Exercici 11. Siguin $a, b \in \mathbb{Z}$ nombres enters tals que $\text{mcd}(a, b) = 1$. Calculeu $\text{mcd}(a^2 + b^2, a^2 - b^2, 2ab)$ en funcio de a i b.

Solucio 11

Tenim que $\text{mcd}(a^2 + b^2, a^2 - b^2, 2ab) = \text{mcd}(2a^2, a^2 + b^2, 2ab)$, distiguierm per casos en funcio de la paritat de a i b:

1. Cas a i b parells tenim que es imposible ja que llavors $\text{mcd}(a, b) \geq 2$ o $\text{mcd}(a, b) = 0$(si $a = b = 0$),
2. Cas a parell i b imparell o viceversa (el desenvolupment sera analog), tenim que $a^2 + b^2 = 4l + 4k^2 + 4k + 1 = 2(2k + 2l + 2k^2) + 1$, per tant $a^2 + b^2$, es imparell i aleshores $\text{mcd}(2a^2, a^2+b^2, 2ab) = 1$, ja que suposem que $\exists n > 1$ tal que $\text{mcd}(2a^2, a^2+b^2, 2ab) = n$, tenim que n ha de ser imparell ja que si fos parell no seria divisor de $a^2 + b^2$, sigui q un dels primers de la descomposicio en primers de n, tenim que, $q|n$ i $n|2a^2$, $n|a^2 + b^2$ o $n|2ab$, per la transitivitat de $|$, q divideix els tres membres del m.c.d., com que $q|a^2 + b^2$ i $q|2a^2$(i q es imparell ja que divideix $a^2 + b^2$), tenim que $q|a^2$, i per tant $q|b^2$, i per la primertat de q, extraiem que $q|a$ i $q|b$, i com q es primer tenim que $q > 1$, i per tant $\text{mcd}(a, b) \leq q > 1$, que comptradiu l'hipotesi que $\text{mcd}(a, b) = 1$, i per tant
$$\text{mcd}(2a^2, a^2 + b^2, 2ab) = 1$$
.
3. Cas a i b imparells, aqui tenim que $a^2 + b^2 = 4k^2 + 4k + 1 + 4l^2 + 4l + 1 = 2(2k^2 + 2k + 2l^2 + 2l + 1)$, i per tant, $a^2 + b^2$, i els altres membres del m.c.d, clarament, tambe, i tenim llavors que $\text{mcd}(2a^2, a^2 + b^2, 2ab) = 2$, ja que suposem que $\exists n > 2$ tal que $\text{mcd}(2a^2, a^2 + b^2, 2ab) = n$, aleshores tenim que $n|2a^2$ i $n|a^2 + b^2$, $\implies n|2a^2 - 2(a^2 + b^2) = -2b^2 \implies n|2b^2$, com que tenim que $\text{mcd}(a, b) = 1$, implica que no tenen cap factor en comu i per tant a^2 i b^2, clarament tampoc, per tant, $k|2$*, el que implica que $k \neq 2$ que contradiu el que hem suposat al principi, i per tant
$$\text{mcd}(2a^2, a^2 + b^2, 2ab) = 2$$
.

*Tenim que el raonament es cert ja que sigui q un nombre primer que apareix en la descomposicÃ^3*denombresprimersdentenimque*q—2a^2 i $q|2b^2$ i $q|2ab$, llavors $q|2$ o $q|a^2$, si $q|a^2 \implies q|a$, q no pot divir aleshores b i tampoc b^2, per tant com q no divideix b^2, $q|2$, i com es primer $q = 2$, com q es un factor primer de n $\exists c$ tal que $qsc = 2a^2$, i com $q = 2$, $sc = a^2$, i com $qsc' = 2b^2$, i per l'argument anterior $sc' = b^2$, i tenim que $s|b^2$ i $s|a^2$, ara com a^2 i b^2 no tenen factors en comu al no tenir-ne a i b, tenim que s $= 1$, i per tant $n = 2$. Que contradiu que $n > 2$.