Tony Cai

Week 5 - CS230 Homework

1) Proof: We can prove that the product of any five consecutive integers is divisible by 120 with a direct proof. To start, we can observe that out of 5 consecutive integers, 1 integer will be divisible by 5, at least 1 integer will be divisible by 2 that is not also divisible by 4, at least one integer will be divisible 3, and at least one integer will be divisible 4. This means that the resulting product of any five consecutive integers will look like the following expression, where $x \in \mathbb{Z}, x \geq 1$:

$$5 \cdot 4 \cdot 3 \cdot 2 \ (x)$$

$$120(x),$$

By the definition of divisibility (Definition 2.8) where a non zero integer a divides an integer b if $b = ak$ for some integer k, we can observe that $120 \cdot x \mid 120k$ is true. Thus, we can conclude that the product of any five consecutive integers is divisible by 120. □

2] a) Proof: Towards a proof by contradiction, assume that the curve

$x^2+y^2-3=0$ has at least one rational point where $x, y \in \mathbb{Q}$.

If we express x and y as irreducible fractions, then $x=\frac{a}{b}$

where $a, b \in \mathbb{Z}$, and $\gcd(a,b)=1$. Plugging this into the equation, we would get

$$\frac{a^2}{b^2}+y^2=3$$

$$y^2 = 3-\frac{a^2}{b^2}$$

$$y^2 = \frac{3b^2-a^2}{b^2}$$

$(by)^2 = 3b^2-a^2$, which would imply $(by)^2 \in \mathbb{Z}$ because $3b^2-a^2$ would yield an integer. Since $by \in \mathbb{Q}$ then $by \in \mathbb{Z}$ must also be true. Let $c=by$, where $c \in \mathbb{Z}$. We can plug c into our equation:

$$c^2 = 3b^2-a^2$$

$$a^2+c^2 = 3b^2$$

From this equation, we can observe that $3 \mid (a^2+c^2)$. In <u>Homework 1 Question 9</u>, we proved that $z^2 \equiv 0 \bmod 3$ or $z^2 \equiv 1 \bmod 3$ where $z \in \mathbb{Z}$, which means we can deduce that since $3 \mid (a^2+c^2)$, then $3 \mid a^2$ and $3 \mid c^2$. Therefore, since we know $3 \mid a$ and $3 \mid c$ must also be true, then we can substitute $3s$ and $3t$ for a and c, where $t, s \in \mathbb{Z}$. Thus we would get:

$$9s^2+9t^2=3b^2$$

$$3s^2+3t^2=b^2$$

$3(s^2+t^2)=b^2$, which tells us that $3 \mid b^2$ and thus $3 \mid b$.

This contradicts our previous statement of $\gcd(a,b)=1$ or x being a fully reduced fraction since 3 would be a factor of a, b, and c as shown. Thus, we have proven with a proof of contradiction that x^2+y^2-3 has no rational points. □

2] a) Proof: Towards a proof by contradiction, assume that the curve

$x^2+y^2-3=0$ has atleast one rational point where $x, y \in \mathbb{Q}$.

If we express x and y as irreducible fractions, then $X = \frac{a}{b}$ and

where $a, b, \in \mathbb{Z}$, and $\gcd(a, b) = 1$. Plugging this into the equation,

we would get

$$\frac{a^2}{b^2} + y^2 = 3$$
$$y^2 = 3 - \frac{a^2}{b^2}$$
$$y^2 = \frac{3b^2 - a^2}{b^2}$$
$$(by^2) = 3b^2 - a^2$$

, which would imply $(by)^2 \in \mathbb{Z}$ because $3b^2 - a^2$ would yield an integer. Since $by \in \mathbb{Q}$ then $by \in \mathbb{Z}$ must also be true.

Let $c = by$, where $c \in \mathbb{Z}$. We can plug c into our equation:

$$c^2 = 3b^2 - a^2$$
$$a^2 + c^2 = 3b^2$$

From this equation, we can observe that $3 \mid (a^2+c^2)$. In <u>Homework 1 Question 9</u>, we proved that $z^2 \equiv 0 \bmod 3$ or $z^2 \equiv 1 \bmod 3$ where $z \in \mathbb{Z}$, which means we can deduce that since $3 \mid (a^2+c^2)$, then $3 \mid a^2$ and $3 \mid c^2$. Therefore, Since we know $3 \mid a$ and $3 \mid c$ must also be true, then we can substitute $3s$ and $3t$ for a and C, where $t, s \in \mathbb{Z}$. Thus we would get:

$$9s^2 + 9t^2 = 3b^2$$
$$3s^2 + 3t^2 = b^2$$
$$3(s^2+t^2) = b^2$$

, which tells us that $3 \mid b^2$ and thus $3 \mid b$.

This contradicts our previous statement of $\gcd(a, b) = 1$ or x being a fully reduced fraction since 3 would be a factor of a, b, and c as shown. Thus, we have proven with a proof of contradiction that x^2+y^2-3 has no rational points. $\square$

2)b) From a) we proved that $x^2+y^2-3=0$ has no rational points. We know $\sqrt{3}$ is irrational because if we plug in $y=0$, then $\sqrt{3}$ is a solution for x and since all solutions are irrational by the result of a) then $\sqrt{3}$ is irrational

Proof:

3) Towards a contradiction, we can assme that $Q(k)$ is prime for some $k \in \mathbb{N}$.

We can observe that $Q(k) = a_0 + a_1 k + a_2 k^2 + \dots + a_n k^n = p$, where $p \in \mathbb{Z}$, p is prime, and $a_i \in \mathbb{N}$. Since all the coefficients are positive natural numbers and k is a natural number, Q is increasing on the interval (k, ∞). Suppose we can find $Q(k+p)$ where $p = Q(x)$. We could be able to write $Q(k+p)$ as:

$$Q(k+p) = a_0 + a_1(k+p) + \dots + a_n (k+p)^n$$
$$= a_0 + a_1 k + p a_1 + \dots + a_n k^n + a_n p^n$$

We can observe that $a_0 + p a_1 + p a_2 + \dots + a_n p^n$ could be divisible by $Q(k)$ since p is attached to all a_i values with the exception of a_0 which is a constant. Therefore, the entire $Q(k+p)$ integer is divisible by p. We know that this is a contradiction because $Q(k+p)$ would be composite and since $Q(k)$ must share a value that is not prime with $Q(k+p)$ then this contradicts our previous assumption that $Q(k)$ is prime.

Therefore, we can conclude that there exists $k \in \mathbb{N}$ such that the integer $Q(k)$ is not prime.

D

4) a) In order for f to be injective, $f(x_1) \neq f(x_2)$ for all distinct $x_1, x_2 \in A$ in the function $f: A \to B$. We can see that this isn't true for f since $f(0,0) = (0,0)$ and $f(0,1) = (0,0)$, so these two different inputs could not produce a unique output or $f(x_1) = f(x_2)$, so f is <u>not injective</u>.

"Towards a contradiction" In order for f to be surjective, $\forall b \in B \ \exists^{\leq 1} x \in A,\ f(x) = b$ in the function $f: A \to B$. We can see that this is false for f since there is no ordered pair (x,y) such that $f(x,y) = (1,0)$. We know there is no ordered pair because $f(x,y) = (1,0)$ which implies $xy = 1$ and $x^3 = 0$. However, $x^3 = 0$ is the same as $x = 0$, which would mean $xy = 0$, and since we previously defined xy to be equal to 1, then we would get a contradiction. Thus because ~~because~~ there is no (x,y) such that $f(x,y) = (1,0)$ then we know f is <u>not surjective</u>.

b) $f \circ f : \mathbb{R}^2 \to \mathbb{R}^2$

$f(x,y) = (xy, x^3)$

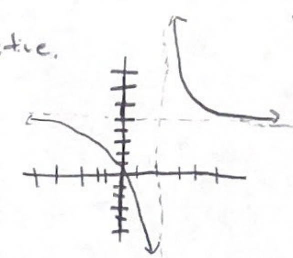
$f \circ f = f(xy, x^3) = \boxed{f \circ f = (x^4 y,\ x^3 y^3)}$

5] $g : \mathbb{R} - \{2\} \to \mathbb{R} - \{5\}$ $\quad g(x) = \dfrac{5x+1}{x-2}$

Proof: Using functions & Inverse

a) In order to prove that g is a bijection, then by definition, we must prove that g is both an injection and a surjection. We can note that as the x value approaches 2 from the negative side, then the y-value approaches $-\infty$ or $\lim_{x \to 2^-} \frac{5x+1}{x-2} = -\infty$. We can also note that as the x value approaches 2 from the positive side, then the y-value approaches ∞ or $\lim_{x \to 2^+} \frac{5x+1}{x-2} = \infty$. Additionally, we can observe that as we approach $x = -\infty$, the function approaches 5 from $y = -\infty$, but will never actually reach 5, and as we approach $x = \infty$, the function also approaches 5, but this time from $y = \infty$. Thus we can tell that g is injective since every input or x value of $\mathbb{R} - \{2\}$, has a unique output in $\mathbb{R} - \{5\}$ that is not repeated, as explained. We can also tell that g is surjective since we've proven that every output value of $\mathbb{R} - \{5\}$ can be achieved using the input values of $\mathbb{R} - \{2\}$ as seen with the limits that result in ∞ or $-\infty$, but not 5. Therefore we can conclude that g is bijective since we've proven g to be both injective and surjective.

Graph provided for additional clarity:



We can also show that g has an inverse that exists in $\mathbb{R} - \{5\}$ as shown in part b, so we know g is bijective. □

*Supplemental proof also provided.

b) $g^{-1} : \mathbb{R} - \{5\} \to \mathbb{R} - \{2\}$

$y = \dfrac{5x+1}{x-2}$ $\quad x = \dfrac{5y+1}{y-2}$ $\quad x(y-2) = 5y+1$

$x(y-2) - (5y+1)$

$xy - 2x - 5y - 1$

$xy - 5y = 2x + 1$

$y(x-5) = 2x+1$

$y = \dfrac{2x+1}{(x-5)}$

$$\boxed{g^{-1}(x) = \frac{2x+1}{(x-5)}}$$

5) Supplemental Proof with Inverses :

a) In order to prove that g is bijective, we must show that g is both bijective and surjective.

We can show that g is bijective

If g is injective then $g(x) = g(y)$. We can simplify and express this in the following way:

$$\frac{5x+1}{x-2} = \frac{5y+1}{y-2} \longrightarrow (5x+1)(y-2) = (5y+1)(y-2)$$

$$5xy - 10y + x = 5xy - 10x + y$$

$$-11y = -11x$$

$$y = x$$

Thus g is a injective since every x value has a unique g(x) value

If g is surjective then we can let $f = g^{-1}$. The work to find the inverse is shown below:

$$y = \frac{5x+1}{x-2} \qquad x = \frac{5y+1}{y-2} \qquad x(y-2) = 5y+1 \qquad xy - 5y = 2x+1$$

$$f = \frac{2x+1}{x-5}$$

$$f\circ g = f(g(x)) = f\left(\frac{5x+1}{x-2}\right) = \frac{2\left(\frac{5x+1}{x-2}\right)+1}{\left(\frac{5x+1}{x-2}\right)-5} = \frac{\frac{10x+2+x-2}{x-2}}{\frac{5x+1-5x+10}{x-2}} = \frac{11x}{11} = x$$

$$g\circ f = g(f(x)) = g\left(\frac{2x+1}{\cancel{x-5}}\right) = \frac{5\left(\frac{2x+1}{x-5}\right)+1}{\frac{2x+1}{x-5}-2} = \frac{10x+5+x-5}{2x+1-2x+10} = \frac{11x}{11} = x$$

Thus g is surjective as well.

Therefore g is both bijective and surjective. $\square$