Problem 1.

Prove Bernoulli's inequality:

$$(1+x)^n \geq 1 + nx$$

for all non-negative integers n and real numbers $x > -1$.

Solution:

- Base case ($n = 0$): $(1+x)^0 = 1 \geq 1 = 1 + 0x$. So the base case is true.
- Induction: Assume that for $k \geq 0$, $(1+x)^k \geq 1 + kx$. Then:

$$\begin{aligned}(1+x)^{k+1} = (1+x)(1+x)^k &\geq (1+x)(1+kx) \\ &= 1 + x + kx + kx^2 \\ &= 1 + (k+1)x + kx^2 \\ &\geq 1 + (k+1)x\end{aligned}$$

  The last step follows from the fact that $kx^2 \geq 0$.
  This proves the $(k+1)$-th case.

- Conclusion: The result follows by induction.

Problem 2.

Given sets A and B, define their *symmetric difference* by:

$$A\Delta B = (A - B) \cup (B - A) = (A \cup B) - (A \cap B)$$

Prove that for any sets A, B and C, the following holds:

$$(A\Delta B)\Delta C = A\Delta(B\Delta C)$$

Solution:

Note first that for any sets X and Y:

$$X\Delta Y = (X - Y) \cup (Y - X) = (Y - X) \cup (X - Y) = Y\Delta X$$

Note also that we can write $A\Delta B = (A \cap B^c) \cup (B \cap A^c)$.

$$\begin{aligned}
&(A\Delta B)\Delta C \\
&= (((A \cap B^c) \cup (B \cap A^c)) \cap C^c) \cup (C \cap ((A \cap B^c) \cup (B \cap A^c))^c) \\
&= (((A \cap B^c) \cap C) \cup ((B \cap A^c) \cap C^c)) \cup (C \cap ((A^c \cup B) \cap (B^c \cup A))) \\
&= ((A \cap B^c \cap C^c) \cup (B \cap A^c \cap C^c)) \cup (C \cap ((A^c \cap (B^c \cup A)) \cup (B \cap (B^c \cup A)))) \\
&= ((A \cap B^c \cap C^c) \cup (B \cap A^c \cap C^c)) \cup (C \cap ((A^c \cap B^c) \cup (A^c \cap A)) \cup ((B \cap B^c) \cup (B \cap A)))) \\
&= ((A \cap B^c \cap C^c) \cup (B \cap A^c \cap C^c)) \cup (C \cap ((A^c \cap B^c) \cup \emptyset) \cup (\emptyset \cup (B \cap A)))) \\
&= ((A \cap B^c \cap C^c) \cup (B \cap A^c \cap C^c)) \cup (C \cap ((A^c \cap B^c) \cup (B \cap A))) \\
&= ((A \cap B^c \cap C^c) \cup (B \cap A^c \cap C^c)) \cup ((C \cap (A^c \cap B^c)) \cup (C \cap (B \cap A))) \\
&= ((A \cap B^c \cap C^c) \cup (B \cap A^c \cap C^c)) \cup ((C \cap A^c \cap B^c) \cup (C \cap B \cap A)) \\
&= (A \cap B^c \cap C^c) \cup (B \cap A^c \cap C^c) \cup (C \cap A^c \cap B^c) \cup (C \cap B \cap A)
\end{aligned}$$

Now switching $A \mapsto B$ (B with A), $B \mapsto C$ (C with B) and $C \mapsto A$ (A with C), we obtain:

$$\begin{aligned}
&(B\Delta C)\Delta A \\
&= (B \cap C^c \cap A^c) \cup (C \cap B^c \cap A^c) \cup (A \cap C^c \cap B^c) \cup (A \cap C \cap B) \\
&= (B \cap A^c \cap C^c) \cup (C \cap A^c \cap B^c) \cup (A \cap B^c \cap C^c) \cup (C \cap B \cap A) \\
&= (A \cap B^c \cap C^c) \cup (B \cap A^c \cap C^c) \cup (C \cap A^c \cap B^c) \cup (C \cap B \cap A) \\
&= (A\Delta B)\Delta C
\end{aligned}$$

In the equalities above, we used the fact that the operations $\cap$ and $\cup$ are associative (i.e. the order doesn't matter).

As $(B\Delta C)\Delta A = A\Delta(B\Delta C)$ by the remark above, it follows that:
$(A\Delta B)\Delta C = A\Delta(B\Delta C)$.

Problem 3. Solve the following linear congruences:

(a) $3x \equiv 15 \mod 18$

(b) $4x \equiv 14 \mod 18$

Solution:

(a) gcd(3,18) $= 3 \times$ gcd(1,6) $= 3$. Here, note that 3 divides 15, and so the equation has a solution. Also, note that 3 divides 3, 15 and 18. Therefore, we can divide through the equation by 3, and therefore: $x \equiv 5 \mod 6$ – which is the solution.

(b) gcd(4,18) $= 2 \times$ gcd(2,9) $= 2$ which divides 18 and so the equation has a solution. Here, note that 2 divides 4, 14 and 18. Therefore, we can divide through the equation by 2, whence: $2x \equiv 7 \mod 9$.
Now we ought to find gcd(2,9) $= 1$ as a linear combination of 2 and 9 using the Euclidean algorithm:

$$9 = 4 \cdot \mathbf{2} + 1$$

$$2 = 2 \cdot \mathbf{1} + 0$$

So gcd(2,9) $= 1 = 1 \cdot \mathbf{9} + (-4) \cdot \mathbf{2}$.
Now reducing mod 9, we have $1 \equiv 1 \cdot \mathbf{9} + (-4) \cdot \mathbf{2} \equiv 2 \cdot (-4) \mod 9$.
Thus: $2 \cdot (-4) \equiv 1 \mod 9$ and so: $2 \cdot ((-4) \cdot 7) \equiv 7 \mod 9$. Therefore, the solution is $x \equiv (-4) \cdot 7 \equiv -28 \equiv 4 \mod 9$, i.e. $x \equiv 8 \mod 9$.

Problem 4.

(a) Consider the diophantine equation $98n + 35m = 13$ where n and m are integers. Does it possess any solutions? If so, prove it. If not, explain why.

(b) Solve the diophantine equation $98n + 35m = 14$ where n and m are integers.

Solution:

- We first need to find gcd(98,35):

$$98 = 2 \cdot \mathbf{35} + 28$$

$$35 = 1 \cdot \mathbf{28} + 7$$

$$28 = 4 \cdot \mathbf{7} + 0$$

  Therefore, gcd(98,35) $= 7$ and 7 does not divide 13. So this equation has no solution.

- As seen above, gcd(98,35) $= 7$ and 7 divide 14. So this equation has a solution.
  Now as 7 divides all of 98, 35 and 14, we can divide through the equation by 7 to obtain: $14n + 5m = 2$. We can now work on this reduced equation.
  As gcd(14,5) $= 1$, we can find 1 as a linear combination of 14 and 5.
  Indeed: $1 = (-1) \cdot 14 + 3 \cdot 5$, and so: $14 \cdot (-2) + 5 \cdot 6 = 2$. So a special solution to our equation is $(-2, 6)$.
  Therefore, the solution to our equation is: $(n, m) = (-2 + 5q, 6 - 14q)$ where $q \in \mathbb{Z}$.

Problem 5.

Let n be a positive integer and $\{x_i\}$ be positive real numbers. Using the principle of induction, prove that:

$$\frac{1}{2^n}\sum_{i=1}^{2^n} x_i \geq \left(\prod_{i=1}^{2^n} x_i\right)^{1/2^n}$$

Answer:

Since n is **positive**, $n \geq 1$.

- Base case ($n = 1$): Let x_1 and x_2 be two positive integers. Then, the claim is that: $\frac{1}{2}(x_1 + x_2) \geq (x_1 \cdot x_2)^{1/2} = \sqrt{x_1 x_2}$ which is true since:

  $$\frac{1}{2}(x_1 + x_2) \geq \sqrt{x_1 x_2} \Leftrightarrow x_1 + x_2 \geq 2\sqrt{x_1 x_2} \Leftrightarrow (x_1 + x_2)^2 \geq 2x_1 x2 \Leftrightarrow x_1^2 + x_2^2 \geq 0$$

  The rightmost proposition is always true, and the equivalences hold because x_1 and x_2 are positive real numbers.

- Induction: Assume that for any $n \geq 1$ and any 2^n positive real numbers $x_1, x_2, \ldots, x_{2^n}$, we have:

  $$\frac{1}{2^n}\sum_{i=1}^{2^n} x_i \geq \left(\prod_{i=1}^{2^n} x_i\right)^{1/2^n}$$

  We need to show that for any 2^{n+1} positive real numbers:

  $$\frac{1}{2^{n+1}}\sum_{i=1}^{2^{n+1}} x_i \geq \left(\prod_{i=1}^{2^{n+1}} x_i\right)^{1/2^{n+1}}$$

  Note that $2^{n+1} = 2^n + 2^n$. So let $x_1, \cdots, x_{2^n}, x_{2^n+1}, \cdots, x_{2^{n+1}}$ be 2^{n+1} positive numbers. Then:

  $$\frac{1}{2^{n+1}}\sum_{i=1}^{2^{n+1}} x_i = \frac{1}{2 \cdot 2^n}\sum_{i=1}^{2^{n+1}} x_i = \frac{1}{2}\left(\frac{1}{2^n}\sum_{i=1}^{2^n} x_i + \frac{1}{2^n}\sum_{i=2^n+1}^{2^{n+1}} x_i\right)$$

  Now relabeling $y_j = x_{2^n+j}$ for $1 \leq j \leq 2^n$ so that $y_1 = x_{2^n+1}, \ldots, y_n = x_{2^n+2^n} = x_{2^{n+1}}$, we obtain that the numbers $\{y_j\}$ form a collection of 2^n positive numbers.
  Therefore, by the induction hypothesis:

  $$\frac{1}{2^n}\sum_{j=1}^{2^n} y_j \geq \left(\prod_{j=1}^{2^n} y_j\right)^{1/2^n}$$

  But by the same induction hypothesis, we have:

  $$\frac{1}{2^n}\sum_{i=1}^{2^n} x_i \geq \left(\prod_{i=1}^{2^n} x_i\right)^{1/2^n}$$

So as:

$$\frac{1}{2^{n+1}}\sum_{i=1}^{2^{n+1}} x_i = \frac{1}{2}\left(\frac{1}{2^n}\sum_{i=1}^{2^n} x_i + \frac{1}{2^n}\sum_{i=2^n+1}^{2^{n+1}} x_i\right) = \frac{1}{2}\left(\frac{1}{2^n}\sum_{i=1}^{2^n} x_i + \frac{1}{2^n}\sum_{j=1}^{2^n} y_j\right)$$

It follows that:

$$\frac{1}{2^{n+1}}\sum_{i=1}^{2^{n+1}} x_i \geq \frac{1}{2}\left(\left(\prod_{i=1}^{2^n} x_i\right)^{1/2^n} + \left(\prod_{j=1}^{2^n} y_j\right)^{1/2^n}\right)$$

Letting $a = \left(\prod_{i=1}^{2^n} x_i\right)^{1/2^n}$ and $b = \left(\prod_{j=1}^{2^n} y_j\right)^{1/2^n}$, we can see that both a and b are positive as the roots of products of positive numbers, and so, using the base case:

$$\frac{1}{2}(a+b) \geq (ab)^{1/2}$$

Hence:

$$\frac{1}{2}\left(\left(\prod_{i=1}^{2^n} x_i\right)^{1/2^n} + \left(\prod_{j=1}^{2^n} y_j\right)^{1/2^n}\right) \geq \left(\left(\prod_{i=1}^{2^n} x_i\right)^{1/2^n}\left(\prod_{j=1}^{2^n} y_j\right)^{1/2^n}\right)^{1/2} = \left(\left(\prod_{i=1}^{2^n} x_i \cdot \prod_{j=1}^{2^n} y_j\right)^{1/2^n}\right)^{1/2}$$

So then:

$$\frac{1}{2}\left(\left(\prod_{i=1}^{2^n} x_i\right)^{1/2^n} + \left(\prod_{j=1}^{2^n} y_j\right)^{1/2^n}\right) \geq \left(\prod_{i=1}^{2^n} x_i \cdot \prod_{j=1}^{2^n} y_j\right)^{1/2^{n+1}} = \left(\prod_{i=1}^{2^n} x_i \cdot \prod_{j=1}^{2^n} x_{2^n+j}\right)^{1/2^{n+1}},$$

as $y_j = x_{2^n+j}$ for $1 \leq j \leq 2^n$.

But, $\prod_{i=1}^{2^n} x_i \cdot \prod_{j=1}^{2^n} x_{2^n+j} = x_1 \cdot x_2 \cdot \dots \cdot x_{2^n} \cdot x_{2^n+1} \cdot \dots \cdot x_{2^{n+1}} = \prod_{i=1}^{2^{n+1}} x_i$. Therefore:

$$\frac{1}{2^{n+1}}\sum_{i=1}^{2^{n+1}} x_i \geq \left(\prod_{i=1}^{2^{n+1}} x_i\right)^{1/2^{n+1}}$$

- Conclusion: the result follows by induction.

Problem 6.

Consider the equation $x^n + y^n = z^n$.
Show that if it has a rational solution, then it has an integer solution.
(That is, show that if $x, y, z \in \mathbb{Q}$ satisfy that equation, then there are numbers $k, \ell, m \in \mathbb{Z}$ depending on x, y, z which also satisfy that equation.)

Solution:

Let $x = \frac{p}{q}, y = \frac{s}{t}$ and $z = \frac{u}{v}$ be rational numbers where all of $p, q, s, t, u, v \in \mathbb{Z}$, and $q \neq 0$, $t \neq 0$ and $v \neq 0$. So then:

$$\begin{aligned} x^n + y^n = z^n &\Rightarrow \left(\frac{p}{q}\right)^n + \left(\frac{s}{t}\right)^n = \left(\frac{u}{v}\right)^n \\ &\Rightarrow \frac{p^n}{q^n} + \frac{s^n}{t^n} = \frac{u^n}{v^n} \\ &\Rightarrow \frac{p^n t^n + s^n q^n}{q^n t^n} = \frac{u^n}{v^n} \\ &\Rightarrow (p^n t^n + s^n q^n) v^n = q^n t^n u^n \\ &\Rightarrow p^n t^n v^n + s^n q^n v^n = q^n t^n u^n \\ &\Rightarrow (ptv)^n + (sqv)^n = (qtu)^n \end{aligned}$$

So ptv, sqv and qtu satisfy the equation as well. As all of $p, q, s, t, u, v \in \mathbb{Z}$, it follows that $ptv, sqv, qtu \in \mathbb{Z}$ and therefore, $(k, \ell, m) = (ptv, sqv, qtu)$ is an integer solution to the original equation.
(Note that k, ℓ and m indeed depend on x, y and z since these depend on p, q, s, t, u and v.)

Problem 7.

Which of the following formulae define well-defined functions $f : \mathbb{Q}^2 \to \mathbb{Q}$? If they do not, explain why.

(a) $f\left(\frac{a}{b}\right) = a + b$

(b) $f\left(\frac{a}{b}\right) = \frac{b}{a}$

(c) $f\left(\frac{a}{b}\right) = \frac{a^2}{b^2}$

Solution:

(a) $f\left(\frac{1}{2}\right) = 1 + 2 \neq 2 + 4 = f\left(\frac{2}{4}\right)$, yet $\frac{1}{2} = \frac{2}{4}$. So this function is not well-defined.

(b) $f(0)$ does not exist since it results in a division by 0. So this function is not well-defined.

(c) $f\left(\frac{a}{b}\right) = \frac{a^2}{b^2} = \left(\frac{a}{b}\right)^2$ and the square function is well-defined in general.
So this function is well-defined.