Team Contest Round 1

Alex Anderson, Timothy Chu, Holden Lee, et al

August 2010

1 Algebra

1. Prove that for all real a, b, c,

$$2^{-2/3}(\max(a,b,c) - \min(a,b,c)) \geq \sqrt[3]{|a-b||b-c||a-c|}.$$

Solution Without loss of generality, suppose $a \geq b \geq c$. Then by the Arithmetic Mean-Geometric Mean inequality,

$$\begin{aligned} 2^{-2/3}(\max(a,b,c) - \min(a,b,c)) &= 2^{1/3} \cdot \frac{(a-b)+(b-c)+\frac{1}{2}(a-c)}{3} \\ &\geq 2^{1/3} \cdot \sqrt[3]{(a-b)(b-c)\frac{1}{2}(a-c)} \\ &= \sqrt[3]{(a-b)(b-c)(a-c)} \end{aligned}$$

2. Does there exist a nonlinear function f from the nonnegative reals to the nonnegative reals so that

$$\min_{0<x<t}[f(x)+f(t-x)] \leq f(t) \leq \max_{0<x<t}[f(x)+f(t-x)]$$

for all positive t?

Solution Yes. Let $f(x) = 2^{\lfloor \log_2(x) \rfloor}$. (Define $f(0) = 0$.) Then

$$f(x) = 2^{\lfloor \log_2(x) \rfloor} = 2^{\lfloor \log_2(x)-1 \rfloor} + 2^{\lfloor \log_2(x)-1 \rfloor} = 2^{\lfloor \log_2(x/2) \rfloor} + 2^{\lfloor \log_2(x/2) \rfloor} = f(x/2) + f(x/2).$$

Hence the inequalities obviously hold.

3. Let $x, y > 0$. Prove that

$$\frac{18}{(x+y)^4} \leq \frac{2}{(x-y)^4} + \frac{1}{x^3y+y^3x}$$

and find when equality holds.

By Titu's Lemma,

$$\begin{aligned}\frac{2}{(x-y)^4}+\frac{1}{x^3y+y^3x} &= 2\left(\frac{1^2}{(x-y)^4}+\frac{2^2}{8(x^3y+y^3x)}\right)\\ &\geq 2\left(\frac{(1+2)^2}{(x-y)^4+8(x^3y+y^3x)}\right)\\ &= \frac{18}{(x+y)^4}\end{aligned}$$

Equality occurs when

$$\frac{1}{(x-y)^4}=\frac{1}{4(x^3y+y^3x)},$$

i.e. when $4(x^3y+y^3x)=(x-y)^4$; multiplying by 2 and adding $(x-y)^4$,

$$(x+y)^4=3(x-y)^4.$$

Taking fourth roots, we get $x+y=\sqrt[4]{3}(x-y)$, giving

$$x=\frac{\sqrt[4]{3}\pm 1}{\sqrt[4]{3}\mp 1}y.$$

4. 7 points $Q_1,\ldots,Q_7$ are equally spaced on a circle of radius 1 centered at O. Point P is on ray OQ_7 so that $OP=2$. Find the product

$$\prod_{k=1}^{7} PQ_i.$$

Solution Letting ray OQ_1 be the positive real axis, Q_i represent the 7th roots of unity ω^i in the complex plane. Hence PQ_i equals $|2-\omega^i|$. The roots of $x^7-1=0$ are just the roots of unity, so $x^7-1=\prod_{i=0}^{6}(x-\omega^i)$. Plugging in $x=2$ gives $\prod_{k=1}^{n} PQ_i=|2^7-1|=127$.

5. Find all polynomials $p(x)=a_nx^n+\cdots+a_1x+a_0$ satisfying the following:

   (a) $\{a_n,a_{n-1},\ldots,a_1,a_0\}=\{0,1,\ldots,n-1,n\}$, and $a_n\neq 0$.

   (b) $p(x)$ has only rational roots.

Solution Since all coefficients of $p(x)$ are nonnegative, $p(x)=0$ has no negative roots. Then it factors as

$$p(x)=(p_1x+q_1)\cdots(p_nx+q_n).$$

We divide into 2 cases.

(a) $x\nmid p(x)$. Then the constant term is $\sum_{1\leq i\neq j\leq n} p_iq_j\geq n(n-1)$ so $n\leq 2$.

(b) $x\mid p(x)$. Then only one factor is x (as else both the coefficients of $1,x$ are zero), without loss of generality $q_n=0$. Then the coefficient of x is $\sum_{1\leq i\neq j\leq n-1} p_iq_j\leq n(n-1)$. In order for this to be less than or equal to n, we must have $n\leq 3$.

We can easily find all polynomials of degree at most 2 that work:

$$x,\ x^2 + 2x = x(x+2),\ 2x^2 + x = x(2x+1).$$

Since $x(x+1)^2$ does not work, when $p(x)$ has degree 3 we must have equality in item (b), $p_1q_2 + p_2q_1 = 3$. This gives two possibilities:

$$2x^3 + 3x^2 + x = x(x+1)(2x+1),\ x^3 + 3x^2 + 2x = x(x+1)(x+2).$$

6. For a polynomial

$$p(x) = a_nx^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$$

define

$$\Gamma(p(x)) = a_0^2 + a_1^2 + \cdots + a_n^2.$$

Let $g(x) = 3x^2 + 7x + 2$. Find $f(x) \in \mathbb{R}[x]$ such that

(a) $f(0) = 1$ and

(b) For all $n \geq 0$, $\Gamma(f(x)^n) = \Gamma(g(x)^n)$.

Solution For $p(x) = a_nx^n + \cdots + a_0, a_n \neq 0$ define $p^*(x) = a_0x^n + \cdots + a_n$. Then $\Gamma(p)$ is the coefficient of x^n in $p(x)p^*(x)$. It is easy to see that

$$(fg)^* = f^*g^*.$$

We show that $g(x) = (3x+1)(2x+1)$ works. Note $g(0) = 1$, and

$$g(x)g^*(x) = (3x+1)(2x+1)(x+3)(x+2) = (3x+1)(x+2)(x+3)(2x+1) = f(x)f^*(x).$$

Hence $\Gamma(g(x)^m)$ is the coefficient of x^{mn} in

$$g(x)^m[g(x)^m]^* = [g(x)g^*(x)]^m = [f(x)f^*(x)]^m = f(x)^m[f(x)^m]^*$$

so $\Gamma(g^m) = \Gamma(f^m)$ for all m.

2 Combinatorics

1. Let n, m, k be positive integers such that $n \geq km$. Find the number of m-tuples of positive integers $(a_1, \ldots, a_m)$ so that

$$a_1 + \cdots + a_m = n$$

and $a_i \geq k$ for each i.

Solution Subtracting $k-1$ from each term, the problem is equivalent to finding the number of m-tuples of positive integers $(b_1, \ldots, b_m)$ summing up to $n-(k-1)m$. The number of ways to do this is the number of ways to put $m-1$ dividers in the spaces between $n-(k-1)m$ balls, since we can associate each m-tuple $(b_1, \ldots, b_m)$ with the configuration consisting of b_i balls in between the $(i-1)$th and ith divider (divider number 0 being at the front). Hence the number of ways is

$$\binom{n-(k-1)m-1}{m-1}.$$

2. Pam has a list of numbers 1 through n, permuted randomly, in a row. She reads the numbers from left to right, circling the numbers 1, then 2, and so on. If she reaches the end of the list with numbers left uncircled, she starts reading from the beginning of the list again. What is the probability that she finishes circling all numbers the second time she reads the list (and not before)?

   Solution We first count the number of permutations that require two readings. Consider the set A_1 of positions whose numbers are read on the first reading and the set A_2 of positions whose numbers are read on the second reading. They partition the set $\{1, 2, \cdots, n\}$ so there are 2^n choices for A_1, A_2. However, we must exclude the possibilities where all numbers in A_2 come after numbers in A_1; this happens in $n+1$ cases, when A_1 consists of numbers 1 through i and A_2 consists of $i+1$ through n, where $0 \le i \le n$. Thus the total number of such permutations is $2^n - n - 1$, and the probability is
   $$\frac{2^n - n - 1}{n!}.$$

3. For positive integers $a_1, \ldots, a_{2010}$ such that $a_1 - a_2, a_2 - a_3, \ldots, a_{2009} - a_{2010}$ are all distinct, find the minimum possible number of distinct elements of the set $\{a_1, \ldots, a_{2010}\}$.

   Solution If there are k distinct elements in the set $\{a_1, \ldots, a_{2010}\}$ then the maximum possible number of pairwise differences is $k(k-1)+1$, since there are $k(k-1)$ ways to choose an ordered pair of distinct elements, and a difference of 0 is also possible. Since $45 \cdot 44 + 1 = 1981 < 2009$, there must be at least 46 elements.

   Now we show that $k = 46$ is possible. We can choose distinct $b_1, \ldots, b_{46}$ so that the $b_i - b_j$ are all distinct for the different ordered pairs of distinct (i, j); for example, we can take $b_i = 2^i$. Now consider the directed complete graph on 46 vertices $V_1, \ldots, V_{46}$. It has $46 \cdot 45 = 2070$ edges. Since the indegree and outdegree of each vertex is equal, and the graph is connected, there exists an Euler tour, i.e. a sequence of 2071 vertices $V_{t_1} \ldots V_{t_{2071}}$ so that each edge occurs once. Let $a_i = b_{t_i}$ (the number corresponding to the vertex visited at the ith step); then by construction all the differences are distinct.

4. The students at AwesomeMath were divided into 18 teams for the team contest, each with an arbitrary but nonzero number of people. After a change in rules they regrouped into 12 teams. Prove that at least 7 students are in larger teams than before.

   Solution If a student is in a team with n people, define his or her *importance* to be $\frac{1}{n}$. The sum of all the importances of the students on a team is 1, so the sum of importances of all students is the number of teams. At the start this number is 18; at the end this number is 12. Since each student's importance is in $(0, 1]$, a student's importance can only change by less than 1. Thus the importance of at least 7 students must have decreased; they are in larger teams.

5. Let S be a set of n positive integers, and let m be a positive integer. Prove that there are at least 2^{n-m+1} subsets of S with sum of elements divisible by m. Include the empty set in your count.

Solution The assertion is trivial if $n < m$. So suppose $m \geq n$. Let $\sigma(T)$ denote the sum of elements of T; by convention $\sigma(\phi) = 0$. We say that a set T *attains* k modulo m if $\sigma(T') \equiv k \pmod{m}$ for some $T' \subseteq T$.

Lemma 2.1: There exists a subset of at most $m-1$ elements of S attaining every value modulo m attained by S.

Proof. Suppose that S attains k values. It suffices to prove the following statement: for $i < k$, there exists a subset $S_i \subseteq S$ attaining $i+1$ values modulo m. We do this by induction. For $i = 0$, take $S_0 = \phi$.

Now suppose we have found S_i, $i < k-1$. Let A be the smallest subset of S with $\sigma(A)$ not attained by S. There must exist $a \in A \backslash S_i$. Set $S_{i+1} = S_i \cup \{a\}$. Then S_{i+1} attains all the values attained by S_i and the additional value $\sigma(S)$ because S_i attains $\sigma(A - \{a\})$ (by minimality of A). This concludes the induction. □

Choose a subset T as in Lemma 2.1. Then $S \backslash T$ has at least $n - m + 1$ elements. We show that we can associate each subset $A \subseteq S \backslash T$ with a distinct subset of S with sum of elements divisible by m. Since T attains all sums attained by S, there exists a subset T' of T with $\sigma(T') \equiv \sigma(A \cup T) \pmod{m}$. Then $\sigma(A \cup (T \backslash T')) \equiv 0 \pmod{m}$; we associate A with $A \cup (T \backslash T')$. In this way we get at least 2^{n-m+1} subsets satisfying the given conditions.

6. Let $f(n, r)$ denote the maximum number of edges a graph with n vertices can have so that it does not contain a complete bipartite subgraph $K_{r,r}$. Prove that

$$f(n, r) \leq cn^{2-1/r}$$

for some constant c depending only on r.

Solution

Lemma 2.2: Let G be a graph with n vertices. Let V be the set of vertices. If $K_{r,r}$ is not contained in G, then

$$\sum_{a \in V} \binom{d(a)}{r} \leq (r-1)\binom{n}{r}.$$

Proof. We count in two ways the number of pairs $(a, \{b_1, \ldots, b_r\})$ where $a, b_1, \ldots, b_r \in V$, and a is connected to all the b_i by edges. On one hand, for each $a \in A$ there are $\binom{d(a)}{r}$ choices for the sets $\{b_1, \ldots, b_r\}$. On the other hand, there are at most $(r-1)\binom{n}{r}$ such sets because if there were more, then some $\{b_1, \ldots, b_r\}$ would appear in r pairs, say as pairs with $a_1, \ldots, a_r$. Then $a_1, \ldots, a_r, b_1, \ldots, b_r$ would be the vertices of a $K_{r,r}$ contained in G. □

We may assume $r > 1$. Consider a graph G as in Lemma 2.2 with e edges. We can bound $\binom{x}{r} \geq -k + c_1 x^r$ for $x \geq 0$ by some constants k and some $c_1 > 0$. Then by the

Power Mean inequality,

$$-kn + c_1 n \underbrace{\left(\sum_{a\in V} \frac{d(a)}{n}\right)^r}_{(2e/n)^r} \le -kn + c_1 \sum_{a\in V} d(a)^r \le \sum_{a\in V} \binom{d(a)}{r} \le (r-1)\binom{n}{r} \le n^r.$$

Then solving for e we get (for some constants $c_2, c_3 > 0$)

$$\frac{c_2 e^r}{n^{r-1}} \le n^r + kn \implies e \le \sqrt[r]{\frac{1}{c_2}(n^{2r-1} + kn^r)} \le c_3 n^{2-1/r}.$$

3 Geometry

1. Let ABC be a triangle where the incircle touches BC, CA, AB at D, E, F. AD intersects the incircle again at P. If $PD = 6$, $PE = 3$, $PF = 2$, then find $\frac{DF\cdot DE}{PF\cdot PE}$.

   Solution Since AE, AF are tangent to the incircle, we have pairs of similar triangles $\triangle APF \sim \triangle AFD$ and $\triangle APE \sim \triangle AED$. So we have $\frac{FD}{PF} = \frac{AD}{AF} = \frac{AD}{AE} = \frac{ED}{PE} = t$. Therefore, we can write $FD = 2t$ and $DE = 3t$. Noting that $\angle PFD = \pi - \angle PED$, we can use the law of cosines to get

$$\frac{2^2 + (2t)^2 - 6^2}{2(2)(2t)} + \frac{3^2 + (3t)^2 - 6^2}{2(3)(3t)} = 0$$
$$t^3 - \frac{11}{2} = 0$$

   So $t^2 = \sqrt[3]{\frac{121}{4}}$ which is our answer (as the other root is negative).

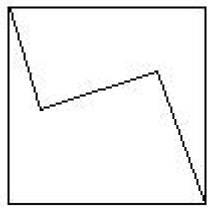
2. Given points X, Y, Z, construct a triangle $\triangle ABC$ for which X is the circumcenter, Y is the midpoint of BC and Z is the foot of the altitude from B to AC.

   Solution Draw a line perpendicular to XY through Y. B, C lie on this line. Further, $BY = CY = YZ$, so draw a circle centered at Y with radius YZ. This gives you B, C (with C, Z on the same side of line XY. Then draw a circle centered at X with radius $BX = CX$ and that intersects CZ again at A.

   Proof of construction: Clearly, $AX = BX = CX$, $BY = CY$ by construction. Further, Z is on AC and $\angle BZC = 90°$ since Z lies on the circle with diameter BC. So X, Y, Z have the desired relations.

3. For which numbers n can a square be cut into concave n-gons?

   Solution For $n \ge 5$ this is possible by cutting along the diagonal.



For $n = 4$ this is impossible. Suppose we could divide the square into m concave quadrilaterals. All the m reflex angles must be at different interior points; hence those points contribute a sum of $360°m$ to the total sum of angles of the quadrilateral. Counting the angles of the square, the total sum of angles is at least $360°m + 180°$. However, since each quadrilateral has sum of angles $360°$, this sum also equals $360°m$, contradiction.

4. Let A be a fixed point and l a fixed line. P is a variable point on l. Q is a point on ray AP such that $AP \cdot AQ = k^2$ where k is some constant. Find the locus of Q.

   Solution This is just an inversion of a line with center A and radius of k. Draw a circle through A that intersects the line at S, T such that $AS = AT = k$. The locus of Q is that circle minus the point A.

5. A regular pentagon $ABCDE$ is dilated about anywhere with a dilation of positive magnitude and then rotated $36°$ to pentagon $A'B'C'D'E'$. Find the minimum value of $AA' + BB' + CC' + DD' + EE'$.

   Solution Let the center of dilation be O. Let $A'O$ intersect AB at A'', and define B'', C'', E'', D'' similarly. Since the angle of rotation is $\frac{72°}{2}$, $AA''A'$ is a right angle, and likewise for B, C, D, and E. Then this means that $AA' + BB' + CC' + DD' + EE' \geq AA'' + BB'' + CC'' + DD'' + EE''$.

   Now we claim that $AA'' + BB'' + CC'' + DD'' + EE''$ is constant and equal to half the perimeter. Indeed, this is true when O is the center of $ABCDE$, and if we translate O by a vector $\vec{v}$, then the sum changes by $\vec{v} \cdot (\vec{AB} + \vec{BC} + \vec{CD} + \vec{DE} + \vec{EA}) = 0$.

   The minimum is attainable by dilating $ABCDE$ around O and rotating it so that A', B', C', D', E' are midpoints of AB, BC, CD, DE, EA.

6. Altitudes from B, C meet the angle bisector of $\angle A$ in $\triangle ABC$ at P, Q, respectively. R is such that $PR \parallel AB$ and $QR \parallel AC$. If X is a point such that BX and CX are tangents to the circumcircle of $\triangle ABC$, then prove that A, R, X are collinear.

   Solution Let D, E be the intersection of PR and AC and the intersection of QR and AB, respectively. Let B' and C' be the feet of the perpendiculars from B to AC and C to AB, respectively. Since $AE \parallel DR$ and $AD \parallel ER$,

   $$\angle DPA = \angle PAE = A/2 = \angle QAD = \angle QAE.$$

   Hence $\triangle PAD \sim \triangle QAE$ are similar isosceles triangles. Note $\triangle APB' \sim \triangle AQC'$ since both are right triangles with an angle of $A/2$.

Putting this together,

$$\frac{AD}{AP} = \frac{AE}{AQ} = \frac{AP}{AQ} = \frac{AB'}{AC'} = \frac{AC}{AB}.$$

Since $ADRE$ is a parallelogram, the diagonal AR bisects DE. Thus AR is a median in $\triangle ADE$. However, $\triangle ADE$ and $\triangle ABC$ are linked by a reflection across the angle bisector of A and a homothety. Since the median and symmedian are isogonal, AR is the symmedian from A in $\triangle ABC$. Since AX is the same symmedian, A, R, X are collinear.

4 Number Theory

1. a, b, c, d, e are positive integers satisfying $a^3+b^3+c^3+d^3 = e^3$. Find the largest positive integer n so that n is guaranteed to divide at least one of a, b, c, d, e.

   Solution The answer is 7. Note $x^3 \equiv 0$ or $\pm 1 \pmod 7$. If none of a, b, c, d is 0 modulo 7, then the LHS is either -4, -2, 0, 2, or 4, so it must be 0. Then $7|e$. 7 is the least since $1^3 + 1^3 + 5^3 + 6^3 = 7^3$.

2. Find all triplets of positive integers (a, b, n) that satisfy $a^2 + b^2 = 2^n$.

   Solution Since 2^n is even, a, b are either both even or both odd. If a, b are odd, then $a^2 + b^2 \equiv 1 + 1 \equiv 2 \pmod 4$. Hence $n = 1$, and $a = b = 1$. If a, b are both even, let 2^k be the greatest power of 2 dividing both a, b. Then

   $$\left(\frac{a}{2^k}\right)^2 + \left(\frac{b}{2^k}\right)^2 = 2^{n-2k}.$$

   One of $\frac{a}{2^k}$, $\frac{b}{2^k}$ must be odd, so they are both odd, and equal to 1. Thus all solutions are given by

   $$(a, b, n) = (2^k, 2^k, 2k + 1), k \in \mathbb{N}_0.$$

3. Find all polynomials with integer coefficients $P(x)$ such that

   $$\sum_{i=1}^{\infty} \frac{1}{2010^{P(i)}}$$

   is rational.

   Solution We use the following fact:

   Fact 4.1: Let $n > 2$ be a positive integer. Then the base n-representation of p is periodic if and only if p is rational.

   In order for the sum to converge, $P(i)$ must be nonconstant and eventually positive. There exists L so that $P(i)$ is increasing for $i \geq L$. Then we just need $\sum_{i=L}^{\infty} \frac{1}{2010^{P(i)}}$ to be rational. This sum gives the base 2010 representation; it is rational only if the representation is periodic. The number of 0's between consecutive 1's is $P(i+1) - P(i)$.

If P has degree greater than 1, then $P(i+1) - P(i)$ goes to infinity as $i \to \infty$; hence the base 2010 representation is not periodic. On the other hand, linear P work since then the number of 0's between consecutive 1's is constant. Hence the answer is all linear polynomials with positive leading term.

4. Prove that for any positive integer k there exists an arithmetic sequence $\frac{a_1}{b_1}, \frac{a_2}{b_2}, \ldots, \frac{a_k}{b_k}$ of rational numbers, where a_i, b_i are relatively prime positive integers for each $i = 1, 2, \ldots, k$ such that $a_1, b_1, a_2, b_2, \ldots, a_k, b_k$ are all distinct and $\gcd(b_1, b_2, \ldots, b_k) = 1$.

   Solution Let $a_i = \frac{K\text{lcm}(1,2,\cdots,k)}{i} + 1$ and $b_i = \frac{\text{lcm}(1,2,\cdots k)}{i}$. The $\frac{a_i}{b_i}$ form an arithmetic sequence as

$$\frac{a_i}{b_i} = \frac{\text{lcm}(1,2,\cdots,k) + i}{\text{lcm}(1,2,\cdots,k)}.$$

   Note a_i, b_i are relatively prime, and $\gcd(b_1, \ldots, b_k) = 1$ (as else $\text{lcm}(1, \ldots, k)/\gcd(b_1, \ldots, b_k)$ would be a common multiple of $1, \ldots, k$ as well). Choose K large enough so that all the a_i's are larger than the b_i's; then none of the numbers are equal.

5. Suppose $f(x)$ is a polynomial of degree d taking integer values such that

$$m - n \mid f(m) - f(n)$$

   for all pairs of integers (m, n) satisfying $0 \le m, n \le d$. Is it necessarily true that

$$m - n \mid f(m) - f(n)$$

   for all pairs of integers (m, n)?

   Solution Yes.

   Lemma 4.2: For $n \in \mathbb{N}_0$, let $l_n = \text{lcm}(1, 2, \ldots, n)$ $(l_0 = 1)$.

$$m - n \mid l_i \left[\binom{m}{i} - \binom{n}{i} \right]$$

   for all $m, n \in \mathbb{Z}, i \in \mathbb{N}_0$. (Note $\binom{x}{n}$ is defined as $\frac{x^{\underline{n}}}{n!}$.)

   Proof. We induct on i. For $i = 0$ this is trivial. Suppose it true for $i - 1$. Write the RHS like this:

$$\frac{l_i}{i}\left[m\binom{m-1}{i-1} - n\binom{n-1}{i-1}\right] = \frac{l_i}{i}\left[m\left(\binom{m-1}{i-1} - \binom{n-1}{i-1}\right) + (m-n)\binom{n-1}{i-1}\right]$$

   Since $\frac{l_i}{i}$ is an integer, by the induction hypothesis, $m - n$ divides this expression, finishing the induction step. □

   Lemma 4.3: Let d be the degree of polynomial f. We show that the following are equivalent:

   (a) For every $m, n \in \mathbb{Z}$, $m - n \mid f(m) - f(n)$.

(b) For some set S of $d+1$ consecutive integers, $m-n \mid f(m)-f(n)$ for all $m,n\in S$.

(c) There are $a_0, a_1, \ldots, a_n \in \mathbb{Z}$ with

$$f(x) = a_n l_n \binom{x}{n} + a_{n-1} l_{n-1} \binom{x}{n-1} + \cdots + a_0 l_0 \binom{x}{0}.$$

Proof. The assertions $(a) \Rightarrow (b)$ and $(c) \Rightarrow (a)$ are clear from Lemma 4.2.

Suppose (b) holds. First assume that $S = \{0, 1, \ldots, n\}$. We inductively build the sequence $a_0, a_1, \ldots$ so that the polynomial

$$P_m(x) = a_m l_m \binom{x}{m} + a_{m-1} l_{m-1} \binom{x}{m-1} + \cdots + a_0 l_0 \binom{x}{0}$$

matches the value of $f(x)$ at $x = 0, \ldots, m$. Define $a_0 = f(0)$; once $a_0, \ldots, a_m$ have been defined, let

$$a_{m+1} = \frac{f(m+1) - P_m(m+1)}{l_{m+1}}.$$

Note this is an integer since $m+1 | P_m(m+1) - P_m(0)$ by Lemma 4.2, $m+1 | f(m+1) - f(0)$ by hypothesis, and $f(0) = P_m(0)$. Noting that $\binom{x}{m+1}$ equals 1 at $x = m+1$ and 0 for $0 \le x \le m$, this gives $P_{m+1}(x) = f(x)$ for $x = 0, 1, \ldots, m+1$. Now $P_n(x)$ is a degree n polynomial that agrees with $f(x)$ at $x = 0, 1, \ldots, n$, so they must be the same polynomial.

Now if (b) holds, then by the argument above on a translated function, (c) holds for the translated function and (a) holds; in particular, (b) holds for $S = \{0, 1, \ldots, n\}$. Use the above argument to get the desired representation in (c). □

6. Let n be a positive integer and p a prime satisfying $p > n^2 + 1$. Prove that for any nonzero residue m modulo p, there exist $a_1, \ldots, a_n$, none of them equal to 0, satisfying

$$a_1^n + a_2^n + \cdots + a_n^n \equiv m \pmod{p}.$$

Solution For subsets $A, B \subseteq \mathbb{Z}/p\mathbb{Z}$, let $A + B$ denote $\{a + b \mid a \in A, b \in B\}$. We use the following theorem:

Theorem 4.4 (Cauchy-Davenport)**:** For any $A, B \subseteq \mathbb{Z}/p\mathbb{Z}$,

$$|A + B| \ge \min(p, |A| + |B| - 1).$$

For any $A_1, \ldots, A_n \subseteq \mathbb{Z}/p\mathbb{Z}$,

$$|A_1 + \cdots + A_n| \ge \min(p, |A_1| + \cdots + |A_n| - (n-1)).$$

Note the perfect $g := \gcd(n, p-1)$th powers modulo p are the perfect nth powers modulo p. Indeed, if t is a primitive root, then

$$t^{kg} = t^{kn((n/g)^{-1} \bmod p-1)}.$$

The problem statement is equivalent to $(\mathbb{Z}/p\mathbb{Z})^\times \subseteq \underbrace{A+\cdots+A}_{n}$.

Now the set $A = \{x^n \mid x \neq 0\}$ in $\mathbb{Z}/p\mathbb{Z}$ has at least $\frac{p-1}{g}$ elements, namely t^{kg} for $0 \le k < \frac{p-1}{g}$. By Cauchy-Davenport,

$$\underbrace{|A+\cdots+A|}_{n} \ge n\left(\frac{p-1}{g}\right) - (n-1)$$

If $g < n$, then $g \le n/2$ and this value is at least p, and we are done. So assume $n = p$; then $|A+\cdots+A|$ is equal to

$$p - n > (n-1)\cdot\frac{p-1}{n} + 1.$$

However, $(A+\cdots+A)\backslash\{0\}$ is a multiple of $\frac{p-1}{n}$ since we can partition $(A+\cdots+A)\backslash\{0\}$ into sets of size $\frac{p-1}{n}$, namely, if $a \in (A+\cdots+A)$ then

$$\left\{at^{kn} \mid 0 \le k < \frac{p-1}{n}\right\} \subseteq A.$$

Indeed, if $a = a_1^n + \cdots + a_n^n$ then $at^{kn} = (a_1t^k)^n + \cdots + (a_nt^k)^n$. (In other words $A+\cdots+A$ is a union of cosets of $\{t^{kn}\}$ in the group $(\mathbb{Z}/p\mathbb{Z})^\times$.) Since $|(A+\cdots+A)\backslash\{0\}| > (n-1)\cdot\frac{p-1}{n}$, we have $|(A+\cdots+A)\backslash\{0\}| = p-1$, and $A+\cdots+A$ has all the nonzero residues modulo p.

5 Problem Credits

A1 Holden Lee

A2 Holden Lee

A3 Timothy Chu

A4 Holden Lee

A5 Juan Ignacio Restrepo

A6 Putnam 1985/A6 (suggested by Daniel Vitek)

C1 Holden Lee

C2 Holden Lee and Brian Basham

C3 Based off China 2006/2

C4 Based off AMY 2006 (Pigeonhole Principle)

C5 Holden Lee

C6 *Graph Theory*, by Reinhard Diestel, Exercise 7.11

G1 Alex Anderson

G2 Alex Anderson

G3 Timothy Chu

G4 Alex Anderson

G5 Timothy Chu

G6 suggested by Alex Anderson

N1 Holden Lee

N2 Holden Lee

N3 Timothy Chu

N4 Based off APMO 2009/4

N5 Holden Lee

N6 Holden Lee