GUIA DOCENT DE MATEMÀTICA DISCRETA

1. IDENTIFICACIÓ DE L'ASSIGNATURA

Nom: Matemàtica Discreta
Codi: 27991
Crèdits: 12
Tipus: Obligatòria

2. OBJECTIUS

Un dels objectius d'aquesta assignatura és introduir a l'alumne a les eines algebraiques bàsiques. Per això, es dedica especial atenció, durant la primera part del curs, a l'ús adequat del llenguatge matemàtic. Així, es fa una breu introducció a les aplicacions entre conjunts i les relacions d'equivalència, donant ja uns primers models discrets que s'apliquen a problemes concrets de combinatòria. A la segona part del curs, i ja de manera més concreta, l'objectiu és que a partir de l'estudi d'exemples ben coneguts com són els nombres enters i els polinomis, l'alumne s'introdueixi en el procés d'abstracció observant les propietats anàlogues dels dos anells i poder així començar a estudiar les primeres estructures algebraiques (anells, grups, cossos finits...)

Aquesta assignatura ha de contribuir a que l'alumne adquireixi una adequada formació matemàtica, havent vist un bon nombre de teoremes i demostracions, que el permeti començar a entendre quan una demostració és necessària i a construir-la ell mateix. També ha d'adquirir hàbits crítics davant les afirmacions matemàtiques i, sobretot, ha de desenvolupar un esperit combatiu davant dels problemes.

3. CONTINGUTS

1- Conjunts i aplicacions

- Llenguatge bàsic de conjunts.
- Aplicacions entre conjunts. Aplicacions injectives, exhaustives i bijectives. Composició.
- Permutacions. Descomposició en cicles disjunts. Signe.
- Relacions d'equivalència i particions. Conjunt quocient. El conjunt quocient $\mathbb{Z}/(n)$.

2- Combinatòria

- Aplicacions entre conjunts i compteig. Conjunt finit/infinit.
- Principi de les caixes. Principi de l'addició.
- Aplicacions, paraules i seleccions ordenades. Seleccions ordenades amb i sense repetició.
- Subconjunts. Seleccions no ordenades sense repetició. Nombres binomials.
- Seleccions no ordenades amb repetició. Teorema del binomi.
- Principi de la criba. La funció d'Euler.
- Permutacions amb repetició i nombres multinomials. Teorema multinomial.

3- Enters i congruències

- Divisió entera. Màxim comú divisor i mínim comú múltiple.
- Algorisme d'Euclides. Equacions diofàntiques.
- Nombres primers entre ells i nombres primers. Factorització en primers.
- Congruències. Els anells $\mathbb{Z}/(m)$.
- El criptosistema RSA.
- Noció d'anell i de morfisme d'anells.

4- Polinomis

- Definició de l'anell de polinomis sobre un cos.
- Divisió entera de polinomis. Màxim comú divisor i mínim comú múltiple.
- Polinomis irreductibles i polinomis primers entre ells. Descomposició en irreductibles.
- Zeros d'un polinomi.
- Números complexos. Arrels d'un número complex. Descomposició en irreductibles a $\mathbb{C}[x]$ i a $\mathbb{R}[x]$.
- Polinomis sobre el cos de p elements.
- Els anells $K[x]/(m(x))$.

5- Grups

- Definició de grup. Exemples bàsics: grups de permutacions, $\mathbb{Z}/(m)$, grups de matrius, grup dels invertibles d'un anell, grups de moviments.
- Subgrups. Teorema de Lagrange.
- Subgrup normal i grup quocient. Morfisme de grups. Teorema d'isomorfisme.
- Classificació dels grups cíclics.

6- Cossos finits

- Característica d'un cos finit. Cos primer i nombre d'elements d'un cos finit.
- Teorema de l'element primitiu.

4. TEMPS DE DEDICACIÓ DE L'ALUMNE.

TIPUS D'ACTIVITAT	Descripció	Hores
ACTIVITATS PRESENCIALS	Classes de Teoria	60
	Classes de Problemes	60
	Classes de Pràctiques	0
	Activitats Tutoritzades	32
	Realització de proves parcials	4
	Realització d'examens finals	8
ACTIVITATS NO PRESENCIALS	Estudiar Teoria	60
	Fer exercicis	30
	Preparar Entrevistes	4
	Preparar proves parcials	8
	Preparar exàmens finals	32

Cal tenir en compte que, tal i com s'explicarà a l'apartat de mètode, hi ha 30 hores d'activitats presencials tutoritzades en que l'alumne es troba suposadament en un aula fent exercicis de l'assignatura. Així doncs aquestes hores corresponen també a hores d'estudi d'exercicis.

5. CAPACITATS O DESTRESES A ADQUIRIR

Teòriques

- Aprendre el llenguatge de conjunts (unió, intersecció, complementari, producte cartesià) i utilitzar-lo correctament en demostracions. No aprofundirem en la noció formal de conjunt.

- Aprendre a desenvolupar-se amb facilitat amb aplicacions entre conjunts (composicions, antiimatges de subconjunts) i dominar les nocions d'exhaustivitat, injectivitat, bijectivitat i inversa d'una aplicació.
- Entendre la noció de conjunt quocient. Diferenciar entre classe i representant. Entendre'n el perquè de l'ús i la simplificació que ens aporta en demostracions (per deduir les fórmules de combinatòria, per exemple). Entendre la necessitat de demostrar que quelcom està ben definit en un conjunt quocient.
- Coneixement de les propietats de $\mathbb{Z}/(m)$ com a conjunt quocient.
- Entendre la formalització del concepte intuïtiu de comptar elements d'un conjunt finit de cara a desenvolupar matemàticament els models i principis bàsics de la combinatòria.
- Coneixement de la definició de cardinal d'un conjunt finit.
- Coneixement dels principis i models bàsics de combinatòria (Principi de les caixes, Principi de l'addició i de la multiplicació, principi de la criba, seleccions ordenades/no ordenades amb repetició/sense repetició, permutacions amb repetició). Entendre'n les demostracions.
- Aprendre la definició i les propietats de la funció φ d'Euler.
- Aprendre els conceptes bàsics de l'aritmètica i divisibilitat d'enters (divisió entera, divisor i múltiple, màxim comú divisor i mínim comú múltiple, identitat de Bézout, descomposició en primers). Conèixer les propietats i les seves demostracions.
- Aprendre els conceptes bàsics de l'aritmètica i divisibilitat de polinomis (grau, divisió entera, divisor i múltiple, màxim comú divisor i mínim comú múltiple, identitat de Bézout, descomposició en primers). Conèixer les propietats i les seves demostracions.
- Entendre el paral.lelisme entre les nocions de divisibilitat en enters i en polinomis (valor absolut/grau, positiu/mònic, ± 1 / constants no nul.les, primer/irreductible, ...).
- Conèixer la relació entre les arrels d'un polinomi i la descomposició del polinomi.
- Entendre les nocions d'anell, d'invertible i de divisor de zero en general i conèixer alguns exemples a part dels enters i els polinomis.
- Entendre $K[x]/(f(x))$ com a conjunt quocient i com a anell.
- Entendre la noció abstracta de grup.
- Entendre les demostracions de les propietats bàsiques de grups.
- Entendre els conceptes de subgrup generat per un element, ordre d'un element i grup cíclic.
- Conèixer el Teorema de Lagrange.
- Entendre el concepte de morfisme de grups i grup quocient.
- Entendre l'estudi dels cossos finits on utilitzen les tècniques d'aritmètica modular, de polinomis, de grups i d'àlgebra lineal que han anat apareguent al llarg del curs.
- Entendre l'estructura quocient: la compatibilitat d'una relació d'equivalència amb una operació a l'hora de definir una operació al conjunt quocient.

Pràctiques

- Coneixement exhaustiu a nivell pràctic del grup de les permutacions d'un conjunt finit (composició, descomposició en cicles disjunts, ordre i signe).
- Adquirir familiaritat en l'ús del conjunt quocient anant més enllà de la definició teòrica. Saber-hi treballar en casos concrets.

- Coneixement de les propietats bàsiques dels nombres combinatoris i multinomials i la seva aplicació al càlcul de potències.
- Utilitzar la identitat de Bézout per a la resolució d'equacions diofàntiques.
- Aprendre a utilitzar la identitat de Bézout per resoldre problemes teòrics.
- Conèixer i tenir familiaritat amb $\mathbb{Z}/(m)$ i les seves propietats com a anell (invertibles, divisors de zero, resolució d'equacions).
- Aplicar el petit Teorema de Fermat i la congruència d'Euler per al càlcul de potències a $\mathbb{Z}/(m)$.
- Dominar els llenguatges d'equacions diofàntiques, de congruències i d'equacions a $\mathbb{Z}/(m)$ i entendre l'avantatge de cadascun d'ells. Saber traduir els problemes amb facilitat d'un a l'altre llenguatge i trobar el més adient per a la seva resolució.
- Descompondre polinomis a $\mathbb{C}[x], \mathbb{R}[x], \mathbb{Q}[x]$ i $\mathbb{Z}/(p)[x]$ (p primer).
- Comptar polinomis irreductibles a $\mathbb{Z}/(p)[x]$, comptar divisors d'un polinomi. Aplicar tècniques de combinatòria en aquest àmbit.
- Saber calcular a $K[x]/(f(x))$ en el cas de $K = \mathbb{Z}/(p)$.
- Conèixer els exemples següents de grups $\mathbb{Z}, S_n, \mathbb{Z}/(m)$, invertibles de $\mathbb{Z}(m)$, grup additiu de les matrius, grup de les matrius invertibles, complexes no nuls amb el producte, arrels complexes de la unitat. Treballar-hi els conceptes bàsics de grups.
- Aplicar el Teorema de Lagrange per trobar subgrups i ordres d'elements.
- Utilitzar les eines per conèixer i classificar els grups cíclics i els seus subgrups.
- Saber calcular a cossos finits concrets de la forma $\mathbb{Z}/(p)[x]/(f(x))$ (aritmètica i resolució d'equacions senzilles)

de Modelització

- Utilitzar el llenguatge d'aplicacions per modelar problemes de combinatòria.
- Saber traduir a llenguatge matemàtic els problemes de comptar. Aprendre a adscriure'ls a un model conegut escaient o bé construir una petita variant dels models coneguts si és necessari.
- Aprendre a resoldre problemes de planteig on es tractin quantitats enteres i que es poden resoldre utilitzant equacions diofàntiques i congruències.

6. **REQUISITS.**

   És difícil enumerar els requisits necessaris per a aquesta assignatura, ja que el que es pretén és donar un marc abstracte en què treballar determinats conceptes matemàtics bàsics que l'alumne de ben segur coneix.

   Tot i això, aquest procés d'abstracció es fa amb una rigorositat matemàtica amb la qual l'alumne pot no estar molt familiaritzat. És per això que es requerirà una especial dedicació en aquest sentit.

   D'altra banda, el que si que és indispensable és un bon coneixement a nivell pràctic de l'aritmètica entera i certa habilitat en la manipulació d'expressions algebraiques que s'usaran per generalitzar determinats conceptes.

7. **METODOLOGIA.**

   Aquesta assignatura té dues hores setmanals de teoria i dues hores de problemes.

Els alumnes disposaran amb antelació dels apunts de l'assignatura i se'ls aconsella que se'ls mirin abans de la classe de teoria. El coneixement de les nocions introduïdes, els enunciats dels teoremes i les seves aplicacions són imprescindibles a l'hora de posar-se a atacar els problemes. Però també és bàsica la comprensió de les demostracions dels teoremes i proposicions per tal de resoldre els problemes amb tècniques semblants. Durant l'explicació del professor o amb hores de consulta els alumnes haurien de preguntar tots els dubtes que tinguin.

Es disposarà d'una llista de problemes i setmanalment hi haurà dues sessions de problemes d'una hora. En aquestes, el professor resoldrà alguns dels exercicis per tal que l'alumne aprengui els mètodes addiets per a cada tipus de problema.

D'altra banda, periòdicament es realitzaran unes sessions de problemes en què els alumnes treballaran en grups les llistes de problemes, preguntant al professor tantes vegades com els sigui necessari (si no comprenen l'enunciat, si estan encallats i volen una pista, si volen que els corregeixi el que han escrit...) i si és convenien el professor explicarà la resolució dels problemes més representatius de la llista. En aquest moment és bàsica la participació dels estudiants per contrastar la seva resolució amb la del professor, corregir-la o aportar diferents maneres d'abordar els problemes. És importantísssim que l'alumne s'hagi barallat a fons amb els problemes, i per tant, també és convenient que preparin la llista abans d'anar a classe. A banda del treball fet a classe, els alumnes hauran d'acabar les llistes pel seu compte.

Periòdicament es proposarà un exercici per entregar. Aquest pot ser dels que ja hi havia a la llista que s'ha estat treballant aquests dies o bé un de nou que el professor plantejarà a classe. Aquest es resoldrà generalment usant tècniques similars a les que ja s'han usat amb els altres exercicis de la llista així que és convenient haver-la treballat a fons per poder-hi aplicar els coneixements adquirits. A més, cada dues entregues de problemes, es faran entrevistes amb l'alumne en què es comentaran els exercicis entregats. És per això que seria convenient que l'alumne es guardi una còpia d'aquests per poder preparar l'entrevista. En aquests s'intentarà orientar a l'alumne en la manera correcta d'escriure o redactar arguments matemàtics.

A més, l'assignatura disposa d'una pàgina al "campus virtual" on hi anirem penjant les llistes d'exercicis, els apunts de l'assignatura, material extra i qualssevol informació referent a l'assignatura.

A banda de tot això els alumnes disposaran d'unes hores de consulta al despatx del professor de teoria i de problemes, on podran consultar dubtes, demanar ajuda per a la resolució d'un pas determinat d'un problema, etc.

8. **Avaluació**

Primera Convocatòria (Juliol)

- Un 25% de la nota correspon a l'avaluació continuada. Aquesta nota s'obté de:

  l'entrega i correcció dels problemes,

  les entrevistes en què es discutiran els problemes anteriorment lliurats i,

  2 proves d'una durada de dues hores.

  D'aquí s'obtindrà una nota sobre 10 que anomenarem c
- L'altre 75% es farà amb notes d'examens. Aquesta nota es pot obtenir de 2 maneres
  - **Per parcials**
    Al final de cada semestre es farà un examen sobre la matèria d'aquell semestre. L'alumne obtindrà així dues notes p_1 i p_2 (sobre 10) del primer i del segon parcial respectivament. Si un alumne té les notes $p_1 \geq 3$ i $p_2 \geq 3$, llavors la seva nota per parcials és

$N_1 = 0.25 \cdot c + 0.35 \cdot p_1 + 0.4 \cdot p_2$.
Si $N_1 \geq 5$, llavors l'alumne pot triar entre dues opcions:

(a) Que N_1 sigui la seva nota a la convocatòria de juny.

(b) Presentar-se a l'examen final per millorar aquesta nota. En aquest cas l'alumne obtindrà com a mínim la nota N_1 a la convocatòria de juliol.

– **Per final**
Després del segon parcial es farà un examen final de tota l'assignatura. Diguem j a la nota d'aquest examen i posem

$$N = 0.25 \cdot c + 0.75 \cdot j.$$

La nota de la convocatòria de juliol és:
$max(N_1, N, 5)$ si $j \geq 5$ o $max(N_1, N)$ si $j < 5$.
Nota: *Si un alumne té la nota $N_1 < 5$ i no es presenta a l'examen final tindrà un "no presentat" a la convocatòria de juliol.*

Segona Convocatòria (Setembre)

Hi haurà un examen global de tota l'assignatura. Aleshores la nota de la segona convocatòria s'obté seguint el mateix procés de la primera convocatòria (per final) substituint la nota de l'examen final de juliol (j) per la de l'examen de setembre (s).

9. **Bibliografia**

Bibliografia bàsica

Antoine, R.; Camps, R. i Moncasi, J. Apunts de Matemàtica Discreta

Biggs, N.L. Matemática Discreta *Ed Vicens Vives, 1994.*

Dorronsoro, J.; Hernández, E. Números, grupos y anillos *Addison-Wesley/Universidad Autónoma de Madrid, 1996.*

Bibliografia complementària

Basart, J.M.; Rifà, J.; Villanueva, M. Fonaments de Matemàtica Discreta. *Materials UAB, 36. 1997*

Cedó, F.; Gisin, V. Àlgebra Bàsica *Manuals de la Universitat Autònoma de Barcelona. Publicacions UAB, 1997*

10. **Professorat**

Ramon Antoine	Francesc Perera	Ferran Cedó
Teoria i Problemes	*Problemes*	*Problemes dirigits*
C1/324, 935811395	C1/210, 935814542	C1/352, 935814156
ramon@mat.uab.es	perera@mat.uab.es	cedo@mat.uab.es