MATH 240 Assignment 2

Mihail Anghelici 260928404

February 22, 2021

Question 1

(a)

$$\begin{aligned} n^5 - n &= n(n^2-1)(n^2+1) \\ &= n(n^2-1)(n^2-4+5) \\ &= n(n^2-1)((n-2)(n+2)+5) \\ &= n(n^2-1)(n-2)(n+2) + 5n(n^2-1) \\ &= (n-2)(n-1)n(n+1)(n+2) + 5(n-1)n(n+1) \end{aligned}$$

The expression $(n-2)(n-1)n(n+1)(n+2)$ represents 5 successive numbers, so one of them has to be divisible by 5 which automatically makes all the factor divisible by 5. The factor $5(n-1)n(n+1)$ is evidently also divisible by 5. Finally, by fact, $a \mid c \wedge b \mid c \Longrightarrow (a+b) \mid c$, so $5 \mid n^5 - n$.

(b)

We show the contrapositive $(\overline{q} \Longrightarrow \overline{p})$, that is $\sqrt[3]{x}$ is rational then x is rational.

$$\sqrt[3]{x} = x^{1/3} = \frac{a}{b} \qquad , a, b \in \mathbb{Z} \text{ reduced}, \Longrightarrow x = \frac{a^3}{b^3}.$$

Since $a, b \in \mathbb{Z}$, then $a^k, b^k \in \mathbb{Z}$ for $k \in \mathbb{Z}_+$. Indeed, the cube of any rational number remains rational, and the fraction remains reduced, so we conclude $x = (a/b)^3$ is rational. Thus, since $(\overline{q} \Longrightarrow \overline{p}) \Longleftrightarrow (p \Longrightarrow q)$,then $\sqrt[3]{x}$ is irrational if x is irrational indeed.

Question 2

(a)

We show $\nexists\ x, y \mid 8x + 2y = 3$ by contradiction.

$$8x + 2y = 3 \iff 4x + y = {}^{3}\!/_{2},$$

If $x \in \mathbb{Z} \Longrightarrow 4x \in \mathbb{Z}$. The sum of two integer numbers remains an integer number so $4x + y \in \mathbb{Z}$, but $3/2 \in \mathbb{Q}$ and $\mathbb{Z} \subsetneq \mathbb{Q}$. This is a contradiction. So indeed, there are no integers x, y such that $8x + 2y = 3$.

(b)

Let us assume $\sqrt{p}$ is rational ,for $p \in \mathbb{P}$. Then,

$$\begin{aligned} \sqrt{p} = {}^{a}\!/_{b} \quad , a, b \in \mathbb{Z} \text{ reduced} , &\Longrightarrow b^2 p = a^2 \qquad (1)\\ &\Longrightarrow p \mid a^2 \Longrightarrow p \mid a \text{ , by lemma, since } (\mathbb{N} \subset \mathbb{Z}). \end{aligned}$$

And so,

$$p \mid a \Longrightarrow \exists\ c \text{ s.t } a = pc \Longrightarrow a^2 = p^2 c^2,$$

Substituting (1) we get

$$\begin{aligned} &\Longrightarrow b^2 p = p^2 c^2 \Longrightarrow b^2 = pc^2\\ &\Longrightarrow p \mid b^2 \Longrightarrow p \mid b \text{ , by lemma, since } (\mathbb{N} \subset \mathbb{Z}). \end{aligned}$$

That is actually a contradiction since by definition a rational number is expressed as a reduced fraction, whence $p \nmid a$ and $p \nmid b$ at the same time. $\therefore \sqrt{p} \notin \mathbb{Q} \Longrightarrow \sqrt{p} \in \mathbb{R} \backslash \mathbb{Q}$.

Question 3

(a)

Base case : For $n = 1$, $4 \mid 7 - 3 \Longrightarrow 4 \mid 4$ ✓.

Inductive step : Let us assume $4 \mid 7^n - 3^n$, we show $4 \mid 7^{n+1} - 3^{n+1}$.

$$4 \mid 7^{n+1} - 3^{n+1} = 4 \mid (7^n 7 - 3^n 3) = 4 \mid ((4+3)7^n - 3^n 3) = 4 \mid (4(7^n) + 3(7^n - 3^n)).$$

We first use the fact $a|b \wedge a|c \Longrightarrow a|(b+c)$ so it suffices to show that $4 \mid 4(7^n)$ and $4 \mid 3(7^n - 3^n)$.The first factor is trivial, $4 \mid 4(7^n)$ indeed. Then, use the divisors property $a \mid kb$ for $k \in \mathbb{Z}$, which follows immediately from the definition of divisors. So $4 \mid 3(7^n - 3^n)$ holds by the property outlined above and by induction hypothesis. We conclude that

$$4 \mid (4(7^n) + 3(7^n - 3^n)) \Longrightarrow 4 \mid 7^{n+1} - 3^{n+1} \qquad \therefore p(n) \text{ holds } \forall n \in \mathbb{N}.$$

(b)

Base case : For $n = 1$, the union operator vanishes and we are left off with $A_1 \backslash B = A_1 \backslash B$ ✓.

Inductive step : Let us assume

$$\bigcup_{i=1}^{n}(A_i \backslash B) = \left(\bigcup_{i=1}^{n} A_i\right) \backslash B, \quad \text{we show,} \quad \bigcup_{i=1}^{n+1}(A_i \backslash B) = \left(\bigcup_{i=1}^{n+1} A_i\right) \backslash B.$$

We have

$$\begin{aligned}\bigcup_{i=1}^{n+1}(A_i \backslash B) &= \bigcup_{i=1}^{n}(A_i \backslash B) \cup (A_{n+1} \backslash B) \\ &= \left(\bigcup_{i=1}^{n} A_i\right) \backslash B \cup (A_{n+1} \backslash B)\end{aligned}$$

We use the alternative form of the set difference operation ;

$$= \left(\bigcup_{i=1}^{n} A_i \cap \overline{B}\right) \cup \left(A_{n+1} \cap \overline{B}\right)$$

Here we use the distributivity law generalized to n elements and the idempotent law, obtaining

$$\begin{aligned}&= \left(\bigcup_{i=1}^{n} A_i \cup A_{n+1}\right) \cap \overline{B} \\ &= \bigcup_{i=1}^{n+1} A_i \cap \overline{B} = \left(\bigcup_{i=1}^{n+1} A_i\right) \backslash B \qquad \therefore p(n) \text{ holds } \forall n \in \mathbb{N}.\end{aligned}$$

Question 4

(a)

$$729 = (3)243 = (3^2)81 = (3^3)27 = (3^4)9 = (3^5)3 = 3^6.$$

(b)

727 is already a prime number. The prime factor is itself.

(c)

$$111 = (11)(1)(2)(3)(2^2)(5)(3)(2)(7)(2^3)(3^2)(2)(5) = (2^8)(3^4)(5^2)(7)(11),$$

which are indeed all prime numbers.

Question 5

(a)

$$\begin{aligned} \gcd(2100, 240) &= \gcd(240, 180) \\ &= \gcd(180, 60) \\ &= 3 \end{aligned} \qquad \begin{aligned} 2100 &= 8(240) + 180 \\ 240 &= 1(180) + 60 \\ 180 &= 3(60) + 0. \end{aligned}$$

(b)

The prime factors of 240 are $240 = 2(120) = 2^3(30) = (2^4)(3)(5)$. The prime factors of 2100 are $2100 = 2^2(525) = 2^2(5^2)(21) = (2^2)(5^2)(3)(7)$.

(c)

$$\begin{aligned} 2100 &= 8(240) + 180 \\ 240 &= 1(180) + 60 \\ 180 &= 3(60) + 0 \end{aligned} \qquad \begin{aligned} 60 &= 240 - 1(180) \\ 60 &= 240 - 1(2100 - 8(240)) \\ 60 &= 9(240) - 1(2100) \end{aligned}$$

We conclude that $s = 9$ and $t = -1$.

Question 6

(a)

Let $d_1 = \gcd(a, b)$, then $d_1 \mid a$ and $d_1 \mid b$ by definition of gcd . Then by fact, $d_1 \mid (a + b)$ as well. Similarly, let $d_2 = \gcd(a + b, a - b)$, then $d_2 \mid a + b$ and $d_2 \mid a - b$ by definition of gcd . Then by fact, $d_2 \mid a$ and $d_2 \mid b$ as well. d_1 and d_2 have the exact same set of divisors, so they must be the same, as it is the greatest common divisor.

$$\therefore \gcd(a, b) = \gcd(a + b, a - b) \qquad \square.$$

(b)

$$a \mid bc \implies \exists\ x \in \mathbb{Z} \text{ s.t } bc = ax,$$

Dividing both sides by d, which is non-zero since gcd $\neq 0$, we get

$$\frac{b}{d}c = \frac{a}{d}x. \tag{2}$$

Then, since $\gcd(a, b) = d$ this implies, by definition of gcd, that $d \mid a$ and $d \mid b$. So in other words, $\exists\ s, t \in \mathbb{Z}$ s.t $a = ds$ and $b = dt$. Substituting the latter in (2),

$$\frac{b}{d}c = \frac{a}{d}x \Longrightarrow \frac{dt}{d}c = \frac{a}{d}x \Longrightarrow tc = \frac{a}{d}x.$$

Here $t, x \in \mathbb{Z}$ but x/t,a quotient of integers, is not necessarily in $\mathbb{Z}$. In our case, assume $x/t \notin \mathbb{Z}$. Define $x/t := x' \notin \mathbb{Z}$, then $c = (a/d)x'$; regardless of what a/d is, the RHS is not in $\mathbb{Z}$,while the LHS, $c \in \mathbb{Z}$ because $a \mid bc \Longrightarrow c \in \mathbb{Z}$. This is a contradiction, so x' must be in $\mathbb{Z}$. Then we conclude,

$$ct = \frac{a}{d}x \Longrightarrow c = \frac{a}{d}x' \Longrightarrow \frac{a}{d} \mid c \quad \text{,since } x' \text{ is arbitrary} \qquad \square.$$