MATH-2106

Foundations of Mathematical Proof

Homework Assignments

Wenqi He

School of Mathematics

Georgia Institute of Technology

This collection is organized in reverse chronological order

MATH 2106 Homework 6

Wenqi He

November 4, 2018

11.3.2

The partitions are $\{\{a\},\{b\},\{c\}\}$, $\{\{a,b\},\{c\}\}$, $\{\{a,c\},\{b\}\}$, $\{\{b,c\},\{a\}\}$, and $\{\{a,b,c\}\}$. Each partition corresponds to an equivalence relation on $\{a,b,c\}$.

11.3.4

i

- Reflexivity: $\forall x \in A : \exists X \in P$ such that $x \in X$, therefore by definition of R, xRx
- Symmetry: Suppose xRy, then $\exists X \in P : x \in X \wedge y \in X$, which also implies yRx.
- Transitivity: Suppose xRy, yRz, then $\exists X \in P : x \in X \wedge y \in X$, and $\exists Y \in P : y \in Y \wedge z \in Y$. Furthermore, Y must be the same as X, because $y \in X \cap Y \neq \emptyset$, which cannot be true if $X \neq Y$ since P is a partition. Therefore $z \in Y = X$, and by definition of R, xRz.

Therefore, R is indeed an equivalent relation on A.

ii

Let $S := \{[a], a \in A\}$ be the set of equivalence classes of R. We will show that $S = P$:

For any $X \in P$, we can pick an arbitrary $x \in X$. Now consider its equivalence class $[x]$. For any $a \in [x]$, we have aRx, then by definition of R and the fact that X is the only subset that contains x (because P is a partition), $a \in X$. Since $\forall a \in [x] : a \in X$, we have $[x] \subseteq X$. On the other hand, for any $a \in X$, aRx by definition of R, so $a \in [x]$, and therefore $X \subseteq [x]$. The above results imply that $X = [x]$, which means that X is a equivalence class, or expressed formally, $X \in S$. Since $\forall X \in P : X \in S$, we have shown that $P \subseteq S$.

Now for any equivalence class $Y \in S$, we can pick any $a \in Y$, then by definition of equivalence classes, $Y = [a]$. Since P is a partition, $\exists X \in P$ such that $a \in X$. We can show that $Y = [a] = X \in P$ in the same way as the previous paragraph. Since $\forall Y \in S : Y \in P$, we have shown that $S \subseteq P$.

Therefore, $S = P$. In other words, P is the set of equivalence classes of R.

12.1.6

Domain: $\mathbb{Z}$. Codomain: $\mathbb{Z}$. Range: $\{4n+1 : n \in \mathbb{Z}\}$. $f(10) = 4 \cdot 10 + 5 = 45$.

12.1.8

No. There isn't a $(x, y) \in f$ for all $x \in \mathbb{Z}$. For example, suppose $x = 2$, then there doesn't exist an integer y that satisfies the equation.

12.1.12

Yes. Domain: $\mathbb{R}^2$. Codomain: $\mathbb{R}^3$. Range: $\{(x, y, z) \in \mathbb{R}^3 : z = \frac{x}{3} + \frac{y}{2}\}$

12.2.10

Let $y = \left(\frac{x+1}{x-1}\right)^3$, then $x = \frac{1 + y^{1/3}}{y^{1/3} - 1}$, which means that

$$f^{-1}(x) = \frac{1 + x^{1/3}}{x^{1/3} - 1}$$

Since f is invertible, f must be bijective.

12.2.18

1. Suppose $\frac{(-1)^n(2n-1)+1}{4} = \frac{(-1)^m(2m-1)+1}{4}$, where $n, m \in \mathbb{N}$ then $(-1)^n(2n-1) = (-1)^m(2m-1)$. If n and m have different parities, then

   $$2n - 1 = 1 - 2m \quad \Rightarrow \quad n + m = 1$$

   which is impossible since $n \geq 1$ and $m \geq 1$. Therefore m and n must have the same parity,

   $$2n - 1 = 2m - 1 \quad \Rightarrow \quad n = m$$

   Since $\forall m, n : f(m) = f(n) \Rightarrow m = n$, f is injective.

2. For any $z \in \mathbb{Z}$ and $z > 0$, we have $2z \in \mathbb{N}$, and

   $$f(2z) = \frac{(-1)^{2z}(2 \cdot 2z - 1) + 1}{4} = \frac{4z - 1 + 1}{4} = z$$

   For any $z \in \mathbb{Z}$ and $z \leq 0$, we have $-2z + 1 > 0 \Rightarrow -2z + 1 \in \mathbb{N}$, and

   $$f(-2z+1) = \frac{(-1)^{-2z+1}(2(-2z+1) - 1) + 1}{4} = \frac{-(-4z + 2 - 1) + 1}{4} = z$$

   This shows that $\forall z \in \mathbb{Z} : \exists x \in \mathbb{N} : f(x) = z$, therefore f is surjective.

Since f is both injective and surjective, it's bijective.

12.4.8

$$\begin{aligned}(g \circ f)(m,n) &= g(f(m,n)) = g(3m-4n, 2m+n) \\ &= (5(3m-4n)+(2m+n), 3m-4n) \\ &= (17m-19n, 3m-4n)\end{aligned}$$

$$\begin{aligned}(f \circ g)(m,n) &= f(g(m,n)) = f(5m+n, m) \\ &= (3(5m+n)-4(m), 2(5m+n)+(m)) \\ &= (11m+3n, 11m+2n)\end{aligned}$$

12.4.10

$$\begin{aligned}(f \circ f)(x,y) &= f(f(x,y)) = f(xy, x^3) \\ &= (xy \cdot x^3, (xy)^3) \\ &= (x^4 y, x^3 y^3)\end{aligned}$$

12.5.4

Let $y = e^{x^3+1}$, then

$$\log y = x^3 + 1$$
$$x^3 = \log y - 1$$
$$x = (\log y - 1)^{1/3} = f^{-1}(y)$$

So $f^{-1}(x) = (\log x - 1)^{1/3}$.

12.5.10

From 12.2.8, the inverse $f^{-1} : \mathbb{Z} \to \mathbb{N}$ is:

$$f^{-1}(z) = \begin{cases} 2z, & z > 0 \\ -2z+1, & z \leq 0 \end{cases}$$

MATH 2106 Homework 5

Wenqi He

October 18, 2018

1

Let n, m, f be the number of vertices, edges and faces, respectively. Then since each edge is on the boundary of exactly two faces, and each face is enclosed by at least 4 edges (for there are no 3-cycles), we have

$$2m = \sum_{i=1}^{f} deg(F_i) \geq \sum_{i=1}^{f} 4 = 4f \quad \Rightarrow \quad m \geq 2f$$

Then according to Euler's characteristic formula,

$$\begin{aligned}
&n - m + f = 2 \\
\Rightarrow\ & 4 = 2n - 2m + 2f \leq 2n - 2m + m = 2n - m \\
\Rightarrow\ & m \leq 2n - 4
\end{aligned}$$

2

K_5 has $5 \cdot 4/2 = 10$ edges, but a planar graph with 5 vertices can have at most $3 \cdot 5 - 6 = 9$ edges, so K_5 is nonplanar. $K_{3,3}$ has $6 \cdot 3/2 = 9$ edges, but a planar graph with 6 vertices and no 3 cycles can have at most $2 \cdot 6 - 4 = 8$ edges, so $K_{3,3}$ is also nonplanar.

8.2

If $x \in \{6n : n \in \mathbb{Z}\}$ then $x = 6k = 2(3k) = 3(2k)$ for some integer k, so $x \in \{2n : n \in \mathbb{Z}\}$ and $x \in \{3n : n \in \mathbb{Z}\}$, therefore

$$\{6n : n \in \mathbb{Z}\} \subseteq \{2n : n \in \mathbb{Z}\} \cap \{3n : n \in \mathbb{Z}\}$$

Now suppose $x \in \{2n : n \in \mathbb{Z}\}$ and $x \in \{3n : n \in \mathbb{Z}\}$, then $x = 2i = 3j$ for some integers i, j. By Euclid's lemma, $3 \mid i$, so we can write i as $3k$. Then $x = 2(3k) = 6k$ for some integer k, and so $x \in \{6n : n \in \mathbb{Z}\}$. Therefore

$$\{2n : n \in \mathbb{Z}\} \cap \{3n : n\, n\mathbb{Z}\} \subseteq \{6n : n \in \mathbb{Z}\}$$

We have shown that both directions hold, so

$$\{2n : n \in \mathbb{Z}\} \cap \{3n : n \in \mathbb{Z}\} = \{6n : n \in \mathbb{Z}\}$$

8.8

Suppose $x \in A \cup (B \cap C)$, then by definition, $x \in A \vee (x \in B \wedge x \in C)$, then by distributive law, $(x \in A \vee x \in B) \wedge (x \in A \vee x \in C)$. In terms of sets, $x \in (A \cup B) \cap (A \cup C)$. Therefore by definition,

$$A \cup (B \cap C) \subseteq (A \cup B) \cap (A \cup C)$$

If we follow the same steps but apply the distribution law in the other direction, we will get

$$(A \cup B) \cap (A \cup C) \subseteq A \cup (B \cap C)$$

Since both directions hold,

$$(A \cup B) \cap (A \cup C) = A \cup (B \cap C)$$

8.18

Suppose $(x, y) \in A \times (B - C)$, then by definition of Cartesian products and set differences, $x \in A \wedge (y \in B \wedge y \notin C)$. Since $x \in A \wedge y \in B$, by definition of Cartesian products, $(x, y) \in A \times B$. And since $x \in A$ but $y \notin C$, again by definition of Cartesian products, $(x, y) \notin A \times C$. Then by definition of set differences, $(x, y) \in A \times B - A \times C$. So

$$A \times (B - C) \subseteq A \times B - A \times C$$

Now suppose $(x, y) \in A \times B - A \times C$, then $(x \in A \wedge y \in B) \wedge \neg(x \in A \wedge y \in C)$. From the second statement, $x \notin A \vee y \notin C$, and from from the first statement $x \in A$, in order for both statements to be true, it must be true that $y \notin C$. So now we have $x \in A \wedge (y \in B \wedge y \notin C)$, by definition of Cartesian products and set differences, $(x, y) \in A \times (B - C)$, and therefore

$$A \times B - A \times C \subseteq A \times (B - C)$$

Since both directions hold,

$$A \times (B - C) = A \times B - A \times C$$

11.1.8

For any $x \in \mathbb{Z}$, the only $y \in \mathbb{Z}$ that satisfies $|x - y| < 1$ is x itself. Therefore, we have

- $|x - x| = 0 < 1 \Rightarrow xRx$, so R is reflexive.
- $xRx \Rightarrow xRx$, so R is symmetric.
- $(xRx \wedge xRx) \Rightarrow xRx$, so R is transitive.

R is the identity relation.

11.1.16

- $x^2 = x^2$, therefore $x^2 \equiv x^2 \pmod 4$, so R is reflexive.
- If xRy, then $x^2 \equiv y^2 \pmod 4$. Because congruence relation is symmetric, $y^2 \equiv x^2 \pmod 4$, then by definition yRx. So R is symmetric.
- If xRy, yRz then $x^2 \equiv y^2 \pmod 4$ and $y^2 \equiv z^2 \pmod 4$. Because congruence relation is transitive, $x^2 \equiv z^2 \pmod 4$, then by definition xRz. So R is transitive.

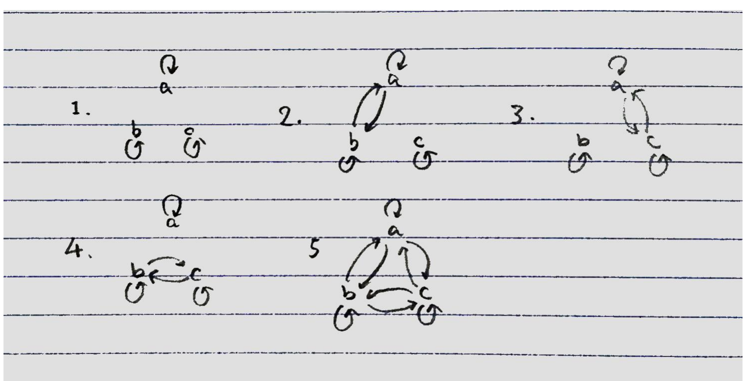
11.2.4

Starting from b,

- $bRc \Rightarrow cRb$.
- $bRc \wedge cRe \Rightarrow bRe \Rightarrow eRb$.
- $bRe \wedge eRa \Rightarrow bRa \Rightarrow aRb$.
- $bRa \wedge aRd \Rightarrow bRd \Rightarrow dRb$.

Therefore $[b] = A$. There is only one equivalence class.

11.2.6



11.2.10

Because R and S are both equivalence relations, for all $x \in A$, $(x,x) \in R$ and $(x,x) \in S$, and therefore $(x,x) \in R \cap S$. so $R \cap S$ is reflexive. If $(x,y) \in R \cap S$, then $(x,y) \in R$ and $(x,y) \in S$. By symmetry, $(y,x) \in R$ and $(y,x) \in S$, therefore $(y,x) \in R \cap S$. So $R \cap S$ is symmetric. Finally, if $(x,y) \in R \cap S$ and $(y,z) \in R \cap S$, then by transitivity

$$\Big((x,y) \in R \wedge (y,z) \in R\Big) \Rightarrow (x,z) \in R, \quad \Big((x,y) \in S \wedge (y,z) \in S\Big) \Rightarrow (x,z) \in S$$

so $(x,z) \in R \cap S$. Therefore $R \cap S$ is also transitive. Since $R \cap S$ has all three properties, it is a equivalence relation.

MATH 2106 Homework 4

Wenqi He

October 2, 2018

1

a

Let σ denote a Hamilton path, and let I_σ be a random vairable that takes value 1 if the tournament contains such a path and 0 otherwise. The number of Hamilton paths is a random variable

$$N = \sum_{\sigma} I_\sigma$$

The expectation of N is

$$E[N] = E[\sum_{\sigma} I_\sigma] = \sum_{\sigma} E[I_\sigma] = \sum_{\sigma} 1 \cdot P(\sigma) + 0 = \sum_{\sigma} \left(\frac{1}{2}\right)^2 = 3! \left(\frac{1}{2}\right)^2 = \frac{3}{2}$$

b

Denote the players as a, b, c. The possible outcomes are

$a \to b$	$b \to c$	$c \to a$	3 Hamiltonian paths
$a \to b$	$b \to c$	$a \to c$	1
$a \to b$	$c \to b$	$c \to a$	1
$a \to b$	$c \to b$	$a \to c$	1
$b \to a$	$b \to c$	$c \to a$	1
$b \to a$	$b \to c$	$a \to c$	1
$b \to a$	$c \to b$	$c \to a$	1
$b \to a$	$c \to b$	$a \to c$	3

The average is $\frac{12}{8} = \frac{3}{2}$

2

Consider K_k. If all edges in K_k are colored red, then there is a red K_k, Otherwise, if not all edges are red, then there must be a blue edge. So $R(k, 2) \leq k$. Now consider K_{k-1}. If all edges are colored red, then the graph contains neither a red K_k nor a blue edge, so $R(k, 2) > k - 1$. Therefore, $R(k, 2) = k$.

3

Consider any vertex v, there are two possibilities:

- Suppose there are at least 6 red edges incident to it. Pick any 6 vertices other than v that are incident to these edges. Since in a clique every pair of vertices are connected by an edge, these 6 vertices form a K_6. Since $R(3,3) = 6$, there exists either a red K_3 or blue K_3 in this K_6. If it's blue then we are done. If it's red, then we can form a red K_4 by adding the 3 red edges connecting each of these vertices to v.
- Suppose there are fewer than 6 red edges incident to v, then there must be more than $9 - 6 = 3$ blue edges. In other words, there are at least 4 blue edges. Any 4 vertices other than v that are incident to these blue edges form a K_4. If it's red then we are done. Otherwise, if any of the edges in this K_4 is blue, since the two edges connecting them to v are also blue, they together form a blue K_3.

Thus we can always find either a red K_4 or a blue K_3 in an arbitrary coloring of K_{10}, which means that $R(4,3) \leq 10$.

4

Consider a random coloring of the elements. The probability that a set is monochromatic is

$$P(monochromatic) = P(red) + P(blue) = 2 \cdot \left(\frac{1}{2}\right)^k = \left(\frac{1}{2}\right)^{k-1}$$

If we define a random variable for each set S

$$I_S = \begin{cases} 1, & \text{if } S \text{ is monochromatic} \\ 0, & \text{otherwise} \end{cases}$$

then the number of monochromatic sets in a collection of m k-sets is $X = \sum_{i=1}^{m} I_{s_i}$, and

$$E[X] = E[\sum_{i=1}^{m} I_{s_i}] = \sum_{i=1}^{m} E[I_{s_i}] = \sum_{i=1}^{m} \left[1 \cdot \left(\frac{1}{2}\right)^{k-1} + 0\right] = m\left(\frac{1}{2}\right)^{k-1}$$

if $m < 2^{k-1}$, then

$$m\left(\frac{1}{2}\right)^{k-1} < 2^{k-1}\left(\frac{1}{2}\right)^{k-1} = 1$$

Since X can only take integer values, it must be zero for at least one Red-Blue coloring, which means that there exists a coloring such that none of the S_i is monochromatic. Therefore by definition, the collection of m k-sets always admits a proper Red-Blue coloring when $m < 2^{k-1}$.

7.6

1. From right to left: If $y = x^2$, $LHS = x^3 + x^4 = RHS$. If $y = -x$, $LHS = x^3 - x^3 = 0 = x^2 - x^2 = RHS$.

2. From left to right: $x^3 + x^2y - y^2 - xy = (x^2 - y)(x + y) = 0$, therefore $y = x^2$ or $y = -x$

7.8

1. From right to left: Suppsoe $a \equiv b \pmod 2$, then $a - b = 2k$. Suppose $a \equiv b \pmod 5$, then $5 \mid a - b$, By Euclid's lemma $5 \mid k$. Rewrite k as $5n$: $a - b = 2 \cdot 5n = 10n$, therefore $a \equiv b \pmod{10}$.

2. From left to right: Suppose $a \equiv b \pmod{10}$, then $a - b = 10k = 2 \cdot 5 \cdot k$. Therefore $2 \mid a - b$ and $5 \mid a - b$, or equivalently, $a \equiv b \pmod 2$ and $a \equiv b \pmod 5$.

7.18

We can simply construct such a set. For example: $X = \mathbb{N} \cup \{\mathbb{N}\}$, or $X = \mathbb{N} \cup \mathcal{P}(\mathbb{N})$.

10.2

Base case: When $n = 1$, the statement is $1^2 = \dfrac{1 \cdot 2 \cdot 3}{6} = 1$, which is true.

Inductive step: Suppose the statement is true for $k \geq 1$, then

$$\begin{aligned}
1 + \cdots + k^2 + (k+1)^2 &= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \\
&= \frac{(k+1)\Big[k(2k+1) + 6(k+1)\Big]}{6} \\
&= \frac{(k+1)(2k^2 + 7k + 6)}{6} \\
&= \frac{(k+1)(k+2)(2k+3)}{6} = \frac{(k+1)\Big[(k+1)+1\Big]\Big[2(k+1)+1\Big]}{6}
\end{aligned}$$

So the statement is true for $k + 1$. By induction it's true for all n.

10.10

Base case: When $n = 0$, the statement becomes 3 divdes $5^0 - 1 = 0$. which is true.

Inductive step: Suppose for $k \geq 0$, $3 \mid \left(5^{2k} - 1\right)$, then

$$\begin{aligned}
5^{2k} &= 3m + 1 \\
5^{2(k+1)} - 1 &= 25 \cdot 5^{2k} - 1 \\
&= 25 \cdot (3m + 1) - 1 \\
&= 25 \cdot 3m + 24 \\
&= 3(25m + 8)
\end{aligned}$$

so $3 \mid \left(5^{2(k+1)} - 1\right)$. By induction, the statement is true for all $n \geq 0$.

10.24

Base case: When $n = 1$,

$$LHS = 1\binom{1}{1} = 1 = 1 \cdot 2^{1-1} = 1 = RHS$$

Inductive step: Suppose for $m \geq 1$,

$$\sum_{k=1}^{m} k\binom{m}{k} = m2^{m-1}$$

then

$$\begin{aligned}
\sum_{k=1}^{m+1} k\binom{m+1}{k} &= \sum_{k=1}^{m+1} k\left[\binom{m}{k} + \binom{m}{k-1}\right] \\
&= \sum_{k=1}^{m+1} k\binom{m}{k} + \sum_{k=1}^{m+1} k\binom{m}{k-1} \\
&= \sum_{k=1}^{m+1} k\binom{m}{k} + \sum_{k=0}^{m} (k+1)\binom{m}{k} \\
&= \sum_{k=1}^{m+1} k\binom{m}{k} + \sum_{k=0}^{m} k\binom{m}{k} + \sum_{k=0}^{m} \binom{m}{k} \\
&= 2\sum_{k=1}^{m} k\binom{m}{k} + \sum_{k=0}^{m} \binom{m}{k} \\
&= 2 \cdot m2^{m-1} + 2^m \\
&= (m+1)2^m = (m+1)2^{(m+1)-1}
\end{aligned}$$

So the statement is true for $m + 1$. By induction, the statement is true for all $n \geq 1$.

MATH 2106 Homework 2

Wenqi He

September 6, 2018

Problem 1

$GCD(a, b)$ can be written as an integer combination of a and b:

$$g = ax + by$$

If $c \mid a$ and $c \mid b$, then $c \mid RHS$, and therefore $c \mid LHS$

Problem 2

If M is prime, then it's already a contradiction. On the other hand, if it's composite, then it must be divisible by some p_i. Suppose $p_i \mid M$. Since p_i also divides every term on the right side except the i-th term

$$p_i \mid M - \sum_{j \neq i} A_j \Rightarrow p_i \mid A_i$$

where A_i denotes the i-th term. If $p_i \mid A_i$, then p_i must divide some p_j where $j \neq i$, since the prime factorization of the i-th term doesn't contain p_i. However, p_j is only divisible by 1 and itself, so this is a contradiction.

Problem 3

Apply the GCD algorithm;

$$\begin{aligned}
990 &= 11 \cdot 84 + 66 \\
84 &= 1 \cdot 66 + 18 \\
66 &= 3 \cdot 18 + 12 \\
18 &= 1 \cdot 12 + 6 \\
12 &= 2 \cdot 6 + 0
\end{aligned}$$

so $GCD(990, 84) = GCD(12, 6) = 6$.

$$\begin{aligned}
6 &= 18 - 12 \\
&= 18 - (66 - 3 \cdot 18) = -1 \cdot 66 + 4 \cdot 18 \\
&= -1 \cdot 66 + 4 \cdot (84 - 66) = 4 \cdot 84 - 5 \cdot 66 \\
&= 4 \cdot 84 - 5 \cdot (990 - 11 \cdot 84) = -5 \cdot 990 + 59 \cdot 84
\end{aligned}$$

Scale the equation by 4:

$$-20 \cdot 990 + 236 \cdot 84 = 24$$

To find the general solution, we can add and subtract multiples of

$$lcm(a, b) = \frac{ab}{gcd(a, b)} = \frac{990 \cdot 84}{6}$$

$$\begin{aligned}
-20 \cdot 990 + 236 \cdot 84 + \frac{990 \cdot 84}{6}t - \frac{990 \cdot 84}{6}t &= 24 \\
990\left(-20 + \frac{84}{6}t\right) + 84\left(236 - \frac{990}{6}t\right) &= 24 \\
990\,(-20 + 14t) + 84\,(236 - 165t) &= 24
\end{aligned}$$

Therefore,

$$\begin{cases} x = -20 + 14t \\ y = 236 - 165t \end{cases}$$

1.4.6

$$\mathcal{P}(\{1, 2\}) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$$
$$\mathcal{P}(\{3\}) = \{\emptyset, \{3\}\}$$

$\mathcal{P}(\{1, 2\}) \times \mathcal{P}(\{3\}) =$
$\{(\emptyset, \emptyset), (\emptyset, \{3\}), (\{1\}, \emptyset), (\{1\}, \{3\}), (\{2\}, \emptyset), (\{2\}, \{3\}), (\{1, 2\}, \emptyset), (\{1, 2\}, \{3\})\}$

1.4.18

$$|P(A \times P(B)| = 2^{|A \times P(B)|} = 2^{|A| \cdot |P(B)|} = 2^{|A| \cdot 2^{|B|}} = 2^{m \cdot 2^n}$$

1.8.4

$$\bigcup_{i \in \mathbb{N}} A_i = \{2n : n \in \mathbb{Z}\}, \quad \bigcap_{i \in \mathbb{N}} A_i = \{0\}$$

1.8.8

$$\bigcup_{\alpha\in\mathbb{R}} \{\alpha\} \times [0,1] = \{(x,y) \in \mathbb{R}^2 : 0 \le y \le 1\}, \quad \bigcap_{\alpha\in\mathbb{R}} \{\alpha\} \times [0,1] = \emptyset$$

1.8.14

Yes. if $x \in \bigcap_{\alpha\in I} A_\alpha$, then $\forall \alpha \in I : x \in A_\alpha$. Now since $J \subseteq I$,

$$\alpha' \in J \Rightarrow \alpha' \in I \Rightarrow x \in A_{\alpha'}$$

In other words, $\forall \alpha' \in J : x \in A_{\alpha'}$, or equivalently $x \in \bigcap_{\alpha\in J} A_\alpha$. Therefore,

$$x \in \bigcap_{\alpha\in I} A_\alpha \Rightarrow x \in \bigcap_{\alpha\in J} A_\alpha$$

or equivalently,

$$\bigcap_{\alpha\in I} A_\alpha \subseteq \bigcap_{\alpha\in J} A_\alpha$$

2.5.10

The statement is only false when $(P \wedge Q) \vee R$ is true but $R \vee S$ is false. In order for $R \vee S$ to be false, both R and S must be false. And because $(P \wedge Q) \vee R$ is true, $P \wedge Q$ must be true, and so P, Q are both true.

2.6.6

P	Q	R	$P \wedge Q \wedge R$	$\neg(P \wedge Q \wedge R)$	$\neg P$	$\neg Q$	$\neg R$	$(\neg P) \vee (\neg Q) \vee (\neg R)$
T	T	T	T	F	F	F	F	F
T	T	F	F	T	F	F	T	T
T	F	T	F	T	F	T	F	T
T	F	F	F	T	F	T	T	T
F	T	T	F	T	T	F	F	T
F	T	F	F	T	T	F	T	T
F	F	T	F	T	T	T	F	T
F	F	F	F	T	T	T	T	T

Note that the columns corresponding to $\neg(P \wedge Q \wedge R)$ and $(\neg P) \vee (\neg Q) \vee (\neg R)$ have the same truth values.

2.6.10

$$(P \Rightarrow Q) \vee R = (\neg P \vee Q) \vee R = \neg P \vee Q \vee R$$
$$\neg((P \wedge \neg Q) \wedge \neg R) = \neg(P \wedge \neg Q) \vee R = (\neg P \vee Q) \vee R = \neg P \vee Q \vee R$$

Therefore they are equivalent.

Homework 1

Wenqi He

December 2, 2018

1

1.1

All p_i's are odd, so their product must be odd. Therefore $p_1p_2\cdots p_n$ has either the form $4k+3$ or $4k+1$. Note that

$$(4k+3)^2 = 16k^2 + 24k + 9 = 4(4k^2 + 6k + 2) + 1$$

$$(4k+1)^2 = 16k^2 + 8k + 1 = 4(4k^2 + 2k) = 1$$

which means that $(p_1p_2\cdots p_n)^2$ is of the form $4k+1$. Adding 2 gives the form $4k+3$.

1.2

Suppose there exists a p_i that divides M. Since $p_i|(p_1p_2\cdots p_n)^2$,

$$p_1|\Big(M - (p_1p_2\cdots p_n)^2\Big)$$

or equivalently $p_1|2$. However, $p_i \geq 3$ by definition, so it cannot divide 2. This is a contradiction, which means that no p_i can divide M.

1.3

If M is prime, then it already contradicts the hypothesis that p_i's are all the primes of the form $4k+3$, since M would be a new prime of that form and it's larger than any of the p_i's. Now suppose M is composite. Note that: *i*) Since M is odd, it cannot be divided by 2. *ii*) From the result of 1.2, none of p_i's divide M, and since we assumed that p_i's are the only primes of the form $4k+3$, no prime of the form $4k+3$ divides M. Thus we conclude that $M = \prod q_i$ where q_i's have the form $4k+1$. However, that cannot be true, because if we have $a = 4m+1$ and $b = 4n+1$, then

$$ab = (4m+1)(4n+1) = 16mn + 4m + 4n + 1 = 4(4mn + m + n) + 1$$

It can be shown inductively that $M = \prod q_i$ must be of the form $4k+1$, which is a contradiction because we already showed that M is of the form $4k+3$.

2

Suppose there are only a finite number of primes of the form $3k+2$, Let $p_1 = 2, p_2 = 5, \cdots, p_n$ denote the n primes. Consider

$$M = 3\prod_{i=2}^{n} p_i + 2$$

M is of the form $3k+2$, so if it is prime then we already have an contradiction, because it would be a prime of the form $3k+2$ that's not included in $\{p_i\}$. Now suppose it's composite. Obviously it's not divisible by 3 because $3 \nmid 2$. M is also not divisible by p_i, because we know that

$$p_i \mid 3\prod_{i=2}^{n} p_i$$

If $p_i \mid M$ then $p_i \mid 2$, which cannot be true because the only prime that divides 2 is 2, and we excluded $p_1 = 2$ when constructing M. Since 3 is the only prime of the form $3k$, and we assumed that p_i's are the only primes of the form $3k+2$, it must be true that M is a product of primes of the form $3k+1$ only. However, that cannot be true because the product of any two number of the form $3k+1$ is still $3k+1$:

$$(3m+1)(3n+1) = 3(3mn+m+n)+1$$

Therefore the hypothesis that there are only finitely many primes of the form $3k+2$ is false, meaning there are infinitely many such primes.

3

3.1

$$\begin{aligned}
561 &= 22 \cdot 25 + 11 \\
25 &= 2 \cdot 11 + 3 \\
11 &= 3 \cdot 3 + 2 \\
3 &= 1 \cdot 2 + 1 \\
2 &= 2 \cdot 1
\end{aligned}$$

$gcd(561, 25) = gcd(25, 11) = gcd(11, 3) = gcd(3, 2) = gcd(2, 1) = 1$

3.2

$$\begin{aligned}
1 &= 3 - 1 \cdot 2 \\
&= 3 - 1 \cdot (11 - 3 \cdot 3) \\
&= -1 \cdot 11 + 4 \cdot 3 \\
&= -1 \cdot 11 + 4 \cdot (25 - 2 \cdot 11) \\
&= 4 \cdot 25 - 9 \cdot 11 \\
&= 4 \cdot 25 - 9 \cdot (561 - 22 \cdot 25) \\
&= -9 \cdot 561 + 202 \cdot 25
\end{aligned}$$

$x = -9$ and $y = 202$

1.1.16

$$\{\cdots, -6, -4, -2, 0, 2, 4, 6, \cdots\}$$

1.1.22

$$\{i^2 + 2 : i \in \mathbb{Z}^+\}$$