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 $x, y, z \in \mathbb{Z}$

$$x \equiv x, \quad x \equiv y \Rightarrow y \equiv x, \quad x \equiv y \text{ e } y \equiv z \Rightarrow x \equiv z.$$

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*

$$\begin{aligned} x + y &\equiv x' + y', \\ x \cdot y &\equiv x' \cdot y'. \end{aligned}$$

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

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

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

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 $p \mid y$.

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

$$\binom{0}{0} = 1$$

$$\binom{1}{0} = 1 \qquad \binom{1}{1} = 1$$

$$\binom{2}{0} = 1 \qquad \binom{2}{1} = 2 \qquad \binom{2}{2} = 1$$

$$\binom{3}{0} = 1 \qquad \binom{3}{1} = 3 \qquad \binom{3}{2} = 3 \qquad \binom{3}{3} = 1$$

$$\binom{4}{0} = 1 \qquad \binom{4}{1} = 4 \qquad \binom{4}{2} = 6 \qquad \binom{4}{3} = 4 \qquad \binom{4}{4} = 1$$

$$\binom{5}{0} = 1 \qquad \binom{5}{1} = 5 \qquad \binom{5}{2} = 10 \qquad \binom{5}{3} = 10 \qquad \binom{5}{4} = 5 \qquad \binom{5}{5} = 1$$

$$\binom{6}{0} = 1 \qquad \binom{6}{1} = 6 \qquad \binom{6}{2} = 15 \qquad \binom{6}{3} = 20 \qquad \binom{6}{4} = 15 \qquad \binom{6}{5} = 6 \qquad \binom{6}{6} = 1$$

$$\binom{7}{0} = 1 \qquad \binom{7}{1} = 7 \qquad \binom{7}{2} = 21 \qquad \binom{7}{3} = 35 \qquad \binom{7}{4} = 35 \qquad \binom{7}{5} = 21 \qquad \binom{7}{6} = 7 \qquad \binom{7}{7} = 1$$

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* $\binom{p}{i} = \binom{p-1}{i} + \binom{p-1}{i-1}$.

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.

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* $[x+1]^p = [x+1]$.

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

Indicación: use el ejercicio 7.

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* $1^k + 2^k + 3^k + \cdots + (p-1)^k \equiv 0 \pmod{p}$*?*

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 $\operatorname{ord}_p(x) \le p-1$ 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.