Reto 3

Simone Spada

1 Solución

El conjunto $S_r := \{\text{soluciones } (\text{mod } 2^{\text{r}} \times 35)\}$ de las soluciones de la ecuación

$$8n^2 - 32n + 3 \equiv 0 \pmod{2^r \times 35}$$

es el siguiente:

Si $r \leq 3$**:**

$$S_r = \{1, 3, 8, 31\} + 35h$$

con $h = 0, 1, ..., (2^r - 1)$.
En particular,

$$|S_r| = 2^{r+2}$$

Si $4 \leq r \leq 5$**:**

$$S_r = \{1, 3, 31, 43\} + 70h$$

con $h = 0, 1, ..., (2^{r-1} - 1)$.
En particular,

$$|S_r| = 2^{r+1}$$

Si $r > 5$**:**

$$S_r = 36^{r-4}\{1, 3, 8, 31\} + \left(1 - 36^{r-4}\right)\{1, 3\} + \left(2^{r-4} \times 35\right) h$$

con $h = 0, 1, ..., 15$.
En particular,

$$|S_r| = 2^7$$

2 Demostración

$$8n^2 - 32n + 3 = 8\,(n-1)\,(n-3)$$

Vamos ad analizar el problema en función de r

2.1 Caso $r = 0$

8 es inversible en $\mathbb{Z}/35\mathbb{Z}$, entonces es suficiente buscar las soluciones de

$$\begin{cases} (n-1)(n-3) \equiv 0 \pmod 5 \\ (n-1)(n-3) \equiv 0 \pmod 7 \end{cases} \Leftrightarrow \begin{cases} n \equiv 1,3 \pmod 5 \\ n \equiv 1,3 \pmod 7 \end{cases} \Leftrightarrow n \equiv 1,3,8,31 \pmod{35}$$

$2^{r+2} = 4$ soluciones.

2.2 Caso $r = 1$

Las soluciones de $8(n-1)(n-3) \equiv 0 \pmod{2\times5\times7}$ son las soluciones de $4(n-1)(n-3) \equiv 0 \pmod{35}$.
4 es inversible, así que las soluciones son quellas del caso $r = 0$

$$n \equiv 1,3,8,31 \pmod{35} \Leftrightarrow n \equiv 1,3,8,31,36,38,43,66 \pmod{70}$$

$2^{r+2} = 8$ soluciones.

2.3 Caso $r = 2$ ó $r = 3$

Como antes, tenemos las mismas soluciones $\pmod{35}$, levantadas $\pmod{2^r \times 35}$. Es decir,

$$S_r = \{1,3,8,31\} + 35h$$

con $h = 0,1,...,(2^r - 1)$.
2^{r+2} soluciones.

2.4 Caso $r > 3$

Sea $s := r - 3$.
Tenemos que buscar las soluciones de

$$(n-1)(n-3) \equiv 0 \pmod{2^s \times 35}$$

y levantarlas $\pmod{2^r \times 35}$, sumando $2^s \times 35h$, con $h = 0,...,7$.

2.4.1 Caso $s = 1 \leftrightarrow r = 4$

Tenemos que solucionar el sistema

$$\begin{cases} (n-1)(n-3) \equiv 0 \pmod 2 \\ (n-1)(n-3) \equiv 0 \pmod{35} \end{cases} \Leftrightarrow \begin{cases} n \equiv 1 \pmod 2 \\ n \equiv 1,3,8,31 \pmod{35} \end{cases}$$

$$\Leftrightarrow n \equiv 1,3,31,43 \pmod{70}$$

$$\Leftrightarrow S_r = \{1,3,31,43\} + 70h$$

con $h = 0,...,7$.
$2^{r+1} = 2^5$ soluciones

2.4.2 Caso $s = 2 \leftrightarrow r = 5$

Solucionamos

$$\begin{cases} (n-1)(n-3) \equiv 0 \pmod 4 \\ (n-1)(n-3) \equiv 0 \pmod{35} \end{cases} \Leftrightarrow \begin{cases} n \equiv 1, 3 \pmod 4 \\ n \equiv 1, 3, 8, 31 \pmod{35} \end{cases}$$

$$\Leftrightarrow n \equiv 1, 3, 31, 43, 71, 73, 101, 113 \pmod{140} \Leftrightarrow n \equiv 1, 3, 31, 43 \pmod{70}$$

$$\Leftrightarrow S_r = \{1, 3, 31, 43\} + 70h$$

con $h = 0, ..., 15$.
$2^{r+1} = 2^6$ soluciones

2.4.3 Caso $s > 2 \leftrightarrow r > 5$

Solucionamos

$$\begin{cases} (n-1)(n-3) \equiv 0 \pmod{2^s} \\ (n-1)(n-3) \equiv 0 \pmod{35} \end{cases}$$

Fijamosnos sobre

$$(n-1)(n-3) \equiv 0 \pmod{2^s}$$

sea ahora $x := n - 3$,

$$(n-1)(n-3) \equiv 0 \pmod{2^s} \Leftrightarrow x(x+2) \equiv 0 \pmod{2^s}$$

Si $x \equiv 0 \pmod{2^s}$**:**

$$n \equiv 3 \pmod{2^s}$$

Si $x + 2 \equiv 0 \pmod{2^s}$**:**

$$n \equiv 1 \pmod{2^s}$$

Si $2 \mid x \wedge 4 \nmid x$**:** entonces

$$2^{s-1} \mid x + 2 \Leftrightarrow x + 2 \equiv 0 \pmod{2^{s-1}} \Leftrightarrow x \equiv -2 \pmod{2^{s-1}} \Leftrightarrow n \equiv 1 \pmod{2^{s-1}}$$

$$\Leftrightarrow n \equiv 1, (1 + 2^{s-1}) \pmod{2^s}$$

Si $2 \mid x + 2 \wedge 4 \nmid x + 2$**:** entonces

$$2^{s-1} \mid x \Leftrightarrow x \equiv 0 \pmod{2^{s-1}} \Leftrightarrow n \equiv 3 \pmod{2^{s-1}}$$

$$\Leftrightarrow n \equiv 3, (3 + 2^{s-1}) \pmod{2^s}$$

Si $4 \mid x \wedge 4 \mid x+2$**:** imposible!

Las soluciones entonces son

$$n \equiv 1, 3, (1+2^{s-1}), (3+2^{s-1}) \pmod{2^s} \Leftrightarrow n \equiv 1, 3 \pmod{2^{s-1}}$$

Así tenemos:

$$\begin{cases} n \equiv 1, 3 & \pmod{2^{s-1}} \\ n \equiv 1, 3, 8, 31 & \pmod{35} \end{cases}$$

con el teorema chino del resto, sacamos las 8 soluciones $\pmod{2^{s-1} \times 35}$ y las levantamos $\pmod{2^r \times 35}$ sumando $2^{s-1} \times 35h$, donde $h = 0, ..., 15$.
Tenemos 2^7 soluciones.

2.5 Encontrar las soluciones en el caso $s > 2 \leftrightarrow r > 5$

En general, si tenemos $m_1, m_2 \in \mathbb{N}$ tales que $(m_1, m_2) = 1$, y tenemos $k_1, k_2 \in \mathbb{Z}$, por el teorema chino de los restos, el sistema de congruencias

$$\begin{cases} x \equiv k_1 \pmod{m_1} \\ x \equiv k_2 \pmod{m_2} \end{cases}$$

tiene exactamente una solución $\pmod{m_1 m_2}$.
Por la identidad de Bezout, existen dos números $a, b \in \mathbb{Z}$ tales que

$$am_1 + bm_2 = 1$$

Notamos que

$$am_1 \equiv 1 \pmod{m_2}$$

$$bm_2 \equiv 1 \pmod{m_1}$$

Entonces se verifica que la solucion buscada será

$$x \equiv k_2 a m_1 + k_1 b m_2 \pmod{m_1 m_2}$$

Hemos visto que, para solucionar el nuestro problema, simplemente tenemos que encontrar a y b que verifiquen la identidad de Bezout. Como $am_1 \equiv 1 \pmod{m_2}$, a es el inverso de m_1 en $\mathbb{Z}/m_2\mathbb{Z}$. Entonces, si $m_1 = 2^{s-1}, m_2 = 35$, en $\mathbb{Z}/35\mathbb{Z}$ tenemos

$$a = \left(2^{s-1}\right)^{-1} = \left(2^{-1}\right)^{s-1} = 18^{s-1} = 18^{r-4}$$

Ahora podemos sacar b por substitución:

$$b = \frac{1 - am_1}{m_2} = \frac{1 - 18^{s-1} \times 2^{s-1}}{35} = \frac{1 - 36^{s-1}}{35} = \frac{1 - 36^{r-4}}{35}$$

Tenemos entonces todos los elementos para definir las soluciones:

$$S_r = 36^{r-4}\{1, 3, 8, 31\} + \left(1 - 36^{r-4}\right)\{1, 3\} + \left(2^{r-4} \times 35\right) h$$

donde $h = 0, ..., 15$.