdot 190 + \underline{14}$

$190 = 16 \cdot 11 + \underline{14}$

$11 = 16 \cdot 0 + \underline{11}$

$(48.879)_{10} \longrightarrow (BEEF)_{16}$

8) ¿65.314.638.792 es divisible por 24?

Dado que 3 y 8 son coprimos podemos aplicar la regla de divisibilidad del 3 y 8 para conocer si el número es divisible por 24.

regla para 3

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

$3 \mid 54$ ✓

regla para 8

$2 + 2(9) + 4(7) = 48$

$8 \mid 48$ ✓

Por lo tanto, el número es divisible por 24

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

Por el pequeño teorema de Fermat si n no es divisible por p entonces $n^{p-1} \equiv 1 \pmod p$

Multiplicando por n, obtenemos:

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

$$n^p \equiv n \pmod p$$

Usando esta congruencia, podemos reescribir $n^p - n$ como $n - n$

$$\rightarrow \quad n - n \equiv 0 \pmod p$$

esto quiere decir $n-n$ es divisible por p y su residuo es cero.
Concluimos que n^p-n es divisible por p un numero primo.

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

$314 = 159 \cdot 1 + 155$
$159 = 155 \cdot 1 + 4$
$155 = 4 \cdot 38 + 3$
$4 = 3 \cdot 1 + 1$
$3 = 1 \cdot 3 + 0$

- $155 = 314(1) + 159(-1)$
- $4 = 159(1) + 155(-1)$
- $3 = 155(1) + 4(-38)$
- $1 = 4(1) + 3(-1)$

$$1 = 4(1) + 3(-1)$$
$$1 = 4(1) + (-1)[155(1) + 4(-38)]$$
$$1 = 4(1) + 155(-1) + 4(-38)$$
$$1 = 4(39) + 155(-1)$$
$$1 = (39)[159(1) + 155(-1)] + 155(-1)$$
$$1 = 159(39) + 155(-39) + 155(-1)$$
$$1 = 159(39) + 155(-40)$$
$$1 = 159(39) + (-40)[314(1) + 159(-1)]$$
$$1 = 159(39) + 314(-40) + 159(40)$$
$$1 = 159(79) + 314(-40)$$

$$x = -40$$
$$y = 79$$

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

La afirmación es incorrecta ya que si tomamos $m=4$, $a=2$, $b=4$

$$4 \equiv 16 \pmod 4$$

$$\begin{cases} 2 \equiv 4 \pmod 4 \\ 2 \equiv -4 \pmod 4 \end{cases}$$

2 no es congruente con cero o "menos cero".

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

$$1066 \equiv 1776 \pmod m$$

$$\rightarrow m \mid 1066 - 1776 = -710$$

$$-710 \equiv 0 \pmod m$$

Los divisores positivos de 710 son:

$$\begin{array}{r|l} 710 & 2 \\ 355 & 5 \\ 71 & 71 \\ 1 & \end{array} \qquad 710 = 2 \times 5 \times 71$$

	2^0	2^1
$\times 5^1$	1	2
	5	10
$\times 71^1$	71	142
	355	710

los enteros positivos que satisfacen $1066 \equiv 1776 \pmod m$ son:

$$1, 2, 5, 10, 71, 142, 355, 710$$

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

$$n^3 - (n+1)^3 \not\equiv 0 \pmod 5$$

$$n^3 + 3n^2 + 3n + 1 - n^3$$

$$3n^2 + 3n + 1 \not\equiv 0 \pmod 5$$

Para $n = 0 \longrightarrow 3(0)^2 + 3(0) + 1$

$$\downarrow$$

$$1 \equiv 1 \pmod 5$$

Para $n = 1 \longrightarrow 3(1)^2 + 3(1) + 1$

$$\downarrow$$

$$7 \equiv 2 \pmod 5$$

para $n = 2 \longrightarrow 3(2)^2 + 3(2) + 1$

$$\downarrow$$

$$19 \equiv 4 \pmod 5$$

para $n = 3 \longrightarrow 3(3)^2 + 3(3) + 1$

$$\downarrow$$

$$37 \equiv 2 \pmod 5$$

Para $n = 4 \longrightarrow 3(4)^2 + 3(4) + 1$

$61 \equiv 1 \pmod 5$

Así, concluimos que $5 \nmid n^3 - (n+1)^3$

14) Encuentre un entero positivo n tal que $3^2 | n$, $4^2 | n+1$, $5^2 | n+2$

el sistema de congruencias se plantea así:

$$n \equiv 0 \pmod 9$$
$$n \equiv 15 \pmod{16}$$
$$n \equiv 23 \pmod{25}$$

$\text{mod} = 9 \cdot 16 \cdot 25$
$\text{mod} = 3600$

$C_1 = 3600 / 9 = 400$
$C_2 = 3600 / 16 = 225$
$C_3 = 3600 / 25 = 144$

Ahora, calculando el inverso multiplicativo de los valores C_1, C_2, C_3:

$400 \cdot d_1 \equiv 1 \pmod 9 \qquad d_1 = 7$
$225 \cdot d_2 \equiv 1 \pmod{16} \qquad d_2 = 1$
$144 \cdot d_3 \equiv 1 \pmod{25} \qquad d_3 = 4$

Solución particular

$n = 0 \cdot 400 \cdot 7 + 15 \cdot 225 \cdot 1 + 23 \cdot 144 \cdot 4$
$0 + 3375 + 13.248 = \underline{16.623}$

Solución general

$n = 16.623 \equiv 2223 \pmod{3600}$

$n = 2223 + 3600K$

- 2223 es un entero positivo tal que $3^2 | n$, $4^2 | n+1$, $5^2 | n+2$

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

Usando el teorema de euler tenemos que dados a,n coprimos

$\rightarrow a^{\varphi(n)} \equiv 1 \pmod m$

para encontrar el ultimo digito de 7^{355} debemos resolver la congruencia $7^{355} \pmod{10}$ y sabemos que $MCD(7,10) = 1$

$\rightarrow \quad 7^{\varphi(10)} \equiv 1 \pmod{10}$

$\rightarrow \quad 7^{4} \equiv 1 \pmod{10}$

entonces: $7^{355} \equiv (7^4)^{88} \cdot 7^3 \pmod{10}$

$7^{355} \equiv 1 \cdot 3 \pmod{10}$

$7^{355} \equiv 3 \pmod{10}$

Por lo tanto, el ultimo digito es 3.

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

Se plantea el siguiente sistema de congruencias

$n \equiv 4 \pmod{3}$

$n \equiv 5 \pmod{4}$

mod $= 3 \cdot 4$
mod $= 12$

$C_1 = 12/3 = 4$
$C_2 = 12/4 = 3$

Calculando el inverso multiplicativo de C_1, C_2

$4 \cdot d_1 \equiv 1 \pmod{3} \qquad d_1 = 1$
$3 \cdot d_2 \equiv 1 \pmod{4} \qquad d_2 = 3$

solución particular

$n = 4 \cdot 4 \cdot 1 + 5 \cdot 3 \cdot 3 = 61 \equiv 1 \pmod{12}$

la unica posible solución del sistema es 1, lo que concluye que el unico factor comun es 1.