Corbes hiperel·líptiques i corbes de gènere menor o igual que 3

Resum de la línia de recerca. Durant els anys 70, 80 i 90 es van produir avenços molt importants en l'aritmètica de les corbes el·líptiques, entre altres motius a causa de la facilitat amb què es pot treballar explícitament a partir de les seves equacions, a l'increment en l'ús d'eines de càlcul numèric i simbòlic, i a les seves aplicacions aritmètiques a l'estudi d'equacions diofàntiques (Frey) i tecnològiques per al disseny de sistemes criptogràfics (Koblitz). Des de mitjans dels 90 s'ha començat a estudiar les corbes de gènere 2 i les seves jacobianes (i, més en general, les corbes hiperel·líptiques) des d'un punt de vista explícit-computacional, tant pel que fa l'estudi de la seva aritmètica (punts racionals, grup de Mordell-Weil de la jacobiana, cossos de definició, grups d'automorfismes, etc.) com en les seves aplicacions a la criptografia i els codis correctors. L'equip d'investigació té una experiència considerable en l'estudi de les corbes hiperel·líptiques i, en particular, les corbes de gènere 2.