MA 1971 Exercise Set 3 Answers

Hubert J. Farnsworth

April 12, 2021

1. Suppose that p and $p+2$ are twin primes with $p > 3$. Suppose that $6 \nmid (p+1)$. Then one of the following cases must occur. In each case we will arrive at a contradiction.

   If $p+1 = 6k+1$ then $p = 6k$. This shows that $6 \mid p$, which gives the contradiction that p is not prime.

   If $p+1 = 6k+2$ then $p+2 = 3(2k+1)$. This shows that $3 \mid (p+2)$. Since $p+2 > 3$, $p+2$ must be a multiple of 3 which gives the contradiction that $p+2$ is not prime.

   If $p+1 = 6k+3$ then $p = 2(3k+1)$. This shows that $2 \mid p$ Since $p > 3$, p must be a multiple of 2 which gives the contradiction that p is not prime.

   If $p+1 = 6k+4$ then $p = 3(2k+1)$. Similar to before, this implies the contradiction that p is not prime.

   If $p+1 = 6k+5$ then $p+2 = 6(k+1)$. Similar to before, this implies the contradiction that $p+2$ is not prime.

   Conclude that since $6 \nmid (p+1)$ implies a contradiction in any of the five possible cases given above, we must in fact have $6 \mid (p+1)$.

2. **Lemma** For $a \in \mathbb{Z}$, $3 \mid a^2$ iff $3 \mid a$.

   Proof: If $3 \mid a$ then $a = 3k$ for some integer k and so $a^2 = 3(3k^2)$. Therefore $3 \mid a^2$.

   Suppose $3 \mid a^2$ but $3 \nmid a$. Then either $a = 3k+1$ or $a = 3k+2$ for some integer k from which we obtain $a^2 = 3(3k^2+2k)+1$ in the former case and $a^2 = 3(3k^2+4k+1)+1$ in the latter. In both cases we have contradicted the assumption that $3 \mid a^2$. Therefore, if $3 \mid a^2$ it must follow that $3 \mid a$.

   Answer to Exercise 2: Suppose that $\sqrt{3}$ is rational. Then we can write $\sqrt{3} = p/q$ where $p \in \mathbb{Z}$, $q \in \mathbb{Z}^+$ and $\gcd(p,q) = 1$. Then, $3q^2 = p^2$ which shows that $3 \mid p^2$. But $3 \mid p^2$ implies that $3 \mid p$ so that we can write $p = 3k$ for some integer k. Then $3q^2 = p^2 = 9k^2$ and so $q^2 = 3k^2$. This shows that $3 \mid q^2$ and consequently that $3 \mid q$. Therefore $3 \mid p$ and $3 \mid q$, which contradicts the assumption that $\gcd(p,q) = 1$.

3. $$\begin{aligned}
F_{n-1}^2 - 2(F_{n-2}-1)^2 &= \left(2^{2^{n-1}}+1\right)^2 - 2\left(2^{2^{n-2}}+1-1\right)^2 \\
&= \left(2^{2^{n-1}}\right)^2 + 2\left(2^{2^{n-1}}\right) + 1 - 2\left(2^{2^{n-2}}\right)^2 \\
&= \left(2^{2^{n-1}}\right)^2 + 2\left(2^{2^{n-1}}\right) + 1 - 2\left(2^{2^{n-1}}\right) \\
&= \left(2^{2^{n-1}}\right)^2 + 1 \\
&= 2^{2^n} + 1 \\
&=: F_n
\end{aligned}$$

4. **Lemma** For $a \in \mathbb{Z}$, $2 \mid a^2$ iff $2 \mid a$.

Proof: The proof of this lemma is nearly identical (in fact slightly simpler) to the proof of the lemma used for Exercise 2 and is therefore omitted.

Answer to Exercise 4: Let $x = 2m+1$ and $y = 2n+1$ are both positive integers with $m, n \in \mathbb{Z}$ and suppose that $x^2 + y^2$ is a perfect square with $x^2 + y^2 = k^2$ for some $k \in \mathbb{Z}$.

$$\begin{aligned}
k^2 &= x^2 + y^2 \\
&= (2m+1)^2 + (2n+1)^2 \\
&= 4m^2 + 4m + 1 + 4n^2 + 4n + 1 \\
&= 2(2m^2 + 2m + 2n^2 + 2n + 1) \\
&= 2[2(m^2 + m + n^2 + n) + 1] \\
&= 2r, \quad r := 2(m^2 + m + n^2 + n) + 1
\end{aligned}$$

This shows that $k^2 = 2r$ and that r is an odd integer. Then k^2 is even, from which it follows that k is even (by the lemma). Thus $k = 2q$ for some integer q and $4q^2 = k^2 = 2r$. But then $2q^2 = r$, which produces the contradiction that r is also even. Since this contradiction arose from supposing that $x^2 + y^2$ is a perfect square, conclude that if x and y are odd positive integers that $x^2 + y^2$ is not a perfect square.

5. **Lemma** $3 \mid (10^k - 1) \quad \forall k \in \mathbb{Z}^+$. This is equivalent to the statement $10^k \equiv 1 \mod 3$.

Proof (Induction):
1) $k = 1$: It is clear that $3 \mid (10^1 - 1)$ since $10^1 - 1 = 9 = 3 \cdot 3$.
2) Suppose $3 \mid (10^k - 1)$ so that $10^k - 1 = 3j$ for some integer j. Then $10^{k+1} - 1 = 10(10^k - 1) + 9 = 10(3j) + 9 = 3(10j + 3)$ which shows that $3 \mid (10^{k+1} - 1)$.

Answer to Exercise 5: Let $n = d_0 + 10d_1 + 10^2 d_2 + \cdots + 10^k d_k$ for some $k \in \{0, 1, 2, \dots\}$ so that the digits of n are $d_0, d_1, \dots, d_k \in \{0, 1, \dots, 9\}$.

($\implies$) Suppose that $3 \mid (d_0 + d_1 + \cdots + d_k)$. Then there are integers $k, j_1, \dots, j_k$.

$$\begin{aligned}
3k &= d_0 + d_1 + \cdots + d_k \\
3k + (10^1 - 1)d_1 &= d_0 + 10d_1 + d_2 + \cdots + d_k \\
3k + (10^1 - 1)d_1 + (10^2 - 1)d_2 &= d_0 + 10d_1 + 10^2 d_2 + \cdots + d_k \\
3k + (10^1 - 1)d_1 + (10^2 - 1)d_2 &= d_0 + 10d_1 + \dots 10^k d_k = n \\
3k + 3j_1 d_1 + 3j_2 d_2 + \cdots + 3j_k d_k &= n \quad \text{(using the lemma)} \\
3(k + j_1 d_1 + j_2 d_2 + \cdots + j_k d_k) &= n \implies 3 \mid n
\end{aligned}$$

($\impliedby$) Suppose that $3 \mid n$. Then $3k = n = d_0 + 10d_1 + \cdots + 10^k d_k$ for some integer k. Using the lemma, there exist integers $j_1, \dots, j_k$ such that:

$$\begin{aligned}
3k &= d_0 + 10d_1 + 10^2 d_2 + \cdots + 10^k d_k \\
3k - (10^1 - 1)d_1 - (10^2 - 1)d_2 + \cdots - (10^k - 1)d_k &= d_0 + d_1 + d_2 + \cdots + d_k \\
3k - 3j_1 d_1 - 3j_2 d_2 - \cdots - 3j_k d_k &= d_0 + d_1 + \cdots + d_k \\
3(k - j_1 d_1 - \cdots - j_k d_k) &= d_0 + d_1 + \cdots + d_k \implies 3 \mid (d_0 + \cdots + d_k)
\end{aligned}$$

($\iff$) A proof using modular arithmetic. This proof assumes a few basic properties of modular arithmetic.

$$\begin{aligned}
&3 \mid n \\
&\iff 0 \equiv n \mod 3 \\
&\iff 0 \equiv (d_0 + \ldots 10^k d_k) \mod 3 \\
&\iff 0 \equiv d_0 \mod 3 + 10d_1 \mod 3 + \ldots 10^k d_k \mod 3 \\
&\iff 0 \equiv d_0 \mod 3 + d_1 \mod 3 + \cdots + d_k \mod 3 \\
&\iff 0 \equiv (d_0 + d_1 + \cdots + d_k) \mod 3 \\
&\iff 3 \mid (d_0 + d_1 + \cdots + d_k)
\end{aligned}$$