Homework: Week 4

Joseph Ismailyan

Math 100
Due: 27 October, 2017
Professor Boltje
MWF 9:20a-10:25a

Section 3.5

6.

The statement is **false** because it does not take into account the subsets $A_1 \cap A_2, A_2 \cap A_3$, and $A_1 \cap A_3$ so these will be double counted and give the wrong cardinality.

8.

This problem can be split into four simpler problems of choosing one card from each suit, then multiplying them to find the overlap. After that, we add the number of ways to get only red cards.

$$\overset{heart}{\tbinom{13}{1}} * \overset{diamond}{\tbinom{13}{1}} * \overset{spade}{\tbinom{13}{1}} * \overset{clover}{\tbinom{13}{1}} = \binom{13}{1}^4$$

$$\binom{13}{1}^4 + \binom{26}{4} = 43,511$$

Chapter 4

6.

Proposition Let $a, b, c \in \mathbb{Z}$
If $a|b$, and $a|c$ then $a|(b+c)$

Proof. Suppose $a|b$ and $a|c$. By definition, $a|b$ means there is an integer n with $b = an$ and $a|c$ means there is an integer m with $c = am$. Thus, $a|(b+c)$ means $(b+c) = an + am \to (b+c) = (n+m)a$ for the integer $x = (n+m)$. Therefore $a|(b+c)$. ∎

8.

Proposition Let $a \in \mathbb{Z}$
If $5|2a$ then $5|a$.

Proof. Suppose $5|2a$. Then $2a = 5b$ where $b \in \mathbb{Z}$. Since $2a$ is even, we can say that $5n$ is also even. Then n must be even, because an odd n would produce an odd $5n$ which cannot be equal to $2a$. So then $b = 2m$ where $m \in \mathbb{Z}$. Then $2a = 5(2m) \to 2a = 10m$ simplifies to $a = 5m$. The equation $a = 5m$ means $5|a$ by definition of divisibility. ∎

10.

Proposition Let $a, b \in \mathbb{Z}$.
If $a|b$ then $a|(3b^3 - b^2 + 5b)$.

Proof. Suppose $a|b$ where $a, b \in \mathbb{Z}$. Since $a|b$, there exists an integer n where $b = an$, which we can substitute that into the equation $(3b^3 - b^2 + 5b) = (3(an)^3 - (an)^2 + 5(an))$
$= (3a^3b^3 - a^2b^2 + 5an)$
$= (3a^2b^3 - ab^2 + 5n)a$
$= ma$ where $m = (3a^2b^3 - ab^2 + 5n)$
Therefore $(3b^3 - b^2 + 5b) = ma$ for some integer m.
Thus, $a|(3b^3 - b^2 + 5b)$. ■

20.

Proposition Let $a \in \mathbb{Z}$.
If $a^2|a$ then $a \in \{-1, 0, 1\}$.

Proof. Suppose $a^2|a$ where $a \in \mathbb{Z}$.
Since $a^2|a$, there exists an integer n where $a = na^2$. Subtracting a from both sides gives us $0 = na^2 - a$
$\implies 0 = a(na - 1)$. So $a = 0$ or $0 = na - 1 \implies na = 1$. Therefore a can be $-1, 0$, or 1.
Thus $a = \{-1, 0, 1\}$. ■

24.

Proposition If $n \in \mathbb{N}$ and $n \geq 2$ then the numbers $n!+2, n!+3, n!+4, n!+5, ...n!+n$ are all composite.
Proof. Suppose $n \in \mathbb{N}$ and $n \geq 2$, and $k \in \{2, 3, ..., n\}$. Consider the definition of a prime number *A whole number that cannot be divided evenly by numbers other than 1 or itself.* In order to prove the proposition, we must prove that all numbers through $n! + n$ have more divisors than just 1 and itself. First lets consider $n! + 2 = 2(\frac{n!+2}{2}) = 2(\frac{n!}{2} + 1)$ which makes it clear that 2 is a divisor. Since $n \geq 2$, it cannot be equal to 2 and so it is a composite number. We can apply this same logic to $n! + n = n(\frac{n!+n}{n}) = n(\frac{n!}{n} + 1)$ which shows that n is a divisor. Since $n \geq 2$, it cannot be equal to n and so it is a composite number. And finally, we can use these examples to prove the general case with the arbitrary value k. If $n! + k$ then $k(\frac{n!+k}{k}) = k(\frac{n!}{k} + 1)$ which shows k to be a divisor. Since $n \geq 2$, it cannot be equal to k and so it is a composite number. Therefore the numbers $n! + 2, n! + 3, n! + 4, n! + 5, ...n! + k$ are all composite. ■

26.

Proposition Every odd integer is a difference of two squares.
Proof. Suppose $n, m \in \mathbb{Z}$ and k is an odd integer, which by definition of being odd, in the form $2m - 1$. The difference of two squares can be defined as such: $k = 2m - 1 \rightarrow 2m - 1 = (n)^2 - (n - 1)^2$ which can be simplified to $n^2 - (n^2 - 2n + 1) = n^2 - n^2 + 2n - 1 = 2n - 1$.. The number $2n - 1$ is not divisible by 2 so it odd. Therefore, every odd integer is a difference of two squares. ■

Additional Hwk

Proposition Let $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$, $a = qn + r$, $b = q'n + s$ with $q, q' \in \mathbb{Z}$, $r, s \in \{0, 1, \ldots, n-1\}$. $a \equiv b \pmod{n}$ if and only if $r = s$

Note: To complete this proof if the "if and only if" format, I'll first prove that if $a \equiv b \pmod{n}$ then $r = s$. Followed by if $r = s$ then $a \equiv b \pmod{n}$.

Part A

Proposition Let $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$, $a = qn + r$, $b = q'n + s$ with $q, q' \in \mathbb{Z}$, $r, s \in \{0, 1, \ldots, n-1\}$. If $a \equiv b(\text{mod } n)$ then $r = s$.

Proof. Suppose $a \equiv b \pmod{n}$. Then $b - a$ is divisible by n, which is notated by $n|b-a$. Then, by the definition of divisibility, $b - a = dn, d \in \mathbb{Z}$. Then we can simplify to $dn = b - a$ $\rightarrow q'n+s-(qn+r) = q'n+s-qn-r = q'n-qn+(s-r) = (q'-q)n+(s-r)$. Since $r-s$ is divisible by n, it follows that $s - r$ must be 0 since $1 - n \leq r - s \leq n - 1$. $s - r = 0$ only if $r = s$, therefore if $a \equiv b(\text{mod}n)$ then $r = s$.

Part B

Proposition Let $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$, $a = qn + r$, $b = q'n + s$ with $q, q' \in \mathbb{Z}$, $r, s \in \{0, 1, \ldots, n-1\}$. If $r = s$. then $a \equiv b(\text{mod } n)$.

Proof. Suppose $r = s$. This means that a and b have the same remainder after being divided by n. So then $b - a$ must also be divisible by n, which can be shown by $b-a = q'n+r-(qn+r) = q'n+r-qn-r = (q'-q)n$. Therefore $b - a$ is divisible by n which can be written as $a \equiv b(\text{mod}n)$

Part C

In part A I showed that if $a \equiv b(\text{mod}n)$ then $r = s$, or $a \equiv b(\text{mod}n) \implies r = s$, and in part B I showed that if $r = s$ then $a \equiv b(\text{mod}n)$, or $r = s \implies a \equiv b(\text{mod}n)$. Therefore we can combine these statements and get $a \equiv b(\text{mod}n) \Leftrightarrow r = s$ ■