Reto 3

Carlos Quesada

1. Solución

Para la ecuación:

$$8n^2 - 32n + 24 \equiv 0 \ \ mod(35 \cdot 2^r)$$

La cantidad de soluciones según el valor de r es:

$r = 1 \rightarrow 8$ soluciones
$r = 2 \rightarrow 16$ soluciones
$r = 3 \rightarrow 32$ soluciones
$r = 4 \rightarrow 32$ soluciones
$r = 5 \rightarrow 64$ soluciones
$r \geq 6 \rightarrow 128$ soluciones

y las soluciones en concreto son:

$r \leqslant 3 \rightarrow x = \{1, 3, 8, 31\} + 35k$ con $k \in \{0, 2^r - 1\}$

$r \in \{4, 5\} \rightarrow x = \{1, 3, 31, 43\} + 70k$ con $k \in \{0, 2^{r-1} - 1\}$

$$r \geqslant 6 \rightarrow x = \{1, 3, 3 - 2 \cdot 36^{r-4}, 1 + 2 \cdot 36^{r-4}, 1 + 7 \cdot 36^{r-4}, 3 + 5 \cdot 36^{r-4}$$
$$1 + 30 \cdot 36^{r-4}, 3 + 28 \cdot 36^{r-4}\} + 35 \cdot 2^{r-4}k \text{ con } k \in \{0, \ldots, 15\}$$

2. Demostración

Lo primero que se observa es que la ecuación se puede expresar como:

$$8 \cdot (n-1)(n-3) \equiv 0 \ \ mod(2^r \cdot 35)$$

Vemos que para conocer las soluciones tenemos primero que resolver la ecuación para módulo 5, para módulo 7 y para módulo 2, y en este último caso ir subiendo las soluciones con Hensel. La solución final sera la combinación de todas ellas con el teorema chino del resto. Entonces sólo quedará demostrar que efectivamente esas son todas las soluciones, es decir que no hay ninguna que no nos venga dada por Hensel.
Empecemos por lo fácil, módulo 5 tenemos:

$$3 \cdot (n-1)(n-3) \equiv 0 \ \ mod(5)$$

y comprobando todos los valores de n entre 0 y 4 (ambos incluidos), vemos que sólo se cumple para n=1,3. Procediendo de la misma manera para módulo 7, obtenemos $(n-1)(n-3) \equiv 0 mod(7)$, que de nuevo tiene soluciones sólo para n=1,3.
Pasamos así al caso 2, sin duda el más complicado. Si r es menor o igual que 3, tenemos las ecuaciones:

$$8 \cdot (n-1)(n-3) \equiv 0 \ \ mod(2)$$

$$8 \cdot (n-1)(n-3) \equiv 0 \ \ mod(4)$$

$$8 \cdot (n-1)(n-3) \equiv 0 \ \ mod(8)$$

En todas ellas el módulo es un divisor de 8, lo cual hace que todo el lado izquierdo de la igualdad se anule, provocando así que para todo n, n sea solución. Por tanto las soluciones a la ecuación módulo 2, 4 y 8 son $\{0,1\}$, $\{0,1,2,3\}$ y $\{0,1,2,3,4,5,6,7\}$ respectivamente.
Para r=4, esto es, módulo 16, la ecuación también se simplifica, quedando:

$$8(n^2+3) \equiv 0 \ \ mod(16)$$

la ecuación tiene solución si y solo si n^2+3 es un número par. Esto ocurre cuando n^2 es un número impar, ya que un número impar mas(o menos) otro número impar, es par. Y para que n^2 sea impar, n ha de ser impar también. Esto quiere decir que las soluciones son los números impares menores que 16, es decir $\{1,3,5,7,9,11,13,15\}$.

A partir de r=5 no se pueden hacer simplificaciones de este estilo, y hay que trabajar directamente con Hensel. Los 4 pasos anteriores por supuesto podrían haberse hecho también por Hensel, pero me parecía mas bonito, rápido y variado hacerlo de esta forma. El lema dice que si tenemos una raíz a para un p^r, y $f'(a) \equiv 0 \ mod(p)$, entonces si $f(a) \equiv 0 \ mod(p^{r+1})$, a sube a otras p raíces. Como en nuestro caso p es dos, si se cumplen estas condiciones, cada raíz sube a dos raíces. Dadas las características de nuestro problema, la condición sobre la derivada siempre se cumple ya que:

$$f'(n) = 16n - 32 = 2 \cdot (8n - 16) \equiv 0 \ mod(2) \ \forall n \in Z$$

así que sólo queda ver cuales de las raíces de p^r suben a p^{r+1}. Las raíces que subirán(en todos los casos) son las congruentes con 1 ó 3 módulo(2^{r-4}). Parece un número arbitrario, pero en el fondo tiene total sentido. Lo demostraré por inducción:

Caso 1(paso de 2^4 a 2^5) Como sabemos que son raíces módulo 16 tenemos que:

$$8 \cdot (n-1)(n-3) = 16 \cdot k \Rightarrow (n-1) \cdot (n-3) = 2 \cdot k$$

Buscamos entre ellas las que también lo sean módulo 32, esto es:

$$8 \cdot (n-1)(n-3) = 32 \cdot l \Rightarrow (n-1) \cdot (n-3) = 4 \cdot l$$

Éste, es un caso un poco particular, porque 1 y 3 es lo mismo módulo 2, pero en cualquier caso se cumple que los n que son solución módulo 4 son los congruentes con 1 y 3 módulo 2 (que efectivamente es 2^{5-4}).

Caso inducción(paso de 2^{r-1} a 2^r) Como sabemos que son raíces módulo 2^{r-1} tenemos que:

$$8 \cdot (n-1)(n-3) = 2^{r-1} \cdot k \Rightarrow (n-1)(n-3) = 2^{r-4} \cdot k$$

Buscamos entre ellas las que también lo sean módulo 2^r, esto es:

$$8 \cdot (n-1)(n-3) = 2^r \cdot l \Rightarrow (n-1)(n-3) = 2^{r-3} \cdot l$$

Es claro que los números de la forma $n \equiv 1, 3 \ mod(2^{r-3})$ son soluciones del problema. Lo son trivialmente para la segunda ecuación y por tanto lo son para la primera(basta tomar $k = 2 \cdot l$). Pero veamos que hay más. Los siguientes números que parece lógico tomar son los de la forma $n \equiv 1, 3 \ mod(2^{r-4})$, ya que eran soluciones en el paso anterior. Tomemos en

concreto $n \equiv 1 \ mod(2^{r-4})$. Si lo sustituimos en la segunda ecuación obtenemos que $n-1$ es un número de la forma $2^{r-4} \cdot a$ y $n-3$ es número par, ya que n es impar, e impar menos impar es par. Así obtenemos:

$$2^{r-4} \cdot a \cdot 2 \cdot b \equiv 2^{r-3} \cdot l$$

Basta tomar $l = a \cdot b$ (que podemos ya que son enteros) y nuestra igualdad se cumple. Operando de la misma forma para $n \equiv 3 \ mod(2^{r-4})$ vemos que éstos n's también son solución.

Veamos porqué no hay más soluciones que estas. Si dos números a y b cumplen $a \cdot b \equiv 0 \ mod(c) \Rightarrow mcd(a,c) \neq 1$ ó $mcd(b,c) \neq 1$. Así en nuestra ecuación $mcd((n-3), 2^{r-3}) \neq 1$ ó $mcd((n-1), 2^{r-3}) \neq 1$. Supongamos que la primera es cierta. En ese caso tenemos que $n-3$ es un número par, esto es: $(n-3) = 2^{r-k} \cdot l$ donde $r > k \geq 3$ y l es un número impar (podría ser el 1). Así $(n-1) = 2 + 2^{r-k} \cdot l$ y obtenemos

$$2^{r-k} \cdot l \cdot (2 + 2^{r-k} \cdot l) = 0 \ mod(2^{r-3}) \Rightarrow$$

$$2^{r-k+1} \cdot (1 + 2^{r-k-1} \cdot l) \cdot l = 0 \ mod(2^{r-3}) \Rightarrow$$

$$2^{r-k+1} \cdot \text{impar} \cdot \text{impar} = 2^{r-3} \cdot m \Rightarrow$$

$$\text{impar} = 2^{k-4} \cdot m \text{ lo cual es imposible}$$

Si tomamos ahora el otro caso, aquel en el que $mcd((n-1), 2^{r-3}) \neq 1$ el razonamiento es exactamente el mismo, por tanto las únicas soluciones a $8 \cdot (n-1)(n-3) \equiv 0 \ mod(2^r)$ son $\{1,3\} mod(2^{r-4})$.

Por tanto tenemos las soluciones para módulos 5, 7 y 2^r. Sólo falta aplicar el teorema chino del resto, y obtendremos el resultado final. Apliquemos primero el teorema a 5 y 7 para todas las soluciones. Obtenemos:

$$x \equiv 1 \ mod(5), x \equiv 1 \ mod(7) \Rightarrow x \equiv 7 \cdot 1 \cdot 3 + 5 \cdot 1 \cdot 3 \equiv 36 \equiv 1 \ mod(35)$$

$$x \equiv 1 \ mod(5), x \equiv 3 \ mod(7) \Rightarrow x \equiv 7 \cdot 3 \cdot 3 + 5 \cdot 1 \cdot 3 \equiv 78 \equiv 8 \ mod(35)$$

$$x \equiv 3 \ mod(5), x \equiv 1 \ mod(7) \Rightarrow x \equiv 7 \cdot 1 \cdot 3 + 5 \cdot 3 \cdot 3 \equiv 66 \equiv 31 \ mod(35)$$

$$x \equiv 3 \ mod(5), x \equiv 3 \ mod(7) \Rightarrow x \equiv 7 \cdot 3 \cdot 3 + 5 \cdot 3 \cdot 3 \equiv 108 \equiv 3 \ mod(35)$$

Por tanto las soluciones son $\{1, 3, 8, 31\} mod(35)$. Hagamos ahora el teorema chino entre 35 y 2^{r-4}, ya que las soluciones módulo 2^r venían en función de 2^{r-4}. Aquí tenemos el problema de que r varía y necesitamos una fórmula general. Primero necesitamos el inverso de 2^r modulo 35 y viceversa. El primero es fácil, tenemos que el inverso de dos es 18, con lo que el de 2^{r-4} es 18^{r-4}. El segundo término es algo más complicado. Sin embargo tengamos en cuenta el primer sistema de ecuaciones:

$$x \equiv 1 \ mod(2^{r-4}), x \equiv 1 \ mod(35)$$

Sabemos trivialmente que la solución es uno, y si aplicamos por otro lado el teorema chino con los datos que ya tenemos podemos despejar el inverso multiplicativo de 35 módulo 2^{r-4}, al que llamaremos i:

$$1 = x = 2^{r-4} \cdot 1 \cdot 18^{r-4} + 35 \cdot 1 \cdot i = 36^{r-4} + 35i \Rightarrow i = \frac{1 - 36^{r-4}}{35}$$

Así ya podemos calcular todas las posibles soluciones:

$$x \equiv 1 \ mod(35), x \equiv 1 \ mod(2^{r-4}) \Rightarrow x = 1 \ mod(35 \cdot 2^{r-4})$$

$x \equiv 1 \ mod(35), x \equiv 3 \ mod(2^{r-4}) \Rightarrow$

$$x \equiv 36^{r-4} \cdot 1 + (1 - 36^{r-4}) \cdot 3 \equiv 3 - 2 \cdot 36^{r-4} \ mod(35 \cdot 2^{r-4})$$

$x \equiv 3 \ mod(35), x \equiv 1 \ mod(2^{r-4}) \Rightarrow$

$$x \equiv 36^{r-4} \cdot 3 + (1 - 36^{r-4}) \cdot 1 \equiv 1 + 2 \cdot 36^{r-4} \ mod(35 \cdot 2^{r-4})$$

$x \equiv 3 \ mod(35), x \equiv 3 \ mod(2^{r-4}) \Rightarrow$

$$x \equiv 36^{r-4} \cdot 3 + (1 - 36^{r-4}) \cdot 3 \equiv 3 \ mod(35 \cdot 2^{r-4})$$

$x \equiv 8 \ mod(35), x \equiv 1 \ mod(2^{r-4}) \Rightarrow$

$$x \equiv 36^{r-4} \cdot 8 + (1 - 36^{r-4}) \cdot 1 \equiv 1 + 7 \cdot 36^{r-4} \ mod(35 \cdot 2^{r-4})$$

$x \equiv 8 \ mod(35), x \equiv 3 \ mod(2^{r-4}) \Rightarrow$

$$x \equiv 36^{r-4} \cdot 8 + (1 - 36^{r-4}) \cdot 3 \equiv 3 + 5 \cdot 36^{r-4} \ mod(35 \cdot 2^{r-4})$$

$x \equiv 31 \ mod(35), x \equiv 1 \ mod(2^{r-4}) \Rightarrow$

$$x \equiv 36^{r-4} \cdot 31 + (1 - 36^{r-4}) \cdot 1 \equiv 1 + 30 \cdot 36^{r-4} \ mod(35 \cdot 2^{r-4})$$

$x \equiv 31 \ mod(35), x \equiv 3 \ mod(2^{r-4}) \Rightarrow$

$$x \equiv 36^{r-4} \cdot 31 + (1 - 36^{r-4}) \cdot 3 \equiv 3 + 28 \cdot 36^{r-4} \ mod(35 \cdot 2^{r-4})$$

Por último adjunto un programa escrito en SAGE que resuelve ele ejercicio, para r dados, y que me ayudo a calcular los valores, y a empezar con el problema:

```
for i in range(5,13):
  m=(2^i)
  solucion=[]
  print'para modulo=%s i=%s'%(m,i)
  for j in range(1,m):
    if (8*(j^2)-32*j+24)%m==0:
       solucion.append(j)
  print(solucion)
```