

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

Capítol 0. Un garbell d'Eratòstenes

Secció 0.0. Una versió bàsica

Secció 0.1. La llista dels nombres primers

Secció 0.2. Observacions

Capítol 1. Tests de primeritat

Secció 1.0. Introducció

Secció 1.1. Tests o certificats?

Secció 1.2. Test de Solovay-Strassen

Secció 1.3. Test de Miller-Rabin

Secció 1.4. Certificació de nombres compostos

Secció 1.5. Comparació dels tests

Capítol 2. Certificats de primeritat

Secció 2.0. Introducció

Secció 2.1. Un certificat bàsic

Secció 2.2. La funció Certifica(pp,fp_{pmu},ff)

Secció 2.3. El certificat de Pocklington

Secció 2.4. Comprovació de certificats

Capítol 3. Construcció certificada de nombres primers

Secció 3.0. Introducció

Secció 3.1. Primers de 112 bits

Secció 3.2. Primers de 480 bits

Secció 3.3. Primers de 512 bits

Secció 3.4. Els valors obtinguts

Capítol 4. Un algoritme general de factorització

Secció 4.0. Introducció

Secció 4.1. Els passos inicials

Secció 4.2. L'algoritme bàsic

Secció 4.3. La funció Reparteix(lta)

Secció 4.4. Refinament de factoritzacions

Secció 4.5. Primera versió de la funció Factoritza(nn)

Capítol 5. Algoritme de divisió

Secció 5.0. Introducció

Secció 5.1. El primer pas, el garbell

Secció 5.2. Dividim

Secció 5.3. Exemples

Secció 5.4. Segona versió de la funció Factoritza(nn)

Capítol 6. Mètode de Fermat

Secció 6.0. Introducció

Secció 6.1. El mètode

Secció 6.2. La funció

Secció 6.3. Exemples

Secció 6.4. Observació

Capítol 7. Mètode rho de Pollard

Secció 7.0. Introducció

Secció 7.1. El fonament teòric

Secció 7.2. L'algoritme

Secció 7.3. La funció PollardRho(nn, tt, ff)

Secció 7.4. Tercera versió de la funció Factoritza(nn)

Capítol 8. Mètode p-1 de Pollard

Secció 8.0. Introducció

Secció 8.1. Descripció del mètode p-1

Secció 8.2. La funció PollardPmU(nn, ff)

Secció 8.3. Quarta versió de la funció Factoritza(nn)

Secció 8.4. Exemples

Capítol 10. Construcció certificada de claus RSA

Secció 10.0. Introducció

Secció 10.1. Restriccions per a les claus RSA per a signatura digital

Secció 10.2. Primers de 112 bits

Secció 10.3. Primers de 480 bits

Secció 10.4. Primers de 1024 bits

Secció 10.5. Primers de 2048 bits

Secció 10.6. Els valors obtinguts per a una possible clau

Apèndix 0. Manual de les funcions

Secció A0.0. Introducció

Secció A0.1. Garbell d'Eratòstenes

Secció A0.2. Tests de primeritat i certificats de composició

Secció A0.3. Certificats de primeritat

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