Proof Portfolio 3

Jon Bayert

December 9, 2020

Theorem 1. *If x and y are positive real numbers, then $2\sqrt{xy} \leq x + y$.*

Proof. We know that any real number squared has to be greater or equal to 0. Thus, $0 \leq (x-y)^2$. To begin, add $4xy$ on both sides:

$$\begin{aligned} 4xy &\leq (x-y)^2 + 4xy \\ &= x^2 - 2xy + y^2 + 4xy, \text{ expanding the square term} \\ &= x^2 + 2xy + y^2, \text{ collect the } xy \text{ terms} \\ &= (x+y)^2, \text{ factor} \end{aligned}$$

Since x and y must be positive, $4xy$ is positive. Also, since $(x+y)^2$ is positive, we can take the square roots of both sides. So, $2\sqrt{xy} \leq (x+y)$. Therefore if x and y are positive real numbers, then $2\sqrt{xy} \leq (x+y)$. □

Theorem 2. *Given that $A \subseteq X$, and $B \subseteq X$, then $A \subseteq B$, $A \cap B^{\mathsf{C}} = \emptyset$, and $A^{\mathsf{C}} \cup B = X$ are equivalent.*

Proof. First, it needs to be shown that $(A \subseteq B)$ is equivalent to $(A \cap B^{\mathsf{C}} = \emptyset)$. To begin we need to show that if $(A \subseteq B)$ then $(A \cap B^{\mathsf{C}} = \emptyset)$. Assume that $A \subseteq B$ and $x \in A$, then it follows that $x \in B$. Since $x \in B$ and x is in the universal set X, then $x \notin B^{\mathsf{C}}$. Since every item in A is not in B^{C}, the intersection of A and B^{C} is empty. Likewise, it needs to be shown that the converse is true. First assume $(A \cap B^{\mathsf{C}} = \emptyset)$, then by definition of intersection $\forall y \in A, y \notin B^{\mathsf{C}}$. Since $y \notin B^{\mathsf{C}}$ but $y \in X$, then $y \in B$. So since every element in A is also in B, then $A \subseteq B$. Therefore, if $A \cap B^{\mathsf{C}} = \emptyset$, then $A \subseteq B$. Thus, $(A \subseteq B) \equiv (A \cap B^{\mathsf{C}} = \emptyset)$.

Now examine $A \cap B^{\mathsf{C}} = \emptyset$, so applying the compliment on each side $(A \cap B^{\mathsf{C}})^{\mathsf{C}} = \emptyset^{\mathsf{C}}$. Applying De Morgan's Law on the left side we get $A^{\mathsf{C}} \cup (B^{\mathsf{C}})^{\mathsf{C}} = A^{\mathsf{C}} \cup B$. On the right side of the equation the complement of the empty set is the universal set, which in this case is X. So, if $A \cap B^{\mathsf{C}} = \emptyset$, then $A^{\mathsf{C}} \cup B = X$. Now to show that the converse is true, assume that $A^{\mathsf{C}} \cup B = X$. Applying the complement of each side, it can be shown that $(A^{\mathsf{C}} \cup B)^{\mathsf{C}} = X^{\mathsf{C}}$. Again using De Morgan's Law on the right and the fact that the complement of X equals the $\emptyset$, it is shown that $A \cap B^{\mathsf{C}} = \emptyset$. So $A \cap B^{\mathsf{C}} = \emptyset$ and $A^{\mathsf{C}} \cup B = X$ are equivalent.

Therefore by the transitive property, $A \subseteq B$, $A \cap B^{\mathsf{C}} = \emptyset$, and $A^{\mathsf{C}} \cup B = X$ are equivalent. □

Theorem 3. *Every prime except* 2 *or* 3 *has the form* $6q+1$ *or* $6q+5$ *where* $q \in \mathbb{Z}$.

Proof. Since this theorem only examines prime numbers we can restrict out domain to natural numbers. This theorem can also be written as a contrapositive as follows: if a natural number k is not in the form $6q+1$ or $6q+5$, then k is either 2 or 3 or a composite number. Any natural number can be written as $6q+1$ $6q+2$, $6q+3$, $6q+4$, $6q+5$ or $6q+6$, where $q \in \mathbb{Z}$ and $q \geq 0$. So, k has to equal $6q+2$, $6q+3$, $6q+4$, or $6q+6$.

In the first case, $6q+2$ can be written as the product of two natural numbers, $2(3q+1)$. So k is either 2 or a composite number. The next case, $6q+3 = 3(2q+1)$, can either be written as 3 or a multiple of three. Likewise $6q+4 = 2(3q+2)$, and $6q+6 = 6(q+1)$, so these are composite. So k is composite numbers or 2 or 3. Thus, every prime number except for 2 or 3 will have the form $6q+1$ or $6q+5$

□

Theorem 4. *$\sqrt[4]{13}$ is irrational.*

Proof. Assume the negation that $\sqrt[4]{13}$ is rational, then $\sqrt[4]{13} = \frac{p}{q}$, where $p \in \mathbb{Z}$, $q \in \mathbb{N}$ and $\frac{p}{q}$ is fully reduced. Therefore,

$$\begin{aligned} \sqrt[4]{13} &= \frac{p}{q} \\ 13 &= \frac{p^4}{q^4} \\ 13q^4 &= p^4 \end{aligned}$$

Notice that p^4 is divisible by two integers 13 and q^4. Since p^4 is divisible by 13 and 13 is prime, then p must be divisible by 13. Thus, p can be written as $13k$, where $k \in \mathbb{Z}$. From above, it can be shown that $q^4 = \frac{p^4}{13} = \frac{(13k)^4}{13} = 13^3k^4$. Thus, 13 is a divisor of q^4, and 13 is a divisor of q. Since 13 is a divisor of both p and q, then $\frac{p}{q}$ can be reduced, which is a contradiction. So $\sqrt[4]{13}$ must be irrational.

$\square$

Theorem 5. $\displaystyle\sum_{i=1}^{n} \frac{1}{\binom{i+1}{2}} = 2 - \frac{2}{n+1}$ *for* $n \geq 2$.

Proof. This can be proved through induction. The initial case, $n = 2$, can be evaluated as follows

$$\begin{aligned}
\sum_{i=1}^{2} \frac{1}{\binom{i+1}{2}} &= \frac{1}{\binom{2}{2}} + \frac{1}{\binom{3}{2}} \\
&= \frac{1}{1} + \frac{1}{3} \\
&= \frac{4}{3}
\end{aligned}$$

This is equivalent to the formula where $2 - \frac{2}{n+1} = 2 - \frac{2}{3} = \frac{4}{3}$. Thus the theorem holds where $n = 2$.

For the inductive step, it must be shown, if $\sum_{i=1}^{k} \frac{1}{\binom{i+1}{2}} = 2 - \frac{2}{k+1}$ where $k \geq 2$, then $\sum_{i=1}^{k+1} \frac{1}{\binom{i+1}{2}} = 2 - \frac{2}{(k+1)+1}$. This can begin as follows:

$$\begin{aligned}
\sum_{i=1}^{k+1} \frac{1}{\binom{i+1}{2}} &= \sum_{i=1}^{k} \frac{1}{\binom{i+1}{2}} + \frac{1}{\binom{k+1+1}{2}} \\
&= 2 - \frac{2}{k+1} + \frac{1}{\binom{k+1+1}{2}}, \text{ by the inductive hypothesis} \\
&= 2 - \frac{2}{k+1} + \frac{1}{\frac{(k+2)!}{2!k!}}, \text{ the definition of a binomial coefficient} \\
&= 2 - \frac{2}{k+1} + \frac{2}{(k+2)(k+1)} \\
&= 2 - \frac{2}{k+1} - \frac{2}{k+2} + \frac{2}{k+1}, \text{ by partial fraction decomposition} \\
&= 2 - \frac{2}{k+2} \\
&= 2 - \frac{2}{(k+1)+1}, \text{ which proves the inductive step}
\end{aligned}$$

Thus, $\sum_{i=1}^{n} \frac{1}{\binom{i+1}{2}} = 2 - \frac{2}{n+1}$ holds for $n \geq 2$. □

Theorem 6. *Given that* $x_0 = 1, x_1 = 3$, *and* $x_n = 6x_{n-1} - 8x_{n-2}$ *for* $n \geq 2$, *then* $x_n = 2^{n-1} + \frac{4^n}{2}$ *for* $n \geq 0$.

Proof. When $n = 0$, $x_0 = 2^{0-1} + \frac{4^0}{2} = 1$. When $n = 1$, $x_1 = 2^{1-1} + \frac{4^1}{2} = 3$. This is consistent with our given values. Thus the initial cases hold.

So to prove the inductive step, it needs to be shown that if $x_k = 2^{k-1} + \frac{4^k}{2}$ for $0 \leq k \leq n$, then $x_{n+1} = 2^{(n+1)-1} + \frac{4^{n+1}}{2}$. From the assumptions, we know that:

$$\begin{aligned}
x_{n+1} &= 6x_n - 8x_{n-1} \\
&= 6\left(2^{n-1} + \frac{4^n}{2}\right) - 8\left(2^{n-2} + \frac{4^{n-1}}{2}\right), \text{ by the inductive assumption} \\
&= 6 \cdot 2^{n-1} + \frac{6 \cdot 4^n}{2} - 8 \cdot 2^{n-2} - \frac{8 \cdot 4^{n-1}}{2} \\
&= 3 \cdot 2^n + 3 \cdot 4^n - 2 \cdot 2^n - 4^n \\
&= (3-2) \cdot 2^n + (3-1) \cdot 4^n, \text{ group the } 2^n \text{ and } 4^n \text{ terms} \\
&= 2^n + 2 \cdot 4^n \\
&= 2^{(n+1)-1} + \frac{4^{n+1}}{2}
\end{aligned}$$

Since the inductive step holds, then $x_n = 2^{n-1} + \frac{4^n}{2}$ for $n \geq 0$. $\square$

Theorem 7. *If $a, b \in \mathbb{Z}$ and $a > b > 0$, then* $\gcd(a,b) = \gcd(a-b,b)$.

Proof. First, assume that $\gcd(a,b) = d$. By definition of greatest common divisor $d|a$ and $d|b$. Since d is a divisor of a and b, $dk_1 = a$ and $dk_2 = b$, where $k_1, k_2 \in \mathbb{Z}$. Notice that since $a > b > 0$ then $d > 0$ and $k_1 > k_2$. So $a - b = dk_1 - dk_2 = d(k_1 - k_2)$. So $d|(a-b)$. Since $d|a$ and $d|(a-b)$, d is a divisor of a and $a - b$ but not necessarily the greatest. So, $\gcd(a-b,a) \geq \gcd(a,b)$.

Now start with $\gcd(a-b,a)$. By definition of greatest common divisor, $\gcd(a-b,a)|a$ and $\gcd(a-b,a)|a-b$. So $\gcd(a-b,a)k_1 = a-b$ and $\gcd(a-b,a)k_2 = a$. So,

$$\begin{aligned} b &= a - \gcd(a-b,a)k_1 \\ &= \gcd(a-b,a)k_2 - \gcd(a-b,a)k_1 \\ &= \gcd(a-b,a)(k_2 - k_1) \end{aligned}$$

This shows that $\gcd(a-b,a)|b$ and we know from before that $\gcd(a-b,a)|a$. So $\gcd(a-b,a)$ is a divisor of a and b but not necessary the greatest. Thus, $\gcd(a-b,a) \leq \gcd(a,b)$.

Since $\gcd(a-b,a) \leq \gcd(a,b)$ and $\gcd(a-b,a) \geq \gcd(a,b)$, $\gcd(a-b,a) = \gcd(a,b)$. $\square$

Theorem 8. *If $n \in \mathbb{N}$, then $1 + (-1)^n(2n-1)$ is a multiple of 4. Also, if x is a multiple of 4, then $\exists n \in \mathbb{N}$ such that $x = 1 + (-1)^n(2n-1)$.*

Proof. First assume that n is a natural number. If n is a positive even number, n can be written as $n = 2k, k \in \mathbb{N}$. So,

$$\begin{aligned} 1 + (-1)^{2k}(2(2k) - 1) &= 1 + \left((-1)^2\right)^k (4k-1), \text{-1 raised to an even power equals 1} \\ &= 1 + (1)(4k-1) \\ &= 4k, \text{ which is a multiple of 4} \end{aligned}$$

Thus $1 + (-1)^{2n}(2n-1)$ is a multiple of 4 when n is even.

Now when n is odd, we know that $n = 2k+1, k \in \mathbb{Z}$. Similar to the last part we can show that

$$\begin{aligned} 1 + (-1)^{2k+1}(2(2k+1) - 1) &= 1 + (-1)^{2k}(-1)^1(4k+2-1) \\ &= 1 + (1)(-1)(4k+1) \\ &= 1 - 4k - 1 \\ &= -4k, \text{ which is a multiple of 4} \end{aligned}$$

Thus $1 + (-1)^{2n}(2n-1)$ is a multiple of 4 for all n.

Now it must be shown that the converse is true. Assume that x is a multiple of 4, so $x = 4k, k \in \mathbb{Z}$. When $x > 0$, there exist a n such that $n = \frac{x}{2} = 2k$. Since $x > 0$ then $n > 0$. So,

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

Thus, if x is multiple of 4 and greater than 0, there exists a $n = \frac{x}{2}$ such that $x = 1 + (-1)^n(2n-1)$.

Now for the case when $x \leq 0$. As we have already stated $x = 4k, k \in \mathbb{Z}$, because x is a multiple of 4. Let $n = \frac{-x}{2} + 1 = -2k + 1$. Since $x \leq 0$ then $n > 1$ so n is positive. It follows that:

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

So for all x that are a multiple of 4 and less than 0, there exist a $n = \frac{-x}{2} + 1$, such that $x = 1 + (-1)^n(2n-1)$.

Thus, for all x that are a multiple of 4, there exist a natural number, such that $x = 1 + (-1)^n(2n-1)$. $\square$

Theorem 9. *If $h(x) = g(f(x))$ and $h(x)$ is bijective then $f(x)$ is injective and $g(x)$ is surjective.*

Proof. Assume that the negation is true, $h(x) = g(f(x))$ and $h(x)$ is bijective, and $f(x)$ is not injective or $g(x)$ is not surjective. Also say that domains and co-domains of the functions are: $f : X \to Y$, $g : Y \to Z$, and $h : X \to Z$.

We have two options $f(x)$ is not injective or $g(x)$ is not surjective. So to start assume that $f(x)$ is not injective. By the definition of injective, there exists an $x_1, x_2 \in X$, such that $x_1 \neq x_2$ and $f(x_1) = f(x_2)$. Since $g(x)$ is a function we know that $g(f(x_1)) = g(f(x_2))$, which can be rewritten as $h(x_1) = h(x_2)$. But it was already shown that $x_1 \neq x_2$, so $h(x)$ can not be injective and thus is not bijective.

Now the second part of the proof we need to assume that $g(x)$ is not surjective. Since $g(x)$ is not surjective, there exists a $z' \in Z$ such that $\forall y \in Y$, $g(y) \neq z'$. By the definition of a function $y = f(x)$ every $x \in X$ has to map to a $y \in Y$, but the last statement showed that $\forall y \in Y$, $g(y) \neq z'$. Thus there exists a $z' \in Z$ such that $\forall x \in X, g(f(x)) = h(x) \neq z'$. However this shows that $h(x)$ is not surjective and thus is not bijective. So this shows that it is a contradiction.

Thus, if $h(x) = g(f(x))$ and $h(x)$ is bijective then $f(x)$ is injective and $g(x)$ is surjective. $\square$

Theorem 10. $\mathbb{N} \times \mathbb{N}$ *is countable.*

Proof. We can form a table of ordered pairs. We can start with $(1, 1)$. Moving one element to right increments the second term by one. Moving one element down increments the first term by one. This will arrange the one set $N = 1, 2, 3, \ldots$ horizontal and the second set of $1, 2, 3, \ldots$ vertical. Thus the ordered pair (a, b) would be placed at the b column and the a row. The table will look like this:

$$
\begin{tikzcd}
(1,1) \arrow[r] & (1,2) \arrow[dl] & (1,3) \arrow[r] & (1,4) \arrow[dl] & \cdots \\
(2,1) \arrow[d] & (2,2) \arrow[ur] & (2,3) \arrow[dl] & \cdots & \\
(3,1) \arrow[ur] & (3,2) \arrow[dl] & \cdots & & \\
(4,1) & \cdots & & & \\
\cdots & & & &
\end{tikzcd}
$$

Now define the $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$. The first term $f(1)$ would start at the top left corner, and then every term after that will follow the arrows. Then the second term would follow the arrow so $f(2) = (1, 2)$. So $f(n)$ is the nth element in this sequence. $f : \mathbb{N} \to \mathbb{N} \times \mathbb{N}$ would start as follows:

$$
\begin{aligned}
f(1) &= (1,1) \\
f(2) &= (1,2) \\
f(3) &= (2,1) \\
f(4) &= (3,1) \\
f(5) &= (2,2) \\
&\cdots
\end{aligned}
$$

This is an injective function because no element is repeated. Since the path never overlaps itself, if $f(x_1) = f(x_2)$, then $(c_1, r_1) = (c_2, r_2)$. Thus $c_1 = c_2$ and $r_1 = r_2$, and they must come from the same row and column in the table. So $x_1 = x_2$, and function f is injective. A

This is a surjective function because it maps to all $\mathbb{N} \times \mathbb{N}$. Any element of $\mathbb{N} \times \mathbb{N}$ can be defined as (x, y) such that $x, y \in \mathbb{N}$. So to find this in the sequence you would just have to go to the element on the x row and the y column.

So thus this is a bijective function, and $\mathbb{N} \times \mathbb{N}$ is countable. $\square$

I have neither given or received nor have I tolerated others use of unauthorized aid. Jon Bayert