A Friendly Introduction to Number Theory
Chapter 14 Solutions

Hunter Matthews

Question 1

If $a^n + 1$ is prime for some numbers $a \geqslant 2$ and $n \geqslant 1$, show that n must be a power of 2.

Proof: Notice the fact that if n is odd, then $a^n + 1 \mid a + 1$. For example, take $2^3 + 1 \mid 2 + 1 = 3$ and $3^3 + 1 \mid 3 + 1 = 7$. Furthermore, let us make the assumption that n is not a power of 2. If this is the case, we can factor it as $n = 2^k m$ such that $m \geqslant 3$ and m is odd. Therefore,

$$a^n + 1 \rightarrow (a^{2^k})^m + 1 \mid a^{2^k} + 1$$

Hence, $a^n + 1$ cannot be prime and n must be a power of 2. ☺

Question 2

Let $F_k = 2^{2^k} + 1$. For example, $F_1 = 5, F_2 = 17, F_3 = 257$, and $F_4 = 65537$. Fermat thought that all the F_k's might be prime, but Euler showed in 1732 that F_5 factors as $641 \cdot 6700417$, and in 1880 Landry showed that F_6 is composite. Primes of the form F_k are called *Fermat primes*. Show that if $k \neq m$, then the numbers F_k and F_m have no common factors; that is, show that $\gcd(F_k, F_m) = 1$.

Proof: Suppose that $0 \leqslant m < k$ with F_m and F_k having a common factor $a > 1$. Then we can say that a divides both $F_0 \cdots F_{k-1}$ and F_k. Hence, a divides the difference and a is forced to become 2 posing a contradiction, because each Fermat number is clearly odd. Therefore, a must be 1 which proves that $\gcd(F_k, F_m) = 1$ 😄

Question 3

The numbers $3^n - 1$ are never prime $if n \geqslant 2$, since they are always even. However, it sometimes happens that $(3^n - 1)/2$ is prime. For example, $3^3 - 1)/2 = 13$ is prime.

(a) Find another prime of the form $(3^n - 1)/2$.

(b) If n is even, show that $(3^n - 1)/2$ is always divisible by 4, so it can never be prime.

(c) Use a similar argument to show that if n is a multiple of 5 then $(3^n - 1)/2$ is never a prime.

(d) Do you think that there are infinitely many primes of the form $(3^n - 1)/2$?

Answer: **(a)** Another prime of the form $(3^n - 1)/2$ would be 13. We can show this by the following computation.

$$(3^3 - 1)/2 = 13$$

which is prime.

(b) Let us assume that n is even, so $n = 2k$. Then we have

$$\frac{(3^{2k} - 1)}{2} = \frac{(9^k - 1)}{2}$$

However, $9k \equiv 1 \pmod 8$, so $(9^k - 1)/2$ is divisible by 4.

(c) Let us assume that n is a multiple of 5, so $n = 5k$. Then we have

$$\frac{(3^{5k} - 1)}{2} = \frac{(243^k - 1)}{2}$$

However, $243 - 1$ is $242 = 2 \cdot 11^2$, so

$$243^k = (2 \cdot 11^2 + 1)^k \equiv 1 \pmod{11^2}$$

so $(243^k - 1)/2$ is divisible by 11^2 and thus will never be a prime.

(d) Although it has yet to be proven, I believe that there are infinitely many primes of the form $(3^n - 1)/2$. 😄