J1. Suppose an infinite non-constant arithmetic progression of integers contains 1 in it. Prove that there are an infinite number of perfect cubes in this progression.

(A perfect cube is an integer of the form k^3, where k is an integer. For example, -8, 0, and 1 are perfect cubes.)

Solution

Let a and d be the first term and the common difference in the arithmetic progression, respectively. Clearly, both a and d are integers. Moreover, since the arithmetic progression is non-constant, $d \neq 0$ (but it could be positive or negative!). Note that for any integer k,

$$\begin{aligned}(1+kd)^3 &= 1+3(kd)+3(kd)^2+(kd)^3 \\ &= 1+d(3k+3k^2d+k^3d^2).\end{aligned}$$

Clearly, if d is positive, then there are infinitely many *positive* integers ℓ such that

$$\ell = 3k+3k^2d+k^3d^2$$

for some integer k. For those values of ℓ, $1+d\ell$ is in the arithmetic progression and it a perfect cube, and the proof is finished.

Suppose now that d is negative. Since

$$3k+3k^2d+k^3d^2 = 3k+(k^2d)(3+kd)$$

and both k^2d and $3+kd$ are negative and decreasing with k for $k \geq 4$, we again get that there are infinitely many *positive* integers ℓ satisfying the same equality. The proof is finished.

J2. Let $ABCD$ be a trapezoid with parallel sides AB and CD, where $BC \neq DA$. A circle passing through C and D intersects AC, AD, BC, and BD again at W, X, Y, and Z respectively. Prove that WZ, XY, and AB are concurrent. **Solution**

$\angle AXY = 180^\circ - \angle DXY = \angle YCD = 180^\circ - \angle ABC$, so $ABYX$ and similarly $ABZW$ are both cyclic. Also, by assumption, $XYZW$ are cyclic.

Note that AB is a radical axis of circles $(ABYX)$, $(ABZW)$. Similarly, points XY is a radical axis of $(ABYX)$ and $(XYZW)$. Finally, WZ is a radical axis of $(ABZW)$ and $(XYZW)$. The result follows from the fact that three circles, when taken in pairs, have concurrent radical axis.

J3. The n players of a hockey team gather to select their team captain. Initially, they stand in a circle, and each person votes for the person on their left.

The players will update their votes via a series of rounds. In one round, each player a updates their vote, one at a time, according to the following procedure: At the time of the update, if a is voting for b, and b is voting for c, then a updates their vote to c. (Note that a, b, and c need not be distinct; if $b = c$, then a's vote does not change for this update.) Every player updates their vote exactly once in each round, in an order determined by the players (possibly different across different rounds).

They repeat this updating procedure for n rounds. Prove that at this time, all n players will unanimously vote for the same person.

Comment. *Unfortunately, the level of difficulty of this problem was the result of an unintentional clerical error. The version of this problem which had been initially slated for the contest was much easier. It had stated, "They repeat the same updating procedure on the second day, the third day, and so on. Prove that eventually, all players will unanimously vote for the same person." In other words, there had been no bound of n rounds.*

Solution 1

Initially, all players are in a cycle. Note that once a player leaves the cycle, they cannot rejoin. Furthermore, a new cycle cannot be created. Hence, at any point in time, the graph corresponding to the votes will be a functional graph with a single cycle.

We will first prove that after $\lfloor \log_2 n \rfloor$ rounds, the cycle will become a self-loop. Then, we will show that in the next $\lfloor \log_2 n \rfloor$ rounds, all other players vote for the player in the self-loop.

To show the first step, assume the cycle has size $K > 1$ at the beginning of a round. Consider arbitrary player a in the cycle who is updating their vote. Say $a \to b \to c$, all in the cycle. Then $a \to c$ now, bumping b out of the cycle and reducing its size to $K - 1$. Note that b can now update their vote as well without affecting the size of the cycle. If we consider all K original players in the cycle, we see that at least $\lceil \frac{K}{2} \rceil$ of them must still be in the cycle at the time of their update, and hence the cycle's size is reduced to at most $\lfloor \frac{K}{2} \rfloor$. After $\lfloor \log_2 n \rfloor$ rounds, the cycle must be reduced to size 1.

Now that the cycle has been reduced to a single player, say z, consider any path from a player a to z. No players can be added to this path now. With a similar argument as the cycle, the length of the path must halve each round. In particular, a path of length L to the cycle gets reduced to length $\lceil \frac{L}{2} \rceil$ (note the ceiling, we had the floor for the cycle). After $\lceil \log_2 n \rceil$ rounds, the path must be reduced to length 1.

Thus, after $\lfloor \log_2 n \rfloor + \lceil \log_2 n \rceil$ rounds, the graph has been completely reduced. For $n \geq 5$, $\lfloor \log_2 n \rfloor + \lceil \log_2 n \rceil \leq 2\lfloor \log_2 n \rfloor + 1 \leq n$. For the other n, we can manually check that $\lfloor \log_2 n \rfloor + \lceil \log_2 n \rceil \le n$.

Comment 1. In this proof, it is important that we consider the cycle size and path sizes in disjoint rounds. In the rounds where the cycle size is decreasing, it's possible for the path sizes to increase by Cn for some constant C.

Comment 2. This proof can actually be refined to prove that $\log_2 n + O(\log_2 \log_2 n)$ rounds are sufficient (and constructions show that this is necessary). Consider a fixed player a and the path from a to the cycle as it changes across the rounds. In round i, let ℓ_i be the number of players which were part of the cycle at the beginning of round i, and became part of this path during round i. (Note that it's possible that a player was part of the path for only a portion of round i, and is no longer part of the path at the end. It should still be counted.) We can see that ℓ_i is bounded by size of the cycle at the start of round i, which we know is $\le \frac{n}{2^{i-1}}$.

Now note that the size of this path after round k is at most

$$1 + \frac{\ell_1}{2^{k-1}} + \frac{\ell_2}{2^{k-2}} + \ldots + \frac{\ell_{k-1}}{2} + \ell_k \le 1 + \frac{kn}{2^{k-1}}.$$

Hence, when $k = \log_2 n + C \log_2 \log_2 n$ for C sufficiently large, we must have that every player is voting for the self-loop.

Solution 2

We will use induction on n.

Inductive Hypothesis. Let G be any functional graph with n nodes and a single cycle. Then after n rounds of the given operation, G will become a self-loop with $n-1$ nodes pointing to it.

Base Case. The cases $n \le 2$ are clear.

Inductive Step. Assume that the hypothesis is proved for $n = k-1$ and $n = k-2$. We will prove it for $n = k$. Consider any initial functional graph with k nodes and a single cycle. Note there is some node a which has in-degree 0 (i.e. no nodes point to it), or all k nodes are in the cycle.

In the first case, consider $G \setminus \{a\}$. Note that all operations except a's own updates are independent of where a is. By the inductive hypothesis, after $k-1$ rounds, $G \setminus \{a\}$ has become a single self-loop and $k-2$ nodes pointing to it. Regardless of where a is, it will point to the self-loop after one more round and we are done.

In the case where all k nodes are in a cycle, consider the very first operation $z \to a \to b \implies z \to b, a \to b$. This creates a zero in-degree node a, but z's operation has been used for the first round so the inductive hypothesis cannot be naively applied. Instead, consider $b \to c$ (possibly $c = z$ if $k = 3$). At some point in the first round, b will be updated. Either c will become another zero in-degree node, or a will be the only node that points to c. Either way, consider $G \setminus \{a, c\}$. By the induction hypothesis, after rounds 2 through $k-1$, this graph will become a self-loop with $k-3$ nodes pointing to it. It's also easy to see that a and c both have in-degree 0 after round 2. Then in one more round after round $k-1$, we must have a and c pointing to the self-loop. So we are done for $n = k$.

By induction, we are done for all n.

Comment. If the problem were instead to prove the result after $2n$ rounds, the induction would be much easier.

J4. Determine all positive integers a, b, c, p where p and $p+2$ are odd primes and

$$2^a p^b = (p+2)^c - 1.$$

Solution

The only solution is $(a, b, c, p) = (3, 1, 2, 3)$. First, factor the right hand side. This gives us

$$2^a p^b = (p+1)((p+2)^{c-1} + (p+2)^{c-2} + \cdots + (p+2) + 1).$$

Since $\gcd(p, p+1) = 1$ it must be the case that $p+1 = 2^x$ for some positive integer $x \le a$ and so $p = 2^x - 1$ and $p+2 = 2^x + 1$. Now for $x \ge 3$, $2^x + 1$ is not prime if x is odd (since it is 0 mod 3) and $2^x - 1$ is not prime if x is even (since it is 0 mod 3). This means $x \le 2$, and the only admissible such x is $x = 2$ since otherwise p is not prime. So, the original equation becomes

$$2^a 3^b = 5^c - 1.$$

Now $3 | (5^c - 1)$, so evaluating $5^c - 1$ mod 3 gives that $c = 2d$ for some positive integer d and hence

$$2^a 3^b = (5^d - 1)(5^d + 1).$$

Observe $5^d - 1$ and $5^d + 1$ are both even and have greatest common divisor 2 because they are 2 apart. Since $4 | (5^d - 1)$ this implies $5^d - 1 = 2^{a-1}$ and $5^d + 1 = 2 \cdot 3^b$. Now, 3 is not a factor of $5^d - 1$ because $5^d - 1 = 2^{a-1}$. Thus, by evaluating mod 3, d must be odd. If $d > 1$, this is impossible as $5^d - 1 = (5-1)(5^{d-1} + 5^{d-2} + \cdots + 5 + 1)$ and the latter factor has an odd prime factor, contradicting $5^d - 1$ is a power of 2. Thus $d = 1$ and so $c = 2$, implying that $2^a 3^b = 24$ so $a = 3$ and $b = 1$. Hence, the only solution is $(a, b, c, p) = (3, 1, 2, 3)$.

J5. A polynomial $c_dx^d + c_{d-1}x^{d-1} + \cdots + c_1x + c_0$ with degree d is *reflexive* if there is an integer $n \geq d$ such that $c_i = c_{n-i}$ for every $0 \leq i \leq n$, where $c_i = 0$ for $i > d$. Let $\ell \geq 2$ be an integer and $p(x)$ be a polynomial with integer coefficients. Prove that there exist reflexive polynomials $q(x), r(x)$ with integer coefficients such that

$$(1 + x + x^2 + \cdots + x^{\ell-1})p(x) = q(x) + x^\ell r(x).$$

Solution 1

Let d be the degree of p and let k be any non-negative integer. We will choose

$$\begin{aligned} q(x) &= \frac{x^{d+k+\ell}p\left(\frac{1}{x}\right) - p(x)}{x-1}, \\ r(x) &= \frac{p(x) - x^{d+k}p\left(\frac{1}{x}\right)}{x-1}. \end{aligned}$$

First, we must show that both q and r are integer polynomials. Consider the numerator in q's definition, $x^{d+k+\ell}p\left(\frac{1}{x}\right) - p(x)$. This is clearly an integer polynomial. As it is equal to 0 when evaluated at $x-1$, $x-1$ divides it. Furthermore, as $x-1$ is monic, the quotient has integer coefficients. The argument for r is similar.

Next, we will show that this choice of q and r satisfies the desired equation. Plugging them into the RHS of the equation gives

$$\begin{aligned} q(x) + x^\ell r(x) &= \frac{x^{d+k+\ell}p\left(\frac{1}{x}\right) - p(x)}{x-1} + x^\ell\left(\frac{p(x) - x^{d+k}p\left(\frac{1}{x}\right)}{x-1}\right) \\ &= \frac{x^{d+k+\ell}p\left(\frac{1}{x}\right) - p(x) + x^\ell p(x) - x^{d+k+\ell}p\left(\frac{1}{x}\right)}{x-1} \\ &= \left(\frac{x^\ell - 1}{x-1}\right)p(x) \\ &= (1 + x + \cdots + x^{\ell-1})p(x) \end{aligned}$$

as desired.

Finally, we will show that q and r are indeed reflexive. We can re-interpret the reflexive condition as such:

Polynomial $a(x)$ is reflexive iff there is an integer $n \geq \deg(a)$ for which

$$a(x) = x^n a\left(\frac{1}{x}\right).$$

We have

$$\begin{aligned} q(x) &= \frac{x^{d+k+\ell}p\left(\frac{1}{x}\right) - p(x)}{x-1} \\ &= x^{d+k+\ell-1} \cdot \frac{p\left(\frac{1}{x}\right) - x^{-(d+k+\ell)}p(x)}{\frac{x-1}{x}} \\ &= x^{d+k+\ell-1} \cdot \frac{x^{-(d+k+\ell)}p(x) - p\left(\frac{1}{x}\right)}{\frac{1}{x} - 1} \\ &= x^{d+k+\ell-1}q\left(\frac{1}{x}\right) \end{aligned}$$

as desired. Similarly,

$$\begin{aligned} r(x) &= \frac{p(x) - x^{d+k}p\left(\frac{1}{x}\right)}{x-1} \\ &= x^{d+k-1} \cdot \frac{x^{-(d+k)}p(x) - p\left(\frac{1}{x}\right)}{\frac{x-1}{x}} \\ &= x^{d+k-1} \cdot \frac{p\left(\frac{1}{x}\right) - x^{-(d+k)}p(x)}{\frac{1}{x} - 1} \\ &= x^{d+k-1}r\left(\frac{1}{x}\right). \end{aligned}$$

Solution 2

We write degree n polynomial p as

$$p(x) := \sum_{i=0}^{n} p_i x^i.$$

Define vector $P \in \mathbb{Z}^{n+1}$ as

$$P := \begin{pmatrix} p_0 & p_1 & \cdots & p_n \end{pmatrix}^T.$$

We also denote $X \in \mathbb{Z}[x]^N$ for N some sufficiently high degree (e.g. $N > 2n + \ell$) as the vector of powers of x, i.e.

$$X := \begin{pmatrix} 1 & x & x^2 \cdots & x^{N-1} \end{pmatrix}^T.$$

For a matrix $M \in \mathbb{Z}^{(n+1)\times N}$, $P^T M X$ is an integer polynomial of degree $< N$. Note that if the non-zero entries of matrix M are horizontally symmetric, then the resulting polynomial must be reflexive.

Let A be the matrix corresponding to $(1 + x + \cdots + x^{\ell-1})p(x)$. The non-zero entries of the matrix form a parallelogram. In particular, A is a sparse matrix with 1s across the upper ℓ diagonals. For example, for $\ell = 3, n = 4$,

$$A = \begin{pmatrix} 1 & 1 & 1 & & & & & \cdots \\ & 1 & 1 & 1 & & & & \cdots \\ & & 1 & 1 & 1 & & & \cdots \\ & & & 1 & 1 & 1 & & \cdots \\ & & & & 1 & 1 & 1 & \cdots \end{pmatrix}.$$

We will now construct matrices $Q, R \in \mathbb{Z}^{(n+1)\times N}$ such that Q and R will correspond to $q(x)$ and $x^\ell r(x)$, respectively. Thus, we require

$$\begin{aligned} & (1 + x + x^2 + \cdots + x^{\ell-1})p(x) = q(x) + x^\ell r(x) \\ \iff \quad & P^T AX = P^T QX + P^T RX \\ \iff \quad & P^T (A - Q - R)X = 0. \end{aligned}$$

So it suffices to find Q and R horizontally symmetric and such that $Q + R = A$. Note that the first ℓ columns of R must also be zero.

As it turns out, many constructions exist. For example, consider Q with 1 entries forming a isosceles triangle with base from 0 to $2n$:

$$Q = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & \cdots \\ & 1 & 1 & 1 & 1 & 1 & 1 & 1 & & \cdots \\ & & 1 & 1 & 1 & 1 & 1 & & & \cdots \\ & & & 1 & 1 & 1 & & & & \cdots \\ & & & & 1 & & & & & \cdots \end{pmatrix}.$$

Then the difference, $R = A - Q$ is

$$R = \begin{pmatrix} & -1 & -1 & -1 & -1 & -1 & -1 & \cdots \\ & & -1 & -1 & -1 & -1 & & \cdots \\ & & & -1 & -1 & & & \cdots \\ & & & & & & & \cdots \\ & & & 1 & 1 & & & \cdots \end{pmatrix}.$$

Extending this triangle structure to an isosceles trapezoid (even a self-intersecting one) works as well. More rigorously, define Q to be the matrix whose entries are 1 at the isosceles trapezoid from (zero-indexed) entries at

$$(0, 0), (0, n + k), (n, k), (n, n)$$

in that order, for any non-negative integer k with $k \geq \ell$. (If we choose $k < n$, the entries may be -1 to account for the self-intersection.) Define R to be the matrix whose entries are -1 at the isosceles trapezoid from entries at

$$(0, \ell), (0, n + k), (n, k), (n, n + \ell).$$

Then their total is the matrix whose entries are 1 at the parallelogram formed by

$$(0,0),(0,\ell-1),(n,n+\ell-1),(n,n),$$

which is precisely A.