Si ho amague, ho trobes?
Aritmètica del rellotge

Mª Joaquina Berral Yerón, Inmaculada Serrano Gómez

Aritmètica del Rellotge

En les activitats 1.1 i 1.2 de la primera sessió has après a xifrar i desxifrar missatges mitjançant un dels mètodes clàssics de clau simètrica: el xifrat de Cèsar.

Una de les característiques, i al mateix temps inconvenient, d'aquest tipus de xifrat és que la seguretat rau en la clau. Si per qualsevol raó es descobreix la clau n'hi ha prou amb calcular la inversa perquè qualsevol persona puga desxifrar un missatge encara que no vaja adreçat a d'ella. A més si una persona necessita comunicar-se de forma confidencial amb bastants persones el número de claus que li fan falta és molt elevat. Fem un petit càlcul:

Si 6 persones es volen comunicar entre si amb un mètode simètric, però de forma que només puguen desxifrar els missatges per parelles. Quantes claus necessiten?

Cada parella ha de seleccionar una clau diferent. Quantes parelles hi ha? El número de claus coincideix amb les diferents formes de fer parelles entre 6 persones, i açò és un problema de combinatòria molt senzill: $\binom{6}{2}=\frac{6!}{2!4!}=\frac{6.5}{2}=15$

1) I si en lloc de 6 n'hi ha n de parelles? _____

   Pots fer un càlcul per conèixer el número de claus per a 1000 persones? _____

   I per a 10000? _____

   I per a 100000? _____

Aquestes quantitats et fan una idea de la quantitat de claus diferents que farien falta. Per això han aparegut altres mètodes de xifrat que reben el nom de sistemes de clau pública que eviten aquest problema. Però per estar al corrent del funcionament d'aquests sistemes cal conèixer alguns resultats de teoria de números (una de les branques de les matemàtiques més antigues i alhora molt actual)

Alguns d'aquests resultats estan relacionats amb l'aritmètica del rellotge. No penses que aquesta iniciativa és actual. Una de les primeres contribucions del matemàtic alemany Karl Friederich Gauss (1777-1855) va ser la invenció de la calculadora del rellotge. No era una màquina material (no oblides l'època que hi va viure), era més bé una idea que aportava noves possibilitats per fer determinades operacions amb números que eren inabordables amb els mètodes de càlcul que es feien servir en aquella època.

Segur que estàs acostumat a representar els números enters com marques disposades al llarg d'una recta que s'estén fins l'infinit:

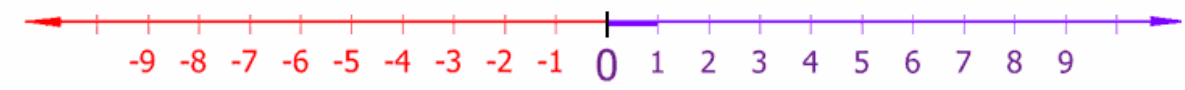


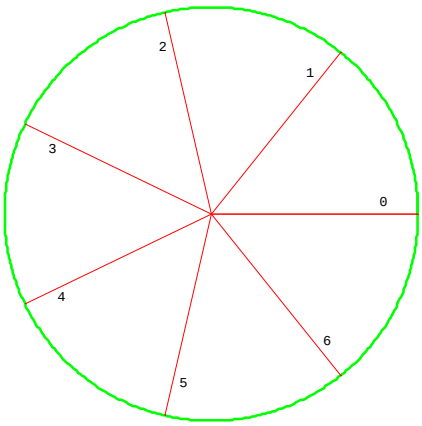
Figura 1

L'aritmètica que coneixes es pot imaginar en termes de desplaçaments a dreta o esquerra al llarg d'aquesta recta. Ara vas a treballar amb altra aritmètica que intuïtivament el que fa és tallar la recta

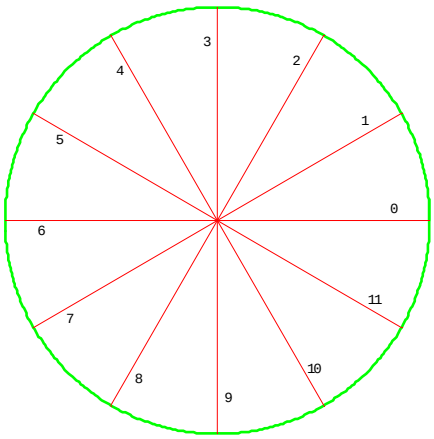
Elaborado por:
Federación Española de Sociedades de Profesores de Matemáticas
MINISTERIO DE EDUCACIÓN
SECRETARÍA DE ESTADO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL
DIRECCIÓN GENERAL DE FORMACIÓN PROFESIONAL

en un determinat punt obtenint d'aquesta forma un segment (finit) i tancar aquesta línia sobre si mateixa per tal de formar un cercle de números en compte d'una línia.

Per exemple, la figura 2 mostra dos rellotges de 7 i de 12 hores (la recta s'ha tallat en el 7 i en el 12 respectivament i s'ha tancat sobre si mateixa). Si observes les hores comencem a comptar en el 0 i el número 7 (12) s'esborra ja que coincideix amb el 0



Rellotge 1: de 7 hores



Rellotge 2: de 12 hores

Figura 2

Si anem a treballar amb aquests rellotges els únics números que podem gastar són: 0, 1, 2, 3, 4, 5 i 6 en el primer i des de 0 fins 11 en el segon.

Des de molt nen vas aprendre a fer operacions amb números enters. L'operació 3 + 2 = 5 la pots simular com un desplaçament a la dreta al llarg de la recta dibuixada en la figura 1: 5 és el mateix que situar-se en el 3 i moure's al llarg de la recta 2 espais fins arribar al 5 (amb l'operació suma sempre ens movem cap a la dreta).

Però en l'aritmètica del rellotge es treballa d'altra forma, per exemple per al rellotge 1: 5 + 4 = 2 (si comencem en el 5 i avancem 4 llocs en l'esfera del rellotge arribem al 2). No és rara aquesta forma de comptar, la fem servir en els rellotges per indicar les hores. Si ara són les 11 del matí per referir-nos a 4 hores més tard no és habitual que diguem l'hora 15 sinó que es més comú dir que seran les 3 de la tarda. El rellotge és molt semblant al nostre rellotge 2 però nosaltres comencem a comptar en 0 i acabem en 11. Aquesta semblança és probablement la causa del nom d'aritmètica del rellotge. En àmbits més teòrics de les Matemàtiques rep el nom d'Aritmètica modular.

Igual que hemos treballat amb l'addició podem també representar el producte. Com interpretem en el rellotge 2 l'operació: 5 x 7? En aritmètica habitual el resultat seria 35 però aquesta hora no existeix en el nostre rellotge. Però si penses una mica, què significa que passen 35 hores?: començant a comptar en 0, en la primera volta del rellotge hauran passat 12 hores, en una segona volta altres 12 i així sucessivament, és a dir per a 35 es donen 2 voltes completes al rellotge (24 hores) i encara queden per recórrer 11 hores, per això diem que en aquesta aritmètica 5 x 7 = 11

Per multiplicar aquests dos números no s'han donat massa voltes però si es van a multiplicar números grans el mètode que acabem de descriure pot ser molt avorrit. Tanmateix existeix d'altra operació que vas aprendre en els teus primers anys de formació matemàtica que et serà d'ajut en aquest treball. Si

Elaborado por:
Federación Española de Sociedades de Profesores de Matemáticas
MINISTERIO DE EDUCACIÓN
SECRETARÍA DE ESTADO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL
DIRECCIÓN GENERAL DE FORMACIÓN PROFESIONAL

ara són les 12 en punt, quin hora serà quan passen 357 hores? Cal esbrinar el número de voltes completes i cas de que sobren les que es recorren en l'última volta. Com donar el resultat de forma ràpida? Doncs clar, dividint 357 entre 12! El quocient de la divisió (29) t'indica el número de voltes completes i el residu de la divisió (8) les hores de la darrera volta. Per això la resposta a la pregunta serà 8 hores.

Per tal familiaritzar-te amb aquestes operacions fes servir els rellotges del maletí de l'espia (discos 3 a 6) i pensa quin hora indicarà el rellotge si han passat les hores indicades en la primera fila de les taules:

Rellotge de 7 hores	0	4	7	11	127	536	- 8	- 13	-45	-536

Com has resolt els 4 últims resultats?

Rellotge de 12 hores	0	4	7	11	127	536	- 8	- 13	-45	-536

Açò mateix es pot fer per a un valor qualsevol n i se sol dir que es treballa mòdul n (recorda que s'anomena aritmètica modular). Per a un valor n determinat, podems considerar el conjunt A= {possibles hores que es poden presentar} = {0, 1, 2,..., n-1}

Anem a reflexionar un poc més sobre la forma d'operar en aquests conjunts i els avantatges que tenen. Per saber el valor d'n amb el qual es treballa s'indica (mod n), per exemple per al rellotge 1

$3 + 3 \equiv 6 \pmod 7$

També farem servir aquesta representació per al producte: $6 \times 6 \equiv 1 \pmod 7$ (s'han donat 5 voltes completes i queda 1 hora)

Practica un poc amb la suma:

$4 + 6 \equiv \pmod 7$	$-4 + 6 \equiv \pmod 7$	$8 + 9 + 2 \equiv \pmod 7$
$9 + 11 \equiv \pmod{12}$	$9 + (-11) \equiv \pmod{12}$	$23 + 79 + 11 \equiv \pmod{12}$

I ara amb el producte:

$4 \times 6 \equiv \pmod 7$	$(-4) \times 6 \equiv \pmod 7$	$8 \times 9 \times 2 \equiv \pmod 7$
$9 \times 11 \equiv \pmod{12}$	$9 \times (-11) \equiv \pmod{12}$	$23 \times 79 \times 11 \equiv \pmod{12}$

Creus que es pot dividir en aquests conjunts? Tot i que treballem amb el conjunt dels números enters aquesta pregunta no sempre té resposta afirmativa. Per exemple en el conjunt dels números enters no pots dividir 5 entre 2 mentre que sí pots dividir 8 entre 2

Has sentit alguna vegada que la divisió és l'operació inversa de la multiplicació? Açò vol dir que $\frac{8}{4} = 8x\frac{1}{4} = 2$ (dividir és el mateix que multiplicar per l'invers del denominador) però ja sabem que no sempre és possible trobar aquest invers.

Elaborado por:
Federación Española de Sociedades de Profesores de Matemáticas
MINISTERIO DE EDUCACIÓN
SECRETARÍA DE ESTADO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL
DIRECCIÓN GENERAL DE FORMACIÓN PROFESIONAL

Si ho amague, ho trobes?
Aritmètica del rellotge

Mª Joaquina Berral Yerón, Inmaculada Serrano Gómez

Quan els valors de n no són massa grans resulta interessant reflectir els resultats de les dos operacions suma i producte en una taula. Completa les dues taules següents

+	**0**	**1**	**2**	**3**	**4**	**5**	**6**
0	0	1	2	3	4	5	6
1	1	2	3				
2							
3							
4							
5							
6							

x	**0**	**1**	**2**	**3**	**4**	**5**	**6**
0	0	0	0	0	0	0	0
1	0	1	2				
2							
3							
4							
5							
6							

Anem a proposar-te un exercici: pots calcular els inversos dels valors 1 a 6 per a un rellotge de 7 hores. Intenta utilitzar la taula anterior per omplir la següent:

número	0	1	2	3	4	5	6
invers							

Pensa el mateix per al rellotge de 12 hores:

número	0	1	2	3	4	5	6	7	8	9	10	11
Invers												

I per a un de 5 hores?

número	0	1	2	3	4
Invers					

I de 6?

número	0	1	2	3	4	5
invers						

¿Sabries dir quan un número qualsevol a té invers mòdul n?

.....

Anem a treballar ara amb potències, sabem que per a $6^2 = 6 \times 6 = 1 \pmod 7$

I si ara volem calcular $6^3 = 6 \times 6 \times 6$ en el matex conjunt? Una possibilitat és multiplicar aquests valors i calcular el residu de la divisió entre 7, però, se t'acudeix altra idea més còmoda?

$6 \times 6 \times 6 \equiv (6 \times 6) \times 6 \equiv 1 \times 6 \equiv 6 \pmod 7$

Hem deduït el resultat sense necessitat de multiplicar 6 x 6 x6. Aquesta fou la idea que va tenir Gauss: podia saber, sense gran esforç, que el resultat d'aquesta operació donava de residu 6 en dividir-lo per 7.

Pensa el resultat i explica la forma d'utilitzar el càlcul d'un d'aquests valors per al següent.

6 x 6 x 6 x 6 ≡ (mod 7)	6 x 6 x 6 x 6 x 6 ≡ (mod 7)

Elaborado por:
Federación Española de Sociedades de Profesores de Matemáticas
MINISTERIO DE EDUCACIÓN
SECRETARÍA DE ESTADO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL
DIRECCIÓN GENERAL DE FORMACIÓN PROFESIONAL

Si ho amague, ho trobes?
Aritmètica del rellotge

Mª Joaquina Berral Yerón, Inmaculada Serrano Gómez

$6 \times 6 \times 6 \times 6 \times 6 \times 6 \equiv$ (mod 7)	$6 \times 6 \times 6 \times 6 \times 6 \times 6 \times 6 \equiv$ (mod 7)

La calculadora del rellotge va demostrar que era molt potent per a treballar amb grans números. Per exemple, sense haver de calcular el valor de 6^{99} la seva calculadora de rellotge li permetia calcular que era 6 el residu de la divisió entre 7. Pot explicar como s'arriba a aquest resultat?

Els estudis de Gauss envers aquest nou tipus d'aritmètica van revolucionar la matemàtica de principis del segle XIX i van ajudar a descobrir noves estructures en els números. Actualment aquesta aritmètica és necessària per garantir la seguretat en Internet on s'utilitzen valors de n molt grans, per exemple serien majors que el número d'àtoms que hi ha en el món que nosaltres podem observar.

Anem hi a treballar un poc més amb potències per al rellotge de 7 hores, és a dir mod 7, tot i que en la taula s'omet la notació totes les potències les has de calcular amb el nostre rellotge

$2^0\equiv$	$2^1\equiv$	$2^2\equiv$	$2^3\equiv$	$2^4\equiv$	$2^5\equiv$	$2^6\equiv$	$2^7\equiv$	$2^8\equiv$	$2^9\equiv$	$2^{10}\equiv$	$2^{11}\equiv$
$3^0\equiv$	$3^1\equiv$	$3^2\equiv$	$3^3\equiv$	$3^4\equiv$	$3^5\equiv$	$3^6\equiv$	$3^7\equiv$	$3^8\equiv$	$3^9\equiv$	$3^{10}\equiv$	$3^{11}\equiv$
$5^0\equiv$	$5^1\equiv$	$5^2\equiv$	$5^3\equiv$	$5^4\equiv$	$5^5\equiv$	$5^6\equiv$	$5^7\equiv$	$5^8\equiv$	$5^9\equiv$	$5^{10}\equiv$	$5^{11}\equiv$
$6^0\equiv$	$6^1\equiv$	$6^2\equiv$	$6^3\equiv$	$6^4\equiv$	$6^5\equiv$	$6^6\equiv$	$6^7\equiv$	$6^8\equiv$	$6^9\equiv$	$6^{10}\equiv$	$6^{11}\equiv$

Observa els resultats i expressa el que ha passat

.....

Ja Gauss havia utilitzat aquesta propietat per treballar amb números grans però fins i tot abans que ell, un altre matemàtic francès, Pierre de Fermat (1601-1655) havia fet un gran descobriment, el petit teorema de Fermat treballant amb rellotges que tenien un número primer d'hores, que representarem per p. Per a aquests rellotges, igual que ha passat en el nostre exemple, per a qualsevol hora a, al calcular a^p sempre dóna per resultat el propi valor a

Per a p = 5, al calcular les diferents potències s'obté 2, 4, 3, 1, 2, 4, 3, 1, 2, 4, 3, 1,... de forma iterativa, però si p=13 ix 3, 9, 1, 3, 9, 1, 3, 9, 1,... l'agulla del rellotge no es deté en totes les hores però ho fa tot seguint un model iteratiu. Utilitzant la notació de Gauss el petit teorema de Fermat el podem expressar: per a qualsevol número primer p i qualsevol valor a sobre l'esfera del rellotge de p hores $a^p \equiv a$ (mod p).

Posteriorment, altre gran matemàtic el suïs Leonard Euler (1707-1783), va generalitzar el resultat de Fermat per a rellotges de N hores amb la peculiaritat de que N=pxq on p i q són dos números primers.

Aquests dos resultats trobaren aplicació posteriorment quan en 1978, Ron Rivest, Adi Shamir i Len Adleman els van rescatar per idear un sistema criptogràfic, conegut per RSA en el seu honor, i que pot ser siga el xifrat de clau pública més estès. Si vols saber-ne més envers aquest tema, pots anar-hi a l'arxiu: "Per saber més"

Elaborado por:
Federación Española de Sociedades de Profesores de Matemáticas
MINISTERIO DE EDUCACIÓN
SECRETARÍA DE ESTADO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL
DIRECCIÓN GENERAL DE FORMACIÓN PROFESIONAL