

Comments on 3.2.14

As you know, in class we looked at 3.2.14 and found the proof for the important half used to show Fermat numbers are not prime. But we got stuck on the reverse implication. It turns out we had the full proof and just did not realize it. So let's spell it out again with clearer notation.

Claim: If $q = 4^n + 1$ and if $3^{(q-1)/2} \equiv -1 \pmod{q}$, then q is prime.

Proof: Note that $3^{q-1} \equiv 1 \pmod{q}$ so the order of 3 mod q must divide $q-1 = 4^n$. Since $3^{(q-1)/2} \equiv -1 \pmod{q}$ the order of 3 must be precisely $q-1$, so q is prime.