The University of Sydney
School of Mathematics and Statistics
NSW 2006 Australia

Sydney University Mathematical Society Problem Competition 2009

1. The sisters Alice, Bess, and Cath have become proficient at factorizing numbers, so their father David invents a puzzle for them. He chooses three secret integers a, b, c, all greater than 1, and then puts a sticker on Alice's forehead showing the number bc (the product of b and c), one on Bess' forehead showing ac, and one on Cath's forehead showing ab. Each of the girls can see her sisters' stickers but not her own, and must try to work out the number on her own sticker, knowing how the numbers were derived. After a few seconds' thought, Alice says smugly "I know my number". Bess then says "I wasn't sure about my number at first, but knowing that Alice knows hers, I know mine". Even after hearing her sisters' comments, Cath can't work out the number on her sticker; but when David gives her the hint that it is even, she can. What is a?

Solution. Note that for Alice, knowing the numbers ab and ac, the knowledge of her number bc is equivalent to the knowledge of a, since $a = \sqrt{\frac{(ab)(ac)}{bc}}$. The fact that she was able to determine a knowing only ab and ac means that a is the unique common proper divisor of ab and ac which is greater than 1. Hence either $\gcd(ab, ac)$ is prime and different from ab and ac, or $\gcd(ab, ac)$ is the square of a prime and equal to either ab or ac. Since $\gcd(ab, ac) = a\gcd(b, c)$, there are three cases:
(i) a is prime and $\gcd(b, c) = 1$;
(ii) a is prime, $b = a$, and $a \mid c$; or
(iii) a is prime, $c = a$, and $a \mid b$.
But if case (ii) held, then b would be the unique common proper divisor of ab and bc which is greater than 1, so Bess would have been able to work out her number right from the beginning, without needing to hear Alice's comment. Similarly, if case (iii) held, Cath would have been able to work out her number right from the beginning. So case (i) must hold. Moreover, after Alice and Bess make their comments, Cath knows every fact we have used so far, so she can deduce that case (i) must hold.

Cath also knows the numbers $u = ac$ and $v = bc$. If $u \nmid v$, then $\gcd(u, v)$ must be c, since a is prime; in this case Cath would be able to work out her number. So it must be that $u \mid v$, i.e. $a \mid b$; since $\gcd(b, c) = 1$, this implies that $a \nmid c$. This fully explains Bess' ability to work out her number, knowing (as she did by that point) ab and bc and the fact that a is prime. Note that it is not possible that $a = b$, because then Bess would have seen the same two numbers that Alice saw, and would have been able to work out her number right from the beginning. Conversely, the fact that $a \neq b$ explains Bess' inability to work out her number when she knew only ab and bc, whose greatest common divisor is composite and different from ab and bc (being equal to b, although Bess didn't know that originally).

So Cath is faced with two composite numbers u and v, where $u \mid v$ and $u \neq v$; equivalently, one composite number u and one number x greater than 1 (set $x = v/u$). She needs to find a prime divisor p of u such that $p \nmid u/p$ (i.e. p occurs only once in the prime factorization of u), and $\gcd(u/p, x) = 1$; the secret numbers are then $a = p$, $b = px$, and $c = u/p$, and Cath's own number is p^2x. Since she cannot work out her number based on this information, there must be more than one prime p satisfying these requirements. However, the information that p^2x is even is enough to specify it completely; so x cannot itself be even, and we must have $p = 2$. So the answer to the question is that $a = 2$. (There is not enough information to determine b and c, but it could be, for example, that $b = 10$ and $c = 3$; the sticker numbers would then be 30 for Alice, 6 for Bess, and 20 for Cath, and events could transpire as stated in the question.)

2. In this problem, a *word* is a finite string of capital letters (not necessarily meaningful in English) in which no letter occurs in two consecutive positions. Thus AFARSFA and BEGEB are words, but ABBA is not. A word is *palindromic* if, like BEGEB, it reads the same backwards as forwards (a single letter counts as a palindromic word, but the empty word does not). We say that a word W is *contained* in another word W' if the letters of W occur in the right order among the letters of W', not necessarily consecutively. For instance, AFRFA, S and FASF are all contained in AFARSFA (as is AFARSFA itself), but SRA is not. Prove that if a word W is n letters long, there are at least n palindromic words which are contained in W.

Solution. Let W be the string $a_1a_2\cdots a_n$. If $n = 0$ (i.e. W is the empty word), then the statement is vacuously true; if $n = 1$ (i.e. W is a single letter), then W itself is palindromic. When $n \geq 2$, we may assume by induction that there are at least $n - 1$ palindromic words contained in $a_1a_2\cdots a_{n-1}$, so it suffices to find a palindromic word which is contained in W but not in $a_1a_2\cdots a_{n-1}$. Suppose that a_n is the letter X and a_{n-1} is the letter Y: by assumption, Y is different from X. Let V be the longest word contained in W which has the form XYXYX$\cdots$YX (possibly the length is just 1, and V consists of the single letter X). If V were contained in $a_1a_2\cdots a_{n-1}$, then it would have to be contained in $a_1a_2\cdots a_{n-2}$ since it does not end with a Y; so we could attach $a_{n-1}a_n$ to V to create a longer word of the same form, contradicting maximality. So V is the desired palindromic word contained in W but not in $a_1a_2\cdots a_{n-1}$.

We can go a bit further and describe which words W of length n contain exactly n palindromic words. Suppose that $W = a_1a_2\cdots a_n$ has this property. Then there must be exactly one palindromic word contained in $a_1a_2\cdots a_k$ which is not contained in $a_1a_2\cdots a_{k-1}$, for all $k = 3, 4, \cdots, n$. This would certainly be the case if the letter a_k does not occur in $a_1a_2\cdots a_{k-1}$. If a_k is the letter X and does occur in $a_1a_2\cdots a_{k-1}$, then the word V constructed as above using a_{k-1} as Y is one palindromic word contained in $a_1a_2\cdots a_k$ which is not contained in $a_1a_2\cdots a_{k-1}$, and V has length ≥ 3. If a_{k-2} is a letter Z different from X, then we would get another such word V' of the form XZXZX$\cdots$ZX, contrary to assumption. So a_{k-2} must be the same letter X as a_k. Hence the occurrences of each letter in W must be in a sequence of positions $a_s, a_{s+2}, a_{s+4}, \cdots, a_{s+2m}$ which are consecutive among the positions of that parity. It is not hard to see that this condition is also sufficient for W to contain exactly n palindromic words.

3. A *repeating number* is a positive integer whose decimal expression consists of two or more occurrences of the same block of digits: examples are 44, 575757, and 616616. Show that there is no repeating number whose square is also a repeating number.

Solution. Suppose for a contradiction that m is a repeating number such that m^2 is also a repeating number. By definition, we have $m = (10^{(p-1)k} + 10^{(p-2)k} + \cdots + 10^k + 1)n$, where n is a k-digit number which is the repeating block, and $p \geq 2$ is the number of occurrences of the block. Note that m has pk digits, so m^2 must have either $2pk - 1$ or $2pk$ digits. Since m^2 is a repeating number, it is divisible by some number of the form $10^{(q-1)\ell} + 10^{(q-2)\ell} + \cdots + 10^\ell + 1$, where $q\ell$ is the number of digits of m^2 and $q \geq 2$. That is, we have

$$\frac{10^{q\ell}-1}{10^\ell - 1} \,\bigg|\, \left(\frac{10^{pk}-1}{10^k-1}\right)^2 n^2. \tag{1}$$

We now distinguish two cases and find a contradiction in each.
Case 1: $q\ell = 2pk - 1$ (which rules out $q = 2$). In this case, since

$$\begin{aligned} 10^{q\ell} - 1 &= 10^{pk-1}(10^{pk}-1) + (10^{pk-1} - 1) \text{ and} \\ 10^{pk} - 1 &= 10(10^{pk-1} - 1) + 9, \end{aligned}$$

the Euclidean algorithm says that $\gcd(10^{q\ell} - 1, 10^{pk} - 1) = 9$. Hence

$$\gcd\left(\frac{10^{q\ell}-1}{9}, \frac{10^{pk}-1}{9}\right) = 1, \text{ which implies } \gcd\left(\frac{10^{q\ell}-1}{10^\ell-1}, \frac{10^{pk}-1}{10^k-1}\right) = 1.$$

Combining this with (1), we conclude that $\frac{10^{q\ell}-1}{10^\ell-1}$ divides n^2. But

$$\frac{10^{q\ell}-1}{10^\ell-1} > 10^{(q-1)\ell} \geq 10^{\frac{2}{3}(2pk-1)} \geq 10^{2k} > n^2,$$

so we have a contradiction.
Case 2: $q\ell = 2pk$. In this case, we have $10^{q\ell} - 1 = (10^{pk}+1)(10^{pk}-1)$. Note that $10^{pk} + 1$ is coprime to $10^{pk} - 1$, since they differ by 2 and are odd. So from (1) we conclude that

$$10^{pk} + 1 \,\bigg|\, \frac{10^\ell - 1}{(10^k-1)^2} n^2$$

But since $n \leq 10^k - 1$,

$$\frac{10^\ell - 1}{(10^k-1)^2} n^2 \leq 10^\ell - 1 \leq 10^{\frac{q\ell}{2}} - 1 = 10^{pk} - 1 < 10^{pk} + 1,$$

so we have a contradiction.

4. Let $a_1, a_2, a_3, \cdots$ be positive real numbers such that $\sum_{n=1}^{\infty} a_n = 1$. Show that $\sum_{n=1}^{\infty} (a_1 a_2 \cdots a_n)^{1/n}$ converges to a value strictly less than e.

Solution. Set $b_n = \dfrac{(n+1)^n}{n^{n-1}}$ for all positive integers n, so that $b_1 b_2 \cdots b_n = (n+1)^n$. Then we have the following chain of equalities and inequalities (where the convergence of each infinite series follows from that of the next):

$$\begin{aligned}
\sum_{n=1}^{\infty}(a_1 a_2 \cdots a_n)^{1/n} &= \sum_{n=1}^{\infty} \frac{(a_1 b_1 a_2 b_2 \cdots a_n b_n)^{1/n}}{(b_1 b_2 \cdots b_n)^{1/n}} \\
&\leq \sum_{n=1}^{\infty} \frac{\frac{1}{n}(a_1 b_1 + a_2 b_2 + \cdots + a_n b_n)}{n+1} \qquad \text{(AM–GM inequality)} \\
&= \sum_{m=1}^{\infty} a_m b_m \sum_{n=m}^{\infty} \frac{1}{n(n+1)} \\
&= \sum_{m=1}^{\infty} a_m b_m \frac{1}{m} \\
&= \sum_{m=1}^{\infty} a_m \left(\frac{m+1}{m}\right)^m \\
&< e\left(\sum_{m=1}^{\infty} a_m\right) = e,
\end{aligned}$$

because $(\frac{m+1}{m})^m$ is an increasing function of m which tends to e as $m \to \infty$.

5. Let A_n be the $n \times n$ matrix whose (i,j)-entry is 1 if $n \leq i+j \leq n+1$ and zero otherwise. Find the eigenvalues of A_n.

Solution. Let $P_n(x) = \det(x1_n - A_n)$ denote the characteristic polynomial of A_n; we need to find the roots of this polynomial. Considering small values of n, we have $P_0(x) = 1$ (the only reasonable definition of determinant of an empty matrix), and $P_1(x) = x - 1$, with root 1. Now suppose that $n \geq 2$. Expanding the determinant along the last row, we have $P_n(x) = xP_{n-1}(x) - (-1)^{n+1}Q_{n-1}(x)$, where $Q_{n-1}(x)$ is the determinant of the matrix obtained from $x1_n - A_n$ by deleting its nth row and 1st column. Expanding the latter determinant along its last column, we find that $Q_{n-1}(x) = -(-1)^{1+(n-1)}P_{n-2}(x)$, so

$$P_n(x) = xP_{n-1}(x) - P_{n-2}(x), \text{ for all } n \geq 2.$$

Now we claim that

$$P_n(2\cos\theta) = \frac{\cos\frac{(2n+1)\theta}{2}}{\cos\frac{\theta}{2}},$$

for all $n \geq 0$ and $0 \leq \theta < \pi$. The $n = 0$ and $n = 1$ cases are easy, so assume that $n \geq 2$ and that the claim is known for $n-1$ and $n-2$. Then

$$P_n(2\cos\theta) = \frac{2\cos\theta\cos\frac{(2n-1)\theta}{2} - \cos\frac{(2n-3)\theta}{2}}{\cos\frac{\theta}{2}} = \frac{\cos\frac{(2n+1)\theta}{2}}{\cos\frac{\theta}{2}},$$

proving the claim by induction. It follows that $P_n(x) = 0$ when $x = 2\cos\frac{(2k+1)\pi}{(2n+1)}$ for $k = 0, 1, 2, \cdots, n-1$. Since $\cos$ is strictly decreasing on $[0,\pi)$, these n values of x are all distinct, and hence they are all the roots of $P_n(x)$.

6. Peg solitaire is sometimes played with an array of pegs which form an equilateral triangle, except that initially there is one position left empty. A move consists of jumping a peg over an adjacent peg into an empty position on the other side, where the line of motion is parallel to one of the sides of the triangle; the peg which was jumped over is then removed. The aim is to have only one peg remaining at the end. (Videos of such a 'Peg Puzzle' can be found online.)

By contrast, the four-dimensional beings in the neighbouring universe play solitaire with an array of pegs forming a regular tetrahedron, initially with one peg missing. A move now affects four consecutive positions rather than three: it consists of jumping a peg over an adjacent peg *and* over a third peg on the other side of that, into an empty position on the other side of the third peg, where the line of motion is parallel to one of the edges of the tetrahedron; *both* pegs which were jumped over are then removed. The aim is to have only one peg or two adjacent pegs remaining at the end. Show that if the initial empty position is in the exact centre of the tetrahedron, this aim cannot be achieved.

Solution. The positions in the tetrahedral array can be labelled by the 4-tuples (a_1, a_2, a_3, a_4) of nonnegative integers such that $a_1 + a_2 + a_3 + a_4 = n - 1$, where n is the number of positions along each edge (we can obviously assume that $n \geq 2$). The number of such 4-tuples is $\binom{n+2}{3} = \frac{n(n+1)(n+2)}{6}$. Two positions are adjacent if their difference is $(1, -1, 0, 0)$ or $(1, 0, -1, 0)$ or any other rearrangement of those coordinates.

The four vertex positions are $(n-1, 0, 0, 0), (0, n-1, 0, 0), (0, 0, n-1, 0), (0, 0, 0, n-1)$. For the centre of the tetrahedron to be an integral position, we must have $n = 4k + 1$ for some positive integer k; the centre is then (k, k, k, k). The initial number of pegs is then $\dfrac{32k^3 + 48k^2 + 22k}{3}$, which is even. Since two pegs are removed in every move, the number of pegs must remain even, so it is impossible to finish with one peg. We need to rule out the possibility of finishing with two adjacent pegs.

We define quantities m_1, m_2, m_3, m_4 (which change as the game progresses) by

$$\begin{aligned} m_i = {} & \text{number of pegs in a position with odd } i\text{th coordinate} \\ & - \text{number of pegs in a position with even } i\text{th coordinate}. \end{aligned}$$

Since the total number of pegs is always even, each m_i is always even. Consider the effect on these m_i's of a move in the direction of the vector $(1, -1, 0, 0)$. If the initial position of the moving peg has an even 1st coordinate, then its final position has an odd 1st coordinate, and of the two pegs which are removed, one has an even 1st coordinate and one has an odd 1st coordinate. So m_1 would increase by 2 in this case; if on the other hand the initial position of the moving peg had an odd 1st coordinate, then m_1 would decrease by 2. Similarly, the effect of the move on m_2 is either to increase it by 2 or to decrease it by 2. Since all the positions involved have the same 3rd coordinate, the effect of the move on m_3 is either to increase it by 2 or to decrease it by 2, depending on whether that coordinate is even or odd; similarly for m_4. The upshot is that if we consider the 4-tuple (m_1, m_2, m_3, m_4) modulo 4, then every move adds $(2, 2, 2, 2)$ to it.

Now the initial configuration of pegs is symmetric under permutations of the coordinates, so the initial value of (m_1, m_2, m_3, m_4) modulo 4 is either $(0, 0, 0, 0)$ or $(2, 2, 2, 2)$ (which of the two it is depends on the parity of k). Hence it must always be either $(0, 0, 0, 0)$ or $(2, 2, 2, 2)$. But for a configuration of just two adjacent pegs, (m_1, m_2, m_3, m_4) modulo 4 obviously consists of two 0's (corresponding to the coordinates which are the same for the two pegs) and two 2's (corresponding to the coordinates which are different for the two pegs). So we have our desired contradiction.

7. Define a sequence of integers $a_0, a_1, a_2, \cdots$ by the initial condition $a_0 = 1$ and the recurrence relation $a_n = \displaystyle\sum_{k=1}^{n} \binom{n-1}{k-1} k!\, a_{n-k}$ for $n \geq 1$. Prove that $a_n - 1$ is always a multiple of n.

Solution. We claim that a_n equals the number of ways to split n objects into ordered lists: in other words, the number of ways to partition $\{1, 2, \cdots, n\}$ into disjoint nonempty subsets and then order each of these subsets (without putting an ordering on the set of subsets). For example, $a_3 = 13$, and there are thirteen ways to split $\{1, 2, 3\}$ into ordered lists:

$$123,\ 132,\ 213,\ 231,\ 312,\ 321,\ 12|3,\ 21|3,\ 13|2,\ 31|2,\ 23|1,\ 32|1,\ 1|2|3,$$

where the vertical lines mark off a new list. We can prove this by induction on n (the $n = 0$ base case is clear). In a partition of $\{1, 2, \cdots, n\}$ as above, the size k of the subset containing the number n can be anything from 1 to n. For fixed k, the number of ways to choose the other $k - 1$ elements of the subset is $\binom{n-1}{k-1}$, the number of ways to order the subset is $k!$, and the number of ways to partition the remaining $n - k$ elements into disjoint ordered subsets is a_{n-k} by the induction hypothesis. Hence the number of ways to partition $\{1, 2, \cdots, n\}$ into disjoint ordered subsets is $\displaystyle\sum_{k=1}^{n} \binom{n-1}{k-1} k!\, a_{n-k} = a_n$, and the claim is proved.

We can now find a (non-closed) formula for a_n by considering the sizes of the subsets in a partition of $\{1, 2, \cdots, n\}$; these sizes form a partition of the number n. For any fixed partition $n = k_1 + k_2 + \cdots + k_\ell$ (where the k_i's are positive integers, in no specific order), we can count the partitions of $\{1, 2, \cdots, n\}$ into ordered subsets of these sizes: choosing the elements of the subset of size k_1, then the elements of the subset of size k_2, and so forth would result in $n!$, but this overcounts by a factor of $\prod_{a\geq 1} m_a(k_\bullet)!$, where $m_a(k_\bullet)$ is the number of times the number a occurs among the k_i's, because we do not want to have a specified order on the set of subsets. Hence

$$a_n = \sum_{\text{partition } k_\bullet \text{ of } n} \frac{n!}{\prod_{a\geq 1} m_a(k_\bullet)!},$$

where every fraction in the sum is in fact an integer. Now the denominator $\prod_{a\geq 1} m_a(k_\bullet)!$ always divides $(\sum_{a\geq 1} m_a(k_\bullet))!$ (the quotient of the latter by the former is a multinomial coefficient). So it always divides $(n-1)!$, except in the sole case for which $\sum_{a\geq 1} m_a(k_\bullet) \geq n$, namely the case of the partition $n = 1 + 1 + \cdots + 1$. So aside from this term $\frac{n!}{n!}$, every term is a multiple of n, and thus $a_n - 1$ is a multiple of n.

8. A regular polygon may be defined as a convex polygon whose vertices all lie on a circle and whose edges all have the same length. A *semi-regular* polygon is a convex polygon which has an even number of vertices all lying on a circle, such that the lengths of its edges, in clockwise order, are $a, b, a, b, \cdots, a, b$ for some $a \neq b$. (For instance, a non-square rectangle is semi-regular.) Prove that, given any regular polygon P, it is possible to construct with straightedge and compass a semi-regular polygon Q which has the same perimeter-length as P and encloses the same area as P.

Solution. For any polygon X, let $\sigma(X)$ denote the quantity $\dfrac{\text{perimeter}(X)^2}{\text{area}(X)}$, which is clearly unchanged after scaling X. It suffices to construct a semi-regular Q such that $\sigma(Q) = \sigma(P)$, because there are then well-known methods (using similar triangles) of re-scaling Q so that it has the same perimeter as P, and hence also the same area. We may as well stipulate that the vertices of Q lie on a circle of radius 1. Here we can take any constructible length (such as the edge-length of P, for example) as the unit of measurement.

Now if P has n vertices (where $n \geq 3$) and circumradius r, its perimeter is $2nr\sin(\frac{\pi}{n})$ and its area is $\frac{1}{2}nr^2\sin(\frac{2\pi}{n})$, so

$$\sigma(P) = \frac{\big(2nr\sin(\frac{\pi}{n})\big)^2}{\frac{1}{2}nr^2\sin(\frac{2\pi}{n})} = 4n\tan(\frac{\pi}{n}).$$

This is a strictly decreasing function of n which tends to 4π (i.e. the σ-value of a circle) as n tends to infinity, because $\frac{\tan(x)}{x}$ is an increasing function on $(0, \frac{\pi}{2})$ which tends to 1 as $x \to 0$.

Suppose that Q is semi-regular with $2k$ vertices (for some $k \geq 2$) and circumradius 1, and let a and b denote its two edge-lengths, as in the question; assume that $a < b$. Then $a = 2\sin(\frac{\pi}{2k} - \theta)$ and $b = 2\sin(\frac{\pi}{2k} + \theta)$ for a unique angle θ satisfying $0 < \theta < \frac{\pi}{2k}$. We have

$$\begin{aligned}\sigma(Q) &= \frac{k^2(2\sin(\frac{\pi}{2k} - \theta) + 2\sin(\frac{\pi}{2k} + \theta))^2}{k(\frac{1}{2}\sin(\frac{\pi}{k} - 2\theta) + \frac{1}{2}\sin(\frac{\pi}{k} + 2\theta))} \\ &= \frac{k^2(4\sin(\frac{\pi}{2k})\cos\theta)^2}{k\sin(\frac{\pi}{k})\cos 2\theta} \\ &= 8k\tan(\frac{\pi}{2k})\frac{\cos^2\theta}{\cos 2\theta} \\ &= 4k\tan(\frac{\pi}{2k})\,(1 + \sec 2\theta).\end{aligned}$$

Thus $\sigma(Q)$ is a strictly increasing continuous function of θ, which tends to $8k\tan(\frac{\pi}{2k})$ (the σ-value of a regular $2k$-gon) as $\theta \to 0$ and tends to $4k\tan(\frac{\pi}{k})$ (the σ-value of a regular k-gon) as $\theta \to \frac{\pi}{2k}$. We conclude that if $k < n < 2k$, there is a unique value of θ for which $\sigma(Q) = \sigma(P)$.

We are now free to choose k in a convenient way. If n is not a power of 2, there is a unique power of 2, namely $k = 2^{\lfloor \log_2(n) \rfloor}$, such that $k < n < 2k$; if n is a power of 2, then $k = \frac{3n}{4}$ has the property that $k < n < 2k$. In either case, the angle $\frac{\pi}{2k}$ is constructible by straightedge and compass, because squares and equilateral triangles are constructible, and angles can be bisected. Since there are standard ways of adding, multiplying, and dividing lengths, and constructing a length equal to the area of a given triangle, it is possible to construct the length $\sigma(P)$, and hence the angle $\theta = \frac{1}{2}\sec^{-1}(\frac{\sigma(P)}{4k\tan(\frac{\pi}{2k})} - 1)$ necessary to make $\sigma(Q)$ equal to $\sigma(P)$. Thus one can construct Q as required.

9. Let $F = \{0, 1, \cdots, p-1\}$ be the field of integers modulo a prime $p \neq 2$. Let X be a nonempty subset of $F^d = \{(x_1, x_2, \cdots, x_d) \mid x_i \in F\}$ for some positive integer d. Prove that there exist $a_1, a_2, \cdots, a_d, b \in F$ such that the equation $a_1x_1 + a_2x_2 + \cdots + a_dx_d = b$ has an odd number of solutions $(x_1, x_2, \cdots, x_d)$ in X.

Solution. If we let V denote the vector space F^d, the dual vector space V^* consists of F-linear functions $f : V \to F$, which are precisely those functions of the form $(x_1, x_2, \cdots, x_d) \mapsto a_1x_1 + a_2x_2 + \cdots + a_dx_d$ for $a_i \in F$. So we have to prove that there exist $f \in V^*$ and $b \in F$ such that $|\{v \in X \mid f(v) = b\}|$ is odd. Suppose for a contradiction that this quantity is even for all f and b.

Let ζ be a primitive complex pth root of 1. Then for $a \in F$, it makes sense to speak of ζ^a. Recall that the minimal polynomial of ζ over $\mathbb{Q}$ is $x^{p-1} + x^{p-2} + \cdots + x + 1$, so $1, \zeta, \cdots, \zeta^{p-2}$

are linearly independent over $\mathbb{Q}$, and $\sum_{a\in F}\zeta^a = 0$. The latter fact implies that for any $v \in V$,

$$\sum_{f\in V^*} \zeta^{f(v)} = \begin{cases} |V^*|, & \text{if } v = 0, \\ 0, & \text{otherwise.} \end{cases}$$

We deduce that for any $w \in X$,

$$\begin{aligned}\sum_{f\in V^*} \zeta^{-f(w)} \left(\sum_{v\in X} \zeta^{f(v)}\right) &= \sum_{v\in X}\sum_{f\in V^*} \zeta^{f(v-w)} \\ &= |V^*|.\end{aligned}$$

However, our assumption means that

$$\sum_{v\in X} \zeta^{f(v)} = \sum_{b\in F} |\{v \in X \mid f(v) = b\}|\, \zeta^b$$

is a linear combination of $1, \zeta, \cdots, \zeta^{p-2}$ with coefficients which are even integers. Hence the same is true for $|V^*|$, contradicting the fact that $|V^*|$ is a power of p and hence odd.

10. For any positive integer n, prove that

$$\sum_{a=0}^{n} \binom{n}{a} a^{n-a}(n-a)^a \le \frac{1}{2}\, n^n.$$

Solution. We can interpret both sides of the inequality combinatorially in terms of trees (connected graphs with no loops, multiple edges or cycles). Let $V = \{v_1, v_2, \cdots, v_n\}$ be fixed, and let $\mathcal{T}_V$ be the set of trees with vertex set V. By a famous result of Cayley, the number of elements of $\mathcal{T}_V$ is n^{n-2}, so n^n equals the number of triples (v, w, T) where $v, w \in V$ and $T \in \mathcal{T}_V$. Let $\mathcal{T}_V^*$ denote the set of such triples.

For any a, $\binom{n}{a}$ is the number of subsets $I \subseteq V$ such that $|I| = a$. For any such subset I, the number of trees $T \in \mathcal{T}_V$ such that $I \cup (V \setminus I)$ is a bipartite decomposition of the vertices of T (i.e. every edge of T joins an element of I with one of $V \setminus I$) is $a^{n-a-1}(n-a)^{a-1}$. (This calculation is equivalent to finding the number of spanning trees of the complete bipartite graph $K_{a,n-a}$, which can be done using Prüfer sequences or Kirchhoff's Matrix–Tree Theorem.) So the left-hand side of our inequality equals the number of quadruples (v, w, T, I) where $(v, w, T) \in \mathcal{T}_V^*$, $I \subseteq V$, $v \in I$, $w \in V \setminus I$, and $I \cup (V \setminus I)$ is a bipartite decomposition for T.

Now for any tree $T \in \mathcal{T}_V$ and $v \in V$, there is a unique $I \subseteq V$ such that $v \in I$ and $I \cup (V \setminus I)$ is a bipartite decomposition for T: namely, I consists of all vertices $v' \in V$ such that $d_T(v, v')$ is even, where $d_T(v, v')$ denotes the distance from v to v' in the tree T (i.e. the number of edges in the unique minimal path between these vertices). So the left-hand side of our inequality equals the number of triples $(v, w, T) \in \mathcal{T}_V^*$ such that $d_T(v, w)$ is odd, and we need to prove that this is less than or equal to half the total number of triples.

Hence it suffices to prove that for all $T \in \mathcal{T}_V$,

$$|\{(v, w) \in V \times V \mid d_T(v, w) \text{ is odd}\}| \le |\{(v, w) \in V \times V \mid d_T(v, w) \text{ is even}\}|. \tag{2}$$

We will do this by showing that the right-hand side of (2) minus the left-hand side equals a square:

$$\sum_{v,w\in V} (-1)^{d_T(v,w)} = \left(\sum_{v\in V} (-1)^{d_T(v,v_n)}\right)^2. \tag{3}$$

To prove (3), we use induction on n (the $n = 1$ case is trivial). Assume that $n \geq 2$ and that the result is known for trees with fewer vertices. Let $1 \leq i_1 < i_2 < \cdots < i_s \leq n-1$ be such that $v_{i_1}, v_{i_2}, \cdots, v_{i_s}$ are the vertices of T adjacent to v_n, and let $T_1, T_2, \cdots, T_s$ with vertex sets $V_1, V_2, \cdots, V_s$ be the connected components of $T \setminus \{v_n\}$ containing these vertices respectively; these are all trees to which the induction hypothesis applies. Note that if $v, w \in V_p$, then $d_T(v,w) = d_{T_p}(v,w)$, because the minimal path between v and w in T_p is also minimal in T. If $v \in V_p$ and $w \in V_q$ where $p \neq q$, then the minimal path between v and w in T passes through v_{i_p}, v_n, and v_{i_q}, so $d_T(v,w) = d_{T_p}(v, v_{i_p}) + d_{T_q}(w, v_{i_q}) + 2$. Thus

$$\begin{aligned}
\sum_{v,w \in V} (-1)^{d_T(v,w)} &= 1 + 2 \sum_{v \in V \setminus \{v_n\}} (-1)^{d_T(v,v_n)} + \sum_{v,w \in V \setminus \{v_n\}} (-1)^{d_T(v,w)} \\
&= 1 + 2 \sum_{v \in V \setminus \{v_n\}} (-1)^{d_T(v,v_n)} + \sum_{p=1}^{s} \sum_{v,w \in V_p} (-1)^{d_{T_p}(v,w)} \\
&\qquad + \sum_{1 \leq p \neq q \leq s} \sum_{\substack{v \in V_p \\ w \in V_q}} (-1)^{d_{T_p}(v,v_{i_p}) + d_{T_q}(w,v_{i_q})} \\
&= 1 + 2 \sum_{v \in V \setminus \{v_n\}} (-1)^{d_T(v,v_n)} + \sum_{p=1}^{s} \left(\sum_{v \in V_p} (-1)^{d_{T_p}(v,v_{i_p})} \right)^2 \\
&\qquad + \sum_{1 \leq p \neq q \leq s} \sum_{\substack{v \in V_p \\ w \in V_q}} (-1)^{d_{T_p}(v,v_{i_p}) + d_{T_q}(w,v_{i_q})} \\
&= 1 + 2 \sum_{v \in V \setminus \{v_n\}} (-1)^{d_T(v,v_n)} + \left(\sum_{p=1}^{s} \sum_{v \in V_p} (-1)^{d_{T_p}(v,v_{i_p})} \right)^2 \\
&= 1 + 2 \sum_{v \in V \setminus \{v_n\}} (-1)^{d_T(v,v_n)} + \left(- \sum_{v \in V \setminus \{v_n\}} (-1)^{d_T(v,v_n)} \right)^2 \\
&= \left(1 + \sum_{v \in V \setminus \{v_n\}} (-1)^{d_T(v,v_n)} \right)^2 \\
&= \left(\sum_{v \in V} (-1)^{d_T(v,v_n)} \right)^2,
\end{aligned}$$

completing the induction step.