14^{th} Annual Harvard-MIT Mathematics Tournament
Saturday 12 February 2011

Team Round A

Warm-Up [50]

1. [**20**] Alice and Barbara play a game on a blackboard. At the start, zero is written on the board. Alice goes first, and the players alternate turns. On her turn, each player replaces x – the number written on the board – with any real number y, subject to the constraint that $0 < y - x < 1$.

   (a) [**10**] If the first player to write a number greater than or equal to 2010 wins, determine, with proof, who has the winning strategy.

   (b) [**10**] If the first player to write a number greater than or equal to 2010 on her 2011th turn or later wins (if a player writes a number greater than or equal to 2010 on her 2010th turn or earlier, she loses immediately), determine, with proof, who has the winning strategy.

   Solution: Each turn of the game is equivalent to adding a number between 0 and 1 to the number on the board.

   (a) Barbara has the winning strategy: whenever Alice adds z to the number on the board, Barbara adds $1-z$. After Barbara's ith turn, the number on the board will be i. Therefore, after Barbara's 2009th turn, Alice will be forced to write a number between 2009 and 2010, after which Barbara can write 2010 and win the game.

   (b) Alice has the winning strategy: she writes any number a on her first turn, and, after that, whenever Barbara adds z to the number on the board, Alice adds $1 - z$. After Alice's ith turn, the number on the board will be $(i - 1) + a$, so after Alice's 2010th turn, the number will be $2009 + a$. Since Barbara cannot write a number greater than or equal to 2010 on her 2010th turn, she will be forced to write a number between $2009 + a$ and 2010, after which Alice can write 2010 and win the game.

2. [**15**] Rachel and Brian are playing a game in a grid with 1 row of 2011 squares. Initially, there is one white checker in each of the first two squares from the left, and one black checker in the third square from the left. At each stage, Rachel can choose to either run or fight. If Rachel runs, she moves the black checker 1 unit to the right, and Brian moves each of the white checkers one unit to the right. If Rachel chooses to fight, she pushes the checker immediately to the left of the black checker 1 unit to the left, the black checker is moved 1 unit to the right, and Brian places a new white checker in the cell immediately to the left of the black one. The game ends when the black checker reaches the last cell. How many different final configurations are possible?

   Solution: Both operations, run and fight, move the black checker exactly one square to the right, so the game will end after exactly 2008 moves regardless of Brian's choices. Furthermore, it is easy to see that if we view running and fighting as operations, they commute. So the order of the moves does not matter, all that matters is how many times Rachel runs and how many times Rachel fights. Each fight adds one white checker to the grid, so two games with different numbers of fights will end up in different final configurations. There are 2009 possible values for the number of fights, so there are 2009 possible final configurations.

3. [**15**] Let n be a positive integer, and let $a_1, a_2, \ldots, a_n$ be a set of positive integers such that $a_1 = 2$ and $a_m = \varphi(a_{m+1})$ for all $1 \leq m \leq n-1$, where, for all positive integers k, $\varphi(k)$ denotes the number of positive integers less than or equal to k that are relatively prime to k. Prove that $a_n \geq 2^{n-1}$.

   Solution: We first note that $\varphi(s) < s$ for all positive integers $s \geq 2$, so $a_m > 2$ for all $m > 1$.

   For integers $s > 2$, let A_s be the set of all positive integers $x \leq s$ such that $\gcd(s, x) = 1$. Since $\gcd(s, x) = \gcd(s, s - x)$ for all x, if a is a positive integer in A_s, so is $s - a$. Moreover, if a is in A_s, a and $s - a$ are different since $\gcd(s, \frac{s}{2}) = \frac{s}{2} > 1$, meaning $\frac{s}{2}$ is not in A_s. Hence we may evenly pair up the elements of A_s that sum to s, so $\varphi(s)$, the number of elements of A_s, must be even. It follows that a_m is even for all $m \leq n-1$.

If $t > 2$ is even, A_t will not contain any even number, so $\varphi(t) \leq \frac{t}{2}$. We may conclude that $a_m \geq 2a_{m-1}$ for all $m \leq n-1$, so $a_n \geq a_{n-1} \geq 2^{n-2}a_1 = 2^{n-1}$, as desired.

Finally, note that such a set exists for all n by letting $a_i = 2^i$ for all i.

Complex Numbers [35]

4. [**15**] Let a, b, and c be complex numbers such that $|a| = |b| = |c| = |a+b+c| = 1$. If $|a-b| = |a-c|$ and $b \neq c$, prove that $|a+b||a+c| = 2$.

Solution:

First Solution. Since $|a| = 1$, a cannot be 0. Let $u = \frac{b}{a}$ and $v = \frac{c}{a}$. Dividing the given equations by $|a| = 1$ gives $|u| = |v| = |1+u+v| = 1$ and $|1-u| = |1-v|$. The goal is to prove that $|1+u||1+v| = 2$.

By squaring $|1-u| = |1-v|$, we get $(1-u)\overline{(1-u)} = (1-v)\overline{(1-v)}$, and thus $1 - u - \bar{u} + |u|^2 = 1 - v - \bar{v} + |v|^2$, or $u + \bar{u} = v + \bar{v}$. This implies $\mathrm{Re}(u) = \mathrm{Re}(v)$. Since u and v are on the unit circle in the complex plane, u is equal to either v or $\bar{v}$. However, $b \neq c$ implies $u \neq v$, so $u = \bar{v}$.

Therefore, $1 = |1+u+\bar{u}| = |1 + 2\,\mathrm{Re}(u)|$. Since $\mathrm{Re}(u)$ is real, we either have $\mathrm{Re}(u) = 0$ or $\mathrm{Re}(u) = -1$. The first case gives $u = \pm i$ and $|1+u||1+v| = |1+i||1-i| = 2$, as desired. It remains only to note that $\mathrm{Re}(u) = -1$ is in fact impossible because u is of norm 1 and $u = -1$ would imply $u = \bar{u} = v$.

Remark: by the rotational symmetry of the circle, it is acceptable to skip the first step of this solution and assume $a = 1$ without loss of generality.

Second Solution. Let a, b, and c, be the vertices of a triangle inscribed in the unit circle in the complex plane. Since the complex coordinate of the circumcenter is 0 and the complex coordinate of the centroid is $\frac{a+b+c}{3}$, it follows from well-known facts about the Euler line that the complex coordinate of the orthocenter is $a+b+c$. Hence the orthocenter lies on the unit circle as well. Is it not possible for the orthocenter not to be among the three vertices of the triangle, for, if it were, two opposite angles of the convex cyclic quadrilateral formed by the three vertices and the orthocenter would each measure greater than 90 degrees. It follows that the triangle is right. However, since $|a-b| = |a-c|$, the right angle cannot occur at b or c, so it must occur at a, and the desired conclusion follows immediately.

5. [**20**] Let a and b be positive real numbers. Define two sequences of real numbers $\{a_n\}$ and $\{b_n\}$ for all positive integers n by $(a+bi)^n = a_n + b_n i$. Prove that

$$\frac{|a_{n+1}| + |b_{n+1}|}{|a_n| + |b_n|} \geq \frac{a^2+b^2}{a+b}$$

for all positive integers n.

Solution: Let $z = a + bi$. It is easy to see that what we are asked to show is equivalent to

$$\frac{|z^{n+1} + \bar{z}^{n+1}| + |z^{n+1} - \bar{z}^{n+1}|}{|z^n + \bar{z}^n| + |z^n - \bar{z}^n|} \geq \frac{2z\bar{z}}{|z+\bar{z}| + |z-\bar{z}|}$$

Cross-multiplying, we see that it suffices to show

$$|z^{n+2} + z^{n+1}\bar{z} + z\bar{z}^{n+1} + \bar{z}^{n+2}| + |z^{n+2} - z^{n+1}\bar{z} + z\bar{z}^{n+1} - \bar{z}^{n+2}|$$
$$+|z^{n+2} + z^{n+1}\bar{z} - z\bar{z}^{n+1} - \bar{z}^{n+2}| + |z^{n+2} - z^{n+1}\bar{z} - z\bar{z}^{n+1} + \bar{z}^{n+2}|$$
$$\geq 2|z^{n+1}\bar{z} + z\bar{z}^{n+1}| + 2|z^{n+1}\bar{z} - z\bar{z}^{n+1}|$$

However, by the triangle inequality,

$$|z^{n+2} + z^{n+1}\bar{z} + z\bar{z}^{n+1} + \bar{z}^{n+2}| + |z^{n+2} - z^{n+1}\bar{z} - z\bar{z}^{n+1} + \bar{z}^{n+2}| \geq 2|z^{n+1}\bar{z} + z\bar{z}^{n+1}|$$

and

$$|z^{n+2} - z^{n+1}\bar{z} + z\bar{z}^{n+1} - \bar{z}^{n+2}| + |z^{n+2} + z^{n+1}\bar{z} - z\bar{z}^{n+1} - \bar{z}^{n+2}| \geq 2|z^{n+1}\bar{z} - z\bar{z}^{n+1}|$$

This completes the proof.

Remark: more computationally intensive trigonometric solutions are also possible by reducing the problem to maximizing and minimizing the values of the sine and cosine functions.

Coin Flipping [75]

In a one-player game, the player begins with $4m$ fair coins. On each of m turns, the player takes 4 unused coins, flips 3 of them randomly to heads or tails, and then selects whether the 4th one is heads or tails (these four coins are then considered used). After m turns, when the sides of all $4m$ coins have been determined, if half the coins are heads and half are tails, the player wins; otherwise, the player loses.

6. [**10**] Prove that whenever the player must choose the side of a coin, the optimal strategy is to choose heads if more coins have been determined tails than heads and to choose tails if more coins have been determined heads than tails.

   Solution: Let $q_n(k)$ be the probability that, with n turns left and $|H-T| = k$, the player wins playing the optimal strategy. Note that k is always even. We prove by induction on n that with n turns left in the game, this is the optimal strategy, and that $q_n(k) \geq q_n(k+2)$.

   Base Case: $n = 1$, if there is one more turn in the game, then clearly if we flip 3 coins and get $|H-T| \geq 3$ then our play does not matter. If we get $|H-T| = 1$ then the optimal strategy is to pick the side so that $|H-T| = 0$. So this is the optimal strategy.

   Now $q_1(0) = \frac{3}{4}$, $q_1(2) = \frac{1}{2}$, $q_1(4) = \frac{1}{8}$ and $q_1(2k) = 0$ for $k \geq 3$. So $q_1(k) \geq q_1(k+2)$ for all k.

   Induction Step: Assume the induction hypothesis for $n-1$ turns left in the game. With n turns left in the game, since $q_{n-1}(k)$ decreases when $k = |H-T|$ increases, a larger value of $|H-T|$ is never more desirable. So picking the side of the coin that minimizes $|H-T|$ is the optimal strategy.

   Now for $k \geq 2$, $q_n(2k) = \frac{1}{8}q_{n-1}(2k-4) + \frac{3}{8}q_{n-1}(2k-2) + \frac{3}{8}q_{n-1}(2k) + \frac{1}{8}q_{n-1}(2k+2)$, and it is clear, by the induction hypothesis that $q_n(2k) \geq q_n(2k+2)$ for all $k \geq 2$. Similar computations make it clear that $q_n(0) \geq q_n(2) \geq q_n(4)$. This completes the induction step.

7. [**15**] Let T denote the number of coins determined tails and H denote the number of coins determined heads at the end of the game. Let $p_m(k)$ be the probability that $|T-H| = k$ after a game with $4m$ coins, assuming that the player follows the optimal strategy outlined in problem 6. Clearly $p_m(k) = 0$ if k is an odd integer, so we need only consider the case when k is an even integer. (By definition, $p_0(0) = 1$ and $p_0(k) = 0$ for $k \geq 1$). Prove that $p_m(0) \geq p_{m+1}(0)$ for all nonnegative integers m.

   Solution:

   First solution. Using the sequences $q_n(k)$ defined above, it is clear that $q_{n+1}(0) = \frac{3}{4}q_n(0) + \frac{1}{4}q_n(2) \leq q_n(0)$. So $q_{n+1}(0) \leq q_n(0)$. Now note that for $k = 0$, $p_n(k) = q_n(k)$, because they are both equal to the probability that after n turns of the optimal strategy $|H-T| = 0$ (this is only true for $k = 0$). It follows that $p_{n+1}(0) \leq p_n(0)$.

   Second solution. When we play the game with $n+1$ turns, there is a $\frac{3}{4}$ chance that after 1 turn $|H-T| = 0$ and a $\frac{1}{4}$ chance that $|H-T| = 2$.

   Now suppose we play the game, and get 2 tails and 1 heads on the first turn. Consider the following two strategies for the rest of the game.

   Strategy A: We pick the fourth coin to be heads, and play the optimal strategy for the other n turns. Our probability of winning is $p_n(0)$.

   Strategy B: We pick the fourth coin to be heads with probability $\frac{3}{4}$ and tails with probability $\frac{1}{4}$, then proceed with the optimal strategy for the rest of the game. This is equivalent to throwing the first 3 coins over again and applying the optimal strategy. Our probability of winning is $p_{n+1}(0)$.

By the theorem in the previous problem, Strategy A is the optimal strategy, and thus our probability of winning employing Strategy B does not exceed our probability of wining employing Strategy A. So $p_n(0) \geq p_{n+1}(0)$.

8. (a) [**5**] Find a_1, a_2, and a_3, so that the following equation holds for all $m \geq 1$:

$$p_m(0) = a_1 p_{m-1}(0) + a_2 p_{m-1}(2) + a_3 p_{m-1}(4)$$

(b) [**5**] Find b_1, b_2, b_3, and b_4, so that the following equation holds for all $m \geq 1$:

$$p_m(2) = b_1 p_{m-1}(0) + b_2 p_{m-1}(2) + b_3 p_{m-1}(4) + b_4 p_{m-1}(6)$$

(c) [**5**] Find c_1, c_2, c_3, and c_4, so that the following equation holds for all $m \geq 1$ and $j \geq 2$:

$$p_m(2j) = c_1 p_{m-1}(2j-2) + c_2 p_{m-1}(2j) + c_3 p_{m-1}(2j+2) + c_4 p_{m-1}(2j+4)$$

Solution: We will show how to find a_1 in the first equation; other coefficients can be evaluated in the same way. a_1 is the probability that, beginning with $|T-H| = 0$, the value of $|T-H|$ remains 0 after using the optimal strategy for one round. This only happens when the first three coins are not all heads or all tails. Therefore, $a_1 = \frac{3}{4}$. It follows that $b_1 = \frac{1}{4}$. The rest of the terms are the binomial coefficients of the expansion of $(\frac{1+1}{2})^3$.

(a) $a_1 = \frac{3}{4}, a_2 = \frac{1}{2}, a_3 = \frac{1}{8}$.
(b) $b_1 = \frac{1}{4}, b_2 = \frac{3}{8}, b_3 = \frac{3}{8}, b_4 = \frac{1}{8}$.
(c) $c_1 = \frac{1}{8}, c_2 = \frac{3}{8}, c_3 = \frac{3}{8}, c_4 = \frac{1}{8}$.

9. [**15**] We would now like to examine the behavior of $p_m(k)$ as m becomes arbitrarily large; specifically, we would like to discern whether $\lim_{m\to\infty} p_m(0)$ exists and, if it does, to determine its value. Let $\lim_{m\to\infty} p_m(k) = A_k$.

(a) [**5**] Prove that $\frac{2}{3}p_m(k) \geq p_m(k+2)$ for all m and k.
(b) [**10**] Prove that A_0 exists and that $A_0 > 0$. Feel free to assume the result of analysis that a non-increasing sequence of real numbers that is bounded below by a constant c converges to a limit that is greater than or equal to c.

Solution:

(a) We proceed by induction.
Base Case: When $n = 1$, we get $\frac{2}{3}p_1(0) = \frac{2}{3} \cdot \frac{3}{4} = \frac{1}{2} > \frac{1}{4} = p_1(2)$. And since $p_1(2k) = 0$ for $k \geq 2$, we get $\frac{2}{3}p_1(k) \geq p_1(k+2)$ for all k.
Induction Step: Assume that $\frac{2}{3}p_i(k) \geq p_i(k+2)$ for all $i \leq n$. This clearly implies $\frac{2}{3}p_{n+1}(k) \geq p_{n+1}(k+2)$ for all $k \geq 4$ by the formula (c) from the previous problem.
Now, for $k = 2$,

$$\begin{aligned}
\frac{2}{3}p_{n+1}(2) &= \frac{2}{3}\left(\frac{1}{4}p_n(0) + \frac{3}{8}p_n(2) + \frac{3}{8}p_n(4) + \frac{1}{8}p_n(6)\right) \\
&\geq \frac{1}{12}p_n(0) + p_{n+1}(4) \\
&\geq p_{n+1}(4)
\end{aligned}$$

by the formula (b) from the previous problem and our induction hypothesis.
For $k = 0$, we write out formula (a) from the previous problem.

$$\begin{aligned}
\frac{2}{3}p_{n+1}(0) &= \frac{2}{3}\left(\frac{3}{4}p_n(0) + \frac{1}{2}p_n(2) + \frac{1}{8}p_n(4)\right) \\
&\geq \frac{1}{4}p_n(0) + \frac{3}{8}p_n(2) + \frac{1}{2}p_n(4) + \frac{1}{8}p_n(6)
\end{aligned}$$

by our induction hypothesis. But $p_{n+1}(2) = \frac{1}{4}p_n(0) + \frac{3}{8}p_n(2) + \frac{3}{8}p_n(4) + \frac{1}{8}p_n(6)$, which is clearly less than the last line above. Thus $\frac{2}{3}p_{n+1}(0) \geq p_{n+1}(2)$. This completes the induction step.

Remark: This is nowhere near the strongest bound. We intentionally asked for a bound strong enough to be helpful in part b, but not strong enough to help with other problems. The strongest bound is $p_n(0) \geq \frac{2+\sqrt{5}}{2}p_n(2)$ and $p_n(2k) \geq (2+\sqrt{5})p_n(2k+2)$ for $k \geq 1$. This is intuitive because $A_0 = \frac{2+\sqrt{5}}{2}A_2$ and for $k \geq 1$, $A_{2k} = (2+\sqrt{5})A_{2k+2}$.

(b) For any n and k, $p_n(2k) \leq (\frac{2}{3})^k p_n(0)$. Now

$$1 = \sum_{k=0}^{\infty} p_n(2k) \leq p_n(0) \sum_{k=0}^{\infty} \left(\frac{2}{3}\right)^k = 3p_n(0).$$

So $p_n(0) \geq \frac{1}{3}$ for all n. This means $p_n(0)$ is a non-increasing sequence that is bounded below by $\frac{1}{3}$. So A_0 exists and $A_0 \geq \frac{1}{3} > 0$.

10. [**20**] Once it has been demonstrated that $\lim_{n\to\infty} p_n(0)$ exists and is greater than 0, it follows that $\lim_{n\to\infty} p_n(k)$ exists and is greater than 0 for all even positive integers k and that $\sum_{k=0}^{\infty} A_{2k} = 1$. It also follows that $A_0 = a_1A_0 + a_2A_2 + a_3A_4$, $A_2 = b_1A_0 + b_2A_2 + b_3A_4 + b_4A_6$, and $A_{2j} = c_1A_{2j-2} + c_2A_{2j} + c_3A_{2j+2} + c_4A_{2j+4}$ for all positive integers $j \geq 2$, where a_1, a_2, a_3, b_1, b_2, b_3, b_4, and c_1, c_2, c_3, c_4 are the constants you found in problem 8. Assuming these results, determine, with proof, the value of A_0.

Solution: By our recurrence relations,

$$\frac{1}{4}A_0 = \frac{1}{2}A_2 + \frac{1}{8}A_4$$

$$\frac{5}{8}A_2 = \frac{1}{4}A_0 + \frac{3}{8}A_4 + \frac{1}{8}A_6$$

and

$$\frac{5}{8}A_{2k} = \frac{1}{8}A_{2k-2} + \frac{3}{8}A_{2k+2} + \frac{1}{8}A_{2k+4}$$

for all $k \geq 2$. So the terms A_{2k} ($k \geq 1$) satisfy a linear recurrence with characteristic equation $x^3 + 3x^2 + 1 = 5x$. The roots of the characteristic equation are 1 and $-2 \pm \sqrt{5}$, so for $k \geq 2$, $A_{2k} = c_1 + c_2(-2+\sqrt{5})^k + c_3(-2-\sqrt{5})^k$. But clearly, $\lim_{k\to\infty} A_{2k} = 0$, so $c_1 = c_3 = 0$. Thus for $k \geq 2$, we are left with $A_{2k} = c_2(-2+\sqrt{5})^k = A_4(-2+\sqrt{5})^{k-2}$.

Now, since $\sum_{k=0}^{\infty} A_{2k} = 1$, we get $1 = A_0 + A_2 + A_4\sum_{j=0}^{\infty}(\sqrt{5}-2)^j = A_0 + A_2 + \frac{A_4}{1-(\sqrt{5}-2)} = A_0 + A_2 + \frac{3+\sqrt{5}}{4}A_4$.

We now have the following equations.

$$1 = A_0 + A_2 + \frac{3+\sqrt{5}}{4}A_4$$

$$0 = 2A_0 - 4A_2 - A_4$$

$$0 = 2A_0 - 5A_2 + 3A_4 + A_6 = 2A_0 - 5A_2 + (1+\sqrt{5})A_4$$

We have three equations with three unknowns. Solving this linear system gives $A_0 = \frac{\sqrt{5}-1}{2}$.

Remark: The fact that $A_0 = \frac{\sqrt{5}-1}{2} > \frac{1}{2}$ means that for arbitrarily large n, the player wins more often than they lose, so the player is at an advantage. In addition the final answer is the reciprocal of the golden ratio, which is simply beautiful.

The probabilistic experiment explored in this problem is a type of random walk. A random walk is an infinite set of moves in some set (usually the R^n lattice but sometimes weird shapes or even fractals) where each move is determined by a random variable. The most basic random walk is a walk on the real line, where the walker starts at 0, and at every move has probability $\frac{1}{2}$ of moving one unit to the left, and probability $\frac{1}{2}$ of moving one unit to the right.

The random walk explored in this problem is what is known as a 'biased' random walk, where the probabilities of movement are asymmetric, and weighted towards a certain direction or outcome. In this example the choice of the side of 1 out of every 4 coins biases the walk towards the origin.

An interesting inquiry for the reader to ponder is, what is the value of A_0 if the game is played with 6 coins flipped each turn, or 8, or $2m$. If the limits A_{2k} exist, they will satisfy a linear recurrence with characteristic equation $\left(\frac{x+1}{2}\right)^{2m-1} = x^{m-1}$, as is evident from this problem, where we solved the $m = 2$ case.

We now give proofs that A_k exists for all even k, and that $\sum_{k=0}^{\infty} A_{2k} = 1$

First note that we can use the inductive argument in problem 9a to prove the stronger bound $p_n(0) \geq \frac{2+\sqrt{5}}{2} p_n(2)$ and $p_n(2k) \geq (2+\sqrt{5})p_n(2k+2)$ for all $k \geq 1$.

Now,

$$p_{n+2}(0) + \frac{1}{4}p_{n+1}(2) = \frac{3}{4}p_{n+1}(0) + \frac{3}{4}p_{n+1}(2) + \frac{1}{8}p_{n+1}(4)$$

$$= \frac{3}{4}p_n(0) + \frac{43}{64}p_n(2) + \frac{27}{64}p_n(4) + \frac{9}{64}p_n(6) + \frac{1}{64}p_n(8)$$

$$= p_{n+1}(0) + \frac{11}{64}p_n(2) + \frac{19}{64}p_n(4) + \frac{9}{64}p_n(6) + \frac{1}{64}p_n(8)$$

$$= p_{n+1}(0) + \frac{1}{4}p_n(2) - \frac{5}{64}p_n(2) + \frac{19}{64}p_n(4) + \frac{9}{64}p_n(6) + \frac{1}{64}p_n(8)$$

$$\leq p_{n+1}(0) + \frac{1}{4}p_n(2)$$

So $p_{n+1}(0) + p_n(2)$ is a non-increasing sequence that is bounded below, so it converges to a limit, call it $A_0 + A_2$. Now $A_2 = -\lim_{n\to\infty} p_{n+1}(0) + \lim_{n\to\infty}(p_{n+1}(0) + p_n(2)) = \lim_{n\to\infty} p_n(2)$.

So $\lim_{n\to\infty} p_n(2)$ exists. It follows from our recursions that A_{2k} exists for all k. Since $p_n(2k) \geq 0$ for all k, it follows that all the A_i are non-negative.

Now we must show that $\sum_{k=0}^{\infty} A_{2k} = 1$. This is not immediately clear because, while a finite sum of limits of sequences equals the limit of the finite sum of the sequences, the sum of the limits does not necessarily equal the limit of the sum if it is an infinite sum.

Now it follows from part 8a, that for any $\epsilon > 0$ there exists N such that $\sum_{k=0}^{N} p_n(2k) > 1 - \frac{\epsilon}{2}$ for all n.

So $\sum_{k=0}^{N} A_{2k} \geq 1 - \frac{\epsilon}{2} > 1 - \epsilon$. Since $A_{2k} \geq 0$ for all k, $\sum_{k=0}^{\infty} A_{2k} \geq 1$.

Now if $\sum_{k=0}^{\infty} A_{2k}$ is greater than 1, or diverges, then there exists a pair j and $\epsilon > 0$ such that $\sum_{k=0}^{j} A_{2k} = 1 + \epsilon$. But, $\sum_{k=0}^{j} p_n(2k) \leq 1$ for all n, so $\sum_{k=0}^{j} A_{2k} \leq 1$, contradiction.

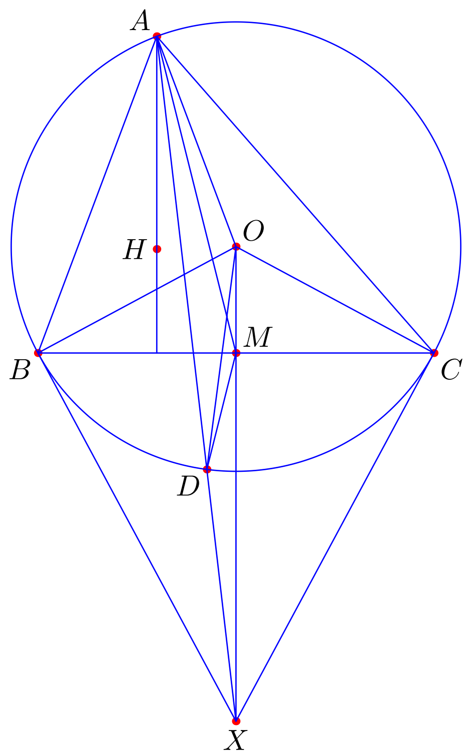
So $\sum_{k=0}^{\infty} A_{2k} = 1$.

Geometry [90]

11. [**20**] Let ABC be a non-isosceles, non-right triangle, let ω be its circumcircle, and let O be its circumcenter. Let M be the midpoint of segment BC. Let the circumcircle of triangle AOM intersect ω again at D. If H is the orthocenter of triangle ABC, prove that $\angle DAH = \angle MAO$.

Solution:

First solution.



Let X be the intersection of the line tangent to ω at B with the line tangent to ω at C. Note that $\triangle OMC \sim \triangle OCX$ since $\angle OMC = \angle OCX = \frac{\pi}{2}$. Hence $\frac{OM}{OC} = \frac{OC}{OX}$, or, equivalently, $\frac{OM}{OA} = \frac{OA}{OX}$. By SAS similarity, it follows that $\triangle OAM \sim \triangle OXA$. Therefore, $\angle OAM = \angle OXA$.

We claim now that $\angle OAD = \angle OAX$. By the similarity $\triangle OAM \sim OXA$, we have that $\angle OAX = \angle OMA$. Since $AOMD$ is a cyclic quadrilateral, we have that $\angle OMA = \angle ODA$. Since $OA = OD$, we have that $\angle ODA = \angle OAD$. Combining these equations tells us that $\angle OAX = \angle OAD$, so A, D, and X are collinear.

Finally, since both AH and OX are perpendicular to BC, it follows that $AH \parallel OX$, so $\angle DAH = \angle DXO = \angle AXO = \angle MAO$, as desired.

Second solution.

Let Y be the intersection of BC with the line tangent to ω at A. Then the circumcircle of triangle AOM has diameter OY, so AD is perpendicular to OY because the radical axis of two circles is perpendicular to the line between their centers. Since Y is on the polar of A, it follows that A is on the polar of Y, so $AD \perp OX$ implies that AD is the polar of Y, i.e. AD is the symmedian from A in triangle ABC. Hence AD and AM are isogonal. Since AH and AO are also isogonal, the desired conclusion follows immediately.

Remark: with sufficient perserverance, angle-chasing solutions involving only the points given in the diagram may also be devised.

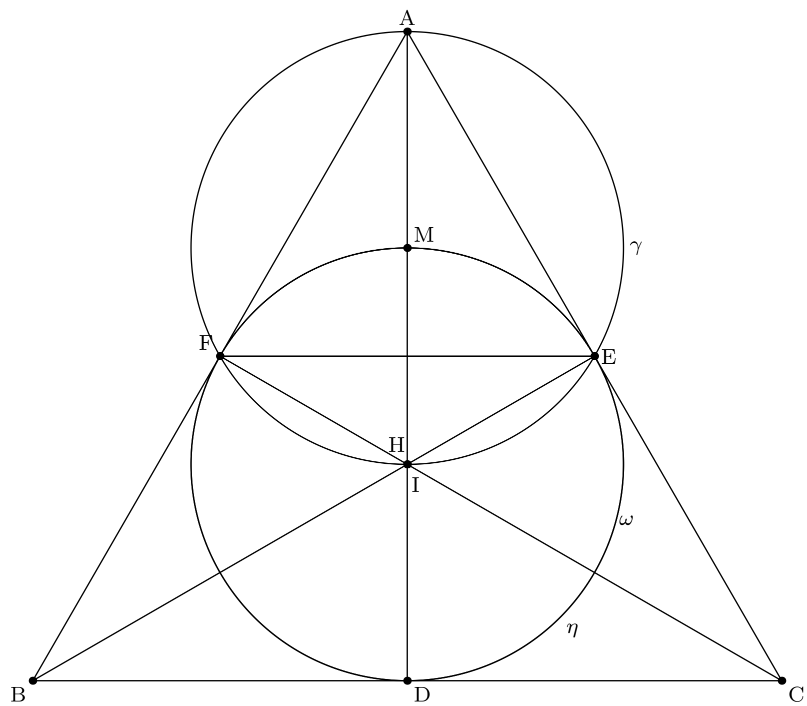
12. [**70**] Let ABC be a triangle, and let E and F be the feet of the altitudes from B and C, respectively. If A is not a right angle, prove that the circumcenter of triangle AEF lies on the incircle of triangle ABC if and only if the incenter of triangle ABC lies on the circumcircle of triangle AEF.

Solution:

This problem is arguably the most difficult among all those appearing in the 2011 Harvard-MIT Mathematics Tournament. Do not feel badly if your team wasted time in a vain attempt to find a solution. It was intended by the author as a serious test for serious geometers.

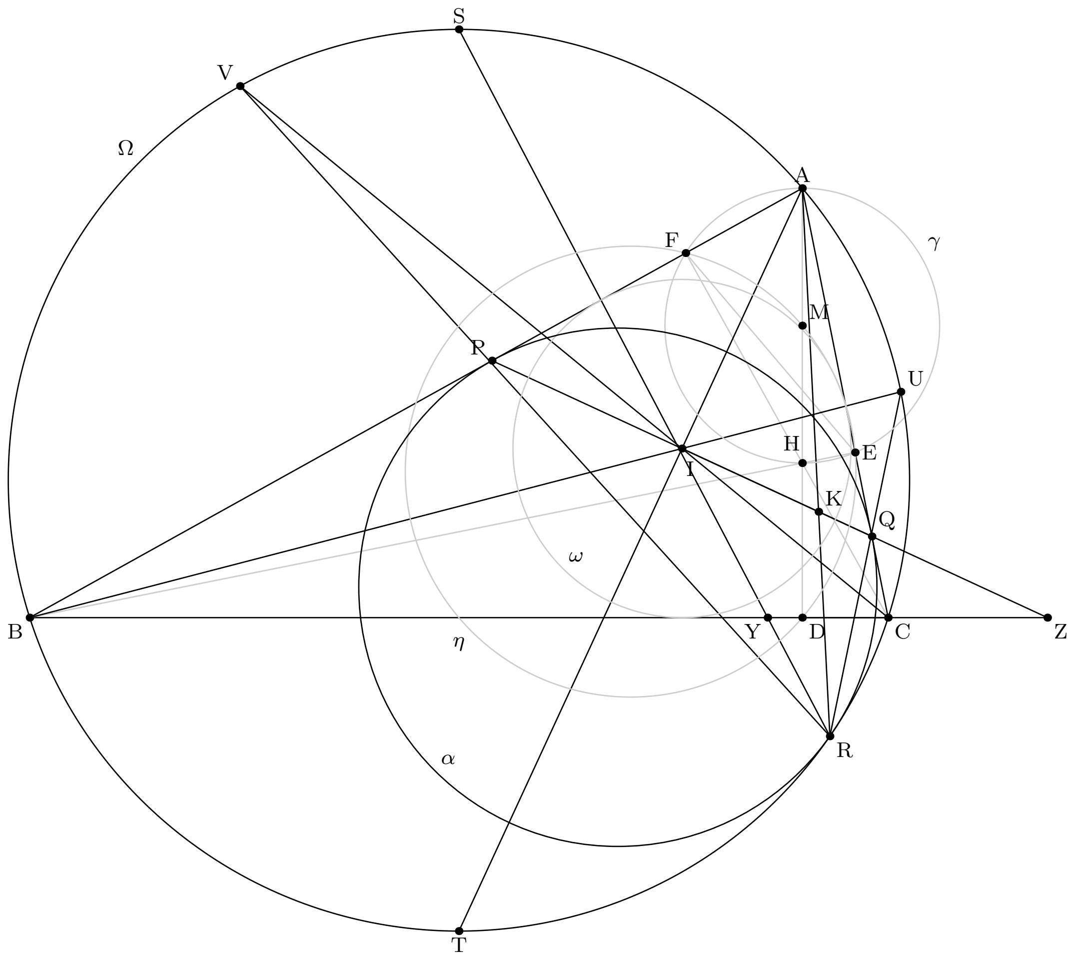
Let D be the foot of the altitude from A. Let H be the orthocenter of triangle ABC. Let M be the midpoint of AH. Let I be the incenter of triangle ABC. Let ω be the incircle of triangle ABC. Let γ be the circumcircle of AEF. Let η be the nine-point circle of triangle ABC.

We first dispense with the case in which $AB = AC$. Since M is the circumcenter of triangle AEF, if the circumcenter of triangle AEF lies on the incircle of triangle ABC, then ω and η intersect in two points: M and D. Since ω and η are tangent by Feuerbach's Theorem, it follows that ω and η are coincident, in which case triangle ABC is equilateral.

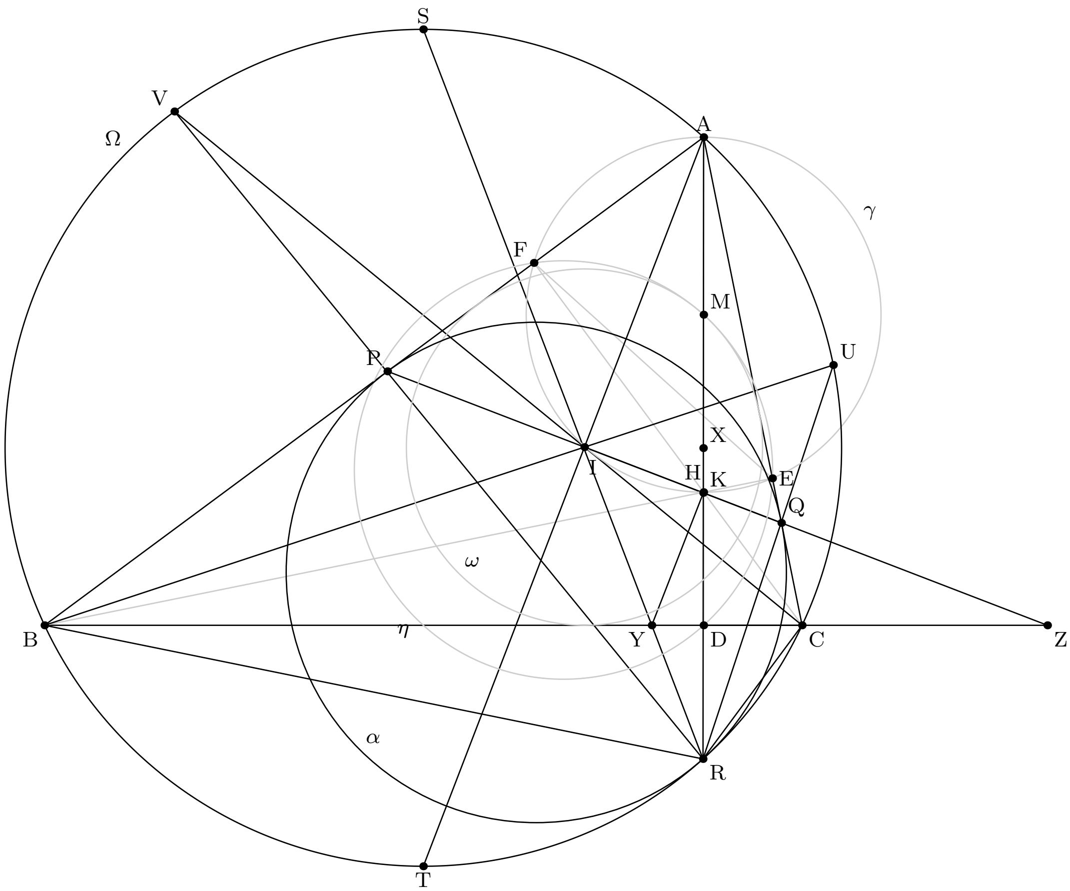


If the incenter of triangle ABC lies on the circumcircle of triangle AEF, then A, I, and H lie on γ. Since no circle may intersect a line in three distinct points and A is distinct from I and H, it follows that I and H are coincident, in which case triangle ABC is equilateral. Since it is clear that if ABC is equilateral, M lies on ω and I lies on γ, this completes the proof in the case that $AB = AC$.

Throughout the remainder of this solution, we assume that $AB \neq AC$. Let Ω be the circumcircle of triangle ABC, and let α be the A-mixtilinear incircle. Let α be tangent to AB at P, to AC at Q, and to Ω at R. Since $AB \neq AC$, lines PQ and BC are not parallel. Let their intersection be Z, and let the bisectors of $\angle A$, $\angle B$, and $\angle C$ intersect Ω at T, U, and V, respectively. Let the point diametrically opposite T on Ω be S. Let lines RS and BC intersect at Y. We introduce a lemma here, namely that I lies on PQ and that Y and Z are harmonic conjugates with respect to B and C.



Let lines AR and PQ intersect at K. Since PA and QA are tangent to α at P and Q, respectively, RK is the symmedian from R in triangle PQR. By Pascal's Theorem applied to cyclic hexagon $ACVRUB$, points Q, I, and P are collinear. Since $AP = AQ$ and AI bisects $\angle PAQ$, I is the midpoint of PQ. Hence RI is the median from R in triangle PQR. It follows that $\angle ICQ = \angle PRA = \angle IRQ$ and $\angle IBP = \angle QRA = \angle IRP$. Hence quadrilaterals $RBPI$ and $RCQI$ are cyclic, so RI is the bisector of $\angle BRC$. It follows also that $\angle BIP = \angle BCI$, so line PQ is tangent to the circumcircle of triangle BIC at I. Since T is the circumcenter of triangle BIC and S is diametrically opposite T on Ω, BS and CS are tangent to the circumcircle of triangle BIC at B and C, respectively. It follows that IS is the symmedian from I in triangle BIC; since RI is the bisector of $\angle BRC$, R, I, and S are collinear. Hence RS is the polar of Z with respect to the circumcircle of triangle BIC, so Y and Z are harmonic conjugates with respect to B and C, as desired.



We now take up the main problem. We first prove that I lies on γ if M lies on ω. If M lies on ω, then M is the Feuerbach point. Let X be the center of the homothety of positive magnitude mapping ω to Ω. Since the center of the homothety of positive magnitude ω to η is M and the center of the homothety of positive magnitude mapping η to Ω is H, it follows by Monge's Circle Theorem that X lies on line MH. Note that R is the center of the homothety of positive magnitude mapping α to Ω. Since the center of homothety of positive magnitude mapping α to ω is A, it follows by the same theorem that R lies on line AX, so points A, M, H, and R are collinear.

Note that triangle BRC is the reflection of triangle BHC about line BC. Since line RY bisects angle BRC, it follows that line HY bisects $\angle BHC$. Let the line through H parallel to PQ intersect BC at Z'. Since $\angle HBA = \angle HCA$, the internal bisectors of $\angle BAC$ and $\angle BHC$ are parallel. Since PQ is perpendicular to AI and BZ' is parallel to PQ, it follows that BZ' is the external bisector of $\angle BHC$. Hence Y and Z' are harmonic conjugates with respect to B and C. It follows that Z and Z' are coincident, and, therefore, that H and K are coincident. We may conclude that $\angle AIH$ is right, which implies the desired result because γ is the circle on diameter AH. (Do think carefully about why this argument fails if $AB = AC$).

Conversely, if I lies on γ, then $\angle AIH$ is right, so points P, H, I, and Q are collinear. Since PQ is perpendicular to AI and the interal bisectors of $\angle BAC$ and $\angle BHC$ are parallel, it follows that PQ is the external bisector of $\angle BHC$. Let the internal bisector of $\angle BHC$ intersect BC at Y'. Then Y' and Z are harmonic conjugates with respect to B and C, so Y and Y' are coincident. Let R' be the reflection of H about line BC. Clearly $R'Y$ is the bisector of $\angle BR'C$, so R', Y, and S are collinear. Since R, Y, and S are collinear and R' also lies on Ω, it follows that R and R' are coincident. Since HR' is perpendicular to BC, it follows that points A, H, and R are collinear.

Let X' be the center of the homothety of positive magnitude mapping ω to Ω. Since the center of the homothety of positive magnitude mapping ω to α is A, and the center of the homothety of positive magnitude mapping α to Ω is R, it follows by Monge's Circle Theorem that X' lies on line AR. Note that H is the center of the homothety of positive magnitude mapping Ω to η. Since the center of the homothety of positive magnitude mapping ω to η is the Feuerbach point, it follows by the same theorem that the Feuerbach point lies on line AR as well. Since AR intersects η at M and D, the Feuerbach point may be either M or D. However, D may not be the Feuerbach point, else the the altitude from A and the bisector of $\angle A$ in triangle ABC would be coincident, contradicting the assumption that $AB \neq AC$. We may conclude that M is the Feuerbach point, so, in particular, M lies on ω, as desired. This completes the proof.

Remark: more computationally intensive solutions are also possible; in particular, it may be observed that the condition $IJ = AM$ is equivalent to the condition $MD/DA' = IJ/JA'$, where J denotes the point where ω is tangent to BC and A' denotes the midpoint of BC. It is left to the reader to determine how to proceed. Let ABC be a triangle, and let E and F be the feet of the altitudes from B and C, respectively. If A is not a right angle, prove that the circumcenter of triangle AEF lies on the incircle of triangle ABC if and only if the incenter of triangle ABC lies on the circumcircle of triangle AEF.

Last Writes [110]

13. [**30**] Given positive integers a and b such that $a > b$, define a sequence of ordered pairs (a_l, b_l) for nonnegative integers l by $a_0 = a$, $b_0 = b$, and $(a_{l+1}, b_{l+1}) = (b_l, a_l \mod b_l)$, where, for all positive integers x and y, $x \mod y$ is defined to be the remainder left by x upon division by y. Define $f(a, b)$ to be the smallest positive integer j such that $b_j = 0$. Given a positive integer n, define $g(n)$ to be $\max_{1 \leq k \leq n-1} f(n, k)$.

   (a) [**15**] Given a positive integer m, what is the smallest positive integer n_m such that $g(n_m) = m$?

   (b) [**15**] What is the second smallest?

Solution:

(a) The answer is F_{m+1}, where $F_1 = 1$,$F_2 = 2$, and $F_{i+1} = F_i + F_{i-1}$ for all $i \geq 2$.

We consider a reverse sequence as follows: starting at $p_0 = (k_0, 0)$ for some positive integer k_0, at each step we can take a pair $p_i = (r_i, s_i)$ to any pair $p_{i+1} = (s_i + k_{i+1}r_i, r_i) = (r_{i+1}, s_{i+1})$ for some positive integer k_{i+1}. It is clear that any such sequence is the reverse of a legal sequence. Thus, n_m is equal to the smallest possible value of the first integer in a possible p_m of a reverse sequence. The pair p_m is uniquely determined by the choice of $k_0, k_1, \ldots, k_m$, and lowering any k_i lowers the first number of p_m. Thus, the minimum possible value occurs when all k_i are equal to 1. In this case, $p_0 = (1, 0), p_1 = (2, 1)$, and $p_{i+1} = (r_i + s_i, r_i)$. It is apparent that $p_i = (F_{i+1}, F_i)$, so the minimum is F_{m+1}.

(b) The answer is L_{m+1}, where $L_1 = 1$,$L_2 = 3$, and $L_{i+1} = L_i + L_{i-1}$.

The only integer n satisfying $g(n) = 1$ is 2, as it is the only positive integer $n > 1$ such that all integers $1 \leq i < n$ divide n. Thus, for $m = 1$, there is no such second smallest integer.

For $m \geq 2$, we once again consider all possible reverse sequences. For any sequence, characterized by $k_0, \ldots, k_m$, if there are at least two k_i not equal to 1, then we can find a smaller possible value (of r_{m+1}) not equal to the minimum possible by setting any one of these k_i to 1. Similarly, if any k_i is at least 3, we can find a smaller possible value not equal to the minimum by setting this k_i to be 2. Thus, the second smallest obtainable value of r_{m+1} must occur when $k_i = 1$ for all $0 \leq i \leq m$ except for some k_j which is equal to 2.

We now claim that the value of r_m is minimized with respect to the above conditions by letting $k_1 = 2$, and $k_i = 1$ for all other $0 \leq i \leq m$. Doing so yields $r_m = L_{m+1}$, with $\{L_i\}$ defined as in the answer. Before we begin our proof, we first note that letting $k_0 = 2$ instead yields $r_m = 2F_{m+1}$, which is strictly larger than L_{m+1} (since it is larger for $m = 1, 2$, andboth sequences satisfy the same recurrence). We therefore assume that $k_0 = 1$.

Proof of claim. Our recurrences for pairs give us that $r_{i+1} = k_{i+1}r_i + s_i, s_{i+1} = r_i$. Thus, we have $r_{i+1} = k_{i+1}r_i + r_{i-1}$. Now suppose we have $k_j = 2$ for a particular j, and for all $i \neq j, 0 \leq i \leq m$, we have $k_i = 1$. Then we have $r_0 = 1, r_1 = 1 + k_1$, and for $2 \leq i \leq m, i \neq j$, we have $r_i = r_{i-1} + r_{i-2}$. We also have $r_j = 2r_{j-1} + r_{j-2}$.

By our reasoning in part (a), $r_i = F_{i+1}$ for $i < j$. Thus, $r_j = 2F_j + F_{j-1} = F_{j+1} + F_j = F_{j+2}$ (where we define $F_0 = 1$). Expressing r_{j-1} as $F_{j+1} - F_{j-1}$, we find $r_{j+1} = F_{j+3} - F_{j-1}, r_{j+2} = F_{j+4} - F_{j-1}, r_{j+3} = F_{j+5} - 2F_{j-1}$, and so on. It is easy to show by induction that for $i > j$, we have $r_i = F_{i+2} - F_{i-j-1}F_{j-1}$. Thus, to minimize $r_m = F_{m+2} - F_{m-j-1}F_{j-1}$, we must maximize $F_{m-j-1}F_{j-1}$.

We claim that $F_{m-j-1}F_{j-1} \leq F_{m-2}$ for $1 \leq j \leq m$.

Proof of claim. It is easy to see (and in fact well-known) that for all positive integers n, F_n counts the number of distinct ways to tile a $1 \times n$ board with 1×1 squares and 1×2 dominoes. Thus $F_{m-j-1}F_{j-1}$ counts the number of ways to tile a $1 \times m - 2$ board with 1×1 squares and 1×2 dominoes such that the $j - 1$th and jth square are not both covered by the same domino, which is at most the number of ways to tile a $1 \times m - 2$ board, as desired.

Since this minimum is reached by letting $j = 1$, we may conclude that the answer is indeed L_{m+1}.

14. [**25**] Given a positive integer n, a sequence of integers $a_1, a_2, \ldots, a_r$, where $0 \leq a_i \leq k$ for all $1 \leq i \leq r$, is said to be a "*k-representation*" of n if there exists an integer c such that

$$\sum_{i=1}^{r} a_i = \sum_{i=1}^{r} a_i k^{c-i} = n.$$

Prove that every positive integer n has a k-*representation*, and that the k-*representation* is unique if and only if 0 does not appear in the base-k representation of $n - 1$.

Solution: Given a positive integer n, a sequence of integers $a_1, a_2, \ldots, a_r$, where $0 \leq a_i \leq k$ for all $1 \leq i \leq r$, is said to be a "*k-representation*" of n if there exists an integer c such that

$$\sum_{i=1}^{r} a_i = \sum_{i=1}^{r} a_i k^{c-i} = n.$$

Prove that every positive integer n has a k-*representation*, and that the k-*representation* is unique if and only if 0 does not appear in the base-k representation of $n - 1$.

Equivalently, a k-representation is given by a sequence $a_p, \ldots, a_q$, for some $p < q$, such that

$$\sum_{i=p}^{q} a_i = \sum_{i=p}^{q} a_i k^i.$$

We first show existence. Let the representation of $n - 1$ in base k be given by $\sum_{i=0}^{r} a_i k^i = n - 1$. Let $l = \sum_{i=1}^{r} a_i(k^{i-1} + k^{i-2} + \cdots + 1)$. Now we extend the sequence $\{a_i\}$ by letting $a_i = k - 1$ if $-l + 1 \leq i \leq -1$ and $a_{-l} = k$. We claim that $a_{-l}, \ldots, a_{r-1}, a_r$ is a k-representation of n. Indeed,

$$\begin{aligned}
\sum_{i=-l}^{r} a_i k^i &= (n-1) + \left(\sum_{i=-l}^{-1} (k-1)n^i\right) + k^{-l} \\
&= (n-1) + (k-1)k^{-1}\frac{1-k^{-l}}{1-k^{-1}} + k^{-l} = n \\
\sum_{i=-l}^{r} a_i &= \left(\sum_{i=0}^{r} a_i\right) + l(k-1) + 1 \\
&= \left(\sum_{i=0}^{r} a_i\right) + \left(\sum_{i=1}^{r} a_i(k^i - 1)\right) + 1 \\
&= \left(\sum_{i=0}^{r} a_i k^i\right) + 1 = n
\end{aligned}$$

Now suppose there is another k-representation $\{b_i\}$ of n; then $\sum b_i = \sum b_i k^i = n$. This implies that $\sum c_i = \sum c_i k^i = 0$ where $c_i = a_i - b_i$. The following claim specifies all possibilities of $\{c_i\}$.

Claim: Suppose that $\sum_{i=p}^{q} c_i k^i = 0$, where $c_i, p, q \in \mathbb{Z}$, $p < q$, and $c_i \in [-k, k]$. Then the sequence $\{c_i\}$ must be the concatenation of subsequences of the form

$$\pm(1, 1-k, 1-k, \ldots, 1-k, -k)$$

, possibly with 0's in between.

Proof. If c_i is not the zero sequence, then without loss of generality, we may assume $c_q > 0$.

Since $\sum_{i=p}^{q} c_i k^i = 0$, we have

$$|c_q k^q| = |c_{q-1}k^{q-1} + \ldots + c_p k^p| \leq k^q + k^{q-1} + \ldots + k^{p+1} < \frac{k}{k-1} k^q \leq 2k^q$$

so $c_q = 1$. Now we have

$$k^q + c_{q-1}k^{q-1} + \ldots + c_p k^p = 0. \tag{1}$$

This means $(k + c_{q-1})k^{q-1} + \ldots + c_p k^p = 0$. Hence, as above,

$$|(k + c_{q-1})k^{q-1}| = |c_{q-2}k^{q-2} + \ldots + c_p k^p| < 2k^{q-1}.$$

Therefore, $|(k + c_{q-1})| < 2$, which means $c_{q-1} = -k$ or $-k+1$.

If $c_{q-1} = -k$, then $c_q k^q + c_{q-1}k^{q-1} = 0$, and we get a subsequence $(1, -k)$.

If $c_{q-1} = -k+1$, then $c_q k^q + c_{q-1}k^{q-1} = k^{q-1}$. Thus

$$k^{q-1} + c_{q-2}k^{q-2} + \ldots + c_p k^p = 0,$$

which has the exact same form as (1). We can then repeat this procedure to obtain a subsequence $(1, 1-k, 1-k, \ldots, 1-k, -k)$.

Once we have such a subsequence, the terms in the sum $\sum_{i=p}^{q} c_i k^i = 0$ corresponding to that subsequence sum to 0, so we may remove them and apply the same argument. □

We now consider the cases.

If the base k representation of $n-1$ contains no 0's, then $a_i \neq 0$ so it is impossible to have $c_i = a_i - b_i = -k$. On the other hand, we know that c_i is composed of subsequences of the form $\pm(1, 1-k, 1-k, \ldots, 1-k, -k)$. Therefore, if $\{c_i\}$ is not the zero sequence, then the fact that $\sum c_i = 0$ implies that we must have both a subsequence $(1, 1-k, 1-k, \ldots, 1-k, -k)$ and a subsequence $-(1, 1-k, 1-k, \ldots, 1-k, -k)$, meaning that there exists i for which $c_i = -k$, contradiction.

If the base k representation of $n-1$ contains a 0, then picking the largest i such that $a_i = 0$, we can change a_i to k and a_{i+1} to $a_{i+1} - 1$, and append a $(1, -k)$ to the end of the sequence. This yields another k-representation of n, so a k-representation of n is unique if and only if the base k representation of $n-1$ contains no 0's, as desired.

15. [**55**] Denote $\{1, 2, ..., n\}$ by $[n]$, and let S be the set of all permutations of $[n]$. Call a subset T of S *good* if every permutation σ in S may be written as $t_1 t_2$ for elements t_1 and t_2 of T, where the product of two permutations is defined to be their composition. Call a subset of U of S *extremely good* if every permutation σ in S may be written as $s^{-1}us$ for elements s of S and u of U. Let τ be the smallest value of $|T|/|S|$ for all good subsets T, and let υ be the smallest value of $|U|/|S|$ for all extremely good subsets U. Prove that $\sqrt{\upsilon} \geq \tau$.

    Solution: Denote $\{1, 2, ..., n\}$ by $[n]$, and let S be the set of all permutations of $[n]$. Call a subset T of S *good* if every permutation σ in S may be written as $t_1 t_2$ for elements t_1 and t_2 of T, where the product of two permutations is defined to be their composition. Call a subset of U of S *extremely good* if every permutation σ in S may be written as $s^{-1}us$ for elements s of S and u of U. Let τ be the smallest value of $|T|/|S|$ for all good subsets T, and let υ be the smallest value of $|U|/|S|$ for all extremely good subsets U. Prove that $\sqrt{\upsilon} \geq \tau$.

Call an element $t \in S$ an *involution* if and only if t^2 is the identity permutation. We claim that the set of all involutions in S constitutes a good subset of S. The proof is simple. Let s be an arbitrary permutation in S. Note that s may be decomposed into a product of disjoint cycles of length at least 2, and suppose that there are m such cycles in its decomposition. For $1 \leq i \leq m$, let l_i denote the length of the ith cycle, so that s may be written as

$$(a_{1,1}a_{1,2}\ldots a_{1,l_1})(a_{2,1}a_{2,2}\ldots a_{2,l_2})\ldots(a_{m,1}a_{m,2}\ldots a_{m,l_m})$$

for some pairwise distinct elements

$$a_{1,1}, a_{1,2}, \ldots, a_{1,l_1}, a_{2,1}, a_{2,2}, \ldots, a_{2,l_2}, \ldots, a_{m,1}, a_{m,2}, \ldots, a_{m,l_m}$$

of $[n]$. Consider the permutations q and r defined by $q(a_{i,j}) = a_{i,l_i+1-j}$ for all $1 \leq j \leq l_i$ and $r(a_{i,1}) = a_{i,1}$ and $r(a_{i,k}) = a_{i,l_i+2-k}$ for all $2 \leq k \leq l_i$, for all $1 \leq i \leq m$, and by $q(x) = r(x) = x$ for all $x \in [n]$ otherwise. Since $q, r \in S$, $q^2 = r^2 = 1$, and $rq = s$, it follows that the set of all involutions in S is indeed good, as desired.

For all integer partitions λ of n, let f^λ denote the number of standard Young tableaux of shape λ. By the Robinson-Schensted-Knuth correspondence, the permutations of $[n]$ are in bijection with pairs of standard Young tableaux of the same shape in such a way that the involutions of $[n]$ are in bijection with pairs of identical standard Young tableaux. In other words, the number of permutations of $[n]$ is equal to the number of pairs of identically shaped standard Young tableaux whose shape is a partition of n, and the number of involutions of $[n]$ is equal to the number of standard Young tableaux whose shape is a partition of n. Hence $n! = \sum_\lambda (f^\lambda)^2$ and $\tau \leq \sum_\lambda \frac{f^\lambda}{n!}$, where both sums range over all partitions λ of n.

For all elements $u \in S$, define the conjugacy class of u to be the set of elements that may be written in the form $s^{-1}us$ for some $s \in S$. It is easy to see that for all $u, u' \in S$, the conjugacy classes of u and u' are either identical or disjoint. It follows that S may be partitioned into disjoint conjugacy classes and that any extremely good subset of S must contain at least one element from each distinct conjugacy class. We claim that the number of distinct conjuguacy classes of S is at least the number of integer partitions of n. It turns out that the two numbers are in fact equal, but such a result is not necessary for the purposes of this problem. Let u be an arbitrary permutation in S. Recall that u may be written as

$$(a_{1,1}a_{1,2}\ldots a_{1,l_1})(a_{2,1}a_{2,2}\ldots a_{2,l_2})\ldots(a_{m,1}a_{m,2}\ldots a_{m,l_m})$$

for some pairwise distinct elements

$$a_{1,1}, a_{1,2}, \ldots, a_{1,l_1}, a_{2,1}, a_{2,2}, \ldots, a_{2,l_2}, \ldots, a_{m,1}, a_{m,2}, \ldots, a_{m,l_m}$$

of $[n]$. Associate to the conjugacy class of u the partition $n = l_{w_1} + l_{w_2} + \ldots + l_{w_m} + 1 + \ldots + 1$, where $w_1, w_2, \ldots, w_m$ is a partition of $1, 2, \ldots, m$ such that $w_1 \geq w_2 \geq \ldots \geq w_m$ and the 1's represent all the fixed points of s. Now note that if s is any permutation in S, $s^{-1}us$ may be written in the form

$$s^{-1}(a_{1,1}a_{1,2}\ldots a_{1,l_1})ss^{-1}(a_{2,1}a_{2,2}\ldots a_{2,l_2})s\ldots s^{-1}(a_{m,1}a_{m,2}\ldots a_{m,l_m})s,$$

which may be written as

$$(b_{1,1}b_{1,2}\ldots b_{1,l_1})(b_{2,1}b_{2,2}\ldots b_{2,l_2})\ldots(b_{m,1}b_{m,2}\ldots b_{m,l_m})$$

for some pairwise distinct elements

$$b_{1,1}, b_{1,2}, \ldots, b_{1,l_1}, b_{2,1}, b_{2,2}, \ldots, b_{2,l_2}, \ldots, b_{m,1}, b_{m,2}, \ldots, b_{m,l_m}$$

of $[n]$ because multiplying by s^{-1} on the left and by s on the right is equivalent to re-indexing the letters $1, 2, \ldots, n$. Hence if partitions of n are associated to all conjugacy classes of S analogously, the same partition that is associated to u is associated to $s^{-1}us$ for all $s \in S$. Since exactly one partition is associated to each conjugacy class, it follows that the number of conjugacy classes cannot exceed the number of partitions, as desired.

To conclude, we need only observe that $\upsilon \geq \sum_\lambda \frac{1}{n!}$ by our above claim, for then

$$n!\sqrt{\upsilon} = \sqrt{n! \sum_\lambda 1} = \sqrt{\left(\sum_\lambda \left(f^\lambda\right)^2\right)\left(\sum_\lambda 1\right)} \geq \sum_\lambda f^\lambda \geq n!\tau$$

by the Cauchy-Schwarz inequality, and this completes the proof.

Remark: more computationally intensive solutions that do not use Young tableaux but instead calculate the number of involutions explicitly and make use of the generating function for the number of integer partitions are also possible.