

Presentació i Objectius de l'assignatura

L'assignatura té com a objectiu ser un introducció als problemes aritmètics i, a la vegada, oferir una visió dels mètodes que intervenen en l'anàlisi i resolució d'aquests problemes. Donat que hi ha massa tipus de problemes en teoria de nombres com per a ser coberts en un curs d'aquestes característiques, el curs es basa principalment en els problemes diofàntics, i s'introdueixen a partir d'aquests la teoria algebraica de nombres en el sentit clàssic.

El curs es divideix en tres parts bastant diferenciades: restes quadràtics, cossos de nombres i cossos p-àdics. El nexa que els uneix es la resolució d'equacions diofàntiques. Per exemple, un dels objectius del curs serà anar resolent certs casos especials de l'equació de Bachet-Mordell $y^2 = x^3 + k$.

A la segona part ens centrarem bàsicament en els cossos quadràtics, extensions de grau dos dels racionals, tot i que algun resultat el farem en general.

Durant tot el curs s'intentarà posar l'èmfasi també en les aplicacions a la criptografia dels resultats obtinguts. També s'introduiran les eines informàtiques que permeten resoldre molts d'aquests problemes: per exemple SAGE, PARI, MAPLE i MAGMA

Coneixements matemàtics previs

Els prerequisits del curs són les assignatures obligatòries d'àlgebra del grau de matemàtiques. És recomanable haver fet l'assignatura de Teoria de Galois.

Programa

1. Introducció a l'Aritmètica

- (a) De que s'ocupa l'Aritmètica?
- (b) Molt breu història de l'Aritmètica.
- (c) Alguns resultats elementals: Ternes pitagòriques.
- (d) Equacions diofàntiques.

2. Teoria de congruències.

- (a) Repàs de resultats bàsics: cossos finits, teorema dels restes.
- (b) Resolució d'equacions mòdul n .

- (c) Solucions mòdul p^r versus solucions mòdul p
- (d) Restes quadràtics mòdul p : símbol de Legendre.
- (e) La llei de reciprocitat quadràtica.
- (f) Algunes aplicacions bàsiques. Criptografia.
- (g) El teorema de Chevalley-Waring.

3. Cossos p -àdics.

- (a) Enters p -àdics de manera elemental.
- (b) Topologia p -àdica i valoracions.
- (c) Completacions de cossos.
- (d) Resolució d'equacions en els p -àdics.
- (e) El principi de Hasse.
- (f) Series de potències i convergència.

4. Cossos de nombres

- (a) Per a que volem estudiar les extensions finites de $\mathbb{Q}$?
- (b) Elements algebraics sobre un anell.
- (c) Discriminant, norma i traça.
- (d) Factorització d'elements en cossos de nombres.
- (e) Ideals primers. Teorema de factorització única.
- (f) Ideals fraccionaris. Grup de classes d'ideals.
- (g) Mètodes geomètrics: el Teorema de Minkowsky.
- (h) Primeres aplicacions.
- (i) El teorema de finitud del grup de classes d'ideals.
- (j) Com convertir un ideal en principal?
- (k) El teorema de les unitats de Dirichlet.

Bibliografia

Bibliografia bàsica

P. Samuel *Teoría algebraica de los números* Ediciones Omega, 1972

I.N. Stewart, D.O. Tall *Algebraic Number Theory* Chapman and Hall, 1979

J.-P. Serre *Cours d'Arithmétique* Presses universitaires de France, Dunod, Paris, 1967

Bibliografia complementària

Z.I. Borevich y I.R. Shafarevich *Number Theory* Academic Press, 1966

J. Cilleruelo, A. Córdoba. *La teoría de los números.* Editorial Mondadori, 1992.

F. Gouvêa *p-adic Numbers: an introduction* Springer-Verlag, Berlin, 1997

L.J. Mordell *Diophantine Equations* Academic Press, 1969

J. Neukirch *Algebraic number theory* Springer-Verlag 1999

Professors

Xavier Xarles.

Avaluació

Durant el curs s'hauran d'entregar problemes individualitzats que contaran fins a un 40 % de la nota final. També es podrà fer un breu treball (de 4 a 8 cares) que contaria fins un 30% de la nota, que consistirà en explicar un resultat no fet directament a classe, amb una referencia concreta d'on mirar-lo. El treball es podrà fer en grup (de 2). El reste de la nota (un mínim d'un 30%) s'obtindrà d'un examen final amb una part de teoria més algun problemes semblants als fets durant el curs.