640:300 WORKSHOP 4
PRIME AND COMPOSITE NUMBERS

A natural number $p > 1$ is called *prime* if p has no positive divisors other than 1 and p. A number $n \in \mathbb{Z}_{>1}$ is called *composite* if there exist $1 \lneq k \lneq n$ and $1 \lneq \ell \lneq n$ such that $n = k\ell$.

(A) *Let* $n \in \mathbb{Z}_{>1}$*. Prove that if* $2^n - 1$ *is prime then* n *is prime.*

(*Hint*. Prove by contradiction: let $x, n \in \mathbb{Z}_{>0}$ and let $1 \lneq k \lneq n$, $1 \lneq \ell \lneq n$ with $n = k\ell$. Then $x^n - 1$ is composite:

$$x^n - 1 = (x^\ell - 1)(x^{\ell(k-1)} + x^{\ell(k-2)} + \ldots x^\ell + 1).)$$

(B) *Let* $a, n \in \mathbb{Z}_{>1}$*. Prove that if* $a^n - 1$ *is prime then* $a = 2$*, and so* n *is prime by* (A)*.*

(*Hint.* Prove by contradiction, and again use the factorization for $x^n - 1$.)