Exercici 6.

(a) Siguin $a, m, n \in \mathbb{N}$ i $n \neq m$. Calculeu $\text{mcd}(a^{2^m}+1, a^{2^n}+1)$

(b) Siguin $m, n \in \mathbb{N}$ i $d := \text{mcd}(m, n)$.Demostreu que $\text{mcd}(2^m-1, 2^n-1) = 2^d - 1$

Solució 8.

(a) Siguin $a, m, n \in \mathbb{N}$ i $n \neq m$. Calculeu $\text{mcd}(a^{2^m}+1, a^{2^n}+1)$

Lema: Sigui a,b,d $\in \mathbb{N}$ i $d|a$ i $d|b$ i $a > b \Rightarrow d|a-b$

Sigui $a = d \times m$ on $m \in \mathbb{N}$ i $b = d \times n$ on $n \in \mathbb{N}$, com a>b tenim què m>n
$\Rightarrow a - b = d(m-n)$ on $(m-n) \in \mathbb{N}$

DEMOSTRACIÓ DE L'ENUNCIAT:

Sigui p $\in \mathbb{N}$ tal què p$|(a^{2^m}+1)$, aplicant l'algorisme de la divisió $a^{2^m}+1 = p \times c + r$ on c és el quocient i r és el residu que serà 0 $\Rightarrow a^{2^m}+1 = p \times c + 0 \Leftrightarrow a^{2^m} = p \times c - 1 \Rightarrow a^{2^m} \equiv -1$ (mod p)

Sense perdre la generalitat podem suposar què n>m, ja què si és al revés es poden intercambiar els termes d'ordre.

Per tant, $(n-m) > 0$
Agafant l'expresió $a^{2^m} \equiv -1$ (mod p)
$\Rightarrow (a^{2^m})^{2^{n-m}} \equiv (-1)^{2^{n-m}}$ (mod p), entrem l'exponent multiplicant
$\Rightarrow (a^{2^m \times 2^{n-m}}) \equiv (-1)^{2^{n-m}}$, sumem els exponenets i 2^{n-m} és un nombre parell
$\Rightarrow a^{2^n} \equiv 1$ (mod p) $\Rightarrow a^{2^n} = p \times c + 1 \Leftrightarrow a^{2^n} - 1 = p \times c + 0 \Rightarrow p|a^{2^n} - 1$
$\Rightarrow$ p divideix a $a^{2^n} - 1$

Ara bé, si p també divideix a $a^{2^n}+1$, aplicant el lema p també dividirà a $(a^{2^n}+1) - (a^{2^n}-1)$. Per tant:
$p|((a^{2^n}+1) - (a^{2^n}-1)) \Rightarrow p|(a^{2^n}+1-a^{2^n}+1) \Rightarrow p|2 \Rightarrow p = 1$ o $p = 2$

Estudiem els casos:
1. Si a és parell $\forall x \in \mathbb{N}$, a^{2^x} serà parell. Per tant $a^{2^n}+1$ i $a^{2^m}+1$ seràn imparell $\Rightarrow \text{mcd}(a^{2^m}+1, a^{2^n}+1) = 1$
2. Si a és imparell $\forall x \in \mathbb{N}$, a^{2^x} serà imparell. Per tant $a^{2^n}+1$ i $a^{2^m}+1$ seràn parells $\Rightarrow \text{mcd}(a^{2^m}+1, a^{2^n}+1) = 2$