12136. *Proposed by Albert Stadler, Herrliberg, Switzerland.* Prove

$$a^2 + b^2 + c^2 \geq a\sqrt[4]{\frac{b^4 + c^4}{2}} + b\sqrt[4]{\frac{c^4 + a^4}{2}} + c\sqrt[4]{\frac{a^4 + b^4}{2}}$$

for all positive real numbers a, b, and c.

12137. *Proposed by Nikolai Beluhov, Stara Zagora, Bulgaria.* A *polyomino* is a region with connected interior that is a union of a finite number of squares from a grid of unit squares. Do there exist a positive integer n with $n \geq 5$ and a polyomino P contained entirely within an n-by-n grid such that P contains exactly 3 unit squares in every row and every column of the grid?

12138. *Proposed by Navid Safaei, Sharif University of Technology, Tehran, Iran.* Let P be a nonconstant polynomial with complex coefficients, and let $Q(x, y) = P(x) - P(y)$. Let k be the number of linear factors of $Q(x, y)$, and let $R(x, y)$ be a nonconstant factor of $Q(x, y)$ whose degree is less than k. Prove that $R(x, y)$ is a product of linear polynomials with complex coefficients.

SOLUTIONS

A Slow Shuffle

12008 [2017, 970]. *Proposed by P. Kórus, University of Szeged, Szeged, Hungary.* You hold in your hand a deck of n cards, numbered 1 to n from top to bottom. Shuffle them as follows. Put the top card in the deck on the bottom and the second card on the table. Repeat this step until all the cards are on the table.
(a) For which n does card number 1 end up at the top of the deck of cards on the table?
(b) Shuffle the deck a second time in the same way. For which n does card number 1 end up at the top of the cards on the table?
(c)* Shuffle the deck a third time in the same way. For which n does card number 1 end up at the top of the cards on the table?
(d)* For which n does this shuffle amount to a permutation consisting of a single cycle?

Solution to **(a)**, **(b)**, *and* **(c)** *by Yury J. Ionin, Central Michigan University, Mt. Pleasant, MI.* Let $\tau_n(i)$ denote the final position of card i resulting from one shuffle. We express τ_n as a composition of $n - 1$ permutations on the positive integers. For $n \geq 2$, define a permutation σ_n on the positive integers by

$$\sigma_n(i) = \begin{cases} n-1 & \text{if } i = 1, \\ n & \text{if } i = 2, \\ i-2 & \text{if } 3 \leq i \leq n, \\ i & \text{if } i > n. \end{cases}$$

Here $1, \ldots, n$ represent the initial deck in the hand, values starting with $n + 1$ represent the initial deck on the table, and σ_n moves the top element to the bottom of the first deck and the second element to the top of the second deck. Note that σ_2 is the identity. Letting $\tau_n = \sigma_2 \cdots \sigma_n$, the first three parts of the problem ask for the values of n such that $\tau_n(1)$, $\tau_n^2(1)$, or $\tau_n^3(1)$ equal 1.

We begin with a formula for $\tau_n(i)$. For any positive integer n, let $f(n)$ be the largest odd divisor of n; note that $f(n) = n$ when n is odd. For $n \geq 2$ and any positive integer i, we claim

$$\tau_n(i) = \begin{cases} \frac{1+f(2n+1-i)}{2} & \text{if } i \leq n, \\ i & \text{if } i > n\,. \end{cases}$$

We prove this by induction on n. The case $n = 2$ holds by inspection, so consider $n \geq 3$. If $i > n$, then $\sigma_k(i) = i$ for $2 \leq k \leq n$, so $\tau_n(i) = i$. When $3 \leq i \leq n$, the induction hypothesis yields

$$\tau_n(i) = \tau_{n-1}(i-2) = \frac{1 + f(2n-1-(i-2))}{2} = \frac{1 + f(2n+1-i)}{2}.$$

Note that $\tau_n(2) = n = \frac{1}{2}(1 + f(2n-1))$, as desired. Finally, for $i = 1$, the induction hypothesis yields

$$\tau_n(1) = \tau_{n-1}(n-1) = \frac{1 + f(n)}{2} = \frac{1 + f(2n+1-1)}{2}.$$

(a) The formula for τ yields $\tau_n(1) = (1 + f(n))/2$, so $\tau_n(1) = 1$ if and only if $f(n) = 1$. This occurs precisely when n is a power of 2.

(b) Since $f(n) \leq n$, we have $\tau_n(1) \leq (1+n)/2 < n$. Thus

$$\tau_n^2(1) = \tau_n\left(\frac{1 + f(n)}{2}\right) = \frac{1 + f\left(2n + 1 - \frac{1}{2}(1 + f(n))\right)}{2},$$

so $\tau_n^2(1) = 1$ if and only if $f\,(2n + 1 - (1 + f(n))/2) = 1$.

We prove first that this cannot happen when $f(n) \equiv -1 \bmod 4$. If $f(n) = 4m - 1$, then $\tau_n^2(1) = 1$ if and only if $f(2n + 1 - 2m) = 1$, which cannot occur since $2n + 1 - 2m$ is not a power of 2.

Hence we may assume $f(n) = 4m + 1$, where $m \in \mathbb{N}$ and $n = 2^k(4m + 1)$. Now $\tau_n^2(1) = 1$ reduces to $f(2^{k+1}(4m + 1) - 2m) = 1$, requiring $2^k(4m + 1) - m$ to be a power of 2, say 2^s. That is, $(2^{k+2} - 1)m = 2^s - 2^k$ with $s \geq k$.

Since $2^{k+2} - 1$ and 2^k are relatively prime, $(2^{k+2} - 1) \mid (2^{s-k} - 1)$. It is an exercise in elementary number theory that $(2^a - 1) \mid (2^b - 1)$ requires $a \mid b$. To see this, write $b = aq + r$ with $0 \leq r < a$. From the formula for a geometric series, $2^a - 1$ divides $2^{aq} - 1$, so $2^a - 1$ divides $2^r(2^{aq} - 1)$, which equals $2^b - 2^r$. Now $2^a - 1$ divides the difference $(2^b - 1) - (2^b - 2^r)$, which equals $2^r - 1$. Since $r < a$, this requires $r = 0$, so $a \mid b$. Thus $(k + 2) \mid (s - k)$, which implies $(k + 2) \mid (s + 2)$.

From $m = (2^s - 2^k)/(2^{k+2} - 1)$, we have $4m + 1 = (2^{s+2} - 1)/(2^{k+2} - 1)$. Since $n = 2^k(4m + 1)$, we thus have the following answer: $\tau_n^2(1) = 1$ if and only if $n = 2^k(2^{s+2} - 1)/(2^{k+2} - 1)$ with $s \geq k \geq 0$ and $k + 2$ dividing $s + 2$. The values under 1000 are the powers of 2 together with 5, 18, 21, 68, 85, 146, 264, and 341.

(c) Now consider the equation $\tau_n^3(1) = 1$. By the formula for τ_n, we have $\tau_n(i) = 1$ if and only if $2n + 1 - i$ is a power of 2; that is, if and only if $i = 2n + 1 - 2^k$ for some k with $n < 2^k \leq 2n$. (There is exactly one such k for each n.) Note also that $\tau_n(\tau_n(1)) = \frac{1}{2}\big(1 + f\,(2n + 1 - \tau_n(1))\big)$. Writing the condition $\tau_n^3(1) = 1$ as $\tau_n(\tau_n(1)) = \tau_n^{-1}(1)$, the requirement reduces to

$$\frac{1}{2}\big(1 + f(2n + 1 - \tau_n(1))\big) = 2n + 1 - 2^k,$$

or $f(2n + 1 - \tau_n(1)) = 4n + 1 - 2^{k+1}$. This requires that $2n + 1 - \tau_n(1) = 2^l(4n + 1 - 2^{k+1})$ for some nonnegative l, or $\tau_n(1) = 2^{k+l+1} - 2^l + 1 - (2^{l+2} - 2)n$. Since $\tau_n(1) = (1 + f(n))/2$, we require $f(n) = 2^{k+l+2} - 2^{l+1} + 1 - (2^{l+3} - 4)n$, which implies $n = 2^m\left(2^{k+l+2} - 2^{l+1} + 1 - (2^{l+3} - 4)n\right)$ for some nonnegative m.

Thus the problem reduces to finding solutions of

$$(2^{l+m+3} - 2^{m+2} + 1)n = 2^m(2^{k+l+2} - 2^{l+1} + 1), \qquad (*)$$

where k, l, m are nonnegative integers and $n < 2^k \leq 2n$.

If n is a solution, then $2^{l+m+3} - 2^{m+2} + 1$ divides $2^{k+l+2} - 2^{l+1} + 1$, so $2^{l+m+3} + 2^{l+1} + 1 \le 2^{k+l+2} + 2^{m+2} + 1$. If $m \ge k$, then $2^{l+m+3} = 1 + \sum_{i=0}^{l+m+2} 2^i > 2^{k+l+2} + 2^{m+2} + 1$. Hence we require $m \le k - 1$.

It remains to ensure $n < 2^k \le 2n$. By replacing n with 2^k in $(*)$ and rearranging terms, we have $n < 2^k$ if and only if $2^{k+l+m+2} + 2^k + 2^{l+m+1} > 2^{k+m+2} + 2^m$, which is true for $l \ge 0$.

Similarly, by replacing n by 2^{k-1} in $(*)$, we have $2n \ge 2^k$ if and only if $2^{l+m+2} + 2^k \le 2^{k+m+2} + 2^{m+1}$. This inequality holds if and only if $l < k$ or $l = k$ and $m + 1 \ge k$. We thus have the following answer: $\tau_n^3(1) = 1$ if and only if

$$n = 2^m(2^{k+l+2} - 2^{l+1} + 1)/(2^{l+m+3} - 2^{m+2} + 1),$$

where $2^{l+m+3} - 2^{m+2} + 1$ divides $2^{k+l+2} - 2^{l+1} + 1$ and either $l < k$ and $m < k$ or $l = k = m + 1$ (which gives $n = 2^m$). The values under 1000 are the powers of 2 together with 3, 10, 14, 36, 51, 60, 136, 141, 248, 528, 819, and 910. To obtain infinitely many examples, let $(k, l, m) = (20t + 4, 1, 1)$ for $t \ge 0$. The resulting value is $(2^{20t+8} - 6)/25$.

Solution to **(d)** *by Richard Stong, Center for Communications Research, San Diego, CA.* The values of n for which the shuffle is a full cycle are those n such that $4n + 1$ is prime and 2 is a primitive root modulo $4n + 1$. In particular, the values of n under 100 are 1, 3, 7, 9, 13, 15, 25, 37, 43, 45, 49, 67, 73, 79, 87, 93, and 97 (see oeis.org/A137310).

To prove the result, we use an alternative description of the shuffle as an iterative process on a pile of n cards. For $n - 1$ steps, indexed from $j = 0$ to $j = n - 2$, at step j take the top two cards and reinsert them with j cards below them. Steps j through $n - 2$ do not change the bottom j cards; these are the cards "on the table" during that time. The remaining $n - j$ cards are still "in the hand." Putting the top two cards between these sets (and incrementing j) moves the top card to the bottom of the deck in hand and puts the next card on the table. The jth step is an even permutation (two steps of rotating the top $n - j$ cards up by one step). Thus the permutation induced by the shuffle is even. It follows that the permutation can be a full cycle only when n is odd.

We now express the shuffle as the permutation π_n that maps each position to the index of the card that occupies it. This is the inverse of τ_n, and it is a cycle if and only if τ_n is a cycle. It is also convenient to index the cards and the positions by the set S of odd integers from 1 to $2n - 1$, treating π_n as a permutation of S. That is, assign the card at position a the value $2a - 1$, which we call a'.

We use the formula for $\tau_n(i)$ to give a formula for $\pi_n(a')$, the modified value of the card ending in position a. We claim $\pi_n(a') = 4n + 1 - 2^{u(a')}a'$, where $u(a')$ is the unique positive integer such that $2^{u(a')}a' \in [2n + 2, 4n]$.

To see this, let $i = 2n + 1 - 2^{u(a')-1}a'$. We have $2n + 1 - i = 2^{u(a')-1}a'$. Since a' is odd, it is the largest odd divisor of $2n + 1 - i$; this is why we express π_n as a permutation of odd values. With $f(2n + 1 - i) = 2a - 1$, the formula $2\tau_n(i) - 1 = f(2n + 1 - i)$ yields $\tau_n(i) = a$. Thus $\pi_n(a') = 2i - 1$, as claimed.

We now show that the condition on n is necessary and sufficient for the shuffle to be a full cycle.

Necessity. Suppose that π_n is a cycle. Let $p = 4n + 1$. We have $\pi_n(a') \equiv -2^{u(a')}a' \bmod p$. Hence any value we can reach starting from $a' = 1$ by iterating π_n has the form $\pm 2^v \bmod p$. If q is a proper odd prime factor of p, then we cannot reach q; thus p must be prime. Since we have shown that n is odd and defined $p = 4n + 1$, we have $p \equiv 5 \bmod 8$. By the law of quadratic reciprocity, 2 is a square modulo an odd prime p if and only if p is congruent to 1 or 7 modulo 8. Hence 2 is not a square.

In addition, Fermat's little theorem implies that $2^{(p-1)/2}$ is congruent to ± 1 modulo p. The value is $+1$ if and only if 2 is a square. Hence -1 is a power of 2, modulo p. This

means that all values we can reach have the form $2^v \bmod p$. For π to be a cycle, these powers must include all odd numbers from 1 to $2n-1$. Since -1 and 2 are also powers of 2 modulo p, we conclude that every nonzero value is a power of 2 modulo p, so 2 is a primitive root.

Sufficiency. Again letting $p = 4n+1$, suppose that p is prime and that 2 is a primitive root modulo p. Since 2 is a primitive root, 2 cannot be a square modulo p, so p is congruent to 3 or 5 modulo 8, again by quadratic reciprocity. Since p has the form $4n+1$, it follows that $p \equiv 5 \bmod 8$ and n is odd.

We prove that π_n^2, the result of shuffling twice, is a cycle; this implies that π_n itself is a cycle. Consider the application of π_n in terms of the cycle of powers of 2 modulo p. Suppose that $\pi_n(a') = b'$, meaning that the card in position a after the shuffle is b. Since $\pi_n(a') = 4n+1-2^{u(a')}a'$, we obtain b' from a' by multiplying by 2 successively to reach the interval $[2n+2, 4n]$ and then subtracting from $4n+1$. Since $a' \le 2n-1$, the result is odd and lies in S.

Modulo p, we have $b' \equiv -2^{u(a')}a'$. Thus b' is the negative of the value that is $u(a')$ steps beyond a' in the cycle of powers of 2. However, $2^{u(a')}a'$ is not in S. Applying the shuffle to obtain c' from b', we have $c' \equiv 2^{u(a')+u(b')}a'$. Thus π_n^2 moves each value some distance along the cycle of powers of 2 and returns each element of S to another value that when reduced modulo p lies in S.

Furthermore, $\pi_n^2(a')$ is the first value after a' in the cycle of powers of 2 that lies in S. Since 2 is a primitive root modulo p, that cycle visits all of S. Hence π_n^2 is a cycle through S, as desired.

Editorial comment. Because it is not known whether there are infinitely many primes for which 2 is a primitive root (this is the Artin conjecture), it is not known whether there are infinitely many examples for part (d). Several solvers observed that, given n, the card atop the shuffled deck is the number that solves the Josephus problem for a circle of n soldiers (see oeis.org/A006257).

Part (a) also solved by D. Fleischman, O. Geupel (Germany), and R. Prather. Parts (a) and (b) also solved by T. Ayton & A. Lopez & R. Tuminello, N. Grivaux (France), J. H. Lindsey II, O. P. Lossers (Netherlands), P. McPolin (UK), L. Meissner & E. Newman & R. Toth & S. Weigel, and the proposer. Parts (a), (b), and (c) also solved by GCHQ Problem Solving Group (UK) and R. Stong. All four parts solved by Armstrong Problem Solving Group.

Reducible Combinations of Elementary Symmetric Polynomials

12017 [2018, 82]. *Proposed by Mowaffaq Hajja, Philadelphia University, Amman, Jordan.* For $n \ge 2$, let R be the ring $F[t_1, \ldots, t_n]$ of polynomials in n variables over a field F. For j with $1 \le j \le n$, let $s_j = \sum \prod_{i=1}^{j} t_{m_i}$, where the sum is taken over all j-element subsets $\{m_1, \ldots, m_j\}$ of $\{1, \ldots, n\}$. This is the *elementary symmetric polynomial* of degree j in the variables $t_1, \ldots, t_n$. Let $f = \sum_{i=0}^{n} c_i s_i$ for some $c_0, \ldots, c_n$ in F with $c_1, \ldots, c_n$ not all 0. Show that f is reducible in R if and only if either $c_0 = \cdots = c_{n-1} = 0$ or $(c_0, \ldots, c_n)$ is a geometric progression, meaning that there is $r \in F$ such that $c_i = rc_{i-1}$ for all i with $1 \le i \le n$.

Solution by Michael Reid, University of Central Florida, Orlando, FL. For sufficiency, f factors as $c_n \prod_{i=1}^{n} t_i$ if $c_0 = \cdots = c_{n-1} = 0$ and as $c \prod_{i=1}^{n}(1 + rt_i)$ if $(c_0, c_1, \ldots, c_n) = (c, cr, \ldots, cr^n)$ with $c, r \ne 0$.

For necessity, suppose that f is reducible, and let g be an irreducible factor. For each t_i, since f has degree 1 in t_i, g has degree 0 or 1 in t_i. Moreover, since g is nonconstant, it has degree 1 in at least one variable. We claim that g has degree 0 in all of the other variables.

To prove the claim, suppose otherwise. By symmetry, we may assume that g has degree 1 in both t_1 and t_2. Since f/g is not constant, g has degree 0 in t_k for some k. Note that f is