4.1.9

(page 124)

Prove that any two numbers of the following sequence are relatively prime:

$$2+1, 2^2+1, 2^4+1, 2^8+1, ..., 2^{2^n}+1, ...$$

Show that this result proves that there are an infinite number of primes.

proof

Let $m, n \in \mathbb{N}, m > n$, and $a = 2^{2^n}$. Then $2^{2^m} = (a)^{2^{m-n}}$. Since $m > n$, 2^{m-n} is even, so $a+1$ divides $a^{2^{m-n}} - 1$. Thus, $2^{2^n}+1$ divides $2^{2^m}-1$ with no remainder. We can write:

$$2^{2^m}+1 = q(2^{2^n}+1)+2$$

By the Euclidean Algorithm:

$$gcd(2^{2^m}+1, 2^{2^n}+1) = gcd(2^{2^n}+1, 2)$$

Since $2^{2^n}+1$ is odd, the gcd is 1.

Now, since any integer greater than 1 has at least 1 prime factor and if we assign a prime factor to each element in the sequence then there is an infinite number of primes be since there is an infinite number of numbers of form $2^{2^n}+1$. Now, since the common greater divisor of any two numbers in the sequence is 1 then there must an infinite number of distinct prime numbers.