

# Aritmética modular

Clase 27

IIC 1253

Prof. Pedro Bahamondes

# Outline

Árboles

Aritmética modular

Teorema de Fermat

Epílogo

# Árboles

Las siguientes definiciones se usan mucho en aplicaciones de los árboles en computación.

## Definición

Sea  $T = (V, E)$  un árbol con raíz  $r$  y  $x$  un vértice cualquiera.

- La **profundidad** de  $x$  es el largo del camino que lo une con  $r$  ( $r$  tiene profundidad 0).
- La **altura** o **profundidad** del árbol es el máximo de las profundidades de sus vértices.
- Los **ancestros** de  $x$  son los vértices que aparecen en el camino entre él y  $r$ . Note que  $x$  es ancestro de sí mismo.
- El **padre** de  $x$  es su ancestro (propio) de mayor profundidad. Diremos que  $x$  es **hijo** de su padre.
- Dos vértices  $x$  e  $y$  con el mismo padre son **hermanos**.

# Árboles binarios

## Definición

Un árbol con raíz se dice **binario** si todo vértice tiene grado a lo más 3; o equivalentemente, si todo vértice tiene a lo más dos hijos.

Podemos distinguir entre hijos izquierdos y derechos

## Teorema

La cantidad de vértices sin hijos de un árbol binario es la cantidad de vértices con exactamente dos hijos más 1.

## Ejercicio

Demuestre el teorema.

# Árboles binarios

## Teorema

La cantidad de vértices sin hijos de un árbol binario es la cantidad de vértices con exactamente dos hijos más 1.

### Demostración:

Por inducción en la cantidad de vértices del árbol binario.

- BI:** El caso base es un árbol compuesto por sólo un vértice, la raíz. Un árbol de estas características tiene sólo una hoja y ningún vértice con dos hijos, luego cumple la propiedad.
- HI:** Supongamos que un árbol binario con  $n$  vértices tiene una hoja más que vértices con dos hijos.
- TI:** Sea  $T$  un árbol binario con  $n + 1$  vértices. Sea  $v$  una hoja de  $T$ , sabemos que  $T - v$  es también un árbol binario y tiene exactamente  $n$  vértices por lo que  $T - v$  cumple con HI, o sea tiene una hoja más que vértices con dos hijos. Supongamos que  $T - v$  tiene  $k$  vértices con dos hijos entonces por HI tiene  $k + 1$  hojas. Lo que podamos decir dependerá de si  $v$  tenía o no un hermano.

# Árboles binarios

- Si  $v$  tiene un hermano en  $T$ , entonces el padre de  $v$  es un vértice con dos hijos en  $T$ . Ahora, en el árbol  $T - v$ , el vértice que era padre de  $v$  tiene sólo un hijo. Lo anterior quiere decir que  $T$  tiene exactamente un vértice más con dos hijos que  $T - v$ , o sea que  $T$  tiene exactamente  $k + 1$  vértices con dos hijos. Ahora también ocurre que  $T$  tiene exactamente una hoja más que  $T - v$ , o sea que  $T$  tiene  $k + 2$  hojas. Hemos concluido que  $T$  tiene  $k + 2$  hojas y  $k + 1$  vértices con dos hijos y por lo tanto cumple con la propiedad.
- Si  $v$  no tiene hermano, entonces el vértice padre de  $v$  en  $T$  se convierte en una hoja en el árbol  $T - v$ , lo que quiere decir que  $T$  y  $T - v$  tienen exactamente la misma cantidad de hojas,  $k + 1$ . El único vértice que ve afectado su cantidad de hijos en  $T - v$  es el padre de  $v$ , este tiene exactamente un hijo en  $T$  y 0 hijos en  $T - v$  por lo que la cantidad de vértices con dos hijos en  $T$  es también la misma que en  $T - v$  e igual a  $k$ . Hemos concluido que  $T$  tiene  $k + 1$  hojas y  $k$  vértices con dos hijos y por lo tanto cumple con la propiedad.

# Árboles binarios

## Teorema

La cantidad de vértices sin hijos de un árbol binario es la cantidad de vértices con exactamente dos hijos más 1.

## Ejercicio

La ANFP está organizando la Copa Chile 2022. Si este año participan  $n$  equipos, ¿cuántos partidos se jugarán?

Respuesta:  $n - 1$

# Árboles binarios

Finalmente, podemos tomar una clase de árboles binarios que se usan mucho para establecer cotas para las aplicaciones de ellos.

## Definición

Un **árbol binario completo** es un árbol binario tal que:

1. Todas las hojas están a la misma profundidad.
2. Todos los vértices que no son hojas tienen exactamente dos hijos.



# Árboles binarios

## Teorema

1. Un árbol binario completo de altura  $H$  tiene exactamente  $2^H$  hojas.
2. Un árbol binario completo de altura  $H$  tiene exactamente  $2^{H+1} - 1$  vértices.
3. Si  $H$  es la altura de un árbol binario completo con  $n$  vértices, entonces  $H \leq \log_2(n)$ .

## Ejercicio

Demuestre el teorema anterior.

# Árboles binarios

## Teorema

Un árbol binario completo de altura  $H$  tiene exactamente  $2^H$  hojas.

### Demostración:

Sea  $T = (V, E)$  un árbol binario completo, demostraremos la propiedad por inducción en la altura  $H$ .

- BI:** Si  $H = 0$  entonces  $T$  corresponde un vértice sin aristas. Luego la cantidad de hojas es igual a  $1 = 2^0 = 2^H$ .
- HI:** Suponemos que todo árbol de altura  $H$  tiene  $2^H$  hojas.
- TI:** Sea  $T$  un árbol de altura  $H + 1$  y raíz  $r$ . Si eliminamos  $r$  del árbol junto con sus aristas incidentes obtenemos un bosque de 2 árboles binarios completos de altura  $H$ . Luego, podemos aplicar la HI, con lo que cada árbol en  $T - r$  tiene  $2^H$  hojas. Es claro que la cantidad de hojas de  $T$  es igual a la suma de todas las hojas de los arboles inducidos al remover  $r$ . Con lo que  $T$  tendrá una cantidad de hojas igual a  $2^H + 2^H = 2 \cdot 2^H = 2^{H+1}$ .

# Árboles binarios

## Teorema

Un árbol binario completo de altura  $H$  tiene exactamente  $2^{H+1} - 1$  vértices.

### Demostración:

Sea  $T$  un árbol binario completo con altura  $H$ . Por el teorema anterior  $T$  debe tener  $2^H$  hojas. Luego, por el otro teorema anterior sabemos que debe tener  $2^H - 1$  vértices con exactamente 2 hijos. Dado que todo vértice en un árbol binario es hoja o tiene 2 hijos, concluimos que  $T$  debe tener  $2^H + (2^H - 1) = 2 \cdot 2^H - 1 = 2^{H+1} - 1$  vértices.

# Árboles binarios

## Teorema

Si  $H$  es la altura de un árbol binario completo con  $n$  vértices, entonces  $H \leq \log_2(n)$ .

## Demostración:

Sea  $T$  un árbol binario completo con  $n$  vértices y altura  $H$ . Sabemos que la cantidad de hojas ( $2^H$ ) tiene que ser menor o igual a la cantidad total de vértices ( $n$ ).

$$2^H \leq n \Rightarrow H \leq \log_2(n)$$

# Objetivos de la clase

- Conocer propiedades básicas de aritmética modular
- Demostrar equivalencias modulares
- Demostrar teorema de Fermat para números primos



# Outline

Árboles

**Aritmética modular**

Teorema de Fermat

Epílogo

# Recordemos. . .

## Definición

La relación **divide a**, denotada por  $|$ , sobre los  $\mathbb{Z} \setminus \{0\}$ , es una relación tal que  $a$  está relacionado con  $b$  si y sólo si  $b$  es múltiplo de  $a$ :

$a|b$  si y sólo si  $\exists k \in \mathbb{Z}$  tal que  $b = ka$ .

$$3|9 \quad 18|72 \quad 7 \nmid 9 \quad 2|-4$$



# Recordemos. . .

## Definición

La relación **equivalencia módulo  $n$** , denotada por  $\equiv_n$ , sobre los enteros, es una relación tal que  $a$  está relacionado con  $b$  si y sólo si  $n|(b - a)$ :

$$a \equiv_n b \text{ si y sólo si } n|(b - a)$$

$$a \equiv_n b \text{ si y sólo si } \exists k \in \mathbb{Z} \text{ tal que } (b - a) = kn.$$

Por ejemplo, dado  $n = 7$ :

$$2 \equiv_7 23$$

$$8 \equiv_7 1$$

$$19 \not\equiv_7 4$$

$$-3 \equiv_7 4$$

# Recordemos. . .

- La relación  $\equiv_n$  es una relación de equivalencia.
- Podemos tomar el conjunto cociente generado por ella sobre  $\mathbb{Z}$ .
- Usando las clases de equivalencia, definimos la suma y la multiplicación.

## Definición

Dado  $n \in \mathbb{N}$ ,  $n > 0$ , definimos

$$\mathbb{Z}_n = \mathbb{Z} / \equiv_n$$

y sus operaciones

$$[i] + [j] = [i + j]$$

$$[i] \cdot [j] = [i \cdot j]$$

## Recordemos. . .

Por simplicidad, renombramos las clases de equivalencia como los números que representan.

### Ejemplo

$$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$$

Calcule  $37 + 18$  y  $26 \cdot 37$ .

# Recordemos...

## Ejemplo

$$\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$$

Calcule  $37 + 18$  y  $26 \cdot 37$ .

$$37 + 18 = [37] + [18] = [37 + 18] = [55] = [0]$$

$$26 \cdot 37 = [26] \cdot [37] = [26 \cdot 37] = [962] = [2]$$

# Aritmética modular

## Teorema (división con resto)

Dados dos enteros  $a$  y  $n$ , siempre podemos expresar  $a$  en términos de  $n$  como  $a = \alpha \cdot n + \beta$ , donde  $\alpha = \left\lfloor \frac{a}{n} \right\rfloor$  es la división entera de  $a$  por  $n$ , y  $\beta$  es el resto de esa división, con  $\alpha, \beta \in \mathbb{Z}$  y  $\beta \geq 0$ .

### Ejemplo

Dados  $a = 3$  y  $n = 2$ , podemos escribir

$$a = \left\lfloor \frac{3}{2} \right\rfloor \cdot 2 + 1 = 1 \cdot 2 + 1$$

Llamamos a este resultado el **Teorema de división con resto**.

Lo damos por demostrado

# Aritmética modular

## Definición

La operación **módulo de  $n$**  entrega el resto de la división por  $n$ .

Se escribe  $a \bmod n$ .

## Ejemplo

$$3 \bmod 2 = 1$$

# Aritmética modular

Con esta operación podemos redefinir la suma y la multiplicación en  $\mathbb{Z}_n$ :

$$[i] + [j] = (i + j) \bmod n$$

$$[i] \cdot [j] = (i \cdot j) \bmod n$$

Una observación importante es que siempre se cumple que

$$0 \leq a \bmod n < n$$

# Aritmética modular

## Teorema

$a \equiv_n b$  si y sólo si  $a \bmod n = b \bmod n$ .

## Ejercicio

Demuestre el teorema.



# Aritmética modular

## Teorema

$a \equiv_n b$  si y sólo si  $a \bmod n = b \bmod n$ .

En primer lugar, sabemos que podemos escribir  $a$  y  $b$  en términos de  $n$ :

$$a = \alpha \cdot n + a \bmod n \tag{1}$$

$$b = \gamma \cdot n + b \bmod n \tag{2}$$

donde  $\alpha, \gamma \in \mathbb{Z}$  son los resultados de las divisiones enteras.

( $\Leftarrow$ ) Suponemos que  $a \bmod n = b \bmod n$ . Por demostrar:  $a \equiv_n b$ .

Si restamos (2) – (1) obtenemos  $b - a = (\gamma - \alpha) \cdot n$ , de donde es claro que  $n \mid (b - a)$ , pues  $(\gamma - \alpha) \in \mathbb{Z}$ . Por lo tanto, se cumple que  $a \equiv_n b$ .

# Aritmética modular

## Teorema

$a \equiv_n b$  si y sólo si  $a \bmod n = b \bmod n$ .

( $\Rightarrow$ ) Por contrapositivo, suponemos que  $a \bmod n \neq b \bmod n$  (3). Por demostrar:  $a \not\equiv_n b$ .

Sin pérdida de generalidad, asumimos que  $a \bmod n < b \bmod n$  (4). Si restamos (2) – (1) obtenemos  $b - a = (\gamma - \alpha) \cdot n + (b \bmod n - a \bmod n)$ .

Como

$$0 \leq a \bmod n, b \bmod n < n$$

por (4) se tiene que  $1 \leq (b \bmod n - a \bmod n) \leq b \bmod n < n$ . Por lo tanto,  $n \nmid (b - a)$ , de donde concluimos que  $a \not\equiv_n b$ .

# Aritmética modular

Corolario

$$a \equiv_n a \bmod n$$

Ejercicio

Demuestre el corolario.

# Aritmética modular

## Corolario

$$a \equiv_n a \bmod n$$

Como sabemos que  $a \bmod n < n$ , se tiene que  $\left\lfloor \frac{a \bmod n}{n} \right\rfloor = 0$ . Luego, si expresamos  $a \bmod n$  en términos de  $n$ :

$$a \bmod n = 0 \cdot n + (a \bmod n) \bmod n$$

$$a \bmod n = (a \bmod n) \bmod n$$

y por el teorema anterior,  $a \equiv_n a \bmod n$ .

# Aritmética modular

## Teorema

Si  $a \equiv_n b$  y  $c \equiv_n d$ , entonces

- $(a + c) \equiv_n (b + d)$

- $(a \cdot c) \equiv_n (b \cdot d)$

## Ejercicio

Demuestre el teorema.

# Aritmética modular

## Teorema

Si  $a \equiv_n b$  y  $c \equiv_n d$ , entonces

$$\blacksquare (a + c) \equiv_n (b + d)$$

$$\blacksquare (a \cdot c) \equiv_n (b \cdot d)$$

Como  $a \equiv_n b$ , por definición sabemos que  $n \mid (b - a)$ , y nuevamente por definición tenemos que  $b - a = k_1 \cdot n$ . Si despejamos  $b$ , y procedemos análogamente desde  $c \equiv_n d$ :

$$b = a + k_1 \cdot n \tag{1}$$

$$d = c + k_2 \cdot n \tag{2}$$

# Aritmética modular

## Teorema

Si  $a \equiv_n b$  y  $c \equiv_n d$ , entonces  $(a + c) \equiv_n (b + d)$ .

$$b = a + k_1 \cdot n \quad (1)$$

$$d = c + k_2 \cdot n \quad (2)$$

Sumamos (1) y (2):

$$b + d = a + c + (k_1 + k_2) \cdot n$$

$$\Leftrightarrow (b + d) - (a + c) = k_3 \cdot n$$

$$\Leftrightarrow n \mid (b + d) - (a + c)$$

$$\Leftrightarrow a + c \equiv_n b + d$$

# Aritmética modular

## Teorema

Si  $a \equiv_n b$  y  $c \equiv_n d$ , entonces  $(a \cdot c) \equiv_n (b \cdot d)$ .

$$b = a + k_1 \cdot n \quad (1)$$

$$d = c + k_2 \cdot n \quad (2)$$

Multiplicamos (1) y (2):

$$b \cdot d = (a + k_1 \cdot n)(c + k_2 \cdot n)$$

$$\Leftrightarrow \quad \quad \quad = a \cdot c + (a \cdot k_2 + c \cdot k_1 + n \cdot k_1 \cdot k_2) \cdot n$$

$$\Leftrightarrow \quad b \cdot d - a \cdot c = k_4 \cdot n$$

$$\Leftrightarrow \quad n \mid b \cdot d - a \cdot c$$

$$\Leftrightarrow \quad a \cdot c \equiv_n b \cdot d$$



# Aritmética modular

## Corolario

- $(a + b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n$
- $a \cdot b \bmod n = ((a \bmod n)(b \bmod n)) \bmod n$

## Ejercicio

Demuestre el corolario.

## Ejercicio

Demuestre que un número es divisible por 3 si y sólo si la suma de sus dígitos es divisible por 3.

## Ejercicio

Calcule  $(55 \cdot 26) \bmod 4$ .

# Aritmética modular

$$\blacksquare (a + b) \bmod n = ((a \bmod n) + (b \bmod n)) \bmod n$$

$$\blacksquare a \cdot b \bmod n = ((a \bmod n)(b \bmod n)) \bmod n$$

Por teorema anterior sabemos que  $a \equiv_n a \bmod n$  y  $b \equiv_n b \bmod n$ . Aplicando el teorema de sumas y multiplicaciones:

$$\begin{aligned} a + b &\equiv_n (a \bmod n) + (b \bmod n) \\ \Leftrightarrow (a + b) \bmod n &= ((a \bmod n) + (b \bmod n)) \bmod n \end{aligned}$$

$$\begin{aligned} a \cdot b &\equiv_n (a \bmod n) \cdot (b \bmod n) \\ \Leftrightarrow (a \cdot b) \bmod n &= ((a \bmod n)(b \bmod n)) \bmod n \end{aligned}$$

# Aritmética modular

## Ejercicio

Demuestre que un número es divisible por 3 si y sólo si la suma de sus dígitos es divisible por 3.

Sabemos que un número entero  $n$  se puede representar como

$$n = d_k \cdot 10^k + \cdots + d_1 \cdot 10 + d_0 \quad (1)$$

donde  $d_i$  es el dígito  $i$ -ésimo de  $n$ . Por ejemplo:

$$1347 = 1 \cdot 10^3 + 3 \cdot 10^2 + 4 \cdot 10 + 7$$

Ahora, tenemos que  $n$  será divisible por 3 si y sólo si  $n \bmod 3 = 0$ .

# Aritmética modular

## Ejercicio

Demuestre que un número es divisible por 3 si y sólo si la suma de sus dígitos es divisible por 3.

Tomamos mod 3 en (1) y usamos el teorema de suma y multiplicación:

$$\begin{aligned}n \bmod 3 &= (d_k \cdot 10^k + \cdots + d_1 \cdot 10 + d_0) \bmod 3 \\&= ((d_k \cdot 10^k) \bmod 3 + \cdots + (d_1 \cdot 10) \bmod 3 + d_0 \bmod 3) \bmod 3 \\&= ((d_k \bmod 3 \cdot 10^k \bmod 3) \bmod 3 + \cdots \\&\quad + (d_1 \bmod 3 \cdot 10 \bmod 3) \bmod 3 + d_0 \bmod 3) \bmod 3\end{aligned}$$

# Aritmética modular

## Ejercicio

Demuestre que un número es divisible por 3 si y sólo si la suma de sus dígitos es divisible por 3.

Notemos que  $\forall k \geq 1, 10^k \bmod 3 = 1$ . Por lo tanto:

$$\begin{aligned} n \bmod 3 &= ((d_k \bmod 3 \cdot 1) \bmod 3 + \dots \\ &\quad + (d_1 \bmod 3 \cdot 1) \bmod 3 + d_0 \bmod 3) \bmod 3 \\ &= ((d_k \bmod 3) \bmod 3 + \dots \\ &\quad + (d_1 \bmod 3) \bmod 3 + d_0 \bmod 3) \bmod 3 \\ &= (d_k \bmod 3 + \dots + d_1 \bmod 3 + d_0 \bmod 3) \bmod 3 \\ &= (d_k + \dots + d_1 + d_0) \bmod 3 \end{aligned}$$

Luego,  $n \bmod 3 = 0$  si y sólo si  $(d_k + \dots + d_1 + d_0) \bmod 3 = 0$ ; es decir, si la suma de los dígitos de  $n$  es divisible por 3.

# Aritmética modular

## Ejercicio

Calcule  $(55 \cdot 26) \bmod 4$ .

$$\begin{aligned}(55 \cdot 26) \bmod 4 &= (55 \bmod 4 \cdot 26 \bmod 4) \bmod 4 \\&= (3 \cdot 2) \bmod 4 \\&= 6 \bmod 4 \\&= 2\end{aligned}$$

# Outline

Árboles

Aritmética modular

**Teorema de Fermat**

Epílogo

# Aritmética modular

## Teorema (Fermat)

Si  $p$  es un número primo, para cualquier entero  $a$  se cumple que  $a^p \equiv_p a$ .

## Ejercicio

Demuestre el teorema.



# Aritmética modular

## Teorema (Fermat)

Si  $p$  es un número primo, para cualquier entero  $a$  se cumple que  $a^p \equiv_p a$ .

Nos pondremos en dos casos.

Caso 1:  $a \geq 0$ . Se hará la demostración por inducción sobre el valor de  $a$ .

BI:  $a = 0 \rightarrow 0^p = 0 \equiv_p 0$

$$a = 1 \rightarrow 1^p = 1 \equiv_p 1$$

HI: Suponemos que  $a^p \equiv_p a$ . Notemos que esto implica que  $p \mid a^p - a$ .

TI: Por demostrar:  $(a+1)^p \equiv_p (a+1)$ , o equivalentemente, que

$$p \mid (a+1)^p - (a+1), \text{ con } 2 \leq a+1 \quad (1)$$

# Aritmética modular

## Teorema (Fermat)

Si  $p$  es un número primo, para cualquier entero  $a$  se cumple que  $a^p \equiv_p a$ .

$$\text{PD: } p \mid (a+1)^p - (a+1), \text{ con } 2 \leq a+1. \quad (1)$$

Por el teorema del binomio, sabemos que  $(a+1)^p = \sum_{k=0}^p \binom{p}{k} a^k$ , con

$\binom{p}{k} = \frac{p!}{k!(p-k)!}$ . Desarrollamos la parte derecha de (1):

$$\begin{aligned} (a+1)^p - (a+1) &= \sum_{k=0}^p \binom{p}{k} a^k - (a+1) \\ &= \sum_{k=1}^{p-1} \binom{p}{k} a^k + \binom{p}{0} a^0 + \binom{p}{p} a^p - (a+1) \end{aligned}$$

# Aritmética modular

## Teorema (Fermat)

Si  $p$  es un número primo, para cualquier entero  $a$  se cumple que  $a^p \equiv_p a$ .

$$\begin{aligned}(a+1)^p - (a+1) &= \sum_{k=0}^p \binom{p}{k} a^k - (a+1) \\&= \sum_{k=1}^{p-1} \binom{p}{k} a^k + \binom{p}{0} a^0 + \binom{p}{p} a^p - (a+1) \\&= \sum_{k=1}^{p-1} \binom{p}{k} a^k + 1 + a^p - a - 1 \\&= (a^p - a) + \sum_{k=1}^{p-1} \binom{p}{k} a^k\end{aligned}$$

# Aritmética modular

## Teorema (Fermat)

Si  $p$  es un número primo, para cualquier entero  $a$  se cumple que  $a^p \equiv_p a$ .

Tenemos entonces que

$$(a+1)^p - (a+1) = (a^p - a) + \sum_{k=1}^{p-1} \binom{p}{k} a^k$$

Por HI, sabemos que  $p \mid a^p - a$ . Por demostrar:  $p \mid \sum_{k=1}^{p-1} \binom{p}{k} a^k$ .

Demostraremos que  $\forall k \in \{1, \dots, p-1\}, p \mid \binom{p}{k}$ . Tenemos que

$$\begin{aligned} \binom{p}{k} &= \frac{p!}{k!(p-k)!} = \frac{p(p-1)\cdots(p-k+1)(p-k)!}{k!(p-k)!} \\ &= \frac{p(p-1)\cdots(p-k+1)}{k!} \end{aligned}$$

# Aritmética modular

## Teorema (Fermat)

Si  $p$  es un número primo, para cualquier entero  $a$  se cumple que  $a^p \equiv_p a$ .

Tenemos entonces que

$$\binom{p}{k} = \frac{p(p-1)\cdots(p-k+1)}{k!}$$

Como los coeficientes binomiales son enteros, el numerador debe ser divisible por el denominador. Como  $p$  es primo y  $k < p$ , sabemos que entre los factores de  $k!$  no puede haber divisores de  $p$ , por lo que necesariamente

$$\frac{(p-1)\cdots(p-k+1)}{k!} \in \mathbb{Z}, \text{ y entonces}$$

$$\binom{p}{k} = p \cdot \alpha, \text{ con } \alpha \in \mathbb{Z}, \text{ y por lo tanto } p \mid \binom{p}{k}.$$

# Aritmética modular

## Teorema (Fermat)

Si  $p$  es un número primo, para cualquier entero  $a$  se cumple que  $a^p \equiv_p a$ .

En conclusión, tenemos que

$$p \mid (a+1)^p - (a+1)$$

y por lo tanto

$$(a+1)^p \equiv_p (a+1)$$

como queríamos demostrar.

Se sigue entonces por inducción el teorema planteado para  $a \geq 0$ .

# Aritmética modular

## Teorema (Fermat)

Si  $p$  es un número primo, para cualquier entero  $a$  se cumple que  $a^p \equiv_p a$ .

Caso 2:  $a < 0$ . Sabemos que  $a \equiv_p a \bmod p$ , y por teorema de multiplicación  $a^p \equiv_p (a \bmod p)^p$ . Ahora, como  $a \bmod p \geq 0$ , corresponde al caso 1 recién demostrado, y por lo tanto  $(a \bmod p)^p \equiv_p a \bmod p$ . Finalmente, tenemos que

$$a^p \equiv_p (a \bmod p)^p \equiv_p a \bmod p \equiv_p a$$

y entonces  $a^p \equiv_p a$ .

# Aritmética modular

## Corolario (Fermat)

Si  $p$  es un número primo y  $a$  es un entero que no es múltiplo de  $p$ , entonces  $a^{p-1} \equiv_p 1$ .

## Ejercicio

Demuestre el corolario.



# Aritmética modular

## Corolario (Fermat)

Si  $p$  es un número primo y  $a$  es un entero que no es múltiplo de  $p$ , entonces  $a^{p-1} \equiv_p 1$ .

Por el teorema anterior:

$$a^p \equiv_p a \Rightarrow p \mid a^p - a \Rightarrow a^p - a = k \cdot p \quad (1)$$

Notemos que  $a \mid a^p - a$ , y por lo tanto  $a \mid k \cdot p$ . Como  $p$  es primo y  $a$  no es múltiplo de  $p$ , necesariamente  $a \mid k$ . Dividiendo (1) por  $a$ :

$$a^{p-1} - 1 = \frac{k}{a} \cdot p, \text{ con } \frac{k}{a} \in \mathbb{Z}.$$

Por lo tanto:

$$p \mid a^{p-1} - 1 \Rightarrow 1 \equiv_p a^{p-1} \Rightarrow a^{p-1} \equiv_p 1$$

# Outline

Árboles

Aritmética modular

Teorema de Fermat

**Epílogo**

# Objetivos de la clase

- Conocer propiedades básicas de aritmética modular
- Demostrar equivalencias modulares
- Demostrar teorema de Fermat para números primos