UAB

aritmètica modular

Congruències

a congruent amb b mòdul n

$$a \equiv b \pmod{n}$$

$$\Updownarrow$$

$$a - b \text{ múltiple de } n$$

$$\Updownarrow$$

$$\text{Resta de } a \div n = \text{Resta de } b \div n$$

Aritmètica del rellotge

Les hores del dia es miren (mod 12)

$$19 \equiv 7 \pmod{12}$$

Propietats aritmètiques

Es pot sumar i multiplicar (mod n)

$$\begin{matrix} a_1 \equiv b_1 \ (n) \\ a_2 \equiv b_2 \ (n) \end{matrix} \Rightarrow \begin{matrix} a_1 + a_2 \equiv b_1 + b_2 \ (n) \\ a_1\, a_2 \equiv b_1\, b_2 \ (n) \end{matrix}$$

NIF

El número del DNI (mod 23) correspon a la lletra de la taula següent:

0T	1R	2W	3A	4G	5M	6Y	7F
8P	9D	10X	11B	12N	13J	14Z	15S
16Q	17V	18H	19L	20C	21K	22E	

ISBN-10

ISBN 0-12-511360-9

90000

9 780125 113601

$$\text{ISBN} = u_1 u_2 u_3 \cdots u_9 u_{10}$$

$$u_{10} \equiv \sum_{k=1}^{9} k\, u_k \pmod{11}$$

Si la suma és 10 (mod 11), $u_{10} = \mathrm{X}$

CCC

$b_1 \cdots b_4$ $b_5 \cdots b_8$ $c_1 c_2$ $n_1 n_2 n_3 \cdots n_9 n_{10}$

Entitat Oficina Número de compte

$c_1 c_2 =$ Dígits de control

$$c_1 \equiv 10 \sum_{k=1}^{8} 2^{k+1} b_k \pmod{11}$$

$$c_2 \equiv 10 \sum_{k=1}^{10} 2^{k-1} n_k \pmod{11}$$

(Si una de les sumes dona 1 (mod 11),
la c corresponent és 1 en comptes de 10)

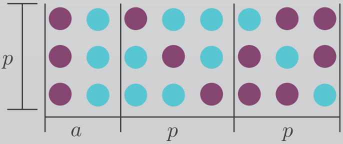
Un codi correcte:

$2019\ 0802\ \ 57\ 7061128355$

Petit Teorema de Fermat

Si p és primer i a qualsevol natural:

$$a^p - a \equiv 0 \pmod{p}$$



Hi ha a^p formes d'acolorir p objectes amb a colors. D'aquestes n'hi ha a que corresponen als acoloriments amb un sol color. La resta es poden agrupar prenent cicles de p disposicions.

Teorema xinès de les restes

$$\begin{cases} x \equiv 1 \ (2) \\ x \equiv 2 \ (3) \\ x \equiv 2 \ (5) \end{cases}$$

$$\Rightarrow \ x \equiv 17 \pmod{30}$$

$$= 17,\ 47,\ 77, \ldots$$

graus de Matemàtiques
Matemàtica computacional
Estadística aplicada
mat.uab.cat

autor Joan Claramunt
Dpt. Matemàtiques

disseny Àrea de Planificació de
Sistemes d'Informació

Universitat Autònoma de Barcelona