Algebra

A1 (IMO 1) Let $a_0 < a_1 < a_2 \dots$ be an infinite sequence of positive integers. Prove that there exists a unique integer $n \geq 1$ such that

$$a_n < \frac{a_0 + a_1 + a_2 + \cdots + a_n}{n} \leq a_{n+1}.$$

Solution. The condition that $a_n < \dfrac{a_0 + a_1 + a_2 + \cdots + a_n}{n}$ means that $a_0 + a_1 + \cdots + a_{n-1} - (n-1)a_n > 0$ and similarly $\dfrac{a_0 + a_1 + a_2 + \cdots + a_n}{n} \leq a_{n+1}$ means $a_0 + \cdots + a_n - na_{n+1} \leq 0$. Let $f(n) = a_0 + \cdots + a_{n-1} - (n-1)a_n$. We are to prove that there exists a unique n such that $f(n) > 0$ but $f(n+1) \leq 0$.

We first claim that $f(n)$ is a decreasing function. To see this, we have

$$f(n) - f(n+1) = (a_0 + a_1 + \cdots + a_{n-1} - (n-1)a_n) - (a_0 + \cdots + a_n - na_{n+1}) = n(a_{n+1} - a_n)$$

and since $\{a_n\}$ is a strictly increasing sequence, we have $n(a_{n+1} - a_n) > 0$, and therefore $f(n) - f(n+1) > 0$ for all n.

The next observation is that $f(1) = a_0 - (1-1)a_1 = a_0 > 0$. Since $f(n)$ decreases by at least 1 as n increases(because $\{a_n\}$) are sequence of integers), we see that there exists an n_0 with $f(n_0) \leq 0$ (in particular we can choose $f(a_0 + 1)$). Since $f(n) \leq 0$ for all $n \geq n_0$, the set $\{n : f(n) > 0\}$ is finite but nonzero since $f(1) > 0$. Let n_1 be the largest element in this set, and we see that $f(n_1) > 0$ but $f(n_1 + 1) \leq 0$, $f(n) > 0$ for $n \leq n_1$ and $f(n) \leq 0$ for all $n > n_1$. Thus this n_1 is the only n fitting the criteria.

A2 Define the function $f : (0,1) \to (0,1)$ by

$$f(x) = \begin{cases} x + \frac{1}{2} & \text{if } x < \frac{1}{2} \\ x^2 & \text{if } x \geq \frac{1}{2} \end{cases}$$

Let a and b be two real numbers such that $0 < a < b < 1$. We define the sequences a_n and b_n by $a_0 = a, b_0 = b$, and $a_n = f(a_{n-1})$, $b_n = f(b_{n-1})$ for $n > 0$. Show that there exists a positive integer n such that

$$(a_n - a_{n-1})(b_n - b_{n-1}) < 0.$$

Solution. We notice that $f(x) > x$ if $x < \frac{1}{2}$, and if $x \geq 12$ then since $x < 1$ as well, we have $f(x) < x$. Hence, it suffices to find n such that either $a_n < \frac{1}{2} \leq b_n$, or $b_n < \frac{1}{2} \leq a_n$.

Suppose otherwise, then for each n, we either have $a_n, b_n < 12$, or $a_n, b_n \geq \frac{1}{2}$. Within each range $(0, \frac{1}{2})$ and $[\frac{1}{2}, 1)$, we also have f monotonous: $f(x) < f(y)$ iff $x < y$. Hence from $a < b$ we also have $a_n < b_n$ for all n. We now consider the difference $b_n - a_n$ in terms of $b_{n-1} - a_{n-1}$:

- If $a_{n-1}, b_{n-1} < \frac{1}{2}$ then $b_n - a_n = b_{n-1} - a_{n-1}$.
- Otherwise we have $b_n - a_n = (b_{n-1} - a_{n-1})(b_{n-1} + a_{n-1})$, and by $\frac{1}{2} \leq a_{n-1} < b_{n-1}$ we also have $b_{n-1} - a_{n-1} > 1$ so $b_n - a_n > b_{n-1} - a_{n-1}$.

Regardless, we always have $b_n - a_n \geq b_{n-1} - a_{n-1}$.

Now let $c = b - a = b_0 - a_0$. We have $b_n - a_n \geq c$ as always. If $n_1 < n_2, \cdots < n_k < n$ are indices such that $a_{n_i} \geq \frac{1}{2}$ then $b_{n_i+1} - a_{n_i+1} = (b_{n_i} - a_{n_i})(b_{n_i} + a_{n_i}) \geq (1+c)(b_{n_i} - a_{n_i})$. Thus we now have $a_n - b_n \geq (1+c)^k c$. Since $0 < a_n < b_n < 1$, $(1+c)^k c < 1$, i.e. $k < -\log_{1+c}(c)$. This also means that regardless of n, the number of $m < n$ with $a_m, b_m, \geq \frac{1}{2}$ is bounded by $-\log_{1+c}(c)$ which does not depend on n. Hence such m's are also finite. This means that there exists an N such that for all $n \geq N$ we have $a_n < \frac{1}{2}$. This is impossible, since $a_n < \frac{1}{2}$ means that $a_{n+1} = a_n + \frac{1}{2} > \frac{1}{2}$. The desired contradiction proves our statement.

A4 Determine all functions $f : \mathbb{Z} \to \mathbb{Z}$ satisfying

$$f\big(f(m) + n\big) + f(m) = f(n) + f(3m) + 2014$$

for all integers m and n.

Answer. The only such function is $f(n) = 2n + 1007$.
Solution. We first consider $m = 0$, and let $f(0) = c$. So plugging $m = 0$ yield $f(n + c) + c = f(n) + c + 2014$, i.e. $f(n + c) - f(n) = 2014$. By considering $n, n + c, n + 2c, \cdots$ we can generalize this statement to $f(n + kc) - f(n) = 2014k$ for all $k \geq 0$. Next, consider $m_1 = m + c$, and therefore $f(m_1) = f(m) + 2014$ and $f(3m_1) = f(3m + 3c) = f(3m) + 3(2014)$. Therefore we have the following:

$$f(f(m_1) + n) + f(m_1) = f(f(m) + n + 2014) + f(m) + 2014$$

and

$$f(n) + f(3m_1) + 2014 = f(n) + f(3m) + 3(2014) + 2014 = f(n) + f(3m) + 4(2014)$$

and therefore $f(f(m) + n + 2014) + f(m) = f(n) + f(3m) + 3(2014)$. Comparing this with the original statement and subtracting both sides, we have $f(f(m) + n + 2014) - f(f(m) + n) = 2(2014)$. Since $f(m) + n$ attains all values in $\mathbb{Z}$ (by varying n), we have $f(n + 2014) - f(n) = 2(2014)$ for all n, or more generally (by following the logic above), $f(n + 2014k) - f(n) = 2k(2014)$.

We now have $f(n + kc) - f(n) = 2014k$ for all $k \geq 0$ and $f(n + 2014\ell) - f(n) = 2\ell(2014)$ for all $\ell \geq 0$. Let $k = 2014$ and $\ell = c$ we have $2014^2 = 2c(2014)$, forcing $c = 1007$ (and therefore $f(0) = 1007$).

We now consider the next set of formulation: $f(f(m) + n) - f(n) = f(3m) - f(m) + 2014$. Denote $d = f(3m) - f(m) + 2014$. This means, for each m, considering the sequence $n, f(m) + n, 2f(m) + n$, etc, we get $f(kf(m) + n) - f(n) = kd$. Considering, that, when $k = 1007$ we have $f(1007f(m) + n) - f(n) = 1007d$, but by above $f(1007f(m) + n) - f(n)$ is also $2014f(m)$, yielding $2014f(m) = 1007d$, or $d = 2f(m)$. This means, $2f(m) = f(3m) - f(m) + 2014$, i.e. $3f(m) = f(3m) + 2014$, or simply $f(3m) = 3f(m) - 2014$. Inductively this also means that for all $m \neq 0$ we have $f(3^k m) = 3^k f(m) - (3^{k-1} + 3^{k-2} + \cdots + 1)2014 = 3^k f(m) - \frac{3^k - 1}{2}(2014)$. By Fermat's little theorem, we can choose k_0 such that $1007 \mid 3^{k_0} - 1$. Thus for this k_0, we have $f(3^k m) = f(m + (3^{k_0} - 1)m) = f(m) + 2(3^{k_0} - 1)m$ (reason being that if $3^{k_0} - 1 = 1007a$ then $f(m + (3^{k_0} - 1)m) = f(m + 1007am) = f(m) + 2014am = f(m) + 2(3^{k_0} - 1)m$). On the other hand the right hand suggests that this sum is also equal to $3^k f(m) - \frac{3^k - 1}{2}(2014)$ and therefore

$$(3^{k_0} - 1)f(m) = 2(3^{k_0} - 1)m + \frac{3^{k_0} - 1}{2}(2014) = (3^{k_0} - 1)(2m + 1007)$$

and therefore $f(m) = 2m + 1007$ (we need to choose $k_0 > 0$ so that $3^{k_0} - 1 \neq 0$, but such k_0 exists by FLT).

Finally, such function works: we have the left hand side as $4(2017) + 6m + 2n$, and same goes to right hand. Q.E.D.

Combinatorics

C1 Let n points be given inside a rectangle R such that no two of them lie on a line parallel to one of the sides of R. The rectangle R is to be dissected into smaller rectangles with sides parallel to the sides of R in such a way that none of these rectangles contains any of the given points in its interior. Prove that we have to dissect R into at least $n+1$ smaller rectangles.

Solution. We will prove this by induction: for $n = 0$, we already have the rectangle R, hence one rectangle needed.

Now consider the set S of n points inside a given rectangle, and a configuration that splits it into $n+1$ rectangles. Let a point P be arbitrary. By induction hypothesis, the rectangle containing $S\backslash\{P\}$ must be dissected into at least n rectangles.

By the problem requirement, P must lie on some boundary, which is a segment that we have drawn to split it into the rectangles. We now recover the dissection of $S\backslash\{P\}$ by the following algorithm:

- Remove the segment ℓ containing P entirely. WLOG assume that it's horizontal.
- The resulting configuration might not be rectangles, but this can fixed in the following way: let the interior of ℓ intersect with vertical lines $\ell_1, \cdots, \ell_k$, then we extend each ℓ_i's to meet the next posible horizontal line.

Now from the second protocol, we know that $k+2$ rectangles correspond to our line ℓ. After the removal of ℓ and extending the ℓ_i's, we have at most $k+1$ rectangles overlapping the space that would otherwise be covered by ℓ. Thus the number of rectangles decrease by at least 1. By induction principle, we have at least n rectangles after the removal of ℓ, so we have at least $n+1$ of them in the beginning.

C2 We have 2^m sheets of paper, with the number 1 written on each of them. We perform the following operation. In every step we choose two distinct sheets; if the numbers on the two sheets are a and b, then we erase these numbers and write the number $a+b$ on both sheets. Prove that after $m2^{m-1}$ steps, the sum of the numbers on all the sheets is at least 4^m .

Solution. We consider the product on the 2^m paper, which is 1 in the beginning. Each time, the product increases by $\frac{(a+b)^2}{ab}$ times, and since $a, b > 0$ and $(a+b)^2 - 4ab = (a-b)^2 \geq 0$, this ratio is at least 4. Thus the product after $m2^{m-1}$ steps is at least $4^{m2^{m-1}} = 2^{m2^m}$. The geometric mean is at least 2^m and by the AM-GM inequality, the arithmetic mean is at least 2^m too. Therefore the sum is at least $2^m \times 2^m = 4^m$.

C3 (IMO 2) Let $n \geq 2$ be an integer. Consider an $n \times n$ chessboard consisting of n^2 unit squares. A configuration of n rooks on this board is peaceful if every row and every column contains exactly one rook. Find the greatest positive integer k such that, for each peaceful configuration of n rooks, there is a $k \times k$ square which does not contain a rook on any of its k^2 unit squares.

Answer. $k = \lceil \sqrt{n} \rceil - 1$
Solution. We show that such k fits if and only if $k^2 < n$. Consider, now, any peaceful configuration with $k^2 < n$. Consider the first $k^2 \times k^2$ squares: squares with coordinates (i, j) with $1 \leq i, k \leq k^2$, and suppose that the condition does not hold true. We now divide the $k^2 \times k^2$ squares into $k \times k$ large grids, each large grid being a $k \times k$ square. By our assumption each large grid contains at least a rook, so there are at least k^2 rooks in the $k^2 \times k^2$ squares. But then these $k^2 \times k^2$ squares span only k^2 columns (and k^2 rows) so there cannot be more than k^2 rooks. This means:

- There are *exactly* k^2 rooks in these $k^2 \times k^2$ squares.
- There is no rook in (i, j) if exactly one of i and j lie in the interval $[1, k^2]$.
- Consequently, the remaining $n - k^2$ rooks must be in the grid (i, j) with $k^2 + 1 \leq i, j \leq n$ (i.e. $m \times m$ square with $m = n - k^2$).

In other words, there are m rooks ($m = n - k^2$) in the bottom right corner of $m \times m$ squares. But then by rotational symmetry the same holds for the top left corner, top right corner and bottom left corner, which would contradict that each column / row contains exactly one rook.

Now we move on to prove that if n and k are such that $n \le k^2$, then there is a peaceful configuration such that any $k \times k$ square contains at least a rook. We first consider the case $n = k^2$, which allows us to consider (like above) $k \times k$ large grid, each of which is a $k \times k$ square. For the (i, j)-th large grid, we place a rook at coordinate (j, i): in other words for each $1 \le i, j \le k$ the rooks are at $((i-1)k + j, (j-1)k + i)$, and it's not hard to see that there are k^2 of them and each of them has different first- and second- coordinates.

To show that each $k \times k$ square must contain at least a rook, consider any $k \times k$ square. Now there are three cases:

- This $k \times k$ square coincides with one of the big square before; by definition it contains at least a rook.
- It overlaps with two of the big squares, and two opposite boundaries of this $k \times k$ square also coincide with the boundary of the two big squares. W.L.O.G. let the rows to be $(i-1)k + 1, \cdots, ik$ (but the columns can be any k consecutive columns). Recall that there are rooks at $((i-1)k + j, (j-1)k + i)$, $j = 1, 2, \cdots, k$. Since the columns of the rooks are $(j-1)k + i$ for $j = 1, 2, \cdots, k$, exactly one of them match the columns covered by this $k \times k$ square. Since the rows are $(i-1)k + j$, the rows of all rooks match the rows covered by this $k \times k$ square, too. Hence there's a rook in this $k \times k$ square.
- Neither of the above holds, so it must overlap with four neighbouring (2×2) big grids. Consider Let the four neighbouring big grids be $(i, j), (i, j+1), (i+1, j), (i+1, j+1)$. We also let the top left corner of our $k \times k$ square be $((i-1)k + a, (j-1)k + b)$ with $1 \le a, b \le k$.

  Considering $(i, j), (i, j+1)$, with rooks at $((i-1)k + j, (j-1)k + i)$ and $((i-1)k + (j+1), jk + i)$. Since our $k \times k$ square covers columns $(j-1)k + b, \cdots, jk + (b-1)$, either $(j-1)k + i$ or $jk + i$ is covered by these intervals. Hence, if both rooks are not in this grid then either $((i-1)k + j)$ or $((i-1)k + (j+1))$ is not covered as row. Similarly, we have the following:
  - Considering $(i+1, j)$ and $(i+1, j+1)$ means that either $ik + j$ or $ik + (j+1)$ is not covered as row.
  - Considering (i, j) and $(i+1, j)$ with rooks at $((i-1)k + j, (j-1)k + i)$ and $(ik + j, (j-1)k + (i+1))$ means either $(j-1)k + i$ or $(j-1)k + (i+1)$ is not covered as column.
  - Similarly considering $(i, j+1)$ and $(i+1, j+1)$ means either $jk + i$ or $jk + (i+1)$ is not covered as column.

  Thus considering our top left rows and columns are in the form $(i-1)k + a$ and $(j-1)k + b$ the only choice is $a = j+1$ and $b = i+1$, which covers rows $(i-1)k + (j+1), \cdots, ik + j$ and columns $(j-1)k + (i+1), \cdots jk + i$. However, $(ik + j, (j-1)k + (i+1))$ itself contains a rook, contradiction.

These effectively solve for $n = k^2$.

For $n < k^2$, all we need to do is simply extend the chess board from n to k^2, put the rooks in the configuration above, and then remove those that do not lie in the first $n \times n$ grid. Now the condition still holds: each $k \times k$ square has at least a rook, and each of the remaining rooks are in different rows and columns. Then iteratively (one by one), we identify a column and a row without a rook, and place one at the intersection of the column and row until we have all n of them. Each $k \times k$ square will still contain a rook since we only add the rooks, not remove them.

Geometry

G1 (IMO 4) Let P and Q be on segment BC of an acute triangle ABC such that $\angle PAB = \angle BCA$ and $\angle CAQ = \angle ABC$. Let M and N be the points on AP and AQ, respectively, such that P is the midpoint of AM and Q is the midpoint of AN. Prove that the intersection of BM and CN is on the circumference of triangle ABC.

Solution. We need to prove that $\angle CBM + \angle BCN = \angle BAC$. Notice that the triangle ABC is similar to both QAC and PBA, so we have $\frac{QN}{QC} = \frac{QA}{QC} = \frac{PB}{PA} = \frac{PB}{PM}$. Coupled with the fact that $\angle APB = \angle AQC = \angle BAC$ we have $\angle CQN = \angle BPM$, so the triangles QNC and PBM are similar, meaning that $\angle CBM + \angle BCN = \angle QNC + \angle QCN = 180° - \angle CQN = \angle AQC = \angle BAC$, as desired.

G3 Let Ω and O be the circumcircle and the circumcentre of an acute-angled triangle ABC with $AB > BC$. The angle bisector of $\angle ABC$ intersects Ω at $M \neq B$. Let Γ be the circle with diameter BM. The angle bisectors of $\angle AOB$ and $\angle BOC$ intersect Γ at points P and Q, respectively. The point R is chosen on the line PQ so that $BR = MR$. Prove that $BR \parallel AC$. (Here we always assume that an angle bisector is a ray.)

Solution. We first notice that OP is the perpendicular bisector of AB, and OQ the perpendicular bisector of BC. Now extend OP to meet Γ again at P_1, and definte Q_1 similarly. If N is the midpoint of BM, then ON is perpendicular to BM, and since BM is the internal angle bisector of $\angle ABC$, line OP and line OQ are symmetric in the line passing through O and parallel to BM. Thus OP and OQ are also symmetric in ON, meaning that PQP_1Q_1 is actually isoceles trapezoid with parallel sides PQ_1 and QP_1. Moreover, if PQ and P_1Q_1 were to intersect at R_1, the points O, N, R_1 are all collinear, and is the perpendicular bisector of PQ_1, QP_1. Considering that BM is the diameter of the circle and $ON \perp BM$, ON is also the perpendicular bisector of BM. Since R_1 is on this perpendicular bisector, $BR_1 = MR_1$, and since R_1 is also on PQ, we have $R = R_1$.

By Brokard's theorem, taking the point of infinity P_∞ determined by the parallel lines PQ_1 and QP_1, we have R as the polar of the line OP_∞ (i.e. the line through O parallel to BM). Consider, now, the lines BR and MR and let them intersect Γ again at B_1 and M_1. Since $BR = MR$, we also have $BM \parallel B_1M_1$. Also by above (Brokard's theorem again), MB_1 and BM_1 intersect at O. Now $\angle MB_1B = 90°$, so BM_1 (i.e. line BR) is perpendicular to MB_1, i.e. MO. But AC is also perpendicular to MO since M is the midpoint of arc AC, so $AC \parallel BR$. Q.E.D.

G5 (IMO 3) Convex quadrilateral $ABCD$ has $\angle ABC = \angle CDA = 90°$. Point H is the foot of the perpendicular from A to BD. Points S and T lie on sides AB and AD, respectively, such that H lies inside triangle SCT and

$$\angle CHS - \angle CSB = 90°, \quad \angle THC - \angle DTC = 90°.$$

Prove that line BD is tangent to the circumcircle of triangle TSH.

Solution. We first show that Q, the circumcenter of CHS, lies on the line AB. To see this, by the identity of angle of chord subtending at the center vs angle subtending on the arc we have

$$2\angle CHS = 360° - \angle CQS$$

since $\angle CHS > 90°$ by the problem definition. Since $CQ = CS$, we have $\angle CSQ = 90° - \frac{\angle CQS}{2} = 90° - \frac{360° - 2\angle CHS}{2} = \angle CHS - 90° = \angle CSB$, implying that Q, S, B are collinear and therefore all lie on line AB. Similarly, naming R as the circumcenter of DHT we have R on AD.

Now, with the fact that AH is perpendicular to BD, the goal reduces to showing that the circumcenter O of TSH lies on AH. But then O is on the perpendicular bisector of SH, which is in turn the internal angle bisector of SQH (i.e. angle bisector of AQH) because $SQ = QH$. Similarly O is on the angle bisector of ARH. So all we need to prove is that the angle bisectors of $\angle SQH$ and $\angle ARH$ intersect at AH. By the angle bisector theorem this is equivalent to proving the following ratio:

$$\frac{AQ}{QH} = \frac{AR}{RH} \to \frac{AQ}{AR} = \frac{QH}{RH}$$

the second equivalence being equivalent to the first, hence we will prove the second one.

Let N be the midpoint of CH, the QR is the perpendicular of CH, hence perpendicular to CH and passes through N. We also have $\angle CBQ = \angle CNQ = 90°$ so C, B, Q, N are concyclic. Similarly C, B, R, N is concyclic. We now have the following ratio, thanks to sine rule:

$$\frac{AQ}{AR} = \frac{\sin\angle QRA}{\sin\angle RQA} = \frac{\sin\angle NCD}{\sin\angle NCB}$$

and since $QH = QC$ and $RH = RC$,

$$\frac{QH}{RH} = \frac{QC}{RC} = \frac{\sin\angle CRQ}{\sin\angle CQR} = \frac{\sin\angle CDN}{\sin\angle CBN}$$

but then $\frac{\sin\angle NCD}{\sin\angle NCB} = \frac{\sin\angle CDN}{\sin\angle CBN}$ if and only if $\frac{\sin\angle NCD}{\sin\angle CDN} = \frac{\sin\angle NCB}{\sin\angle CBN}$. The first ratio is (sine rule again) the same as $\frac{NB}{NC}$ and the second, $\frac{ND}{NC}$, so all we need now is $NB = ND$. To see why this is true, let L be the midpoint of AC. Then since $\angle B = \angle D = 90°$, L is the circumcenter of the qudrilateral $ABCD$, and hence $LB = LD$. Since N is the midpoint of CH we also have $AH \parallel NL$, meaning that $NL \perp BD$. But since L is on the perpendicular bisector of BD, so is N, and therefore $NB = ND$. Q.E.D.

Number Theory

N2 Determine all pairs (x, y) of positive integers such that

$$\sqrt[3]{7x^2 - 13xy + 7y^2} = |x - y| + 1.$$

Answer. $\{x, y\} = \{1, 1\}$ and $\{c^3 + c^2 - 2c - 1, c^3 + 2c^2 - c - 1\}$.
Solution. By symmetry we can assume that $y \geq x$, and let k be such that $y = x + k$. Also, $7x^2 - 13xy + 7y^2 = 7(x^2 - 2xy + y^2) + xy = 7(x - y)^2 + xy = 7k^2 + x(x + k)$. Therefore we now have

$$(k + 1)^3 = 7k^2 + x(x + k)$$

and notice that this is actually a quadratic equation in terms of x, i.e. $x^2 + kx + (7k^2 - (k + 1)^3) = 0$. Since we are finding for integer solutions when x and k are both integers, we need the discriminant $k^2 - 4(7k^2 - (k + 1)^3)$ to be a perfect square. But notice the following:

$$k^2 - 4(7k^2 - (k + 1)^3) = 4k^3 - 15k^2 + 12k + 4 = (k - 2)(4k^2 - 7k - 2) = (k - 2)^2(4k + 1)$$

so either $k = 2$ or $4k+1$ is a perfect square. Since $4k+1$ is odd, we have $4k+1 = (2c+1)^2$ for some nonnegative integer c, leaving $k = c(c+1)$. Hence the following equation obtained by solving the squadratic equation:

$$x = \frac{-k \pm \sqrt{(k - 2)^2(4k + 1)}}{2} = \frac{-c(c + 1) \pm |c(c + 1) - 2| \cdot (2c + 1)}{2}$$

The product of roots is given by $7k^2 - (k + 1)^3$, which is positive only when $k = 2$ and negative for the rest of the cases. For $k = 2$ the discriminant turned out to be 0, so we have $x^2+2x+1=0$, or $(x+1)^2=0$, so $x=-1$ which is impossible because x must be positive. Otherwise, there would be one positive and one negative root in the quadratic equation, and therefore we choose the bigger root given by the plus sign, yielding:

$$x=\frac{-c(c+1)+|c(c+1)-2|\cdot(2c+1)}{2}$$

and

$$y=x+k=\frac{-c(c+1)+|c(c+1)-2|\cdot(2c+1)}{2}+c(c+1)=\frac{c(c+1)+|c(c+1)-2|\cdot(2c+1)}{2}$$

for all $c=0,2,3,4,5,\cdots$. ($c=1$ corresponds to $k=2$). Notice for $c=0$ with $k=0$ we actually have $1=x^2$ so $x=y=1$. Otherwise we have $|c(c+1)-2|>0$ so we can remove the modulus to get

$$x=\frac{-c(c+1)+(c(c+1)-2)\cdot(2c+1)}{2}=c^3+c^2-2c-1$$

and similarly $y=c^3+2c^2-c-1$.

N3 (IMO 5) For each positive integer n, the Bank of Cape Town issues coins of denomination $\frac{1}{n}$. Given a finite collection of such coins (of not necessarily different denominations) with total value at most $99+\frac{1}{2}$, prove that it is possible to split this collection into 100 or fewer groups, such that each group has total value at most 1.

Solution. In fact, we shall prove that for any pile of coins worth at most $n-\frac{1}{2}$ we can split them into n groups, each of total value at most 1.

The key to this problem is to 'group' certain coins according to the following algorithm, in the hope to minimize the number of cape town coins and their denominators. To see this, we perform the following operations iteratively: for each $a>1$ and positive integer b, if there are a coins of value $\frac{1}{ab}$, then we group them together into a single coin of value $\frac{1}{b}$ (notice that the total value never changes). Since the number of coins decrease each iterations and there are only a finite number fo coins, such operation can only be done finitely many times, hence it must terminate. This means, at the end of the process, for each positive integer b and a prime number p (or simply any $p>1$) dividing b, the number of coins of value $\frac{1}{b}$ must be less than p. In particular, if b is even, choosing $p=2$ means there is at most one such coin.

Next, let m be the number of coins with value 1. We place these coins into m separate piles, leaving coins of total value at most $n-m-\frac{1}{2}$. Denote $n_1=n_1-\frac{1}{2}$ and consider the coins of values $\frac{1}{k}$ for $k=2,3,\cdots,2n_1$. We have seen that if k is even then there is at most 1 coin of value $\frac{1}{k}$, and if k is odd, there is at most $k-1$ of them. Consider, also, the fact that $\frac{2i-2}{2i-1}+\frac{1}{2i}<1$ for all $i\geq 2$, we can group all coins of value $\frac{1}{2i-1}$ and $\frac{1}{2i}$ into one pile, for all $i=2,3,\cdots,n_1$ (i.e. n_1-1 of them), and place the coin (if exists; otherwise we just have an empty pile) with value $\frac{1}{2}$ into the last pile, making a total of n_1 piles right now. Now all piles have value at most 1.

We are not done yet: there might still be coins of value $\frac{1}{k}$ for $k>2n_1$. However, the coins in the piles have total value at most $n_1-\frac{1}{2}$, i.e. an average (w.r.t. pile) of at most $1-\frac{1}{2n_1}$. By pigeonhole principle, there must be a pile of value at most $1-\frac{1}{2n_1}$. Since each leftover coin has value less than $\frac{1}{2n_1}$, we can choose any of the leftover coin and put into this pile of value at most $1-\frac{1}{2n_1}$, and after that this pile's value cannot exceed 1. This invariant holds as long as there is a coin not in any pile yet, so we can repeat this argument, find a pile of value at most $1-\frac{1}{2n_1}$ and put a coin into the pile. Eventually, all coins are in the piles. Q.E.D.

N4 Let $n > 1$ be a given integer. Prove that infinitely many terms of the sequence $(a_k)_{k\geq 1}$, defined by

$$a_k = \left\lfloor \frac{n^k}{k} \right\rfloor,$$

are odd. (For a real number x, $\lfloor x \rfloor$ denotes the largest integer not exceeding x.)

Solution. We settle the easier case first: n is odd. Now for each $k = n^m$, we have $\frac{n^k}{k} = n^{k-m} = n^{n^m - m}$ and for sufficiently large m, $n^m \geq m$ ($n \geq 2$ and therefore it's well-known that $n^m \in \Omega(m)$ for each $n > 1$ fixed). This means that $k \mid n^k$ and therefore in this case $a_k = \frac{n^k}{k}$. Since n is odd, so is n^k and therefore $\frac{n^k}{k}$ is also odd.

Now let's see the even case, and we show that there are infinitely many m's such that $k = n^m(n+1)$ will work. To see how this works, consider the following:

$$\frac{n^k}{k} = \frac{n^{n^m(n+1)}}{n^m(n+1)} = \frac{n^{n^m(n+1)-m}}{n+1}$$

we now proceed to a lemma: for $n \geq 2$ even, $\left\lfloor \frac{n^k}{n+1} \right\rfloor$ is even for all $k \geq 1$ odd, and even otherwise. To see why, notice that $\left\lfloor \frac{n^k}{n+1} \right\rfloor$ is even iff n^k is congruent to $0, 1, \cdots, n$ modulo $2n+2$, and odd if congruent to $n+1, \cdots, 2n+1$ modulo $2n+2$. When $k = 1$ the congruence is n; when $k = 2$ we have $n^2 = (n+1)(n-1)+1 = (n+1)(n-2)+n+2$ and since $n-2$ is even, we have $2n+2 \mid (n+1)(n-2)$ and therefore $n^2 \equiv n+2 \pmod{2n+2}$. Finally, when $k = 3$ we have

$$n^3 \equiv (n^2) \cdot n \equiv (n+2)n \equiv n^2 + 2n \equiv n + 2 + 2n \equiv 3n + 2 \equiv n \pmod{2n+2}$$

so the congruence alternates between n and $n+2$ when k is even or odd, completing the proof for our lemma.

To finish the proof, we need to find those (infinitely many) m such that $n^m(n+1) - m$ is even. Since n is even, $n^m(n+1)$ is even for all $m > 0$, which reduces to finding m is even. Thus all $m \geq 2$ even works, Q.E.D.

N5 Find all triples (p, x, y) consisting of a prime number p and two positive integers x and y such that $x^{p-1} + y$ and $x + y^{p-1}$ are both powers of p.

Answer. Any triples in the form $(2, x, 2^k - x)$ provided $2^k > x$, and $(3, 2, 5)$ and $(3, 5, 2)$.
Solution. When $p = 2$, we are only asked to find the pairs where $x + y$ is a power of 2 which is easily settled above. From now on we focus only on odd primes p.

First, we show that x and y cannot be simultanoeusly divisible by p. Otherwise, let $v_p(x) \leq v_p(y)$, then $v_p(y^{p-1}) = (p-1)v_p(y) > v_p(y) \geq v_p(x)$ and therefore $v_p(y^{p-1} + x) = v_p(x)$. If $x = cp^k$ where $k = v_p(x)$ then $y^{p-1} + x = dp^k$ too, with $p \nmid d$. Since this $y^{p-1} + x$ must be a p-th power, we have $d = 1$, but $dp^k > cp^k$ so $1 = d > c \geq 1$, contradiction.

Therefore we have p not dividing x and y. Now let $x \leq y$ and let $x^{p-1} + y = p^k$. THen $p^k \mid y^{p-1} + x$, too. We now have $y \equiv -x^{p-1} \pmod{p^k}$ and $0 \equiv y^{p-1} + x \equiv (-x^{p-1})^{p-1} + x \equiv x^{(p-1)^2} + x = x(x^{(p-1)^2-1} + 1) \pmod{p^k}$. Since $p \nmid x$, we have $p^k \mid x^{(p-1)^2-1} + 1$, i.e. $x^{(p-1)^2-1} \equiv -1 \pmod{p^k}$.

Now by Fermat's Little theorem, $1 \equiv x^{(p-1)^2} \equiv x \cdot (-1) = -x \pmod{p}$ so $p \mid x+1$. We now let $x = cp^\ell - 1$ with $p \nmid c$ and $\ell \geq 1$. We now consider the expansion $(cp^\ell - 1)^{(p-1)^2-1} + 1$, with the following observation:

- The expansion has the form $\displaystyle\sum_{i=1}^{p(p-2)} \binom{p(p-2)}{i} (-1)^{p(p-2)-i} (cp^\ell)^i$, with $i = 0$ ommited since the -1 term is offset by the $+1$ term at $(cp^\ell - 1)^{(p-1)^2-1} + 1$.

- Since $\binom{p(p-2)}{i}$ is divisible by p for all $p \nmid i$ (well-known), this is also true for $i = 2$, and since $\ell \geq 1$, $p^{2\ell+1} \mid \sum_{i=2}^{p(p-2)} \binom{p(p-2)}{i} (-1)^{p(p-2)-i} (cp^\ell)^i$.
- If we consider $i = 1$ we notice that the term is actually $p(p-2)cp^\ell$, with $v_p(p(p-2)cp^\ell) = \ell + 1$.

so these points are enough to show that the highest power of p dividing $x^{(p-1)^2-1} + 1$ is $\ell + 1$. But since this term is also divisible by p^k, we have $\ell \geq k - 1$.

In other words, we have $x \geq p^{k-1} - 1$ but then $x^{p-1} + y = p^k$ so $x^{p-1} < p^k$, i.e. $(p^{k-1} - 1)^{p-1} < p^k$. Since $p \mid x+1$ anyways, we can safely assume that $(p^{k-1}-1)^{p-1} \geq (p-1)^{p-1}$. For $p \geq 5$, $(p-1)^{p-1} > p^2$ so we have $k \geq 3$, but then $(p^{k-2})^{p-1} < (p^{k-1} - 1)^{p-1} < p^k$ so $(k-2)(p-1) < k$, which is impossible. Hence we only consider $p = 3$, i.e. $(3^{k-1}-1)^2 < 3^k$. This holds true for $k = 2$, but not any $k = 3$, and for $k \geq 4$ we can reuse the result $(k-2)(p-1) < k$ i.e. $2(k-2) < k$ to produce a contradiction. Therefore $k = 2$, and $x^2 + y = 3^2 = 9$. Since $p \mid x + 1$ with $x^2 < 9$, the only choice is $x = 2$ and $y = 5$, and it turned out that $5^2 + 2 = 27 = 3^3$ works too.

N6 Let $a_1 < a_2 < \cdots < a_n$ be pairwise coprime positive integers with a_1 being prime and $a_1 \geq n + 2$. On the segment $I = [0, a_1 a_2 \cdots a_n]$ of the real line, mark all integers that are divisible by at least one of the numbers $a_1, \ldots, a_n$. These points split I into a number of smaller segments. Prove that the sum of the squares of the lengths of these segments is divisible by a_1.

Solution. Might as well give an alias for a_1, say p. It's not hard to see that each segment must have length at most p. We show by fixing p and inducting on n that, if $x_1, \cdots, x_{p-1}$ represents the segments with lengths $1, 2, \cdots, p-1$, then there exists a polynomial $P(x)$ such that:

- $P(i) = x_i$, $\forall i = 1, \cdots, p-1$.
- P has coefficient that are rational numbers such that, when written in simplest form, the denominator is not divisible by p.
- P has degree at most $n - 2$.

We proceed by induction on n. When $n = 1$ there's nothing to prove: we have a single segment of length p, so $x_1 = \cdots = x_{p-1} = 0$, which actually fits into the zero polynomial: the polynomial with degree -1, by our convention here.

Now suppose that for some n, the number of segments of length p is $F(n)$ and let P_n be a polynomial (satisfying our aforementioned conditions) such that for each $1 \leq i \leq p-1$, the number of segments of length i is $F(i)$. Now consider what happens when we add a_{i+1}. We have:

- The segment extends from length $a_1 \cdots a_n$ to $a_1 \cdots a_{n+1}$.
- If we do not mark the points divisible by a_{n+1}, we have $F(n)$ segments of length p and $a_{n+1} P_n(i)$ segments of length i.

Let's see what happens when we mark points divisible by a_{n+1}, which might or might not split a segment into two (it cannot split the a segment into three since $a_{n+1} > p$). In the original configuration (where we have length of I as $a_1 \cdots a_n$), take $[x, x+i]$ as any segment of length i. Consider, now, the a_{n+1} copies of it: $[ja_{n+1} + x, ja_{n+1} + x + i]$ for $j = 0, \cdots, a_{n+1}$. For each $k = 1, 2, \ldots, i-1$, among the numbers $ja_{n+1} + x + k, j = 0, \cdots, a_{n+1}$, from the fact that each a_i's are pairwise coprime, exactly one of them is divisible by a_{i+1}. This means, $i - 1$ of the segments are divided further into segments of length $(1, i-1), (2, i-2), \cdots, (i-1, 1)$, while the rest $a_{n+1} - i + 1$ of them remain undivided.

Now for each i, we shall see how many segments are there have length i. Those must correspond to segments of length $j \geq i$ when considering only $a_1, \cdots, a_n$ and not a_{n+1} since considering a_{n+1} only splits them up (potentially). By the fact above, the number of segments of length i can be given by

$$P_n(i)(a_{n+1} - i + 1) + \sum_{j=i+1}^{p-1} 2P_n(j) + 2F(n)$$

We now consider 2 cases. If $n = 1$ then $P_n \equiv 0$ so each term is $2F(n)$, i.e. a constant. Otherwise, P_n is assumed to have degree at most $n-2$. We now consider each term separately:

- $2F(n)$ is constant throughout i, and is an integer (hence constant polynomial integer coefficient).
- $P_n(i)(a_{n+1}-i+1) = (a_{n+1}+1)P_n(i) - iP_n(i)$. $(a_{n+1}+1)$ is constant while $\deg(iP_n(i)) = \deg(P_n) + 1$ so by induction hypothesis, this $(a_{n+1}+1)P_n(i) - iP_n(i)$. $(a_{n+1}+1)$ has degree at most $n-1$. Moreover the polynomial of rational coefficient with denominator not divisible by p is closed under multiplication and addition: the set $\{a/b : a \in \mathbb{Z}, \gcd(b,p) = 1\}$ is a ring.

We leave the middle term out deliberately: let $Q = \sum_{j=1}^{p-1} 2P_n(j)$, then $\sum_{j=i+1}^{p-1} 2P_n(j) = Q - \sum_{j=1}^{i} 2P_n(j)$. Since Q is a constant, we only need to consider the last term $\sum_{j=1}^{i} P_n(j)$, which brings us to a lemma which directly addresses this subproblem:

Lemma: let P be a polynomial of degree $k \leq p-1$ with rational coefficients in terms of $\{a/b : a \in \mathbb{Z}, \gcd(b,p) = 1\}$. Then if $Q(n) = \sum_{i=1}^{n} P(i)$, Q also has the same cclass of coefficients but with degree $k+1$.

Proof: Write $P(n) = \sum_{i=0}^{k} a_i x^k$. Now, we need to solve for $Q = \sum_{i=0}^{k+1} q_i x^i$ such that $Q(n) - Q(n-1) = P(n)$. Nevertheless, we also have the following:

$$\begin{aligned} Q(n) - Q(n-1) &= \sum_{i=0}^{k+1} q_i (n^i - (n-1)^i) \\ &= \sum_{i=0}^{k+1} q_i \sum_{j=0^{i-1}} (-1)^{i-j-1} \binom{i}{j} n^j \end{aligned}$$

where each term $n^i - (n-1)^i$ is a polynomial of degree $i-1$ and leading coefficient i. Putting this into the matrix form, this is what we need to solve:

$$\begin{pmatrix} k & -\binom{k}{2} & \cdots & (-1)^{k-1} \\ 0 & (k-1) & \cdots & (-1)^{k-2} \\ \vdots & & & \\ 0 & 0 & \cdots & 1 \end{pmatrix} \begin{pmatrix} q_{k+1} \\ q_k \\ \vdots \\ q_1 \end{pmatrix} = \begin{pmatrix} a_k \\ a_{k-1} \\ \vdots \\ a_0 \end{pmatrix}$$

and since this system of equations is upper triangular, it has determinant $k!$ which is relatively prime to p since $k < p$. This means, this equation is solvable in q_i's where our coefficients have denominator not divisible by p. Finally, we let $q_0 = 0$, and this proves the lemma.

Now we can finish the proof. Let $P_n(i)$ be the number of segments of length i, and we need to show that p divides $\sum_{i=1}^{p-1} i^2 P_n(i)$. Let $P_n(x) = \sum_{i=0}^{n-2} a_i x^i$, then $\sum_{i=1}^{p-1} i^2 P_n(i) = \sum_{i=0}^{n} a_n (\sum_{j=1}^{p-1} j^{i+2})$. Since a_n has denominator not devisible by p, it suffices to show that $\sum_{j=1}^{p-1} j^{i+2}$ is disivible by p for all $0 \le i \le n-2$. Let g be the primitive root, then we can think $\sum_{j=1}^{p-1} j^{i+2}$ as $\sum_{j=0}^{p-2} (g^j)^{i+2} = \frac{g^{(p-1)(i+2)} - 1}{g^{i+2} - 1}$. The numerator is disivible by p by Fermat's Little theorem; the denominator is not because g is a primitive root of p but $i + 2 \le n < p - 1$. The conclusion then follows.