si $m \mid n \Rightarrow a^m - 1 \mid a^n - 1$

Sug: Usar que $a^k - 1 = (a-1)(a^{k-1} + a^{k-2} + \dots + a^2 + a + 1)$ $\forall a$

$a^m - 1 = (a-1)(a^{m-1} + \dots + a + 1)$

$a^n - 1 = (a-1)(a^{n-1} + \dots + a + 1)$

$m \mid n \Rightarrow n = qm$

$a^n - 1 = a^{qm} - 1 = (a^m)^q - 1 = (a^m - 1)\left((a^m)^{q-1} + (a^m)^{q-2} + \dots + (a^m)^2 + a^m + 1\right)$

número entero

↑ sug. aplicada en a^m en vez de a

entonces $a^n - 1 \mid a^n - 1$

Generalizamos a cualquier resto.

$n = qm + r$

$a^n - 1 = a^{mq+r} - 1 = (a^m)^q \cdot a^r - 1$

$= (a^m)^q \cdot a^r - a^r + a^r - 1$

$= ((a^m)^q - 1)a^r + a^r - 1$

$= (a^m - 1)\underbrace{(a^{m(q-1)} + \dots + 1)a^r}_{\text{número entero}} + a^r - 1$

$0 \leq r < m$

$\Rightarrow 0 \leq a^r - 1 < a^m - 1$

$a^r - 1$ es el resto.

Probar que $mcd(a^n-1, a^m-1) = a^{mcd(m,n)}-1$

sea $d = mcd(n,m)$, $D = mcd(a^n-1, a^m-1)$

$d \mid n \Rightarrow a^d-1 \mid a^n-1$

$d \mid m \Rightarrow a^d-1 \mid a^m-1$

(por la parte anterior)

$a^d-1 \mid mcd(a^n-1, a^m-1)$

quiero probar que es =

Si probamos para el otro lado, ya estaría

$d = mx + ny \qquad x, y \in \mathbb{Z}$

$a^d - 1 = a^{mx+ny} - 1$

$m = kd$

$n = ld$

Si $x \geq 0$: $\qquad mcd(k,l) = 1$

Aunque nosotros, escorrecto. $\quad d = kdx + ldy = d(kx + ly)$ (por ahora en pausa)

(mañana, pretender) $\quad a^m - 1 = KD$ (definición de D)

$a^m = KD + 1$

$a^{mx} = (KD+1)^x = \sum_{i=0}^{x} \binom{x}{i} (KD)^i \cdot 1^{x-i}$

cuando $i > 0$, ~ es múltiplo de KD

$= 1$

$KD \mid a^{mx} - 1 \qquad = (\text{múltiplo de } KD) + \binom{x}{0} (KD)^0 1^{x-0}$

$mcd(a^n - 1, a^m - 1)$

supongo que $m < n$

para aplicar el alg. de Euclides.

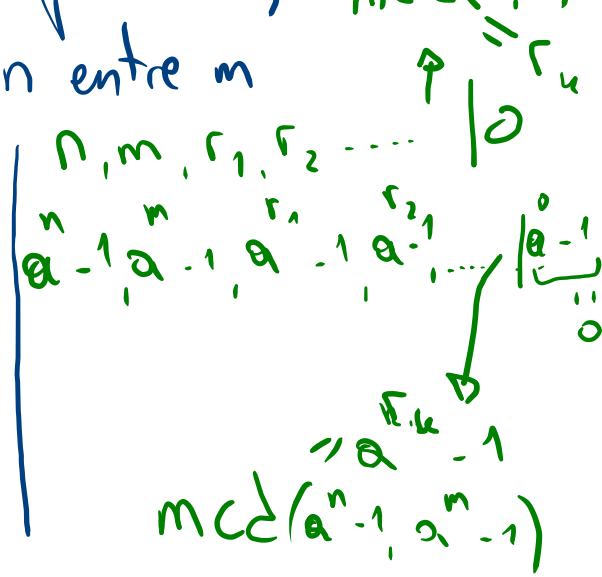
$$a^n - 1 = Q_1(a^m - 1) + \underbrace{a^{r_1} - 1}_{\text{resto (por la parte ant.)}}$$

donde r_1 es el resto de dividir n entre m

esto es. $n = q_1 m + r_1$

$$a^m - 1 = Q_2\left(a^{r_1} - 1\right) + a^{r_2} - 1 .$$

donde $m = q_2 \cdot r_1 + r_2$



Calcular mcd $\left(\underbrace{1\ldots1}_{2010},\ \underbrace{1\ldots1}_{100}\right)$

2010 unos

100 unos

$a = \underbrace{1\ldots1}_{2010} = 10^{2009} + 10^{2008} + \ldots + 10^2 + 10 + 1$ ($10^0 = 1$)

(expresión decimal)

$b = \underbrace{1\ldots1}_{100} = 10^{99} + 10^{98} + \ldots + 10^2 + 10 + 1$

Por la sug. de la parte a.

$$a^k - 1 = (a-1)(a^{k-1} + a^{k-2} + \dots + a^2 + a + 1)$$

Para $a = 10$, $k = 100$

$$10^{100} - 1 = (10-1)\underbrace{(10^{99} + 10^{98} + \dots + 10 + 1)}_{b}$$

$$10^{100} - 1 = (10-1)\,b$$

Para $a = 10$, $k = 2010$

$$10^{2010} - 1 = (10-1)(10^{2009} + 10^{2008} + \dots + 10^2 + 10 + 1)$$

$$= (10-1)\,a$$

$10^{100} - 1 = 9b$, $10^{2010} - 1 = 9a$.

$2010 = 201 \cdot 10$

$100 = 10 \cdot 10$

$mcd(9a, 9b) = 9\, mcd(a, b)$

$mcd(10^{2010} - 1, 10^{100} - 1)$

$= 10^{mcd(2010, 100)} - 1 = 10^{10} - 1$ (parte c)

¿Cuánto vale $mcd(2010, 100)$?

$= 10\, mcd(201, 10) = 10$

$$mcd(9a, 9b) = 9\,mcd(a,b) = 10^{10} - 1 = 1\underbrace{0\ldots0}_{10} - 1$$

$$= \underbrace{9\ldots9}_{10}$$

$$mcd(a,b) = \frac{10^{10}-1}{9} = \underbrace{1\ldots1}_{10}$$

$$mcd\left(\underbrace{1\ldots1}_{2010}, \underbrace{1\ldots1}_{100}\right) = \underbrace{1\ldots\ldots1}_{10}$$

N M $mcd(N,M)$