HMIC 2023
April 15-22, 2023

1. **[6]** Let $\mathbb{Q}^+$ denote the set of positive rational numbers. Find, with proof, all functions $f : \mathbb{Q}^+ \to \mathbb{Q}^+$ such that, for all positive rational numbers x and y, we have

$$f(x) = f(x + y) + f(x + x^2 f(y)).$$

Proposed by: Luke Robitaille

Answer: $\boxed{f(x) = \dfrac{1}{x}}$.

Solution: It is straightforward to check that $f(x) = \frac{1}{x}$ works. We then focus on proving that there are no other solutions. Let $P(x, y)$ denote the given functional equation. First note that for all $x, y \in \mathbb{Q}^+$, $f(x) > f(x + y)$, so f is strictly decreasing and hence injective. Now, for all $x, y \in \mathbb{Q}^+$,

$$\begin{aligned} P(x, y) &\implies f(x) = f(x + y) + f(x + x^2 f(y)) \\ P(x, x^2 f(y)) &\implies f(x) = f(x + x^2 f(y)) + f\big(x + x^2 f(x^2 f(y))\big). \end{aligned}$$

Equating these two equations gives

$$\begin{aligned} f\big(x + x^2 f(x^2 f(y))\big) &= f(x + y) \\ x + x^2 f(x^2 f(y)) &= x + y \\ f(x^2 f(y)) &= \frac{y}{x^2} \end{aligned}$$

for all $x, y \in \mathbb{Q}^+$. In particular, plugging in $x = 1$ gives $f(f(y)) = y$, and replacing y with $f(y)$ gives $f(x^2 y) = \frac{f(y)}{x^2}$ for all $x, y \in \mathbb{Q}^+$. There are two ways to finish.

Finish 1: The above implies that $f(x^2) = \frac{f(1)}{x^2}$ for all $x \in \mathbb{Q}^+$. Since $\{x^2 : x \in \mathbb{Q}^+\}$ is dense in $\mathbb{Q}^+$ and f is decreasing we find that $f(x) = c/x$ for some constant c. Plugging back in now gives $c = 1$.

Finish 2: For all $x \in \mathbb{Q}^+$,

$$\begin{aligned} P\left(x, \frac{9x}{16}\right) \implies f(x) &= f\left(\frac{25x}{16}\right) + f\left(x + x^2 f\left(\frac{9x}{16}\right)\right). \\ &= \frac{16 f(x)}{25} + f\left(x + \frac{16x^2 f(x)}{9}\right) \end{aligned}$$

Hence, we have

$$\begin{aligned} f\left(\frac{25x}{9}\right) = \frac{9f(x)}{25} &= f\left(x + \frac{16x^2 f(x)}{9}\right) \\ \frac{25x}{9} &= x + \frac{16x^2 f(x)}{9} \implies f(x) = \frac{1}{x} \end{aligned}$$

as desired.

2. **[7]** A prime number p is *mundane* if there exist positive integers a and b less than $\frac{p}{2}$ such that $\frac{ab-1}{p}$ is a positive integer. Find, with proof, all prime numbers that are not mundane.

Proposed by: Holden Mui

Answer: $p \in \boxed{\{2, 3, 5, 7, 13\}}$, which can be checked to work.

Solution 1:

The cases $p = 11$, $p = 17$, $p = 19$ fail by $3 \cdot 4$, $3 \cdot 6$, and $4 \cdot 5$, respectively, so assume that $p \geq 21$. The key idea is the following identity:

$$\frac{1}{10} - \left(-\frac{2}{5}\right) = \frac{1}{2}.$$

To see how to utilize this, notice that $10 < \frac{p}{2}$ and $-\frac{5}{2} \pmod{p} = \frac{p-5}{2} < \frac{p}{2}$. Thus, by plugging in $a = 10$ and $a = \frac{p-5}{2}$, we see that both $\frac{1}{10} \pmod{p}$ and $-\frac{2}{5} \pmod{p}$ must be greater than $\frac{p}{2}$, so it must lie in the interval $\left[\frac{p+1}{2}, p-1\right]$.

However, their difference is $\equiv \frac{1}{2} \equiv \frac{p+1}{2} \pmod{p}$, giving a contradiction.

Solution 2:

The case $p = 11$ fails by $3 \cdot 4$, so assume $p = 2^k n + 1 \geq 17$ for some odd n.

- If $n = 1$, then $p = 2^k + 1$. Since $p + 1$ cannot have a divisor greater than 2, $\frac{p+1}{2}$ must be prime, so both $2^{k-1} + 1$ and $2^k + 1$ are consecutive Fermat primes. Since $k - 1$ and k must be powers of 2, this forces $k = 2$, which gives $p = 5$.
- If $n = 3$, then $p = 3 \cdot 2^k + 1$. Since $2p + 1$ cannot have a divisor greater than 4, we have $\frac{2p+1}{3} = 2^{k+1} + 1$ must be prime, $k = 2^c - 1$. $c \in \{1, 2\}$ gives $p \in \{7, 25\}$; the latter is not even a prime. If $c \geq 3$, then
$$5 \mid 3 \cdot 2^{2^c - 1} + 1 = p,$$
contradiction.
- If $n \geq 5$, then
$$2^{k+1} \cdot \frac{p - n}{2} \equiv 1 \pmod{p}$$
shows that this case yields no solutions.

Solution 3:

Assume $p \geq 3$. Let $q > 2$ be the smallest prime not dividing $p - 1$.

Lemma: $q^2 < \frac{p}{2}$ unless $p \in S = \{5, 7, 13, 19, 31, 37, 43, 61, 211\}$.

Proof. Casework on q.

- $q = 3$ gives $p = 5$.
- $q = 5$ gives $p \in \{13, 19, 37, 43\}$.
- $q = 7$ gives $p \in \{31, 61\}$.
- $q = 11$ gives $p = 211$.

No larger q work because

$$13^2 < \frac{2 \cdot 3 \cdot 5 \cdot 7 \cdot 11}{2}$$

and $p_{n+1}^2 < \frac{p_1 p_2 \ldots p_n}{2}$ for $n \geq 5$ by induction using $p_{i+1} < 2p_i$, where p_i are the primes in increasing order. □

Now, $q' \mid (q' - 1)p + 1$ for all primes $q' < q$ by minimality of q, but $q \mid kp + 1$ for some $0 < k < q - 1$, since $q \nmid p - 1$. Therefore, $q \operatorname{rad}(k + 1) \mid kp + 1$, so

$$(q \operatorname{rad}(k+1)) \cdot \frac{kp + 1}{q \operatorname{rad}(k+1)} \equiv 1 \pmod{p}.$$

If $p \notin S$, the first factor can be bounded as

$$q \operatorname{rad}(k+1) < q^2 < \frac{p}{2}$$

and the second factor as

$$\frac{kp+1}{q\,\mathrm{rad}(k+1)} < \frac{(k+1)p}{(k+1)2} = \frac{p}{2}.$$

Therefore, no $p \notin S$ satisfy the problem condition.

To finish the problem, it suffices to show no $p \in S \setminus \{5, 7, 13\}$ work. Indeed,

$$\begin{aligned} 4 \cdot 5 &\equiv 1 \pmod{19} \\ 4 \cdot 8 &\equiv 1 \pmod{31} \\ 5 \cdot 15 &\equiv 1 \pmod{37} \\ 4 \cdot 14 &\equiv 1 \pmod{43} \\ 8 \cdot 23 &\equiv 1 \pmod{61} \\ 4 \cdot 53 &\equiv 1 \pmod{211}, \end{aligned}$$

as desired.

Solution 4: Assume $p \geq 3$. We look for a, b where $|a-b|$ is small. Consider the equation $x(x+k) \equiv 1 \pmod{p}$, which is equivalent to $(2x+k)^2 \equiv 4 + k^2 \pmod{p}$. Taking $k = 1, 2, 6$, at least one of the values $5, 8, 40$ is a quadratic residue modulo p, so this equation has a solution with $k \in \{1, 2, 6\}$. Now take an x satisfying this equation and consider replacing x with $p - k - x$ if this is ≥ 2 and smaller. This gives the desired a, b unless $x < p/2 < x + k$. We now casework based on k.

- If $k = 1$, then $x < p/2 < x + 1$, which force $x = \frac{p-1}{2}$. Hence,

  $$1 \equiv x(x+1) \equiv \left(-\frac{1}{2}\right)\left(\frac{1}{2}\right) \equiv -\frac{1}{4} \pmod{p},$$

  forcing $p = 5$.
- If $k = 2$, then $x < p/2 < x + 2$, which force $x \in \left\{\frac{p-1}{2}, \frac{p-3}{2}\right\} \equiv \left\{-\frac{1}{2}, -\frac{3}{2}\right\}$. Now we have,

  $$\begin{aligned} x \equiv -\frac{1}{2} &\implies 1 \equiv x(x+2) \equiv \left(-\frac{1}{2}\right)\left(\frac{3}{2}\right) \equiv -\frac{3}{4} \pmod{p} \implies p = 7 \\ x \equiv -\frac{3}{2} &\implies 1 \equiv x(x+2) \equiv \left(-\frac{3}{2}\right)\left(\frac{1}{2}\right) \equiv -\frac{3}{4} \pmod{p} \implies p = 7 \end{aligned}$$

  forcing $p = 7$.
- If $k = 6$, then we have $x < p/2 < x + 6$, then $x \in \left\{\frac{p-1}{2}, \frac{p-3}{2}, \ldots, \frac{p-11}{2}\right\} \equiv \left\{-\frac{1}{2}, -\frac{3}{2}, \ldots, -\frac{11}{2}\right\}$. We have

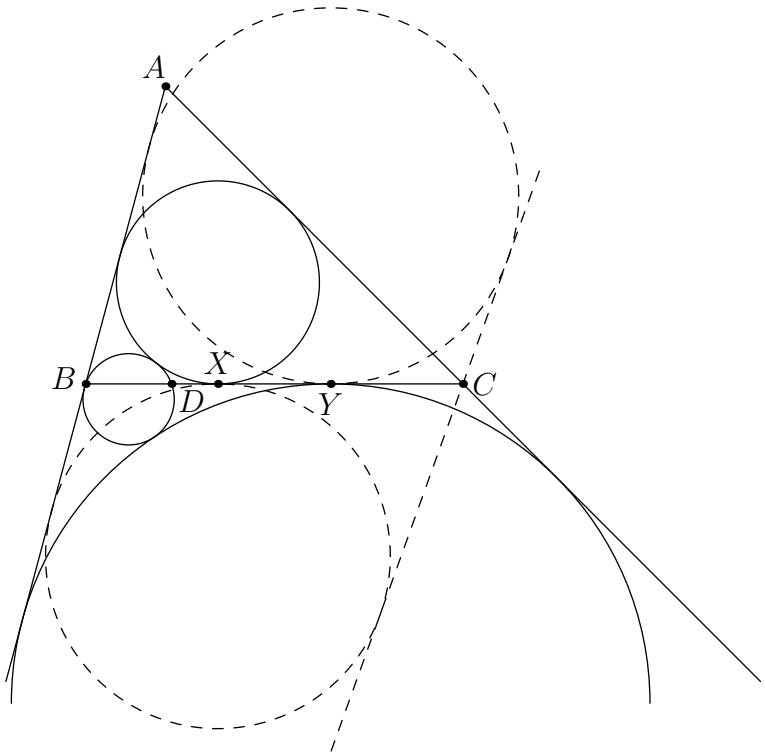
x	$x(x+6)$	p
$-\frac{1}{2}$	$-\frac{11}{4}$	$3, 5$
$-\frac{3}{2}$	$-\frac{27}{4}$	31
$-\frac{5}{2}$	$-\frac{35}{4}$	$3, 13$
$-\frac{7}{2}$	$-\frac{35}{4}$	$3, 13$
$-\frac{9}{2}$	$-\frac{27}{4}$	31
$-\frac{11}{2}$	$-\frac{11}{4}$	$3, 5$

  Thus, all that remains is to eliminate $p = 31$. This is by $4 \cdot 8 \equiv 1 \pmod{31}$.

3. **[9]** Triangle ABC has incircle ω and A-excircle ω_A. Circle γ_B passes through B and is externally tangent to ω and ω_A. Circle γ_C passes through C and is externally tangent to ω and ω_A. If γ_B intersects line BC again at D, and γ_C intersects line BC again at E, prove that $BD = EC$.

Proposed by: Holden Mui

Solution 1: Let $\overline{BC}$ touch the incircle at X and the A-excircle at Y. Since $BX = CY$, it suffices to show that $BP \cdot BC = BX \cdot BY$ by symmetry.



The inversion centered at B with radius $\sqrt{BX \cdot BY}$

- fixes lines $\overline{AB}$ and $\overline{BC}$,
- swaps X and Y,
- sends the incircle to a circle Γ_1 tangent to $\overline{AB}$ and tangent to $\overline{BC}$ at Y,
- sends the A-excircle to a circle Γ_2 tangent to $\overline{AB}$ and tangent to $\overline{BC}$ at X, and
- sends the circle through B tangent to the incircle and A-excircle to a common tangent ℓ of Γ_1 and Γ_2.

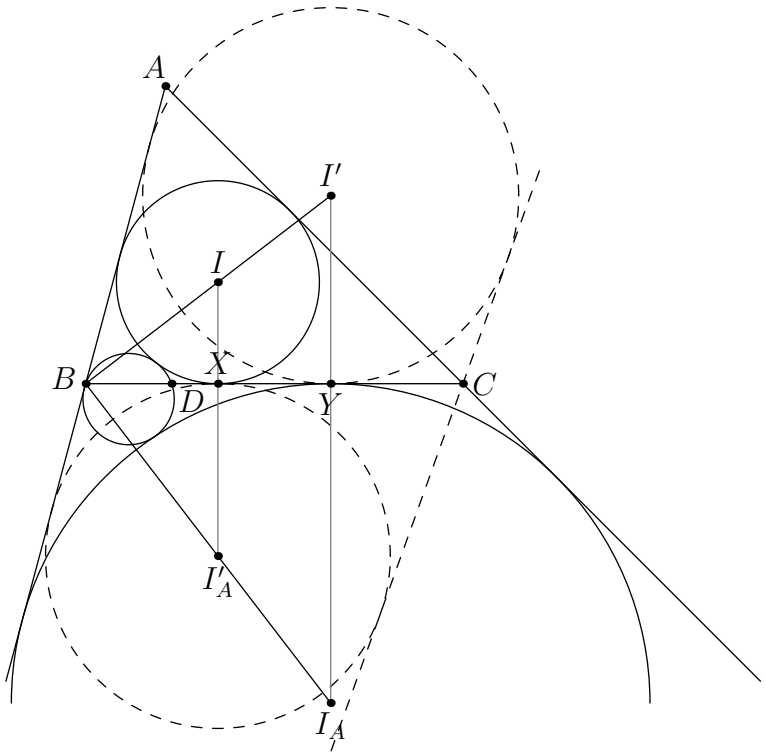
Now, $C \in \ell$ since ℓ must intersect $\overline{BC}$ at a point C' satisfying $BX = C'Y$, so the inversion maps P to C, as desired.

Solution 2: Here is another solution based on inversion at B. First we will need a lemma.

Lemma: Let A, B, C, D lie on a circle, with AC a diameter of this circle. Say E and F are the feet of the altitudes from A and C to BD, respectively. Then ABE is similar to BCF, and $BE = DF$.

Proof. The former is due to angle chasing, the latter is because the midpoint of AC is the circumcenter of $(ABCD)$ and hence equidistant from B and D. □

Now, let X be the A-intouch point, and Y the A-extouch point. The key identity now is that $BD \cdot BC = BX \cdot BY$. Paired with the symmetric statement this now solves the problem.



To prove the statement, invert about B with radius $\sqrt{BX \cdot BY}$. γ_B is sent to the line (not AB) tangent to the images of the incircle and A-excircle; it suffices to prove that this line passes through C. Now, say the centers of these images are I' and I'_A. It suffices to prove that $\angle I'CI'_A = 90^\circ$, or in other words $BI'CI'_A$ is cyclic. Now, evidently $\triangle I'YB \sim \triangle IXB$ and $\triangle I'_AXB \sim \triangle I_AYB$. Moreover $BX = CY$. Hence by the lemma above, I'_A shares two of the same properties as the antipode of I' on $(BI'C)$, so thus they're in fact the same point. So $(BI'CI'_A)$ is cyclic, and so the claim and hence the problem are proved.

Solution 3: Here is a length bashing solution.

Let γ_B intersects AB again at P. Then, notice that ω_A is the mixtilinear excircle of $\triangle BDP$, so an inversion around B with radius $\sqrt{BD \cdot BP}$ followed by reflection across the angle bisector of $\angle DBP$ sends ω_A to the incircle of $\triangle BDP$. Therefore, under inversion, the corresponding tangent points must be swapped, giving

$$(s-c)\left(\frac{BD+BP-DP}{2}\right) = BD \cdot BP \implies BD+BP-DP = \frac{2(BD \cdot BP)}{s-c}.$$

Similarly, notice that under the $\sqrt{BD \cdot BP}$-inversion, ω maps to the D-excircle, so

$$(s-b)\left(\frac{BP+DP-BD}{2}\right) = BD \cdot BP \implies BP+DP-BD = \frac{2(BD \cdot BP)}{s-b}.$$

Adding these two equations together, we find that

$$2BP = 2(BD \cdot BP)\left(\frac{1}{s-b}+\frac{1}{s-c}\right) \implies \frac{1}{BD} = \frac{1}{s-b}+\frac{1}{s-c}.$$

Analogously, we have $\frac{1}{CE} = \frac{1}{s-b} + \frac{1}{s-c}$, so we are done.

Solution 4: Once again, it suffices by symmetry to show $BP \cdot BC = BX \cdot BY$, or equivalently

$BP = \frac{BX \cdot BY}{BX+BY}$. We use Cartesian coordinates, taking B to be the origin and line BC to be the x-axis, with I above the x-axis and I_A below it. Let $I = (t, r)$ and $I_A = (u, -r_A)$ (so $t = BX$ and $u = BY$). Since $BI \perp BI_A$, we have $tu = rr_A$. Let γ_B have center (x, y) and radius z. Note that $P = (2x, 0)$. Now we have that

$$x^2 + y^2 = z^2$$
$$(x-t)^2 + (y-r)^2 = (z+r)^2$$
$$(x-u)^2 + (y+r_A)^2 = (z+r_A)^2.$$

Subtracting the first equation from the second yields $-2xt + t^2 = 2r(y+z)$, and subtracting the first equation from the third yields $-2xu + u^2 = 2r_A(z-y)$. Now, multiplying these equations together gives

$$tu(-2x+t)(-2x+u) = 4rr_A(z^2 - y^2) = 4rr_Ax^2.$$

Dividing by $tu = rr_A \neq 0$ yields that $4x^2 - 2x(t+u) + tu = (-2x+t)(-2x+u) = 4x^2$, so $BP = 2x = \frac{tu}{t+u} = \frac{BX \cdot BY}{BX+BY}$, as desired. ■

4. **[9]** Let $n > 1$ be a positive integer. Claire writes n distinct positive real numbers $x_1, x_2, \ldots, x_n$ in a row on a blackboard. In a *move*, William can erase a number y and replace it with either $\frac{1}{y}$ or $y+1$ at the same location. His goal is to make a sequence of moves such that after he is done, the numbers are strictly increasing from left to right.

   (a) Prove that there exists a positive constant A, independent of n, such that William can always reach his goal in at most $An \log n$ moves.

   (b) Prove that there exists a positive constant B, independent of n, such that Claire can choose the initial numbers such that William cannot attain his goal in less than $Bn \log n$ moves.

   Proposed by: Sean Li

   Solution: We present one solution to (a) and two solutions to (b).

   Solution to (a)

   We use divide and conquer. The base case $n = 1$ is clear. Let $f(n)$ denote the number of moves required for n numbers. Let $x = \lceil n/2 \rceil$ and $y = \lfloor n/2 \rfloor$. Then, William can reach his goal by the following process:

   - Use $f(x)$ moves to make the first x numbers a strictly *decreasing* sequence.
   - Use $f(y)$ moves to make the last y numbers a strictly *decreasing* sequence.
   - Add one to all the numbers, taking n moves. At this point, all the numbers are greater than 1.
   - Take the reciprocal of all the numbers, using n moves. At this point, all the numbers are in $(0, 1)$. Moreover, the first x numbers and the last y numbers form a strictly *increasing* sequence.
   - Finally, add one to the last y numbers.

   Hence, we have

   $$f(n) \leq f\left(\left\lceil \frac{n}{2} \right\rceil\right) + f\left(\left\lfloor \frac{n}{2} \right\rfloor\right) + 2n + \frac{n}{2},$$

   giving $f(n) = O(n \log n)$.

   Double Counting Solution to (b)

   Take $B = 0.01$, and assume n is sufficiently large. Assume for contradiction that William has an algorithm for all possible initial numbers. We first note that if William uses less than x moves, then he can keep adding one to the last number until he uses exactly x move. We henceforth assume that William has an algorithm that uses $x \leq 0.01n \log n$ moves.

   Take arbitrary initial numbers. We claim that if William always has an algorithm that results in the final numbers being increasing after x moves, then he in fact has an algorithm which can result in the

final numbers being in any given ordering after x moves. This is because he can permute the indices of the initial numbers, operate on the permuted numbers to be increasing, and then take the permutation back such that the final numbers are now in the specified ordering after applying x moves (note that each move only acts and depends on one of the values.) In particular, this implies that by applying x moves, William can produce $\geq n!$ possible final states. We now claim this is impossible.

Indeed, there are $\binom{x+n-1}{n-1}$ ways to distribute x moves to each of the n numbers. Moreover, there are two options for each move, giving 2^x choices across all the x moves. Thus, William has

$$2^x \binom{x+n-1}{n-1}$$

choices of moves. When n is sufficiently large, we have

$$\begin{aligned} 2^x \binom{x+n-1}{n-1} &\leq 2^{0.01n \log n} \frac{(x+n-1)^{n-1}}{(n-1)!} \\ &\leq e^{0.01n \log n} \frac{(0.1n \log n)^n}{\left(\frac{n}{10}\right)^n} \\ &= n^{0.01n} (\log n)^n \\ &= n^{0.01n} n^{\log \log n} < \left(\frac{n}{10}\right)^n < n!, \end{aligned}$$

which is a contradiction.

Constructive Solution to (b)

By shifting B it suffices to prove this for sufficiently large n (for the smaller ones just make sure $Bn \log n < 1$.) We now prove the result when $n = k^2$ is a perfect square; the general case follows by shifting B appropriately. Choose the x_is such that

$$\begin{aligned} x_{k^2-k+1} > x_{k^2-2k+1} > \ldots > x_1 \\ > x_{k^2-k+2} > x_{k^2-2k+2} > \ldots > x_2 \\ \ldots \\ > x_{k^2} > x_{k^2-k} > \ldots > x_k. \end{aligned}$$

One may check that there exists no strictly increasing or decreasing subsequence of the $\{x_i\}$s of length $> k$. Now, if William uses less than $Bk^2 \log(k^2)$ moves, then evidently there exists at least $k^2/2$ elements on which he applies at most $2B \log(k^2)$ moves. Let $\lceil 2B \log(k^2) \rceil = N$; note that the number of possible sequences of moves that can be applied to each of these $\leq k^2/2$ elements is $\leq 2^N + 2^{N-1} + \ldots + 1 < 2^{N+1}$. Note that $N = \Theta(\log k^2)$ and so $2^{N+1} = k^{\Theta(1)}$; hence by choosing a sufficiently small B we can ensure that $2^{N+1} < k/2$. This now implies that there exists a set S of $> k$ elements on which the same sequence of moves are applied. Note by our choice of $\{x_i\}$s we know that within S, there exists both a pair (x_i, x_j) for which $i < j$ and $x_i < x_j$, and a pair where $i < j$ yet $x_i > x_j$. But note that any composition of moves acts as a rational function which is monotonic on $(0, \infty)$ (as it has no roots or poles within the given domain.) Hence this implies that either the increasing or decreasing pair must become decreasing after being operated upon by the same sequence of moves, and hence William has not achieved his goal, a contradiction. This thus proves the problem for an appropriate choice of B.

5. **[11]** Let a_1, a_2, ... be an infinite sequence of positive integers such that, for all positive integers m and n, we have that a_{m+n} divides $a_m a_n - 1$. Prove that there exists an integer C such that, for all positive integers $k > C$, we have $a_k = 1$.

Proposed by: Kevin Cong

Solution: For convenience, define $g(x) : \mathbb{N} \to \mathbb{N}$ to be $g(n) = a_n$.

We first prove that $1 \in \mathrm{Im}(g)$. Assume otherwise. First, note that $\gcd(g(m+n), g(m)) = 1$ for all positive integers m, n, so thus if g never takes the value 1 then g is injective (and the values it takes are pairwise relatively prime.) Now, let $g(1) = a$ and $g(2) = b$. Note that for every x, there exists integers m, n, p such that

$$\begin{aligned} g(x+1) &= \frac{ag(x) - 1}{m} \\ g(x+1) &= \frac{bg(x-1) - 1}{n} \\ g(x) &= \frac{ag(x-1) - 1}{p}. \end{aligned}$$

Hence,

$$g(x+1) = \frac{bg(x-1) - 1}{n} = \frac{a^2 g(x-1) - a - p}{mp}.$$

Now, suppose $g(x+1) \geq g(x-1)$. Then we must have $n < b$, $mp < a^2$. Hence there are finitely many choices for (n, m, p), and each such choice leads to finitely many possibilities to $g(x-1)$ unless $bmp = na^2$. But $\gcd(b, a^2) = 1$, so this implies that $b \mid n$, and hence $b \leq n$, which is false. Hence this means that if $g(x+1) \geq g(x-1)$ then $g(x-1)$ must take one of a finite set of possible values.

Now, recall that g is injective. Hence this implies that in fact $g(x+1) \geq g(x-1)$ can only occur a finite number of times, and so for all sufficiently large x, $g(x+1) < g(x-1)$. But this is a contradiction to g being injective, and so our hypothesis was false and hence $1 \in \mathrm{Im}(g)$.

Note that this proof works identically if we scale all the inputs by any positive integer, so this implies that every integer has a multiple in $S := g^{-1}(\{1\})$.

We now finish the problem. Consider the smallest value of $\mathrm{Im}(g)$ not equal to 1 (if it doesn't exist then we are done), and say $g(c)$ is equal to this value. Then note that if $a \in S$, then $g(a+c) \leq g(c) - 1$ and so $a + c \in S$. Now, let kc be a multiple of c which is in S; then $dc \in S$ for all $d \geq k$. Now, for each residue class modulo c, select an element j for which $g(j) \neq 1$ (if no such element exists we'll still be done, as we will see.) Then for all $d \geq k$, $g(j + dc) \leq g(j) - 1$. Hence g is bounded in each residue class, and so g is bounded. Now note that g is injective in $\mathbb{Z}^+ \setminus S$, so in fact $\mathbb{Z}^+ \setminus S$ must be finite! So $g(x) = 1$ for all sufficiently large x, as desired.