Algunos problemas resueltos de la hoja 4

---

7) Escribamos $p = 2^n - 1$, entonces el número de partida es $N = 2^{n-1}p$. Sus divisores son potencias de dos o potencias de 2 por p. Entonces la suma de los divisores menores que N viene dada por:

$$1 + 2 + 2^2 + \cdots + 2^{n-2} + 2^{n-1} + p + 2p + 2^2p + \cdots + 2^{n-2}p.$$

Agrupando, se tiene

$$\big(1 + 2 + 2^2 + \cdots + 2^{n-2}\big)(1 + p) + 2^{n-1}.$$

El primer paréntesis es la suma de una progresión geométrica. Empleando la fórmula, vale $2^{n-1} - 1$. Operando, se obtiene que la expresión anterior es $2^{n-1}p + 2^n - 1 - p$ que coincide con N porque $p = 2^n - 1$.

---

14) Módulo 8, un cuadrado es siempre congruente con alguno de los números 0^2, 1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2. Operando se obtienen, módulo 8, sólo tres resultados distintos: 0, 1 y 4. Sumando tres números del conjunto $\{0, 1, 4\}$ no obtenemos nunca 7 módulo 8, es decir, $a^2 + b^2 + c^2 \equiv 7 \pmod 8$ no tiene solución en enteros. De aquí, ningún número de la forma $8n + 7$ se puede escribir como suma de tres cuadrados.

---

20) El objetivo del problema es deducir $(p-1)! \equiv -1 \pmod p$ para p primo.

a) Por Bézout, $ax + py = 1$ tiene solución y de aquí $ax \equiv 1 \pmod p$ también la tiene. Esto es lo mismo que la existencia del inverso en $\mathbb{Z}_p$. La unicidad es fácil, ya que, si hubiera otra, $ay \equiv 1 \pmod p$, restando se tendría $a(x - y) \equiv 0 \pmod p$, o lo que es lo mismo $p \mid x - y$ y $x \equiv y \pmod p$.

b) Con rigor, debería decir $a \not\equiv 1, p-1 \pmod p$ y que la no igualdad es también módulo p. Si fuera $a \equiv x$, entonces $a^2 \equiv 1$. Equivalentemente, $p \mid a^2 - 1 = (a-1)(a+1)$. Así pues $a \equiv \pm 1 \pmod p$.

c) Por el apartado anterior, $\overline{1}$ y $\overline{p-1}$ son los únicos que coinciden con sus inversos en $\mathcal{U}(\mathbb{Z}_p)$. Entonces para cualquier $k \in \{2, 3, \ldots, p-2\}$, existe $k' \neq k$ en este mismo conjunto tal que $kk' \equiv 1 \pmod p$. De ello se deduce $2 \cdot 3 \cdots (p-2) \equiv 1 \pmod p$.

Finalmente, para deducir el resultado de Wilson basta notar, aplicando el último apartado, que $(p-1)! = 2 \cdot 3 \cdots (p-2) \cdot (p-1) \equiv 1 \cdot (p-1) \equiv -1 \pmod{p}$.

•) [No es un problema sino una duda aparecida en clase] ¿Puede existir una función inyectiva $f : X \longrightarrow Y$ cuando $Y \subsetneq X$?

La respuesta es que sí, para conjuntos infinitos. Por ejemplo $f : \mathbb{R} \longrightarrow \mathbb{R}^+$ dada por $f(x) = e^x$ es inyectiva (de hecho biyectiva). Otro ejemplo un poco más simple es $f : [0,4] \longrightarrow [0,3]$ dada por $f(x) = x/2$.

A continuación hay otros problemas que no se han hecho en las sesiones de problemas

---

1) [Relacionado con la duda anterior] Consideremos las inclusiones $f : A \longrightarrow B$ y $g : B \longrightarrow C$ que por supuesto son inyectivas. Por ser A y C equipotentes, existe una biyección $h : A \longrightarrow C$. Entonces $f : A \longrightarrow B$ y $h^{-1} \circ g : B \longrightarrow A$ son funciones inyectivas entre A y B en los dos sentidos y por el teorema de Cantor-Berstein-Schröder, B y A son equipotentes. Por al transitiva, B y C también lo son.

---

3) Sea n el menor entero estrictamente positivo de S. Si no existiera, por la segunda propiedad, se debe tener $S = \{0\}$. Excluyendo este caso, la primera propiedad asegura $n\mathbb{Z}^+ \subset S$ y la segunda $n\mathbb{Z} \subset S$. Si $n\mathbb{Z} \neq S$ sea $m \in S - n\mathbb{Z}$, entonces $0 < m - [m/n]n < n$ y por la segunda y la primera propiedad $m - [m/n]n \in S$, lo que contradice que n sea mínimo.

---

4) Al ser coprimos, $ax + by = m$ tiene solución. También por ser coprimos, $a \mid m \Rightarrow a \mid y$ y $b \mid m \Rightarrow b \mid x$. Entonces $x = bx'$ y $y = ay'$, que implican $ab(x' + y') = m$.

Tomando $a = 15$ y $b = 6$, que no son coprimos, con $m = 30$ se tiene $a \mid m$ y $b \mid m$ pero $ab \nmid m$.

---

11) Para este problema hay que recordar la fórmula de los números combinatorios:

$$\binom{p}{k} = \frac{p!}{(p-k)!k!}.$$

i) Si $1 \leq k \leq p-1$ entonces $p-k$ y k son menores que p, por tanto p divide al numerador pero no al numerador. Si no es primo, no es cierto, por ejemplo $4 \nmid \binom{4}{2}$. La razón es que si p no es primo puede haber factores en $(p-k)!$ y $k!$ que al ser multiplicados den p.

ii) Utilizando el binomio de Newton,

$$\left(\overline{a}+\overline{b}\right)^p = \overline{a}^p + \sum_{k=1}^{p-1} \binom{p}{k} \overline{a}^{p-k}\overline{b}^k + \overline{b}^p = \overline{a}^p + \overline{b}^p.$$

---

16) Para abreviar, escribamos $(n)_m^{-1}$ el inverso de n módulo m. Entonces según la fórmula que aparece en el teorema chino de los restos, se tiene la solución única módulo $4 \cdot 3 \cdot 7 = 84$ dada por

$$x \equiv 1 \cdot (3 \cdot 7)(3 \cdot 7)_4^{-1} + 2 \cdot (4 \cdot 7)(4 \cdot 7)_3^{-1} + 3 \cdot (4 \cdot 3)(4 \cdot 3)_7^{-1} \pmod{84}.$$

Sustituyendo el cálculo de los inversos, $\overline{21}^{-1} = \overline{1}$ en $\mathbb{Z}_4$, $\overline{28}^{-1} = \overline{1}$ en $\mathbb{Z}_3$ y $\overline{12}^{-1} = \overline{3}$ en $\mathbb{Z}_7$, se llega a $x \equiv 21 + 25 + 108 \pmod{84}$ que sumando y reduciendo el resultado, da $x \equiv 17 \pmod{84}$.
