Pontificia Universidad Católica de Chile
Facultad de Matemáticas
2° semestre 2020

Ayudantía 05

11 de Septiembre

MAT2225 - Teoría de Números

1) Determine si los siguientes enteros se pueden escribir como suma de dos cuadrados. Si se puede, encuentre una suma:

   a) 9!.

   Solución. Notar que $9! = 2^7 \cdot 3^4 \cdot 5 \cdot 7$. Como $v_7(9!) = 1$, no se puede escribir como la suma de 2 cuadrados. ∎

   b) 29.

   Solución. 29 es primo. Buscamos s tal que $s^2 \equiv_{29} -1$. Notar que 12 cumple lo pedido. Construyendo la tabla de $[x - 12y]_{29}$.

x\y	0	1	2	3	4	5
0	0	17	5	22	10	27
1	1	18	6	23	11	28
2	2	19	7	24	12	0
3	3	20	8	25	13	1
4	4	21	9	26	14	2
5	5	22	10	27	15	3

   Tomando los pares $(5, 2)$ y $(0, 4)$ tenemos que

$$5 - 12 \cdot 2 = -12 \cdot 4$$

   Agrupando de manera conveniente, elevando al cuadrado y recordando que $(12)^2 \equiv_{29} -1$, tenemos que

$$5^2 + 2^2 \equiv_{29} 0.$$

   Esto nos da los cuadrados que buscamos. ∎

c) 2020.

Solución. Notar que $2^2 \cdot 5 \cdot 101$. Sabemos que $5 = 2^2 + 1^2$ y que $101 = 100^2 + 1^2$. Trabajando un poco la expresión, se tiene

$$\begin{aligned} 2020 &= 2^2(2+i)(2-i)(10+i)(10-i) \\ &= 2^2(2+i)(10+i)(2-i)(10-i) \\ &= 2^2(19+12i)(19-12i) \\ &= 2^2(19^2+12^2) \\ &= 38^2+24^2. \end{aligned}$$

Esto nos da una solución. ∎

d) $10^9 + 7$.

Solución. Notar que $10^9 + 7 \equiv_4 3$, por lo que no puede ser escrito como suma de 2 cuadrados. ∎

2) Encuentre 2^{2020} (mód 36).

Solución. Lo anterior es equivalente a encontrar 2^{2020} (mód 4) y 2^{2020} (mód 9). Claramente $2^{2020} \equiv_4 0$. Para encontrar 2^{2020} (mód 9), notar que $2^3 \equiv_9 -1$, por lo que

$$2^{2020} \equiv_9 2^{3\cdot 673} \cdot 2 \equiv_9 (2^3)^{673} \cdot 2 \equiv_9 (-1)^{673} \cdot 2 \equiv_9 -2 \equiv_9 7.$$

Como $(4, 9) = 1$, por teorema chino del resto sabemos que existe una única solución a $x \equiv_4 0, x \equiv_9 7$ módulo $\text{mcm}(4, 9) = 36$. Como 16 es solución, tenemos que $2^{2020} \equiv_{36} 16$. ∎

3) Determine si el siguiente sistema de congruencias tiene solución. En caso de tener, encuentre una:

$$\begin{aligned} x &\equiv_{15} 2 \\ x &\equiv_{24} 17 \\ x &\equiv_{28} 9 \end{aligned}$$

Solución. Podemos separar cada congruencia usando teorema chino del resto, por lo que nos queda

$$\begin{aligned} x &\equiv_3 2 \\ x &\equiv_5 2 \\ x &\equiv_3 17 \equiv_3 2 \\ x &\equiv_8 17 \equiv_8 1 \\ x &\equiv_4 9 \equiv_4 1 \\ x &\equiv_7 9 \equiv_7 2 \end{aligned}$$

Notar que $x \equiv_8 1 \Rightarrow x \equiv_4 1$, por lo que podemos omitir la segunda. También aparece $x \equiv_3 2$ dos veces, por lo que podemos sacar una. Haciendo esto y ordenando las congruencias un poco, se tiene

$$\begin{aligned} x &\equiv_3 2 \\ x &\equiv_5 2 \\ x &\equiv_7 2 \\ x &\equiv_8 1 \end{aligned}$$

Ahora, las 3 primeras congruencias se reducen a $x \equiv 2 \pmod{\text{mcm}(3 \cdot 5 \cdot 7)}$, por lo que el sistema anterior se reduce a

$$\begin{aligned} x &\equiv_{105} 2 \\ x &\equiv_8 1 \end{aligned}$$

Como $(8, 105) = 1$, hay solución. Tenemos que $x = 105k + 2$. Luego,

$$105k + 2 \equiv_8 1.$$

Como $105 \equiv_8 1$, se tiene $k + 2 \equiv_8 1$, por lo que $k \equiv_8 7$. Luego, las soluciones son de la forma $105(8n + 7) + 2 = 840n + 212$. ∎

Bonus: Sea $f : \mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$ una permutación y a, b clases de $\mathbb{Z}/5\mathbb{Z}$.

a) Muestre que la sucesión $a, f(a), f^2(a), f^3(a), \ldots$ es periódica.

b) Determine condiciones necesarias y suficientes para que $f^k(a) = f^k(b)$ para algún $k \in \mathbb{N}$. ¿Cuál es el k más pequeño que cumple lo pedido?

c) Sean $g, h : \mathbb{Z}/5\mathbb{Z} \to \mathbb{Z}/5\mathbb{Z}$ dos funciones. Muestre que $a, g(a), g^2(a), \ldots$ y $a, h(a), h^2(a), \ldots$ son eventualmente periódicas.

d) Asuma que existe un k positivo tal que $h^k(a) = g^k(a)$. Encuentre una cota superior para k.

e) Encuentre funciones g, h y tales que lo anterior no ocurra para ningún a.