Bachmann Lautaro

Tarea 9

1. (60 pts)
   (i) Encontrar todas las soluciones de la ecuación en congruencia
   $$30x \equiv 2 \quad (67)$$
   usando el método visto en clase.
   (ii) Dar todas las soluciones x de la ecuación anterior tales que $0 < x < 300$.
2. (40 pts) Encontrar los últimos dos dígitos de 2^{338}. (*Ayuda:* Se cumple que $2^{22} \equiv 4\ (100)$).

1) i) Calculemos el mcd(30, 67) para saber si 30 y 67 son coprimos:

$$\left.\begin{array}{l} \text{Divisores } 30 = 1, 2, 3, 5, 6, 10, 15, 30 \\ \text{Divisores } 67 = 1, 67 \end{array}\right\} \text{mcd}(30,67) = 1$$

Como el mcd es igual a 1, 30 y 67 son coprimos, por ende, la ecuación lineal de congruencia tiene solución.

Ahora, usemos el algoritmo de euclides para eventualmente poder armar las ecuaciones del resto.

$67 = 30.2 + 7 \Rightarrow 7 = 67 + 30.(-2)$
$30 = 7.4 + 2 \Rightarrow 2 = 30 + 7.(-4)$
$7 = 2.3 + 1 \Rightarrow 1 = 7 + 2.(-3)$
$2 = 1.2 + 0$

A partir de estas ecuaciones podemos elaborar una combinación lineal tal que $1 = s.30 + t.67$

$1 = 7 + 2.(-3)$
$1 = 7 + (30 + 7.(-4)).(-3)$
$1 = 7 + 30.(-3) + 7 \cdot 12$
$1 = 7 \cdot 13 + 30 \cdot (-3)$
$1 = (67 + 30.(-2)).13 + 30.(-3)$
$1 = 67 \cdot 13 + 30.(-26) + 30.(-3)$

$\downarrow$

$$1 = 67 \cdot 13 + 30 \cdot (-29)$$

$$\therefore \quad s = -29 \ , \ t = 13$$

A partir de haber encontrado s y t, podemos armar entonces la ecuación lineal de congruencia, intentando llegar a algo similar a $2 \equiv 30\, x_0 \pmod{67}$

$$1 \equiv 67 \cdot 13 + 30 \cdot (-29) \pmod{67}$$
$$1 \equiv 0 \cdot 13 + 30 \cdot (-29) \pmod{67}$$
$$1 \equiv 30 \cdot (-29) \pmod{67}$$
$$1 \cdot 2 \equiv 30 \cdot (-29) \cdot 2 \pmod{67}$$
$$2 \equiv 30 \cdot (-58) \pmod{67}$$

Ahora que llegamos a la estructura que buscabamos, podemos decir que $x_0 = -58$

Sabiendo esto, podemos armar la formula para encontrar todas las soluciones:

$$x = x_0 + k \cdot \left(\frac{m}{d}\right) \implies \boxed{x = -58 + k \cdot 67}$$

ii) Conociendo la ecuación $x = -58 + k + 67$ y teniendo en cuenta que x debe de ser mayor que 0 y menor que 300, y $k \in \mathbb{Z}$ entonces:

$$0 < x < 300$$
$$0 < -58 + k \cdot 67 < 300$$
$$58 < k \cdot 67 < 358$$
$$\frac{58}{67} < k < \frac{358}{67}$$

$$\therefore \quad k \in \left(\frac{58}{67}, \frac{358}{67}\right)$$

Sin embargo, como $k \in \mathbb{Z}$, hay que ver cuales son los enteros presentes en este intervalo

$$\frac{58}{67} < k < \frac{358}{67} \approx 0{,}865 < k < 5{,}343$$

$\therefore$ los enteros presentes son $1, 2, 3, 4, 5$

es decir, $k = \{1, 2, 3, 4, 5\}$

Por lo tanto, encontramos los números K que dan solución a $0 < x < 300$.
Ahora, reemplacemos los respectivos números K en la formula $x = -58 + K \cdot 67$

$x = -58 + 1 \cdot 67$	$x = -58 + 2 \cdot 67$	$x = -58 + 3 \cdot 67$	$x = -58 + 4 \cdot 67$	$x = -58 + 5 \cdot 67$
$x = -58 + 67$	$x = -58 + 134$	$x = -58 + 201$	$x = -58 + 268$	$x = -58 + 335$
$x = 9$	$x = 76$	$x = 143$	$x = 210$	$x = 277$

En conclusión, todas las soluciones x de la ecuación, tal que $0 < x < 300$ son 9, 76, 143, 210, 277.

2) A partir del número 2^{338} y operando con propiedades de las potencias:

$$
\begin{aligned}
2^{338} &\equiv (2^{22})^{15} \cdot 2^{8} \pmod{100} \\
&\equiv (4)^{15} \cdot 2^{8} \pmod{100} \\
&\equiv (2^{2})^{15} \cdot 2^{8} \pmod{100} \\
&\equiv 2^{30} \cdot 2^{8} \pmod{100} \\
&\equiv 2^{22} \cdot 2^{16} \pmod{100} \\
&\equiv 4 \cdot 2^{16} \pmod{100} \\
&\equiv 2^{2} \cdot 2^{16} \pmod{100} \\
&\equiv 2^{18} \pmod{100} \\
&\equiv (2^{9})^{2} \pmod{100} \\
&\equiv (512)^{2} \pmod{100} \\
&\equiv (500+12)^{2} \pmod{100} \\
&\equiv (12)^{2} \pmod{100} \\
&\equiv 144 \pmod{100} \\
&\equiv 100+44 \pmod{100} \\
&\equiv 44 \pmod{100}
\end{aligned}
$$

Al haber llegado a un número de dos cifras, sabemos que este número son las últimas dos cifras, es decir, 2^{338} termina en 44.