1.4.7 *Demostrar que* $(2^a - 1, 2^b - 1) = 2^{(a,b)} - 1$ *para todo a y b.*

Lo resolveremos mediante inducción sobre el máximo entre a y b.

- Sea max(a, b)=1 $\implies$ a=b=max(a, b)=1 $\implies$ $(2^1 - 1, 2^1 - 1) = (1, 1) = 1 = 2^{(1,1)} - 1$.
- Suponemos que $(2^a - 1, 2^b - 1) = 2^{(a,b)} - 1$ para todo a, b tal que $(a, b) < n$.
- Probaremos que el enunciado también se cumple para los a, b con max(a, b)=n. Sin pérdida de generalidad, puede suponerse que $a \leq b$ y que, por tanto, (a, b)=b=n. Por el Algoritmo de la División (Proposición 1.1.2.), existen dos únicos enteros q y r tales que

$$b = aq + r \quad con\ 0 \leq r < a$$

Por otro lado, sea $P(x) = x^q - 1 = (x - 1)(x^{q-1} + \cdots + 1)$, entonces

$$P(2^a) = 2^{aq} - 1 = (2^a - 1)(1 + 2 + 2^{2q} + \cdots + 2^{a(q-1)})$$

$$2^{aq} = (2^a - 1)(1 + 2 + 2^{2q} + \cdots + 2^{a(q-1)}) + 1$$

$$2^{aq}2^r = (2^a - 1)(1 + 2 + 2^{2q} + \cdots + 2^{a(q-1)})2^2 + 2^r$$

$$2^{aq+r} = (2^a - 1)(1 + 2 + 2^{2q} + \cdots + 2^{a(q-1)})2^2 + 2^r$$

$$2^b - 1 = (2^a - 1)(1 + 2 + 2^{2q} + \cdots + 2^{a(q-1)})2^2 + 2^r - 1$$

Por el Algoritmo de la División, vemos que $(2^r - 1)$ es el resto de dividir $2^b - 1$ entre $(2^a - 1)$. En particular, $0 \leq (2^r - 1) < (2^a - 1)$. Por tanto, se cumple:

$$(2^b - 1, 2^a - 1) = (2^a - 1, 2^r - 1)$$

Además, como $b \geq a > r$, entonces $max(a, r) < max(b, a) = n$, luego podemos aplicar la hipótesis de inducción.

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

Finalmente, basta observar que, como consecuencia del Algoritmo de la División, (a, b)=(a, r). Y entonces obtenemos:

$$(2^a - 1, 2^b - 1) = (2^b - 1, 2^a - 1) = (2^a - 1, 2^r - 1) = 2^{(a,r)} - 1 = 2^{(a,b)} - 1$$

Problema escrito por Jesús de los Nietos Valle.