Problema 6 de la hoja 5

Lo más importante, y posiblemente la dificultad de este ejercicio, es pensar cómo dividimos habitualmente con la "división larga" e interpretarlo en términos de congruencias. Por eso antes de resolver el problema veamos como ejemplo la división de 1 entre 7:

$$\begin{array}{rcccccc|l} \mathbf{1} & 0 & & & & & 7 \\ \cline{7-7} & 3 & 0 & & & & 0.142857\ldots \\ & & 2 & 0 & & & \\ & & & 6 & 0 & & \\ & & & & 4 & 0 & \\ & & & & & 5 & 0 \\ & & & & & & 1 \end{array}$$

Digamos que el dividendo de partida, el 1 (en negrita), es el resto cero $r_0 = 1 = 10^0$. Para el siguiente resto, $r_1 = 3$ lo que hemos hecho es bajar un cero, es decir, considerar 10 en lugar de 1 y hallar el resto, por tanto $r_1 \equiv 10^1 \pmod 7$. De la misma forma para $r_2 = 2$ hemos bajado otro cero, esto es $r_2 \equiv 10r_1 \equiv 10^2 \pmod 7$. En general, el n-ésimo resto al dividir 1 entre m viene dado por la fórmula

$$\boxed{r_n \equiv 10^n \pmod m}$$

Insisto en que posiblemente la dificultad del ejercicio esté aquí porque normalmente dividimos sin pararnos a pensar por qué lo hacemos así.

Solución del ejercicio 6. Las condiciones sobre m se pueden parafrasear diciendo que m y 10 son coprimos.

a) Según la congruencia de Euler-Fermat, $10^{\varphi(m)} \equiv 1 \pmod m$. Por tanto, $r_n = r_{n+\varphi(m)}$. Si algo se repite cada P veces, entonces P debe ser múltiplo de su periodo (mínimo). Por ejemplo, si cada 14 días es lunes el periodo de los lunes divide a 14. En nuestro caso el periodo debe dividir a $\varphi(m)$.

b) Según el apartado anterior, $n-1 \mid \varphi(n)$. Si n tiene más de un factor primo, digamos $p_1, p_2, \ldots$, entonces $\varphi(n) = n\prod_{p|n}\big(1-1/p\big) < n\big(1-1/p_1\big) < n-1$ y se llega a una contradicción. Por consiguiente $n = p^k$. Para $k > 1$ también se tiene $\varphi(n) < n-1$.

c) [bastante difícil] Si tiene periodo $p-1$, las potencias $10^1, 10^2, \ldots, 10^{p-1}$ dejan restos distintos módulo p. El resto $r_{(p-1)/2}$ cumple $r^2_{(p-1)/2} \equiv 10^{p-1} \equiv 1 \pmod p$ y además sabemos que no es 1 (porque el periodo es $p-1$), por tanto $r_{(p-1)/2} \equiv 10^{(p-1)/2} \equiv -1$

(mód p). Aquí se ha usado que $x^2 \equiv 1 \pmod{p}$ implica $p \mid (x-1)(x+1)$ y por tanto $x \equiv \pm 1 \pmod{p}$.

A partir de $10^{(p-1)/2} \equiv -1 \pmod{p}$ y de la fórmula para los restos, recordando que están entre 0 y p, se deduce $r_{n+(p-1)/2} = p - r_n$. Ahora bien, la n-ésima cifra decimal la calculamos bajando un 0 y dividiendo entre p, es decir, con $c_n = [10r_n/p]$ donde $[\cdot]$ indica la parte entera. Hay que comprobar $c_n + c_{n+(p-1)/2} = 9$, que según lo anterior se traduce en $[10r_n/p] + [10 - 10r_n/p] = 9$ lo cual es cierto porque es fácil ver que $[10-u] = 9 - [u]$ para todo $u \in [0,10] - \mathbb{Z}$.