Exercici 8.

(a) Siguin a, m, n nombres naturals, $m \neq n$. Calculeu $\mathrm{mcd}(a^{2^m}+1, a^{2^n}+1)$.

(b) Siguin m, n nombres naturals i $d := \mathrm{mcd}(m,n)$. Demostreu que $\mathrm{mcd}(2^m-1, 2^n-1) = 2^d-1$.

Solució 8.

(a) Provarem que

$$\mathrm{mcd}(a^{2^m}+1, a^{2^n}+1) = \begin{cases} 1, & \text{si } a \text{ és parell i } m \neq n, \\ 2, & \text{si } a \text{ és senar i } m \neq n, \\ a^{2^m}+1, & \text{si } m = n. \end{cases}$$

Clarament, si $m = n$, llavors $\mathrm{mcd}(a^{2^m}+1, a^{2^n}+1) = a^{2^m}+1$ i ja hem acabat. Per tant, podem suposar, i ho fem, que $m > n$.

Notem que, en general, per a $r > 2^n$, tenim que

$$a^r + 1 - (a^{2^n}+1) = a^r - a^{2^n} = a^{2^n}(a^{r-2^n}-1)$$

i, com que $\mathrm{mcd}(a^{2^n}, a^{2^n}+1) = 1$, és

$$\begin{aligned} \mathrm{mcd}(a^r+1, a^{2^n}+1) &= \mathrm{mcd}(a^r+1-(a^{2^n}+1), a^{2^n}+1) \\ &= \mathrm{mcd}(a^{2^n}(a^{r-2^n}-1), a^{2^n}+1) \\ &= \mathrm{mcd}(a^{r-2^n}-1, a^{2^n}+1). \end{aligned}$$

Anàlogament, i també per a $s > 2^n$, tenim que

$$a^s - 1 + (a^{2^n}+1) = a^s + a^{2^n} = a^{2^n}(a^{s-2^n}+1)$$

i, com que $\mathrm{mcd}(a^{2^n}, a^{2^n}+1) = 1$, és

$$\begin{aligned} \mathrm{mcd}(a^s-1, a^{2^n}+1) &= \mathrm{mcd}(a^s-1+(a^{2^n}+1), a^{2^n}+1) \\ &= \mathrm{mcd}(a^{2^n}(a^{s-2^n}+1), a^{2^n}+1) \\ &= \mathrm{mcd}(a^{s-2^n}+1, a^{2^n}+1). \end{aligned}$$

Ara, notem que $2^m = 2^{m-n}2^n$, de manera que, per a $m > n$, podem restar 2^n de 2^m una quantitat parella de vegades (2^{m-n} és parell, perquè $m > n$). Així, obtenim que

$$\mathrm{mcd}(a^{2^m}+1, a^{2^n}+1) = \mathrm{mcd}(a^0+1, a^{2^n}+1) = \mathrm{mcd}(2, a^{2^n}+1),$$

que proporciona el càlcul desitjat,

$$\mathrm{mcd}(a^{2^m}+1, a^{2^n}+1) = \begin{cases} 1, & \text{si } a \text{ és parell}, \\ 2, & \text{si } a \text{ és senar}. \end{cases}$$

(b) El resultat és clar si $m = n$. Suposem, doncs, que és $m > n$.

Ara, tenim que

$$2^m - 1 - (2^n - 1) = 2^m - 2^n = 2^n(2^{m-n} - 1)$$

i, com que $\mathrm{mcd}(2^n, 2^n - 1) = 1$, és

$$\mathrm{mcd}(2^m - 1, 2^n - 1) = \mathrm{mcd}(2^n(2^{m-n} - 1), 2^n - 1) = \mathrm{mcd}(2^{m-n} - 1, 2^n - 1);$$

és a dir, podem restar n de m en l'exponent del primer dels dos nombres i el màxim comú divisor no canvia.

Sigui $m = nq + r$, amb $0 \leq r \leq n$, la divisió entera de m entre n. Com que $m > n$, resulta que és $q \geq 1$, i podem iterar q vegades el càlcul anterior; obtenim que

$$\mathrm{mcd}(2^m-1, 2^n-1) = \mathrm{mcd}(2^{m-qn}-1, 2^n-1) = \mathrm{mcd}(2^r-1, 2^n-1) = \mathrm{mcd}(2^n-1, 2^r-1).$$

Apliquem successivament aquest fet d'acord amb l'algoritme d'Euclides per al càlcul del màxim comú divisor de m i n. Obtenim exactament allò que hi ha enunciat:

$$\mathrm{mcd}(2^m - 1, 2^n - 1) = \mathrm{mcd}(2^d - 1, 2^0 - 1) = \mathrm{mcd}(2^d - 1, 0) = 2^d - 1.$$