NMMB331 - HW1

Jan Oupický

1

a

2

a

3

Let's denote $x = \gcd(m, d), y = \gcd(2^m - 1, 2^d - 1)$. We know that $y|2^m - 1$ and $y|2^d - 1 \implies 2^m \equiv 1\,(y), 2^n \equiv 1\,(y) \implies ord_{\mathbb{Z}_y}(2)|m, ord_{\mathbb{Z}_y}(2)|d \implies ord_{\mathbb{Z}_y}(2)|\gcd(m, d) = x$. Therefore $2^x \equiv 1\,(y) \iff \gcd(2^m - 1, 2^d - 1)|2^x - 1$.

Let's denote $x = \gcd(m, d), y = \gcd(2^m - 1, 2^d - 1)$. Assume that $a|2^m - 1, 2^d - 1 \iff 2^m \equiv 1\,(a), 2^n \equiv 1\,(a) \iff ord_{\mathbb{Z}_a}(2)|m, d \iff ord_{\mathbb{Z}_a}(2)|\gcd(m, d) = x \iff 2^x \equiv 1\,(a)$. There have been equivalences everywhere so we have shown $a|2^m - 1, 2^d - 1 \iff a|2^x - 1$. Therefore $2^m - 1, 2^d - 1$ and $2^x - 1$ have the same divisors and ultimately the same greatest one.