Aritmética modular

Clase 26

IIC 1253

Prof. Pedro Bahamondes

Outline

Objetivos de la clase

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

Outline

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:

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

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

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 $n = 7$:

$$2 \equiv_7 23 \qquad 8 \equiv_7 1 \qquad 19 \not\equiv_7 4 \qquad -3 \equiv_7 4$$

Recordemos...

- La relación $\equiv_n$ es una relación de equivalencia.
- Podemos tomar el conjunto cuociente 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 β 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

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

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 $a \equiv_n b$.

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, $n \not| \ (b - a)$, 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

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

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

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

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

Sumamos (1) y (2):

$$\begin{aligned} & b + d = a + c + (k_1 + k_2) \cdot n \\ \Leftrightarrow \quad & (b + d) - (a + c) = k_3 \cdot n \\ \Leftrightarrow \quad & n \mid (b + d) - (a + c) \\ \Leftrightarrow \quad & a + c \equiv_n b + d \end{aligned}$$

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):

$$
\begin{aligned}
& b \cdot d = (a + k_1 \cdot n)(c + k_2 \cdot n) \\
\Leftrightarrow \quad & = a \cdot c + (a \cdot k_2 + c \cdot k_1 + n \cdot k_1 \cdot k_2) \cdot n \\
\Leftrightarrow \quad & b \cdot d - a \cdot c = k_4 \cdot n \\
\Leftrightarrow \quad & n \mid b \cdot d - a \cdot c \\
\Leftrightarrow \quad & a \cdot c \equiv_n b \cdot d
\end{aligned}
$$

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

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

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:

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

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

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

$$n = d_k \cdot 10^k + \cdots + d_1 \cdot 10 + d_0 \tag{1}$$

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:

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

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:

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

Luego, $n \bmod 3 = 0$ si y sólo si $(d_k + \cdots + d_1 + d_0) \bmod 3 = 0$; 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

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.

<u>Caso 1:</u> $a \geq 0$. 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

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

Aritmética modular

Teorema (Fermat)

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

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

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):

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

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

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

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

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 $a^p \equiv_p a$.

<u>Caso 2:</u> $a < 0$. 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 $a^p \equiv_p a$.

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:

$$a^p \equiv_p a \Rightarrow p \mid a^p - a \Rightarrow a^p - a = k \cdot p \tag{1}$$

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

Objetivos de la clase

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