Orbits

CJ Quines

May 1, 2023

Warmup

(IMO 1987) Prove that there is no function $f\colon \mathbb{N} \to \mathbb{N}$ such that $f(f(n)) = n + 1987$ for all n.

(a) In the equation, substitute $f(n)$ for n. In the equation, apply f to both sides. Show that this means $f(f(n)) \equiv n \pmod{1987}$.

(b) Consider a directed graph with the vertices $0, 1, \ldots, 1986$. Draw an arrow $n \to f(n)$. What does $f(f(n)) \equiv n \pmod{1987}$ mean?

(c) In this graph, every vertex is in a cycle. What are the possible cycle sizes in this graph? Conclude there exists a such that $a \equiv f(a) \pmod{1987}$.

(d) Hence, $f(a) = a + 1987k$ for some $k \in \mathbb{Z}$. Hence $f(f(a)) = f(a + 1987k) = f(a) + 1987k$. Then get a contradiction.

Definitions

Let S be a set. Given $f\colon S \to S$:

- f^0 is the identity function on S.
- $f^n = f \circ f^{n-1}$, for all positive integers n. Thus $f^3(x) = f(f(f(x)))$.
- The **preimage** of y is $f^{-1}(y) = \{x \in S \mid f^1(x) = y\}$. We can similarly define $f^{-2}, f^{-3}, \ldots$
- We can extend f to subsets of S by saying $f(X) = \{f(x) \mid x \in X\}$, and similarly for f^n.
- The **orbit** of x, written $\operatorname{orb}_f(x)$, is $\{x, f(x), f^2(x), \ldots\}$. When f is clear, we write $\operatorname{orb}(x)$.
- The **period** of x is the smallest n such that $f^n(x) = x$. If it exists, we call x **periodic**.
- A **fixed point** of f is an x with period 1.
- The **functional graph** of f is a directed graph with vertices in S, and arrows from x to $f(x)$.

These aren't quite standard, so define them when you use them. Facts with no proof necessary:

- The period of x, if it exists, equals the size of its orbit. We abuse notation and write $\operatorname{orb}(x)$ for both the orbit and period of x.[1]
- If $f^n(x) = x$, we must have $\operatorname{orb}(x) \mid n$. Make sure you know why![2]
- If $y \in \operatorname{orb}(x)$, then $\operatorname{orb}(y) \subseteq \operatorname{orb}(x)$. If they're both periodic, $\operatorname{orb}(x) = \operatorname{orb}(y)$.

---

[1] You can tell it's the orbit if it's a set, and it's the period if it's a number. If x isn't periodic, we won't use $\operatorname{orb}(x)$ as a number.

[2] Compare this fact about orders: Let m be the smallest positive integer such that $a^m \equiv 1 \pmod{p}$. Then if $a^n \equiv 1 \pmod{p}$, we must have $m \mid n$. Why does this follow from the fact about orbits?

- In the functional graph, every vertex has outdegree 1. Conversely, a graph where each vertex has outdegree 1 is a functional graph.

- In the functional graph, if S is finite, each connected component has exactly one directed cycle. The rest of the component is a bunch of trees leading into the cycle. The converse is also true. If S is infinite, then instead of a cycle, it can have a ray or a line, but it still has exactly one of these three.

- In the functional graph, if f is injective, each vertex has indegree at most 1. Then connected components are exactly cycles, rays, or lines.

The connected component fact is important, because the connected components partition S. This is what we used for (c) in the warmup to conclude that there's a cycle of size 1. It's a way to frame the problem that makes it easier to reason globally.

Examples

1. (Floyd 1957) Let S be a finite set, and $f\colon S \to S$. Show that, for every $x \in S$, there exists a positive integer n such that $f^n(x) = f^{2n}(x)$.

   Sketch: Let a be the smallest non-negative integer such that $f^a(x)$ is periodic, and let $\ell = \operatorname{orb}(f^a(x))$. Then $f^{a+i}(x) = f^{a+i+k\ell}(x)$ for every non-negative i and k. Pick large k, $i = k\ell - a$, and $n = k\ell$.

   Remark: A similar argument shows there's N such that $f^N(x) = f^{2N}(x)$ for *all* $x \in S$.

2. (Peru TST 2019) In each cell of a chessboard with 2 rows and 2019 columns a real number is written so that:

   - There are no two numbers written in the first row that are equal to each other.
   - The numbers written in the second row coincide with (in some another order) the numbers written in the first row.
   - The two numbers written in each column are different and they add up to a rational number.

   Determine the maximum quantity of irrational numbers that can be in the chessboard.

   Sketch: Let S be the set of numbers in the first row, and $f\colon S \to S$ take a number to the one below it. A cycle with an irrational number has all irrational numbers and even length. Cycles partition S, so some cycle has odd length, and third condition means no cycles of length 1.

3. (Iran 1992) Let X be a finite set, and $f : X \to X$. Suppose there exists a prime p such that $f^p(x) = x$ for all $x \in X$. Let $Y = \{x \in X \mid f(x) \neq x\}$. Prove that $p \mid |Y|$.

   Sketch: If $f^p(x) = x$, then $\operatorname{orb}(x) \mid p$, and thus is either 1 or p. The functional graph's connected components are all cycles of length 1 or p, but these partition X.

4. (ELMO SL 2018) Let $f\colon \mathbb{R} \to \mathbb{R}$ be bijective. Does there always exist infinitely many $g\colon \mathbb{R} \to \mathbb{R}$ such that $f(g(x)) = g(f(x))$ for all $x \in \mathbb{R}$?

   Sketch: Yes. Consider the functional graph. If we have a line, we can let $g = f^n$ on the chain and let g fix everything else. Otherwise it's infinitely many disjoint cycles. Pick any cycle; we can let $g = f$ on this cycle and let g fix everything else.

Problems

1. (Russia TST 2020) Let $f(x) = x^2 + ax - 1$ for some real a. Sasha found 50 real roots of the equation $f^{47}(x) = x$. Prove that this equation has at least 96 real roots. **Hint:** 23

2. (Macedonia TST 2021) Let $S = \{1, 2, 3, \dots 2021\}$ and $f : S \to S$ be a function such that $f^n(n) = n$ for each $n \in S$. Find all possible values for $f(2021)$. **Hint:** 9

3. (Japan 2022) Find all functions $f \colon \mathbb{N} \to \mathbb{N}$, such that for any positive integers m and n,
$$f^{f(n)}(m) + mn = f(m)f(n).$$
Hints: 3 14

4. (USA 2019) A function $f \colon \mathbb{N} \to \mathbb{N}$ satisfies
$$f^{f(n)}(n) = \frac{n^2}{f(f(n))}$$
for all positive integers n. Find all possible values of $f(1000)$. **Hints:** 3 30

5. (ISL 2017) Let S be a finite set, and let $f \colon S \to S$. Suppose that $f \circ g \circ f \neq g \circ f \circ g$ for every $g \colon S \to S$ with $g \neq f$. Show that $f(f(S)) = f(S)$. **Hints:** 25 11

6. (Taiwan TST 2021) Let $g(x) = (|x| + |x - 1| - 1)/2$. Find all $f \colon \mathbb{N} \to \mathbb{N}$ such that
$$f^{g(f(x)-x)}(x) = x$$
for all positive integers n. **Hint:** 21

7. (ISL 2009) Let $P(x)$ be a non-constant polynomial with integer coefficients. Prove that there is no function $T \colon \mathbb{Z} \to \mathbb{Z}$ such that the number of integers x with $T^n(x) = x$ is equal to $P(n)$ for every positive integer n. **Hints:** 24 16

8. (Korea Winter Camp 2017) Find all functions $f : \mathbb{N} \to \mathbb{N}$ satisfying the following conditions:
   - For every $n \in \mathbb{N}$, $f^n(n) = n$.
   - For every $m, n \in \mathbb{N}$, $|f(mn) - f(m)f(n)| < 2017$. **Hints:** 27 3

Harder problems

9. (APMO 2013) Let a, b be positive integers, and let A, B be finite disjoint sets, such that if $i \in A \cup B$, then $i + a \in A$ or $i - b \in B$. Show that $a|A| = b|B|$. **Hints:** 1 13

10. (ELMO 2021) Let $n > 1$ be an integer and let $a_1, a_2, \dots, a_n$ be integers such that $n \mid a_i - i$ for all integers $1 \leq i \leq n$. Prove there exists an infinite sequence $b_1, b_2, \dots$ such that
    - $b_k \in \{a_1, a_2, \dots, a_n\}$ for all positive integers k, and
    - $\displaystyle\sum_{k=1}^{\infty} \frac{b_k}{n^k}$ is an integer. **Hints:** 10 20

11. (China 2014) Let $f \colon X \to X$, where $X = \{1, 2, \dots, 100\}$, be a function satisfying:
    - $f(x) \neq x$ for all $x \in X$; and

- for any $A \subseteq X$ such that $|A| = 40$, we have $A \cap f(A) \neq \varnothing$.

Find the minimum k such that for any such function f, there exist a subset $B \subseteq X$, where $|B| = k$, such that $B \cup f(B) = X$. **Hints:** 4 15

12. (USA TST 2020) Find all integers $n \geq 2$ for which there exists an integer m and a polynomial $P(x)$ with integer coefficients satisfying the following three conditions:
    - $m > 1$ and $\gcd(m, n) = 1$;
    - the numbers $P(0)$, $P^2(0)$, …, $P^{m-1}(0)$ are not divisible by n; and
    - $P^m(0)$ is divisible by n. **Hints:** 17 8
13. (ISL 2012) Let $f : \mathbb{N} \to \mathbb{N}$. Suppose that for every $n \in \mathbb{N}$ there exists a $k \in \mathbb{N}$ such that $f^{2k}(n) = n + k$, and let k_n be the smallest such k. Prove $k_1, k_2, \dots$ is unbounded. **Hints:** 22 19 6
14. (ISL 2010) The rows and columns of a $2^n \times 2^n$ table are numbered from 0 to $2^n - 1$. The cells of the table have been coloured with the following property being satisfied: for each $0 \leq i, j \leq 2^n - 1$, the j-th cell in the i-th row and the $(i + j)$-th cell in the j-th row have the same colour. (The indices of the cells in a row are considered modulo 2^n.) Prove that the maximal possible number of colours is 2^n. **Hints:** 26 2 28
15. (RMM 2019) Find all pairs of integers (c, d), both greater than 1, such that for any prime $p > c(2c+1)$, and any monic integer polynomial Q with degree d, there exists $S \subseteq \mathbb{Z}$ such that
    - $\dfrac{|S|}{p} \leq \dfrac{2c-1}{2c+1}$, and
    - $\displaystyle\bigcup_{s \in S} \{s, Q(s), Q^2(s)), Q^3(s), \dots\} \equiv \{0, 1, \dots, p-1\} \pmod{p}$. **Hints:** 7 29 5
16. (ISL 2015) Let $f : \mathbb{N} \to \mathbb{N}$. Suppose that:
    - if $m, n \in \mathbb{N}$, then $\dfrac{f^n(m) - m}{n} \in \mathbb{N}$; and
    - the set $\mathbb{N} \setminus \{f(n) \mid n \in \mathbb{N}\}$ is finite.

    Prove that $f(1) - 1, f(2) - 2, f(3) - 3, \dots$ is periodic. **Hints:** 3 12 18

Hints

1. Show that the graph with edges $i \to j$ if $j = i + a \in A$ or $j = i - b \in B$ is a functional graph.
2. What's the size of the orbit of $(1, 1)$? Try small n and guess the pattern.
3. Start by showing injectivity.
4. Take a maximum matching in the underlying undirected graph.
5. Of the vertices not in isolated cycles, at least $\frac{1}{d}$ are in the range of Q. This is a good enough bound.
6. Each connected component corresponds to a fixed value of $f^{2x}(a) - x$, so $\mathrm{orb}_{f^2}(a)$ contains all but finitely many positive integers.
7. Answer is $c \geq d$. If $c < d$, take $Q(x) = x^d$ and some $p \equiv 1 \pmod{d}$ prime.
8. For the function $P \bmod p^e$, prove that if $q \mid \mathrm{orb}(0)$, then $q \leq p$.
9. The answer is everything divisible by 43.
10. Think about how $\sum \frac{b}{n^k} = \frac{b}{n} + \frac{1}{n} \sum \frac{b}{n^k}$. You're looking for periodic b.

11. Show there exists n such that $f^{n+2} = f^{2n+1}$.
12. You want to show each orbit is an arithmetic sequence.
13. Use the fact that an orbit returns to itself to count the number of vertices in A and in B.
14. Show that any two numbers are in the same orbit.
15. If the maximum matching has size $2m$, the $100 - 2m$ vertices outside it have to be an independent set.
16. Evaluate P on primes and products of primes.
17. The answer is all n such that there are primes $q < p$ where $p \mid n$ and $q \nmid n$. If so, we can set $m = q$ and interpolate to find P.
18. If the first differences of an orbit are bounded, show it has to be an arithmetic sequence. If it's unbounded, show it has density 0.
19. If the ks are upper bounded, show there's a finite number of connected components.
20. Take indices mod n, and set $f(i) = (a_{-i} + i)/n$.
21. The difference between consecutive terms in the orbit is 0 or 1 $\pmod{\operatorname{orb}(x)}$, but at the end of the orbit we go back to x.
22. Consider the functional graph of f^2. Show it has no cycles.
23. How many things have orbit 47?
24. If c_d is the number of cycles of length d, then $P(n) = \sum_{d|n} d \cdot c_d$.
25. Pick some g that forces $f \circ g \circ f = g \circ f \circ g$.
26. Think about $f(j, i) = (i + j, j) \bmod 2^n$.
27. The second condition is only for multiplicativity; you can replace it with $f(mn) = f(m)f(n)$.
28. The key claims are $\nu_2(F_{6m}) = \nu_2(m) + 3$ and $\nu_2(F_{6m-1} - 1) = \nu_2(F_{6m+1} - 1) = \nu_2(m) + 2$.
29. Q can have at most d fixed points. Vertices of the functional graph have maximum indegree d.
30. Let $m = \min \operatorname{orb}(n)$, what does the equation give?

Sketches

1. If $f^{47}(x) = x$ then $\operatorname{orb}(x)$ is 1 or 47. There's two points with orbit 1, so there's at least 48 points with orbit 47. In particular, the 48 points have to come from at least two different orbits of size 47, meaning there's actually at least 94 points with orbit 47.

2. We have $\operatorname{orb}(2021) \mid 43 \cdot 47$, casework on $\operatorname{orb}(2021)$. If 1, it's 2021. If 2021, it's impossible as $f(1) = 1$. If 47, it's also impossible: if $n \in \operatorname{orb}(2021)$, then $47 \mid n$, but there's only 43 such n, which is less than 47. Similarly if 43, everything in orbit is divisible by 43. We can set $f(2021)$ to any of these.

3. Answer is $f(n) = n + 1$, check it works. Show injectivity by $P(a, n)$ and $P(b, n)$. By $P(n, n)$ we get $f(n) > n$. Functional graph is disjoint rays. By $P(a, b)$ and $P(b, a)$, we get a and b are in the same orbit, thus the ray has all of $\mathbb{N}$.

4. Answer is all evens, give construction. Show injectivity by $P(a)$ and $P(b)$. Let $m = \min \operatorname{orb}(n)$. Then $P(m)$ means $f^{f(m)}(m) f^2(m) = m^2$. Factors in LHS are both in $\operatorname{orb}(n)$, so by minimality they're both m. Thus $f^2(m) = m$, and $\operatorname{orb}(n)$ has size 2, and thus $f^2(n) = n$ for all n. Equation is now $f^{f(n)}(n) = n$. Argue by parity that $f(1000)$ can't be odd.

5. By a similar argument to Floyd, there's some n such that $f^{n+2} = f^{2n+1}$. (If it's eventually periodic, it has period N. Pick large n such that $n \equiv -1 \pmod{N}$.) Set $g = f^n$. Then $f \circ g \circ f = g \circ f \circ g$ so $g = f = f^n$, and thus f is a bijection on $f(S)$.

6. Answer is $f(x) = x$ or $x+1$ pointwise; i.e. we can pick x or $x+1$ for different xs. Suppose $g(f(x)-x) > 0$, then $\operatorname{orb}(x)$ exists, and $\operatorname{orb}(x) \mid g(f(x)-x)$, hence $f(x) - x \equiv 0$ or $1 \pmod{\operatorname{orb}(x)}$. In particular, the difference between consecutive terms in the orbit is 0 or 1 $\pmod{\operatorname{orb}(x)}$, but at the end of the orbit we go back to x, so they're all 0. If $g(f(x)-x) = 0$, then $f(x) = x$ or $x+1$ anyway.

7. Take the functional graph. We can ignore everything not in a cycle. Let c_d be the number of cycles of length d, then $P(n) = \sum_{d \mid n} d \cdot c_d$. For prime p we get $P(p) \equiv c_1 \pmod p$, hence $P(0) \equiv c_1 \pmod p$ for all primes p, and thus $P(0) = c_1$. Also, $P(pq) \equiv c_1 + qc_q \pmod p$. Hence $qc_q \equiv 0 \pmod p$ for any other prime q, hence $c_q = 0$. Hence $P(q) = c_1$ for all primes q, and P is constant, contradiction.

8. Answer is $f(n) = n$, check it works. The hard part is showing second condition gives multiplicativity, which we prove later; for now assume $f(mn) = f(m)f(n)$. Show injectivity by $P(a)$ and $P(b)$. For prime p, we get $\operatorname{orb}(p) \mid p$. If $\operatorname{orb}(p) = p$, then everything in its orbit must also be divisible by p, so $f^{p-1}(p) = kp$ for some p. Then $p = f^p(p) = f(f^{p-1}(p)) = f(kp) = kf(p)$ by multiplicativity. But $f(p)$ is also in the orbit, and also divisible by p, hence $k = 1$ and $f(p) = p$.

   Now we show multiplicativity. If $f(mn) \neq f(m)f(n)$, then

$$\begin{aligned}
f(k) &\le |f(mn) - f(m)f(n)|\, f(k) \\
&= |f(mn)f(k) - f(m)f(n)f(k)| \\
&\le |f(mn)f(k) - f(mnk)| + |f(mnk) - f(m)f(nk)| + |f(m)f(nk) - f(m)f(n)f(k)| \\
&= |f(mn)f(k) - f(mnk)| + |f(mnk) - f(m)f(nk)| + f(m)\,|f(nk) - f(n)f(k)| \\
&< 2017 + 2017 + f(m) \cdot 2017.
\end{aligned}$$

   where the third line follows from the triangle inequality. This means f is bounded above, but f is surjective by first condition, so this is absurd.

9. Consider graph with vertices $A \cup B$ and $i \to j$ if $j = i + a \in A$ or $j = i - b \in B$. We're given each vertex has outdegree at least 1. But a vertex can have indegree at most 1, so outdegrees are exactly 1. This is a functional graph, and consists of disjoint cycles. If the orbit of i has x edges that add a and y edges that subtract b, then its orbit has x elements in A and y in B. But $i = i + ax - by$ so $x/y = b/a$; summing over orbits gives the answer.

10. Take indices mod n and let $f\colon \mathbb{Z} \to \mathbb{Z}$ be $f(i) = (a_{-i} + i)/n$. Then f is upper bounded, so we must have a cycle starting at some x. Then if $k = \operatorname{orb}(x) - 1$, we get

$$x = \frac{a_{-f^k(x)} + f^k(x)}{n} = \frac{a_{-f^k(x)}}{n} + \frac{a_{-f^{k-1}(x)} + f^{k-1}(x)}{n^2} = \cdots = \left(\sum_{i=0}^{k-1} \frac{a_{-f^{k-i}(x)}}{n^{i+1}} \right) + \frac{x}{n^k},$$

    which is an integer, and we can keep going and pick b_is appropriately.

11. Restate with functional graphs. First condition is no self-loops. Second condition is no independent sets of size 40. We are asking for minimum vertex cover. The duality between independent set and vertex covers kinda works. Take a maximum matching in the undirected graph, say size $2m$. The $100 - 2m$ vertices outside are an independent set, so $100 - 2m < 40$ and $m \ge 31$. Take the tails of the edges in the matching, and all vertices outside the matching, total of $m + 100 - 2m \le 69$ vertices. Construction is 30 triangles, an involution, and point the remaining 8 vertices to a vertex in the involution.

12. The answer is all n such that there are primes $q < p$ where $p \mid n$ and $q \nmid n$. Suppose n satisfies this. Set $m = q$ and interpolate to find $P(0), P^2(0), \ldots, P^{q-1}(0), P^q(0) \equiv 1, 2, \ldots, q-1, 0 \pmod{p^{\nu_p(n)}}$ and $P(0) \equiv 0$ for all other primes dividing n. This is the construction.

    Let p be a prime, and write $o(e) = \operatorname{orb}_{P \bmod p^e}(0)$. We claim that if q is a prime such that $q \mid o(e)$, then $q \le p$. If we can show this we're done, as then m can't satisfy $\gcd(m, n) = 1$. Prove through induction on e. For $e = 1$ the orbit can only take on p values anyway. For inductive case, as $P^{o(e)}(0) \equiv 0 \pmod{p^e}$, we also have $P^{o(e)}(0) \equiv 0 \pmod{p^{e-1}}$, and hence $o(e-1) \mid o(e)$. But one of $o(e-1), 2o(e-1), \ldots, (p-1)o(e-1)$ is 0 by pigeonhole, so $o(e)$ must equal one of them. Either q divides the first factor which is less than p, or divides the second factor, which works by inductive hypothesis.

13. First, f has no cycles. If it did, we can set $x = \max \operatorname{orb}_f(n)$, then by condition $f^{2k_x}(x) = x + k_x$ is also in $\operatorname{orb}_f(n)$, contradicting maximality. Pick some a. Define $g\colon \operatorname{orb}_{f^2}(a) \to \operatorname{orb}_{f^2}(a)$ as

$$g(f^{2i}(a)) = f^{2i+2k_{f^{2i}(a)}}(a) = f^{2k_{f^{2i}(a)}}(f^{2i}(a)) = f^{2i}(a) + k_{f^{2i}(a)},$$

    the third equality from the problem statement. Note that g is injective by minimality of $k_{f^{2i}(a)}$. Further, g has no cycles because f has no cycles. Thus g's functional graph is disjoint rays. Suppose the ks are upper bounded by M. Then $g(x) = x + k_{\text{whatever}} \le x + M$, so each ray has density $\ge \frac{1}{M}$, and there's at most M rays.

    Let $\operatorname{orb}_g(f^{2i}(a))$ be one of the rays. If $f^{2x}(a) \in \operatorname{orb}_g(f^{2i}(a))$, expanding the definition shows

$$f^{2x}(a) = f^{2i}(a) + x - i \le x + \max\{f^{2i}(a) - i\} = x + m,$$

    for some constant m, taken over the maximum of all the rays in g. (This is why we need a finite number of rays.) Thus the xth term in $\operatorname{orb}_{f^2}(a)$ is at most $x + m$, and $\operatorname{orb}_{f^2}(a)$ contains all but finitely many positive integers. Finally, $\operatorname{orb}_f(1)$ is the disjoint union of $\operatorname{orb}_{f^2}(1)$ and $\operatorname{orb}_{f^2}(f(1))$. But these can't be disjoint for size reasons.

14. Equivalent to showing that, if $f\colon \mathbb{Z}_{2^n}^2 \to \mathbb{Z}_{2^n}^2$ is $f(j, i) = (i + j, j) \bmod 2^n$, its functional graph has 2^n connected components. We proceed by induction. When both coordinates are even we reduce to the 2^{n-1} case, so there's 2^{n-1} components for those. We claim if at least one coordinate is odd, the orbits all have size $3 \cdot 2^{n-1}$; this would finish the problem. Note $f^k(a, b) = (aF_k + bF_{k-1}, aF_{k-1} + bF_k)$, so we need to calculate when $(a, b) \equiv f^k(a, b) \pmod{2^n}$, and this is now a number theory problem. The key claims are $\nu_2(F_{6m}) = \nu_2(m) + 3$ and $\nu_2(F_{6m-1} - 1) = \nu_2(F_{6m+1} - 1) = \nu_2(m) + 2$, and I won't bother proving these here lol.

15. Answer is $c \ge d$. If $c < d$, take $Q(x) = x^d$, let $p \equiv 1 \pmod{d}$ be prime. Then Q's range has only $1 + \frac{p-1}{d}$ elements, so S must include $\frac{d-1}{d}(p-1)$ elements, which fails the size condition.

    For $c \ge d$, take the functional graph of Q. Let c_k be the number of k-cycles without trees pointing into them. Build S by taking one vertex from each of these cycles, plus every vertex of indegree 0. Of the $p - \sum k \cdot c_k$ vertices not in the cycles, at least $\frac{1}{d}$ of them are in the range of Q. (Q has degree d, so vertices have maximum indegree d.) Thus we can bound the size of S by

$$\sum c_k + \left(1 - \frac{1}{d}\right)\left(p - \sum k \cdot c_k\right) = \frac{d-1}{d} \cdot p + \frac{1}{d} \cdot c_1 - \sum \frac{(k-1)d - k}{d} \cdot c_k \le \frac{d-1}{d} \cdot p + 1,$$

    the last inequality by $c_1 \le d$. As $p > c(2c+1)$, this bound works.

16. Show injectivity by $P(x, n)$ and $P(y, n)$ for large x, y. Functional graph is a finite number of disjoint rays by second condition. We claim each orbit is either an arithmetic sequence or has density 0. Set $g(a) = f^a(x) - x$. Then $g(0) = 0$, and from $P(f^b(x), a - b)$, we get $a - b \mid g(a) - g(b)$.

    Suppose $d_n = g(n+1) - g(n)$ was upper bounded by N. From $a - b \mid d_a - d_b$, setting $a - b > N$ for enough differences we can force d_n to be constant, and then g is an arithmetic sequence, and we're done. Now suppose it was unbounded. Again from $a - b \mid d_a - d_b$, setting $a - b > d_b$ shows it eventually only contains numbers at least d_b, and so the density is at most $\frac{1}{d_b}$, and this is true for any d_b, so it's density 0.

    The orbits have to cover $\mathbb{N}$, and they're all infinite, so they can't have density 0. Thus each orbit is an arithmetic sequence and we're done.