Section 3.3 Question 18

In this problem all variables range over $\mathbb{Z}$, the set of all integers.

(a) Prove that if $a|b$ and $a|c$ then $a|(b+c)$.

Answer: Since $a|b$ there is some integer k such that $b = ka$. Similarly there is some integer ℓ such that $c = \ell a$. Therefore $(b+c) = ka + \ell a = (k+\ell)a$ and so $a|(b+c)$.

(b) Prove that if $ac|bc$ and $c \neq 0$ then $a|b$.

Answer: Since $ac|bc$ there is some integer k such that $bc = kac$. Since $c \neq 0$ we can cancel it from both sides of this equation, leaving us with $b = ka$, so by definition $a|b$.

Section 3.4 Question 10

Prove that for every integer n, n^3 is even iff n is even.

Answer: ($\leftarrow$): Suppose n is even, then there is some k such that $n = 2k$. Therefore $n^3 = (2k)^3 = 2(4k^3)$ and so n^3 is even as well.

($\rightarrow$): Now suppose n is odd, then there is some k such that $n = 2k+1$. Therefore $n^3 = (2k+1)^3 = 8k^3 + 12k^2 + 6k + 1 = 2(4k^3 + 6k^2 + 3k) + 1$ and so n^3 is odd as well.

Note: There are many different correct proofs of the above statement, I have only given one of them.

Section 3.4 Question 11

Consider the following putative theorem:

Theorem? Suppose m is an even integer and n is an off integer. Then $n^2 - m^2 = n + m$.

(a) What's wrong with the following proof of the theorem?

Proof. Since m is even, we can choose some integer k such that $m = 2k$. Similarly, since n is odd we have $n = 2k+1$. Therefore $n^2 - m^2 = (2k+1)^2 - (2k)^2 = 4k^2 + 4k + 1 - 4k^2 = 4k + 1 = (2k+1) + (2k) = n + m$.

Answer: We cannot assume that the same integer k may be used to witness both m's even-ness and n's odd-ness. We must replace the second sentence in the proof by:

Similarly, since n is odd we can choose some integer ℓ such that $n = 2\ell + 1$.

(b) Is the theorem correct? Justify your answer with either a proof or a counterexample.

Answer: This putative theorem can be seen to be false by looking at the example $m = 4$ and $n = 1$. Specifically, $1^2 - 4^2 = -15 \neq 5 = 4 + 1$.

Note: Since $n^2 - m^2 = (n-m)(n+m)$, any situation where $n - m \neq 1$ will be an acceptable counterexample.