Un garbell d'Eratòstenes

Artur Travesa

(versió 2021-04)

Introducció general

L'origen d'aquestes notes es remunta a diferents cursos d'Aritmètica o de Criptografia, a càrrec de l'autor, per a estudiants de Matemàtiques o d'Informàtica de la Universitat de Barcelona.

La idea bàsica és descriure algunes aplicacions importants de l'Aritmètica bàsica (diguem, de nivell de primer curs) a les transmissions xifrades d'informació.

En cap cas es tracta d'un curs de Criptografia, que caldria encabir en espais més amplis de coneixements, que haurien d'incloure, probablement, parts de teoria de la comunicació, de complexitat algorítmica o computacional, d'aprenentatge automàtic, o d'estudi de teories de compartició de secrets, entre d'altres.

El format triat per a la presentació és el d'un *notebook* de *Mathematica*, per la facilitat que té aquest programari per a poder desenvolupar els càlculs no trivials de manera prou senzilla i entenedora, d'una banda, i per a permetre fer una presentació escrita prou raonable des del punt de vista de material escrit, de l'altra. En particular, la possibilitat d'incloure els càlculs dins del text de manera natural en fan una bona eina comunicativa i, alhora, facilita molt el càlcul amb exemples no trivials.

A fi de veure tot el contingut del *notebook* convé executar-lo. Això es pot fer de cop o bé, més recomanable, cel·la a cel·la a mesura que s'avança en la lectura i comprensió dels diferents continguts.

Observació: Per al cas en què no es disposi del programari, hi ha una versió executada del *notebook* en format pdf.

Amb la finalitat doble d'una banda, de no fer textos molt llargs o amb molts continguts, i de l'altra de poder ampliar de manera senzilla els continguts que s'hi tractin, el material s'ha dividit en diferents *notebooks*, que desrivim a continuació, en l'apartat de referències.

Referències

[Cripto- 1]: **Criptografia bàsica (1)**.
Travesa, A.:CriptografiaBasica-1; accessible en forma notebook o en format pdf des de https://travesa.cat/notes/
Contingut: Una iniciació a la codificació de missatges. El criptosistema de Cèsar. El criptosistema de Vigenère.

[Cripto- 2]: **Criptografia bàsica (2)**.
Travesa, A.: CriptografiaBasica-2; accessible en forma notebook o en format pdf des de https://travesa.cat/notes/
Contingut: Els criptosistemes lineals. Els criptosistemes afins. Sufixació de missatges. Farciment de missatges.

[Eratostenes]: **Un garbell d'Eratòstenes.**
Travesa, A.: Eratostenes; accessible en forma notebook o en format pdf des de https://travesa.cat/notes/
Contingut: Un garbell d'Eratòstenes.

[Cripto- 3]: **Primeritat. Construcció de primers**.
Travesa, A.: ConstruccioDePrimers; accessible en forma notebook o en format pdf des de https://travesa.cat/notes/
Contingut: Test de primeritat de Solovay-Strassen. Test de primeritat de Miller-Rabin. Un certificat congruencial de primeritat. Construcció certificada de nombres primers de mida prefixada. Aplicació al càlcul de claus RSA. Aplicació (exercici) al càlcul de claus ElGamal.

[Cripto- 4]: **Factorització**.
Travesa, A.: Factoritzacio; accessible en forma notebook o en format pdf des de https://travesa.cat/notes/
Contingut: Un garbell d'Eratòstenes. Tests de primeritat de Solovay-Strassen i de Miller-Rabin. Un certificat congruencial de primeritat. Un algoritme bàsic de divisó per nombres primers petits. Un algoritme bàsic de divisó per nombres petits. El mètode de factorització de Fermat. El mètode de factorització p-1 de Pollard. El mètode de factorització rho de Pollard.

[RSA]: **Criptosistemes de tipus RSA**.
Travesa, A.: RSA; accessible en forma notebook o en format pdf des de https://travesa.cat/notes/
Contingut: Una descripció bàsica dels criptosistemes de tipus RSA: les claus; xifratge; desxifratge; observacions sobre la seguretat.

[ElGamal]: **El criptosistema ElGamal**.
Travesa, A.: ElGamal; accessible en forma notebook o en format pdf des de https://travesa.cat/notes/
Contingut: Logaritmes discrets. Una descripció bàsica del criptosistema ElGamal: el grup cíclic; les claus; xifratge i desxifratge.

[Tr-1]: Travesa, A.: *Aritmetica*. Edicions de la Universitat de Barelona, col·lecció UB, n. 25. Barcelona, 1998. ISBN:84-8338-031-5.

Un garbell d'Eratòstenes

La funció següent és una implementació bàsica del garbell d'Eratòstenes.

```
Eratostenes[ff_] := Module[{pr, i, j, f, k},
  f = Floor[(ff + 1) / 2];
  pr = Table[1, {i, 1, f}];
  i = 2;
  k = Floor[(Sqrt[ff] + 1) / 2];
  While[i ≤ k,
   If[pr[[i]] == 1, For[j = 2 i (i - 1) + 1, j ≤ f, j += 2 i - 1, pr[[j]] = 0 ]];
   i = i + 1;
  ];
  Complement[Union[{2}, Table[(2 i - 1) pr[[i]], {i, 2, f}]], {0}]
 ]
```

Exemples

Aquesta funció **Eratostenes[ ]** sempre proporciona una llista no buida que, com a mímin, conté el nombre 2.

```
Eratostenes[0]
```

```
{2}
```

Eratostenes[1]

```
{2}
```

Eratostenes[2]

```
{2}
```

Eratostenes[3]

```
{2, 3}
```

Eratostenes[4]

```
{2, 3}
```

Eratostenes[5]

```
{2, 3, 5}
```

Eratostenes[100]

```
{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97}
```

Observacions

1. La funció **Eratostenes[ ]** calcula la llista dels nombres naturals primers menors que una fita raonable en un temps raonable.

```
Timing[er = Eratostenes[1 000 000];]
```

```
{3.384, Null}
```

```
Length[er]
```

```
78 498
```

```
Timing[er = Eratostenes[100 000];]
```

```
{0.3, Null}
```

2. Aquesta implementació de la funció **Eratostenes[ ]** no és, ni de bon tros, òptima.
D'una banda, una bona implementació hauria de fer servir només un bit per a indicar la posició de cada nombre senar menor que la fita; en canvi, aquesta implementació utilitza, probablement, un mínim d'un byte per a cadascuna d'aquestes posicions (si no més). A més a més, caldria treballar directament sobre bits i no sobre bytes.
De l'altra, a més a més del càlcul de les posicions que ens permeten dir quins són els nombres primers, aquesta implementació també calcula explícitament aquests nombres, fet que és, gairebé sempre, innecessari.
3. Finalment, es fa sempre l'assignació **pr[[j]]=0**. Caldria veure si això és més o menys eficient que fer l'assignació condicional només en el cas en què sigui **pr[[j]]=1**; és a dir, si és més o menys eficient que utilitzar la comanda **If[pr[[j]]==1,pr[[j]]=0]**.