Homework: Week 6

Joseph Ismailyan

Math 100
Due: November 13, 2017
Professor Boltje
MWF 9:20a-10:25a

Chapter 7

10.

Proposition:
If $a \in \mathbb{Z}$, then $a^3 \equiv a \pmod 3$. Suppose $a \in \mathbb{Z}$. Consider $(a-1)a(a+1)$to be the product of three consecutive integers, so then the remainder when being divided by 3 must be either $0, 1$ or 2. Then consider the first term of the series, $a - 1 = 3n \rightarrow 3|(a-1)$. Then the next in the series, $a = 3n$ so $3|a$. And lastly, $a-2 = 3n \rightarrow a = 3n-2 = 3(n+1)-1$ then for some integer $m = n+1 \in \mathbb{Z} \rightarrow a = 3m-1 \rightarrow a+1 = 3m$ so $3|(a+1)$. Therefore we can say that $3|(a-1)a(a+1)$ or just $3|(a^3-a)$ which implies $a^3 \equiv a \pmod 3$.

22.

Proposition:
If $n \in \mathbb{N}$, then $4|n^2$ or $4|(n^2-1)$.
Proof. This proof requires two cases, one in which n is *even* and one in which n is *odd*. Once both cases are proven, we can say that Case I is true or Case II is true, since every n in the set of natural numbers is either *even* or *odd*.

Case I
Suppose n is *even*, therefore $n = 2k, n \in \mathbb{Z}$. Then $n^2 = (2k)^2 = 4k^2$. We can then say $n^2 = 4m, m = k^2 \in \mathbb{Z}$ so $4|n^2$.

Case II
Suppose n is *odd*, therefore $n = 2a+1, n \in \mathbb{Z}$. Then $n^2 = (2a+1)^2 = 4a^2 + 4a + 1$. We can then say $n^2 - 1 = 4(a^2 + a) = 4b, b = (a^2 + a) \in \mathbb{Z}$. Therefore $4|(n^2-1)$.

26.

Proposition:
The product of any n consecutive positive integers is divisible by $n!$.
Proof. Suppose we write n consecutive positive integers as $m, (m-1), (m-2), (m-3), ..., (m-(n-1))$. Then the product of these n consecutive positive integers would be $m(m-1)(m-2)(m-3)...(m-(n-1))$. If we write $\frac{m(m-1)(m-2)(m-3)...(m-(n-1))}{n!}$ then it is apparent that we have the number of ways to pick n items from a list of length m. We can then multiply the expression by $\frac{(m-n)!}{(m-n)!}$ then we get $\frac{m(m-1)(m-2)(m-3)...(m-(n-1))(m-n)!}{n!(m-n)!}$ which can be simplified to $\frac{m!}{(m-n)!n!}$. Recall that $\frac{m!}{(m-n)!n!}$ is defined as $\binom{m}{n}$ which yields an integer for all $m \geq n$.

32.

Proposition:
If $n \in \mathbb{Z}$, then $gcd(n, n+2) \in \{1, 2\}$.
Proof. Suppose $d = gcd(n, n+2)$, it follows that $d|n$ and $d|(n+2)$. So $n = da, a \in \mathbb{Z}$ and $n+2 = dc, c \in \mathbb{Z}$. Then substituting $n = da$ into $n+2 = dc$, we get $da + 2 = dc \rightarrow 2 = dc - da \rightarrow 2 = d(c-a) = dm, m \in \mathbb{Z}$. Since $2 = dm$, we know that d is a divisor of 2, and 2 has the divisors $\pm 1, \pm 2$. Since d is the **greatest** common divisor, then $d = 1$ or $d = 2$. Therefore $d \in \{1, 2\}$ and since $d = gcd(n, n+2)$ then $gcd(n, n+2) \in \{1, 2\}$.

32.

Proposition:
If $\gcd(a, b) = \gcd(b, c) = 1$, then $\gcd(ab, c) = 1$.
Proof. Suppose $\gcd(a, b) = \gcd(b, c) = 1$. Then by **Proposition 7.1** we can say $\gcd(a, b) = ak + cl, k, l \in \mathbb{Z}$ and $\gcd(b, c) = bn + cm, n, m \in \mathbb{Z}$. Then $ak = 1 - cl$ and $bn = 1 - cm$. We can then multiply ak and bn which results in $ab(kn) = (1-cl)(1-cm) = 1 - cm - cl - c^2lm$ Then $1 = ab(kn) + c^2lm + cm + cl = ab(kn) + c(clm + m + l) \rightarrow 1 = abx + cy, x = km \in \mathbb{Z}, y = clm + l + m \in \mathbb{Z}$. Since $1 = abx + cy$, then $\gcd(ab, c) = 1$.

36.

Proposition:
Suppose $a, b \in \mathbb{N}$. Then $a = \text{lcm}(a, b)$ if and only if $b|a$.
Proof. Suppose $a = \text{lcm}(a, b)$. By definition, this means $b|a$ and $a|a$. Next, suppose $b|a$. Then $a = bn, n \in \mathbb{Z}$ and $a = ad, d \in \mathbb{Z}$ then $a \geq \text{lcm}(a, b)$. Then since $a|\text{lcm}(a, b)$, we have $\text{lcm}(a, b) = ac, c \in \mathbb{Z}$, which tells us $a \leq \text{lcm}(a, b)$. Since $a \geq \text{lcm}(a, b)$ and $a \leq \text{lcm}(a, b)$, we know that $a = \text{lcm}(a, b)$.

Chapter 8

6.

Proposition:
Suppose A, B, and C are sets. Prove that if $A \subseteq B$, then $A - C \subseteq A - B$.
Proof. Suppose A, B, and C are sets and $A \subseteq B$. Then
$A - C = \{x : (x \in A) \wedge (x \notin C)\}$.
Since $A \subseteq B$, then $x \in B$. Then $B - C = \{x : (x \in B) \wedge (x \notin C)\}$.
Since $x \in A - C$ and $x \in B - C$, then $A - C \subseteq A - B$.

12.

Proposition:
Suppose A, B, and C are sets. then $A - (B \cap C) = (A - B) \cup (A - C)$.
Proof. Consider $A - (B \cap C)$
$= \{x : (x \in A) \wedge (x \notin (B \wedge C))\}$
$= \{x : (x \in A) \wedge (x \notin B \wedge x \notin C))\}$
By DeMorgan's Law
$\{x : ((x \in A) \wedge (x \notin B)) \vee ((x \in A) \wedge (x \notin C))\}$
By Distributive Law
Since
$A - B = \{x : (x \in A) \wedge (x \notin B)\}$
and
$A - C = \{x : (x \in A) \wedge (c \notin C)\}$
then since $(x \in A - B) \vee (x \in A - C)$
$\rightarrow (A - B) \cup (A - C)$.

22.

Proposition:
Let A and B be sets. Prove that $A \subseteq B$ if and only if $A \cap B = A$.
Proof. Suppose $A \cap B = A$. Let $x \in A$ be an arbitrary element. Then since $A \cap B = A$, we know $x \in A \cap B$. So $x \in B$, therefore $A \subseteq B$.
Next suppose $A \subseteq B$. If $x \in A \cap B$, then $x \in A$ so $A \cap B \subseteq A$.
Finally, suppose $A \subseteq B$. If $x \in A$ then $x \in B$, which implies $x \subseteq A \cap B$. Therefore $A \subseteq A \cap B$. Since $A \cap B \subseteq A$ and $A \subseteq A \cap B$ then $A \cap B = A$.

28.

Proposition:
Prove $\{12a + 25b : a, b \in \mathbb{Z}\} = \mathbb{Z}$.
Proof. Suppose $12a + 25b$. Since $a, b \in \mathbb{Z}, 12a + 25b \in \mathbb{Z}$.
Next, suppose the set $X = \{12a + 25b : a, b \in \mathbb{Z}\}$, the set $Y = \mathbb{Z}$, and $y \in Y$. Then consider $12(-2) + 25(1) = 1$ where $a = -2$ and $b = 1$. Then we can multiply the equation by y and get $12(-2y) + 25(y) = y$, where $a = -2y$ and $b = y$. Then $y \in Y$ implies $y \in X$, therefore $Y \subseteq X$. So $\{12a + 25b : a, b \in \mathbb{Z}\} = \mathbb{Z}$.