La joia de l'Aritmètica

L'objectiu general del treball que es proposa és familiaritzar-se amb els conceptes i resultats bàsics de "l'Aritmètica modular" (o de les congruències).

Donat un nombre natural n, una *congruència mòdul n* és una expressió

$$a \equiv b \pmod{n},$$

on a i b són enters; vol dir, simplement, que $a - b$ és múltiple de n. Mòdul n, els enters a i b queden identificats. Per exemple, mòdul 6, els múltiples de 6 representen el 0, i els enters $\ldots, -7, -1, 5, 11, \ldots$ representen un únic element.

En el cor de l'Aritmètica Modular trobem la *Llei de reciprocitat quadràtica*:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}},$$

vàlida per a tot parell de nombres primers senars diferents p i q.

Com a objectiu concret del treball proposem entendre i demostrar l'enunciat anterior (on $\left(\frac{p}{q}\right)$ NO és el nombre racional p/q). La primera prova completa d'aquest resultat fonamental la va obtenir Gauss ara fa més de 200 anys; ell l'anomenava "Teorema d'or" i el qualificava com "La joia de l'Aritmètica". Des d'aleshores, molts matemàtics han treballat per a obtenir-ne noves demostracions; actualment se'n coneixen més de 200.

Prèviament caldria introduir els conceptes bàsics (residu quadràtic, símbol de Legendre, ...) i justificar diverses propietats (resultats de Fermat, Euler, Lagrange, Legendre, ...), per tal de poder enunciar i demostrar la Llei de reciprocitat quadràtica (LRQ).

Si s'escau, el treball es pot completar/ampliar en alguna de les direccions següents:

- Aprofundir en la història del desenvolupament de l'Aritmètica modular.
- Estudiar diverses demostracions (de les "elementals") de la LRQ. Un exercici interessant, per exemple, seria expressar en terminologia moderna la primera demostració que dóna Gauss en la seva obra "Disquisitiones Arithmeticae" (traduïda al català!).

- Estudiar aplicacions de la LRQ en demostracions de resultats interessants com, per exemple, la caracterització dels nombres primers que són suma de dos quadrats.
- Estudiar i programar algun Test de primalitat basat en la LRQ.
- Programar el càlcul de símbols de Legendre, aprofitant la LRQ.

Responsable: Bernat Plans
e-mail: bernat.plans@upc.edu