

Chuck Goodman
Problem of the week 1

For $m > 1$, $\gcd(a, m) = 1$, the order of a modulo m ($\text{ord}_m a$) is the smallest positive integer k such that

$a^k \equiv 1 \pmod{m}$. Notice that $\text{ord}_3 8 = \text{ord}_3 2 = 2$, $\text{ord}_5 8 = \text{ord}_5 3 = 4$ and $\text{ord}_{13} 8 = 4$.

So look at $N = 19 \cdot 8^n + 17$ for $n = 2m$, we have $N \equiv 1 \cdot 1 + 17 \equiv 0 \pmod{3}$, and hence N is not prime.

We have

$$19 \equiv 1 \pmod{3}$$

and we note that

$$8^2 = 64 \equiv 1 \text{ so we can say that}$$

$$\text{ord}_3 8 = 2$$

This holds since $\gcd(8, 3) = 1$

So for n even the problem reduces to

$$19 \cdot 8^{2n} \equiv 1 + 17 \equiv 0 \pmod{3}$$

So the number is not prime since 3 is a divisor!

Now for odd n , consider two cases.

For $n = 3, 7, 11, \dots$

Look at $\pmod{5}$

$$\text{ord}_5 8 = 4$$

$m = 1, 2, 3, \dots$

Let $n = 4m - 1$

$$19 \cdot 8^n \equiv 4 \cdot 8^{-1} \cdot 1 + 17 \equiv 4 \cdot 2 + 17$$

$$\equiv 0 \pmod{5}$$

and the number is divisible by 5

Doing the same thing for 1, 5, 9, ...

Let $n = 4m + 1$, but using $\pmod{13}$

$$\text{ord}_{13} 8 = 4$$

$$19 \cdot 8^n \equiv 6 \cdot 8^1 + 17 \equiv 6 \cdot 8 + 17$$

$$\equiv 65 \equiv 0 \pmod{13}$$

The number is divisible by 13.

So, I concluded the number is always divisible by 13, 5, or 3 and hence never prime!

So this exhausts the non-negative integers and I have proved it is never prime!