Ejercicios sobre congruencias

6 de marzo de 2017

Ejercicio 1. *Fijemos algún $n = 1, 2, 3, 4, \ldots$ Consideremos la siguiente relación sobre los números enteros: se dice que x es **congruente a** y **módulo** n si n divide a $x - y$:*

$$x \equiv y \pmod{n} \Leftrightarrow n \mid (x - y).$$

En otras palabras, x e y tienen el mismo resto de la división por n.

Demuestre que la congruencia módulo n es una relación de equivalencia sobre $\mathbb{Z}$; es decir, para todo $x, y, z \in \mathbb{Z}$

$$x \equiv x, \quad x \equiv y \Rightarrow y \equiv x, \quad x \equiv y \, e \, y \equiv z \Rightarrow x \equiv z.$$

Solución (Martha). Obviamente, $n \mid x - x = 0$ para todo x. Luego, $n \mid (x - y)$ si y solamente si $n \mid (y - x)$. Por fin, si $n \mid (x - y)$ y $n \mid (y - z)$, entonces

$$n \mid (x - y) + (y - z) = x - z.$$

■

Las clases de equivalencia se llaman los **residuos módulo** n. La clase de equivalencia de x se denota por $[x]$. Note que hay n residuos diferentes: $[0]$, $[1]$, $[2]$, $\ldots$, $[n-1]$.

Ejercicio 2. *Demuestre que si $x \equiv x'$, $y \equiv y'$, entonces*

$$x + y \equiv x' + y',$$
$$x \cdot y \equiv x' \cdot y'.$$

Esto quiere decir que la adición y multiplicación tiene sentido para residuos módulo n: podemos definir

$$[x] + [y] := [x + y], \tag{1}$$
$$[x] \cdot [y] := [x \cdot y]. \tag{2}$$

Solución (Javier). Si $n \mid x - x'$ y $n \mid y - y'$, entonces

$$n \mid (x - x') + (y - y') = (x + y) - (x' - y'),$$

y también

$$n \mid (x - x')\, y + x' \,(y - y') = xy - x'y'.$$

Para ver que las definiciones (1) y (2) tienen sentido (no dependen de los representantes particulares de las clases de equivalencia), tenemos que verificar que si $[x] = [x']$ y $[y] = [y']$, entonces

$$[x + y] = [x' + y'],$$
$$[x \cdot y] = [x' \cdot y'].$$

Es lo que acabamos de demostrar. ■

Ejercicio 3. *Demuestre que tiene sentido la cancelación módulo p: si tenemos*

$$x \cdot y \equiv x \cdot y' \pmod{p},$$

donde $p \nmid x$, entonces $y \equiv y' \pmod{p}$.

Indicación: si p es primo, entonces $p \mid xy$ implica $p \mid x$ o $p \mid y$.

Solución (Raúl). $x \cdot y \equiv x \cdot y' \pmod{p}$ significa que $p \mid (x \cdot y - x \cdot y') = x \cdot (y - y')$. Pero $p \nmid x$, y por lo tanto $p \mid (y - y')$. ■

Ejercicio 4. *Sea p un número primo. Demuestre que los coeficientes binomiales $\binom{p}{1}, \binom{p}{2}, \ldots, \binom{p}{p-1}$ son divisibles por p:*

$$p \mid \binom{p}{i} = \frac{p!}{i!\,(p-i)!} \quad \text{para } i = 1, 2, \ldots, p-1.$$

Para $i = 0, p$ tenemos $\binom{p}{0} = \binom{p}{p} = 1$.

$$\begin{array}{ccccccccccccc}
 & & & & & & \binom{0}{0}=1 & & & & & & \\
 & & & & & \binom{1}{0}=1 & & \binom{1}{1}=1 & & & & & \\
 & & & & \binom{2}{0}=1 & & \binom{2}{1}=2 & & \binom{2}{2}=1 & & & & \\
 & & & \binom{3}{0}=1 & & \binom{3}{1}=3 & & \binom{3}{2}=3 & & \binom{3}{3}=1 & & & \\
 & & \binom{4}{0}=1 & & \binom{4}{1}=4 & & \binom{4}{2}=6 & & \binom{4}{3}=4 & & \binom{4}{4}=1 & & \\
 & \binom{5}{0}=1 & & \binom{5}{1}=5 & & \binom{5}{2}=10 & & \binom{5}{3}=10 & & \binom{5}{4}=5 & & \binom{5}{5}=1 & \\
\binom{6}{0}=1 & & \binom{6}{1}=6 & & \binom{6}{2}=15 & & \binom{6}{3}=20 & & \binom{6}{4}=15 & & \binom{6}{5}=6 & & \binom{6}{6}=1 \\
\binom{7}{0}=1 & & \binom{7}{1}=7 & & \binom{7}{2}=21 & & \binom{7}{3}=35 & & \binom{7}{4}=35 & & \binom{7}{5}=21 & & \binom{7}{6}=7 \quad \binom{7}{7}=1
\end{array}$$

Solución (Ariel). Para $i = 1, 2, \ldots, p-1$ en el número

$$\binom{p}{i} = \frac{p\,(p-1)\,(p-2)\cdots(p-i+1)}{i!}$$

p aparece en el numerador, pero $p \nmid i!$, y por lo tanto $p \mid \binom{p}{i}$. ■

Ejercicio 5. *Demuestre que $\binom{p-1}{i} \equiv (-1)^i \pmod{p}$.*

Por ejemplo, $\binom{6}{3} = 20 \equiv 6 \equiv -1 \pmod{7}$ y $\binom{6}{2} = 15 \equiv 1 \pmod{7}$.
Indicación: del ejercicio 4 sabemos que $\binom{p}{i} \equiv 0 \pmod{p}$ para $i = 1, 2, \ldots, p-1$; luego, use la relación de Pascal $\binom{p}{i} = \binom{p-1}{i} + \binom{p-1}{i-1}$.

Primera solución (Dennis). Vamos a usar la existencia de elementos inversos módulo p (véase abajo). Para $i = 0$ la fórmula es evidente: $\binom{p-1}{0} = 1$. Para $i \neq 0$, tenemos

$$\binom{p-1}{i} = \frac{(p-1)\,(p-2)\cdots(p-i)}{i!},$$

donde módulo p,

$$i! = 1 \cdot 2 \cdot 3 \cdots i \equiv (1-p)\,(2-p)\cdots(i-p) = (-1)^i\,(p-1)\,(p-2)\cdots(p-i),$$

así que

$$\binom{p-1}{i} = \frac{(p-1)(p-2)\cdots(p-i)}{i!} \equiv \frac{\cancel{(p-1)}\cancel{(p-2)}\cdots\cancel{(p-i)}}{(-1)^i\cancel{(p-1)}\cancel{(p-2)}\cdots\cancel{(p-i)}} = (-1)^i.$$

■

Segunda solución. El valor inicial es

$$\binom{p-1}{0} = 1.$$

Luego, para $i = 1, \ldots, p-1$ tenemos

$$\binom{p-1}{i} + \binom{p-1}{i-1} = \binom{p}{i} \equiv 0 \pmod{p},$$

es decir,

$$\begin{aligned}
\binom{p-1}{1} &\equiv -\binom{p-1}{0} \equiv -1 \pmod{p},\\
\binom{p-1}{2} &\equiv -\binom{p-1}{1} \equiv +1 \pmod{p},\\
&\cdots\\
\binom{p-1}{i} &\equiv (-1)^i \pmod{p}.
\end{aligned}$$

■

Ejercicio 6. *Demuestre* ***el teorema del binomio módulo*** *p: para p primo se tiene*

$$(x+y)^p \equiv x^p + y^p \pmod{p}.$$

Por ejemplo, $(2+2)^3 = 64 \equiv 1 \pmod 3$ y $2^3 + 2^3 = 16 \equiv 1 \pmod 3$.
Indicación: use el ejercicio 4.

Solución (Alejandra). El teorema del binomio nos dice que

$$(x+y)^p = \sum_{0 \le i \le p} \binom{p}{i} x^{p-i} y^i,$$

pero módulo p los coeficientes $\binom{p}{i}$ son nulos, excepto $\binom{p}{0} = \binom{p}{p} = 1$. ■

Ejercicio 7. *Demuestre el* ***pequeño teorema de Fermat****: para todo $x \in \mathbb{Z}$ se tiene*

$$x^p \equiv x \pmod{p};$$

y si $p \nmid x$, entonces $x^{p-1} \equiv 1 \pmod p$.

Por ejemplo, $2^3 = 8 \equiv 2 \pmod 3$, $2^2 = 4 \equiv 1 \pmod 3$.
Indicación: podemos suponer que la clase de equivalencia $[x]$ representada por algún número $x = 0, 1, 2, \ldots, p-1$. Si $x = 0$, el resultado está claro. Demuestre el paso de inducción: si $[x]^p = [x]$, entonces $[x+1]^p = [x+1]$.

Primera solución (Martha). Vamos a usar el siguiente
Lema. Si $p \nmid x$, entonces los múltiplos de $[x]$ nos dan todos los residuos módulo p:

$$\{[0\cdot x],\ [1\cdot x],\ [2\,x],\ \ldots,\ [(p-1)\,x]\} = \{[0],\ [1],\ \ldots,\ [p-1]\}.$$

Efectivamente, tenemos que ver que los residuos $[n\,x]$ son diferentes para $n = 0, 1, \ldots, p-1$. Y de hecho, si $[m\,x] = [n\,x]$, entonces $[m] = [n]$ por la propiedad de cancelación (ejercicio 3).

Ahora por este lema, si $p \nmid x$, entonces

$$x\cdot(2\,x)\cdots(p-1)\,x = (p-1)!\,x^{p-1} \equiv 1\cdot 2\cdots(p-1) = (p-1)! \pmod p.$$

Luego, $p \nmid (p-1)!$, así que podemos cancelar $(p-1)!$ y concluir que

$$x^{p-1} \equiv 1 \pmod p.$$

Multiplicando esta identidad por x, tenemos

$$x^p \equiv x \pmod p.$$

Si $p \mid x$, es decir $x \equiv 0 \pmod p$, entonces la identidad

$$x^p \equiv x \pmod p$$

es evidente ($0^p = 0$). ■

Segunda solución. En efecto, $0^p = 0$. Luego, el paso de inducción es (usando el ejercicio anterior)

$$[x+1]^p = [(x+1)^p] = [x^p + 1^p] = [x^p] + [1] = [x]^p + [1] = [x] + [1] = [x+1].$$

Si $p \nmid x$, entonces $x^p \equiv x \pmod p$ implica $x^{p-1} \equiv 1$ gracias al ejercicio 3. ■

Ejercicio 8. *Demuestre que si $p \nmid x$, entonces existe $y \in \mathbb{Z}$ (definido de modo único módulo p) tal que $x\,y \equiv 1 \pmod p$. En este caso escribimos $[x]^{-1} = [y]$.*

Indicación: use el ejercicio 7.

Solución. Si $p \nmid x$, entonces $x^{p-1} = x\cdot x^{p-2} \equiv 1 \pmod p$, así que x^{p-2} es inverso a x módulo p.

Para ver que el inverso es único módulo p, notamos que $x\,y \equiv 1$, $x\,y' \equiv 1$ implica $y \equiv y'$ por la propiedad de cancelación. ■

Otra solución. Por el **Lema** de arriba, si $p \nmid x$, entonces la multiplicación por $[x]$ nos da una biyección

$$\begin{aligned}\text{residuos módulo } p &\to \text{residuos módulo } p,\\ [y] &\mapsto [y]\cdot[x].\end{aligned}$$

En particular, para el residuo $[1]$ existe único $[y]$ tal que $[y]\cdot[x] = 1$. ■

Ejercicio 9. *1) Demuestre que $1 + 2 + 3 + \cdots + (p-1) \equiv 0 \pmod p$ para $p \neq 2$.*

Por ejemplo, $1 + 2 + 3 + 4 = 10 \equiv 0 \pmod 5$.

2) Demuestre que $1^2 + 2^2 + 3^2 + \cdots + (p-1)^2 \equiv 0 \pmod p$ para $p \neq 2, 3$.

Por ejemplo, $1^2 + 2^2 + 3^2 + 4^2 = 30 \equiv 0 \pmod 5$.

3) *Demuestre que* $1^3 + 2^3 + 3^3 + \cdots + (p-1)^3 \equiv 0 \pmod{p}$ *para* $p \neq 2$.
Por ejemplo, $1^3 + 2^3 + 3^3 + 4^3 = 100 \equiv 0 \pmod{5}$.

4) *En general, dado k fijo, ¿para cuáles p se va a cumplir* $1^k + 2^k + 3^k + \cdots + (p-1)^k \equiv 0 \pmod{p}$*?*

Solución. En 1), como notó Gauss cuando estudiaba en la primaria, tenemos

$$1 + 2 + 3 + \cdots + (p-1) = (1 + (p-1)) + (2 + (p-2)) + (3 + (p-3)) + \cdots,$$

que es visiblemente divisible por p.

En 2), Dennis nos recordó la fórmula

$$1^2 + 2^2 + 3^2 + \cdots + p^2 = \frac{p\,(p+1)\,(2p+1)}{6}.$$

Si $p \nmid 6$, entonces esta fórmula implica que la suma de cuadrados es divisible por p.

En general, para $S_k(n) := \sum_{0 \leq i \leq n} i^k$ y $k = 1, 2, 3, 4, \ldots$ tenemos fórmulas

$$\begin{aligned} S_1(n) &= \frac{1}{2}\,n^2 + \frac{1}{2}\,n, \\ S_2(n) &= \frac{1}{3}\,n^3 + \frac{1}{2}\,n^2 + \frac{1}{6}\,n, \\ S_3(n) &= \frac{1}{4}\,n^4 + \frac{1}{2}\,n^3 + \frac{1}{4}\,n^2, \\ &\cdots \end{aligned}$$

(véase mi primera lección). Cuando p no aparece en los denominadores, las fórmulas de arriba nos dicen que la suma es divisible por p (el término constante de $S_k(n)$ es siempre nulo). En general, se puede analizar la expresión

$$S_k(n) = \frac{1}{k+1} \sum_{0 \leq i \leq k} \binom{k+1}{i} B_i\, n^{k+1-i}$$

y ver cuáles números primos aparecen en los denominadores. ■

Se dice que un número x es una **raíz primitiva de la unidad módulo** p si las potencias de x nos dan todos los residuos no nulos módulo p:

$$\{[x],\ [x]^2,\ [x]^3,\ [x]^4, \ldots\} = \{[1],\ [2],\ [3],\ \ldots,\ [p-1]\}.$$

Por ejemplo, 2 es una raíz primitiva de la unidad módulo 5:

$$\{[2],\ [2]^2,\ [2]^3,\ [2]^4\} = \{[2],\ [4],\ [8],\ [16]\} = \{[2],\ [4],\ [3],\ [1]\}$$

Módulo todo número primo p existen raíces primitivas de la unidad, pero no es algo obvio y por el momento podemos aceptar este resultado (esto se demuestra en cursos de álgebra).

Ejercicio 10. *Si x es un número entero tal que $p \nmid x$, entonces el* ***orden de x módulo p*** *es el mínimo número natural positivo $k = 1, 2, 3, 4, \ldots$ tal que $x^k \equiv 1 \pmod{p}$. En este caso escribimos* $\operatorname{ord}_p(x) = k$.

1) *Verifique que* $\operatorname{ord}_p(x) \leq p - 1$ *y que la existencia de raíces primitivas módulo p quiere decir que existe algún x de orden* $p - 1$.

2) *Demuestre que* $x^k \equiv 1 \pmod{p}$ *si y solamente si* $\operatorname{ord}_p(x) \mid k$. *En particular,* $\operatorname{ord}_p(x) \mid p-1$.

Indicación: si $x^k \equiv 1$, *la división con resto nos da* $k = n \operatorname{ord}_p(x) + r$, *donde* $r < \operatorname{ord}_p(x)$.

3) *Demuestre que* $\operatorname{ord}_p(x^k) = \frac{\operatorname{ord}_p(x)}{\operatorname{mcd}(k, \operatorname{ord}_p(x))}$.

4) *Demuestre que*

$$1^k + 2^k + \cdots + (p-1)^k \equiv 0 \pmod{p}$$

si $p - 1 \nmid k$. *Por ejemplo,*

$$1^3 + 2^3 + 3^3 + 4^3 = 100 \equiv 0 \pmod{5}.$$

Indicación: use la existencia de una raíz primitiva de la unidad módulo p.

Solución (Rodrigo, Dennis). $x^{p-1} \equiv 1 \pmod{p}$ por el pequeño teorema de Fermat, así que $\operatorname{ord}_p(x) \leq p-1$. Luego, si $\operatorname{ord}_p(x) = p-1$, las potencias de x módulo p

$$[x],\ [x]^2,\ [x]^3,\ \ldots,\ [x]^{p-1}$$

son diferentes y nos dan todos los restos módulo p (en efecto, si $[x]^m = [x]^n$ para $m > n$, entonces $[x]^{m-n} = [1]$).

En 2), para ver que $x^k \equiv 1 \pmod{p}$ implica $\operatorname{ord}_p(x) \mid k$, podemos usar la división con resto: $k = \operatorname{ord}_p(x) + r$ para algún $0 \leq r < \operatorname{ord}_p(x)$. Luego, $x^k = x^{\operatorname{ord}_p(x)}\, x^r \equiv x^r \equiv 1 \pmod{p}$, pero $\operatorname{ord}_p(x)$ es el mínimo número positivo tal que $x^{\operatorname{ord}_p(x)} \equiv 1 \pmod{p}$ y por lo tanto $r = 0$.

En 3) tenemos por la parte 2)

$$(x^k)^m \equiv 1 \pmod{p} \iff \operatorname{ord}_p(x) \mid km$$
$$\iff \frac{\operatorname{ord}_p(x)}{\operatorname{mcd}(k, \operatorname{ord}_p(x))} \mid \frac{km}{\operatorname{mcd}(k, \operatorname{ord}_p(x))} \iff \frac{\operatorname{ord}_p(x)}{\operatorname{mcd}(k, \operatorname{ord}_p(x))} \mid m.$$

En 4), como sugirió Rodrigo, podemos usar la fórmula para las sumas parciales de la serie geométrica:

$$1 + x^k + x^{2k} + \cdots + x^{(p-1)k} = \frac{1 - (x^k)^p}{1 - x^k}.$$

Módulo p tenemos, gracias al pequeño teorema de Fermat,

$$x^k + x^{2k} + \cdots + x^{(p-1)k} = \frac{1 - (x^k)^p}{1 - x^k} - 1 \equiv \frac{1 - x^k}{1 - x^k} - 1 \equiv 0.$$

Aquí $x^k \not\equiv 1 \pmod{p}$ por nuestra hipótesis $p - 1 \nmid k$. ■