Primeritat i factorització

Artur Travesa

(versió 2024-07)

Introducció

C.F. Gauss, a l'inici de l'article 329 de les *Disquisicions Aritmètiques*, fragment que reproduïm de la versió de la Dra. Griselda Pascual Xufré, editada per l'IEC, el 1996, i que recomanem llegir íntegrament (cf. **[Ga-DA]**), escriu:

"El problema de distingir nombres primers de compostos i descompondre aquests en els seus factors primers, que pertany als més importants i més útils de tota l'aritmètica, [...], és tan conegut que seria superflu parlar abundantment d'això. Malgrat tot, [...]"

La idea que guia aquestes notes és descriure elementalment, diguem, a nivell d'un primer curs universitari, com es poden realitzar alguns càlculs d'Aritmètica bàsica amb eines també bàsiques. Només s'haurien d'interpretar, doncs, com un curs d'*Iniciació* a la Teoria computacional de Nombres.

Un curs de Teoria computacional de Nombres s'hauria d'encabir en espais més amplis de coneixements, que haurien d'incloure Teoria de Nombres en tots els vessants (algebraic, analític, geomètric, probabilístic, etcètera), a més a més de teories de complexitat algorítmica o computacional, de computació científica, i de càlcul numèric, entre d'altres.

L'origen de les notes es remunta a diferents cursos d'Aritmètica o de Criptografia que he desenvolupat per a estudiants de Matemàtiques o d'Informàtica a la Universitat de Barcelona. El resultat és conseqüència d'una reflexió sobre com fer accessibles uns continguts bàsics, però no trivials, d'Aritmètica, i aplicar-los a la realització de càlculs prou interessants en temes de Criptografia; per exemple, a la construcció de claus per a criptosistemes de tipus RSA o ElGamal. A més a més, tot i que no n'és l'objectiu principal, el contingut permet assentar algunes bases per a poder estudiar més profundament altres temes de Teoria computacional de Nombres.

El format que he triat per a la presentació d'aquestes notes és "una llibreta de *SageMath* per a cada capítol". N'esmentaré dues raons.

Primerament, aquest programari permet fer càlculs no trivials de manera prou senzilla i entenedora i, a més a més, és d'accés lliure per a tothom interessat i funciona en plataformes també d'accés lliure.

I en segon lloc, permet fer una presentació prou agradable del material escrit; en particular, la possibilitat d'intercalar els càlculs dins del text de manera natural en fan una bona eina comunicativa i, alhora, facilita molt el càlcul d'exemples no trivials.

A fi de veure tot el contingut de cada llibreta convé executar-la. Això es pot fer de cop o bé, i així és més recomanable, cel·la a cel·la a mesura que s'avança en la lectura i la comprensió dels diferents continguts. I a fi de facilitar la seva lectura i, més important, el seu ús, a l'inici de cada capítol s'incorporen les funcions necessàries de capítols anteriors. Això fa innecessari tornar a programar-les cada vegada que es necessiten.

Contingut

Secció A0.4. Construcció de primers

Secció A0.5. Refinament i repartició

Secció A0.6. Mètode de factorització de Fermat

Secció A0.7. Mètode de factorització rho de Pollard

Secció A0.8. Mètode de factorització p-1 de Pollard

Secció A0.9. Algoritme general de factorització

Referències

Fi de la introducció