Correctesa i Anàlisi del Cost de l'Algorisme d'Euclides

Enric Rodríguez

En aquest full estudiarem l'*algorisme d'Euclides* que, donats dos nombres naturals a i b, calcula el seu màxim comú divisor $GCD(a,b)$. Considerem la següent versió:

```
int euclides (int a, int b) {
/* Pre:  a > b i b >= 0 */
/* Post: euclides(a,b) = GCD(a,b) */
   if (b == 0)  return a;
   else         return euclides (b, a%b); }
```

Vegem per inducció sobre N, el nombre de crides recursives, que el codi és correcte:

- **Cas base:** $N = 0$. En aquest cas necessàriament $b = 0$, i per tant $GCD(a,b) = GCD(a,0) = a$, de forma que l'algorisme retorna el valor correcte.
- **Cas inductiu:** Siguin a i b tals que $euclides(a,b)$ fa N crides recursives, amb $N > 0$. Siguin q i r el quocient i el residu de dividir a entre b, de forma que $a = qb + r$ i $0 \leq r < b$. Com que $r = a\%b$, es compleix la precondició de la crida recursiva $euclides(b, a\%b)$. A més, $GCD(a,b) = GCD(b,a) = GCD(b, qb+r) = GCD(b,r)$, i per tant per HI es retorna el valor correcte.

A continuació analitzarem el cost de l'algorisme. A part de la crida recursiva, el treball a realitzar té cost constant. Així doncs, el cost és proporcional al nombre de crides recursives. Per tant ens limitarem a estudiar, donats a i b, quin és el nombre de crides recursives de $euclides(a,b)$.

Sigui F_N la *successió de Fibonacci*: $F_0 = 1$, $F_1 = 1$ i $F_N = F_{N-1} + F_{N-2}$ per $N \geq 2$. Demostrarem per inducció que si per a i b es fan N crides recursives (on $N \geq 1$), aleshores $a \geq F_{N+1}$ i $b \geq F_N$:

- **Cas base:** $N = 1$. Si es fa 1 crida recursiva, llavors $b \neq 0$. Com que $b \geq 0$ per la precondició, ha de ser $b \geq 1 = F_1$. A més, com que també per la precondició $a > b$, tenim $a \geq 2 = F_2$.
- **Cas inductiu:** $N > 1$. Siguin ara a i b tals que $euclides(a,b)$ fa N crides recursives. Siguin també q i r el quocient i el residu de dividir a entre b, de forma que $a = qb + r$ i $0 \leq r < b$. Llavors $euclides(b,r)$ requereix $N-1$ crides recursives. Per HI, $b \geq F_N$ i $r \geq F_{N-1}$. A més, com que $a > b$, necessàriament $q \geq 1$. Així doncs, $a \geq b + r \geq F_N + F_{N-1} = F_{N+1}$.

Queda doncs demostrat que, si $euclides(a,b)$ fa N crides recursives, aleshores $a \geq F_{N+1}$ i $b \geq F_N$. A més, es pot demostrar (vegeu a sota) que per tot $N \geq 0$ es té $F_N \geq \phi^{N-1}$, on $\phi = \frac{1+\sqrt{5}}{2} \approx 1.618$ és l'anomenat *nombre d'or*. Usant això, tenim que si per a i b l'algorisme d'Euclides fa N crides recursives, aleshores $b \geq F_N \geq \phi^{N-1}$, d'on $\log_\phi b \geq N - 1$ i $1 + \log_\phi b \geq N$. Per tant, N és $\mathcal{O}(\log b)$.

Finalment, demostrem per inducció que per tot $N \geq 0$ tenim $F_N \geq \phi^{N-1}$:

- **Cas base 1:** Per a $N = 0$, tenim $F_0 = 1 > \phi^{-1}$ ($\phi^{-1} \approx 0.618$).
- **Cas base 2:** Per a $N = 1$, tenim $F_1 = 1 = \phi^0$.
- **Cas inductiu:** Suposem $N \geq 2$. Observem que $\phi^2 = (\frac{1+\sqrt{5}}{2})^2 = \frac{3+\sqrt{5}}{2} = \phi + 1$. Per tant, per HI, $F_N = F_{N-1} + F_{N-2} \geq \phi^{N-2} + \phi^{N-3} = \phi^{N-3}(\phi + 1) = \phi^{N-1}$.