Solutions of April problems

374. What is the maximum number of numbers that can be selected from $\{1, 2, 3, \cdots, 2005\}$ such that the difference between any pair of them is not equal to 5?

Solution 1. The maximum number is 1005. For $1 \leq k \leq 5$, let $S_k = \{x : 1 \leq x \leq 2005, x \equiv k (\text{mod } 5)\}$. Each set S_k has 401 numbers, and no number is any of the S_k differs from a number in a different S_k by 5 (or even a multiple of 5). Each S_k can be partitioned into 200 pairs and a singleton:

$$S_k = \{k, 5+k\} \cup \{10+k, 15+k\} \cup \cdots \cup \{1990+k, 1995+k\} \cup \{2000+k\} \ .$$

By the Pigeonhole Principle, each choice of 202 numbers from S_k must contain two numbers in one of the pairs and so which differ by 5. At most 201 numbers can be selected from each S_k with no two differing by 5. For example $\{k, 10+k, 20+k, \cdots, 2000+k\}$ will do. Overall, we can select at most $5 \times 201 = 1005$ numbers, no two differing by 5.

Solution 2. [F. Barekat] The subset $\{1, 2, 3, 4, 5, 11, 12, 13, 14, 15, \cdots, 2001, 2002, 2003, 2004, 2005\}$ contains 1005 numbers, no two differing by 5. Suppose that 1006 numbers are chosen from $\{1, 2, \cdots, 2005\}$. Then, at least 1001 of them must come from the following union of 200 sets:

$$\{1, \cdots, 10\} \cup \{11, \cdots, 20\} \cup \cdots \cup \{1991, \cdots, 2001\} \ .$$

By the Pigeonhole Principle, at least one of these must contain 6 numbers, two of which must be congruent modulo 5, and so differ by 5. The result follows.

375. Prove or disprove: there is a set of concentric circles in the plane for which both of the following hold:

(i) each point with integer coordinates lies on one of the circles;

(ii) no two points with integer coefficients lie on the same circle.

Solution. There is such a set of concentric circles satisfying (a) and (b), namely the set of all concentric circles centred at $(\frac{1}{3}, \sqrt{2})$. Every point with integer coordinates lies in exactly one of the circles, whose radius is equal to the distance from the point to the common centre. Suppose that the points (a, b), (c, d) with integer coordinates both lie on the same circle. Then

$$(a - (1/3))^2 + (b - \sqrt{2})^2 = (c - (1/3))^2 + (d - \sqrt{2})^2$$

$$\iff 9a^2 - 6a + 1 + 9b^2 - 18\sqrt{2}b + 18 = 9c^2 - 6c + 1 + 9d^2 - 18\sqrt{2}d + 18$$

$$\iff 9(a^2 + b^2 - c^2 - d^2) - 6(a - c) = \sqrt{2}(18d - 18b) \ .$$

The left member of the last equation and the coefficient of $\sqrt{2}$ in the right member are both integers. Since $\sqrt{2}$ is irrational, both must vanish, so that $b = d$ and

$$0 = 3(a^2 - c^2) - 2(a - c) = (a - c)(3(a + c) - 2) \ .$$

Since a and c are integers, $a + c \neq \frac{2}{3}$, so that $a = c$ and $b = d$. Hence, two points with integer coordinates on the same circle must coincide.

Comment. Since you need a simple example to prove the affirmative, it is cleaner to provide a specific case rather than describe a general case. Some selected the common centre $(\sqrt{2}, \sqrt{3})$, which left them with a more complicated result to prove, that $u + v\sqrt{2} + w\sqrt{3} = 0$ for integers u, v, w implies that $u = v = w = 0$. The argument for this should be provided, since it is possible to determine irrational α, β and nonzero integers p, q, r for which $p + q\alpha + r\beta = 0$ (do it!). An efficient way to do it is to start with

$$u + v\sqrt{2} + w\sqrt{3} = 0 \implies u^2 = 2v^2 + 3w^2 + 2\sqrt{6}vw \ .$$

376. A soldier has to find whether there are mines buried within or on the boundary of a region in the shape of an equilateral triangle. The effective range of his detector is one half of the height of the triangle. If he starts at a vertex, explain how he can select the shortest path for checking that the region is clear of mines.

Solution. Wolog, suppose the equilateral triangle has sides of length 1, so that the range of his detector is $\sqrt{3}/4$. Let the triangle be ABC with A the starting vertex. Since the points B and C must be covered, the soldier must reach the circles of centres B and C and radius $\sqrt{3}/4$. Since $2(\sqrt{3}/4) = \sqrt{3}/2 < 1$, the line of centres is longer than the sum of the two radii and the circles do not intersect. Suppose that the soldier crosses the circumference of the circle with centre B at X and of the circle with centre C at Y. Wolog, let the soldier reach X before Y. Then the total distance travelled by the soldier is not less that

$$|AX| + |XY| \geq |AX| + |XC| - |YC| = |AX| + |XC| - (\sqrt{3}/4) \ .$$

(Use the triangle inequality.)

Let Z be the midpoint of the arc of the circle with centre B that lies within triangle ABC and W be the point of intersection of the circle with centre C and the segment CZ. The ellipse with foci A and C that passes through Z is tangent to the circle with centre B, so that $|AX| + |XC| \geq |AZ| + |ZC|$. Hence the distance travelled by the soldier is at least

$$|AZ| + |ZC| - (\sqrt{3}/4) = 2(\sqrt{7}/4) - (\sqrt{3}/4) = \frac{2\sqrt{7} - \sqrt{3}}{4} \ .$$

(Use the law of cosines in triangle AZB.) This distance is exactly $(\frac{1}{4})(2\sqrt{7} - \sqrt{3})$ when $X = Z$ and X, Y, C are collinear. We show that this corresponds to a suitable path.

Let the soldier start at A, proceed to Z and thence walk directly towards C, stopping at the point W. From the point Z, the soldier covers the points B and M, the midpoint of AC. Let U be any point on AZ and draw the segment parallel to BM through U joining points on AB and AC. From U, the soldier covers every point on the segment. It follows that the soldier covers every point in the triangle ABM.

Suppose the line through W perpendicular to AC meets AC at P and BC at Q. As in the foregoing paragraph, we see that the soldier covers the trapezoid $MBQP$. Note that the lengths of WP, WC and WQ all do not exceed $\sqrt{3}/4$. It follows that every point of the segments CP and CQ are no further from W than $\sqrt{3}/4$. Hence the soldier covers triangle CPQ. Thus, we have a path of minimum length covering all of triangle ABC.

377. Each side of an equilateral triangle is divided into 7 equal parts. Lines through the division points parallel to the sides divide the triangle into 49 smaller equilateral triangles whose vertices consist of a set of 36 points. These 36 points are assigned numbers satisfying both the following conditions:

(a) the number at the vertices of the original triangle are 9, 36 and 121;

(b) for each rhombus composed of two small adjacent triangles, the sum of the numbers placed on one pair of opposite vertices is equal to the sum of the numbers placed on the other pair of opposite vertices.

Determine the sum of all the numbers. Is such a choice of numbers in fact possible?

Solution 1. The answer is $12(9 + 36 + 121) = 1992$.

More generally, let the equilateral triangle be ABC with the numbers a, b, c at the respective vertices A, B, C. Let the lines of division points parallel to BC, AC and AB be called, respectively, $\alpha-$lines, $\beta-$lines and $\gamma-$lines.

Suppose that u and v are two consecutive entries on, say, an $\alpha-$line and p, q, r are the adjacent entries on the next $\alpha-$line. Then $p + v = u + q$ and $q + v = u + r$, whence $p - q = u - v = q - r$. It follows that any two adjacent points on any $\alpha-$line have the same difference, so that the numbers along any $\alpha-$line are in arithmetic progression. The same applies to $\beta-$ and $\gamma-$lines.

In this way, we can uniquely determine the points along the sides AB, BC and AC, and then along each $\alpha-$line, $\beta-$line and $\gamma-$line. However, we need to check that such an assignment is consistent, *i.e.*, does not yield different results for a given entry gained by working along lines from the three different directions. We do this by describing an assignment, and then showing that it satisfies the condition of the problem.

Let an entry be position i $\alpha-$lines from BC, j $\beta-$lines from AC and k $\gamma-$lines from AB. Thus, any entry on BC corresponds to $i = 0$ and the points A, B, C, respectively, correspond to $(i, j, k) = (7, 0, 0), (0, 7, 0), (0, 0, 7)$. Assign to such a point the value $\frac{1}{7}(ia+jb+kc)$. It can be checked that these satisfy the rhombus condition. For example, the points (i, j, k), $(i, j-1, k+1)$, $(i+1, j-1, k)$ and $(i+1, j-2, k+1)$ are four vertices of a rhombus, and the sum of the numbers assigned to the first and last is equal to the sum of the numbers assigned to the middle two.

We sum the entries componentwise. Along the ith $\alpha-$line, there are $8 - i$ entries whose sum is $\frac{1}{7}[i(8 - i)a + \cdots]$. Hence the sum of all entries is

$$\left[\frac{1}{7}\sum_{i=0}^{7} i(8-i)a\right] + \cdots = \frac{1}{7}[1\cdot 7 + 2\cdot 6 + 3\cdot 5 + 4\cdot 4 + 5\cdot 3 + 6\cdot 2 + 7\cdot 1]a + \cdots = 12a + \cdots \ .$$

Summing along $\beta-$lines and $\gamma-$lines, we find that the sum of all entries is $12(a + b + c)$. In the present situation, this number is 1992.

Solution 2. [F. Barekat] Let a, b, c be the entries at A, B, C. As in Solution 1, we show that the entries along each of AB, BC and CA are in arithmetic progression. The sum of the entries along each of these lines are, respectively, $4(a + b)$, $4(b + c)$, $4(c + a)$ (why?), whence the sum of all the entries along the perimeter of triangle ABC is equal to

$$4(a + b) + 4(b + c) + 4(c + a) - (a + b + c) = 7(a + b + c) \ .$$

Let p, q, r, respectively, on AB, BC, CA be adjacent to A, B, C and u, v, w, respectively, on AC, BA, CB be adjacent to A, B, C. When the perimeter of triangle ABC is removed, there remains a triangle XYZ with sides divided into four equal parts and entries x, y, z, respectively, at vertices X, Y, Z. Since

$$a + b = p + v \ , \quad b + c = q + w \ , \quad c + a = r + u \ ,$$

$$\begin{aligned} x + y + z &= [(p + u) - a] + [(q + v) - b] + [(r + w) - c] \\ &= (p + v) + (q + w) + (r + u) - (a + b + c) = a + b + c \ . \end{aligned}$$

The sum of the entries along the sides of XYZ is equal to

$$\frac{5}{2}(x + y) + \frac{5}{2}(y + z) + \frac{5}{2}(z + x) - (x + y + z) = 4(a + b + c) \ .$$

When the perimeter of triangle XYZ is removed from triangle XYZ, there remains a single small triangle with three vertices. The sum of the entries at these vertices is $x + y + z = a + b + c$. Therefore, the sum of all the entries in the triangular array is $12(a + b + c)$. In the present situation, the answer is 1992.

378. Let $f(x)$ be a nonconstant polynomial that takes only integer values when x is an integer, and let P be the set of all primes that divide $f(m)$ for at least one integer m. Prove that P is an infinite set.

Solution 1. Suppose that $p_k(x)$ is a polynomial of degree k assuming integer values at $x = n, n + 1, \cdots, n + k$. Then, there are integers $c_{k,i}$ for which

$$p_k(x) = c_{k,0}\binom{x}{k} + c_{k,1}\binom{x}{k-1} + \cdots + c_{k,k}\binom{x}{0} \ .$$

To see this, first observe that $\binom{x}{k}$, $\binom{x}{k-1}$, $\cdots$, $\binom{x}{0}$ constitute a basis for the vector space of polynomials of degree not exceeding k. So there exist *real* $c_{k,i}$ as specified. We prove by induction on k that the $c_{k,i}$ must in fact be integers. The result is trivial when $k = 0$. Assume its truth for $k \geq 0$. Suppose that

$$p_{k+1}(x) = c_{k+1,0}\binom{x}{k+1} + \cdots + c_{k+1,k+1}$$

takes integer values at $x = n, n+1, \cdots, n+k+1$. Then

$$p_{k+1}(x+1) - p_{k+1}(x) = c_{k+1,0}\binom{x}{k} + \cdots + c_{k+1,k}$$

is a polynomial of degree k which taken integer values at $n, n+1, \cdots, n+k$, and so $c_{k+1,0}, \cdots, c_{k+1,k}$ are all integers. Hence,

$$c_{k+1,k+1} = p_{k+1}(n) - c_{k+1,0}\binom{n}{k+1} - \cdots c_{k+1,k}\binom{n}{1}$$

is also an integer. (This is more than we need; we just need to know that the coefficients of $f(x)$ are all rational.)

Let $f(x)$ be multiplied by a suitable factorial to obtain a polynomial $g(x)$ with integer coefficients. The set of primes dividing values of $g(m)$ at integers m is the union of the set of primes for f and a finite set, so it is enough to obtain the result for g. Note that g assumes the values 0 and 1 only finitely often. Suppose that $g(a) = b \neq 0$ and let $P = \{p_1, p_2, \cdots, p_r\}$ be a finite set of primes. Define

$$h(x) = \frac{g(a + bp_1p_2\cdots p_rx)}{b} \ .$$

Then $h(x)$ has integer coefficients and $h(x) \equiv 1 \pmod{p_1p_2\cdots p_r}$. There exists an integer u for which $h(u)$ is divisible by a prime p, and this prime must be distinct from $p_1, p_2, \cdots, p_r$. The result follows.

Solution 2. Let $f(x) = \sum_k^n a_k x_n$. The number $a_0 = f(0)$ is rational. Indeed, each of the numbers $f(0)$, $f(1)$, $\cdots$, $f(n)$ is an integer; writing these conditions out yields a system of $n+1$ linear equations with integer coefficients for the coefficients a_0, a_1, $\cdots$, a_n whose determinant is nonzero. The solution of this equation consists of rational values. Hence all the coefficients of $f(x)$ are rational. Multiply $f(x)$ by the least common multiple of its denominators to get a polynomial $g(x)$ which takes integer values whenever x is an integer. Suppose, if possible, that values of $f(x)$ for integral x are divisible only by primes p from a finite set Q. Then the same is true of $g(x)$ for primes from a finite set P consisting of the primes in Q along with the prime divisors of the least common multiple. For each prime $p \in P$, select a positive integer a_p such that p^{a_p} does not divide $g(0)$. Let $N = \prod\{p^{a_p} : p \in P\}$. Then, for each integer u, $g(Nu) \not\equiv 0 \pmod{N}$. However, for all u, $g(Nu) = \prod p^{b_p}$, where $0 \leq b_p \leq a_p$. Since there are only finitely many numbers of this type, some number must be assumed by g infinitely often, yielding a contradiction. (Alternatively: one could deduce that $g(Nu) \leq N$ for all u and get a contradition of the fact that $|g(Nu)|$ tends to infinity with u.)

Solution 3. [R. Barrington Leigh] Let n be the degree of f. `Lemma.` Let p be a prime and k a positive integer. Then $f(x) \equiv f(x + p^{nk}) \pmod{p^k}$. `Proof by induction on the degree.` The result holds for $n = 0$. Assume that it holds for $n = m - 1$ and $f(x)$ have degree m. Let $g(x) = f(x) - f(x-1)$, so that the degree of $g(x)$ is $m - 1$. Then

$$\begin{aligned} f(x + p^{nk}) - f(x) &= \sum_{i=1}^{p^{nk}} g(x+i) \\ &= \sum_{i=1}^{p^{(n-1)k}} (g(x+i) + g(x+i+p^{(n-1)k}) + \ldots + g(x+i+(p^k-1)p^{(n-1)k}) \\ &\equiv \sum_{i=1}^{p^{(n-1)k}} p^k g(x+i) \equiv 0 \ , \end{aligned}$$

(mod p^k). [Note that this does not require the coefficients to be integers.]

Suppose, if possible, that the set P of primes p that divide at least one value of $f(x)$ for integer x is finite, and that, for each $p \in P$, the positive integer a is chosen so that p^a does not divide $f(0)$. Let $q = \prod\{p^a : p \in P\}$. Then p^a does not divide $f(0)$, nor any of the values $f(q^n)$ for positive integer n, as these are all congruent modulo p^a. Since any prime divisor of $f(q^n)$ belongs to P, it must be that $f(q^n)$ is a divisor of q. But this contradicts the fact that $|f(q^n)|$ becomes arbitrarily large with n.

Solution 4. [F. Barekat] Let $f(x) = a_n x^n + \cdots + a_0$ where $n \geq 1$. Substituting $n+1$ integers for x yields a system of $n+1$ linear equations for a_0, a_1, $\cdots$, a_n which has integer coefficients. Such a system has rational solutions, so that the coefficients of the polynomial are rational numbers. (This can also be seen by forming the Lagrange polynomial for the $n+1$ values.) Let $g(x)$ be the product of $f(x)$ and c, a common multiple of all the denominators of the a_i. Then $g(x)$ has integer coefficients and takes integer values when x is an integer.

If $a_0 = 0$, then $n|g(n)$ for each integer n, and there are infinitely many primes among the divisors of the $g(n)$ and therefore among the divisor of the $f(n)$ (since only finitely many primes divide c), when n is integral. Suppose that $a_0 \neq 0$, and, if possible, that $g(n)$ is divisible only by the primes $p_1, p_2, \cdots, p_k$ for integer n. Let $ca_0 = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ and let

$$M = \{p_1^{s_1} p_2^{s_2} \cdots p_k^{s_k} : s_i > r_i \forall i\} .$$

The set M has infinitely many elements.

Suppose that $h(x) = (1/ca_0)g(x)$, so that the constant coefficient of $h(x)$ is 1. The polynomial $h(x)$ takes rational values when x is an integer, but only the primes $p_1, p_2, \cdots, p_k$ are involved in the numerator and denominator of these values written in lowest terms. In particular, for $m \in M$, $h(m)$ is an integer congruent to 1 modulo each p_i, so that $h(m) = \pm 1$. However, this would imply that either $h(x) = 1$ or $h(x) = -1$ infinitely often, which cannot occur for an nontrivial polynomail. Hence, there must be infinitely many primes divisors of the values of $g(n)$ for integral n.

Solution 5. [P. Shi] Let t be the largest positive integer for which $f(n)$ is a multiple of t for every positive integer n. Define $g(x) = (1/t)f(x)$. Then $g(n)$ takes integer values for every integer n, the greatest common divisor of all the $g(n)$ (n an integer) is 1, and the set of primes dividing at least one $g(n)$ is a subset of P.

Suppose if possible that $P \equiv \{p_1, p_2, \cdots, p_k\}$ is a finite set. Let $1 \leq i \leq k$. There exists an integer m_i such that $g(m_i)$ is not a multiple of p_i; since $g(m_i + jp_i) \equiv g(m_i) \pmod{p_i}$, $g(n)$ is not a multiple of p_i when $n \equiv m_i \pmod{p_i}$.

By the Chinese Remainder Theorem, there exists infinitely many numbers n for which $n \equiv m_i$ (mod p_i) for each i. For such n, $g(n)$ is not divisible by p_i for any i. At most finitely many such $g(n)$ are equal to ± 1. Each remaining one of the $g(n)$ must have a prime divisor distinct from the p_i, yielding a contradiction. The result follows.

379. Let n be a positive integer exceeding 1. Prove that, if a graph with $2n+1$ vertices has at least $3n+1$ edges, then the graph contains a circuit (*i.e.*, a closed non-self-intersecting chain of edges whose terminal point is its initial point) with an even number of edges. Prove that this statement does not hold if the number of edges is only $3n$.

Solution 1. If there are two vertices joined by two separate edges, then the two edges together constitute a chain with two edges. If there are two vertices joined by three distinct chains of edges, then the number of edges in two of the chains have the same parity, and these two chains together constitute a circuit with evenly many edges. We establish the general result by induction.

When $n = 2$, the graph has 5 vertices at at least 7 edges. Since a graph lacking circuits has fewer edges than vertices, there must be at least one circuit. If there is a circuit of length 5, then any additional edge produces circuit of length 3 and 4. If there is a circuit of length 3, then one of the remaining vertices must be joined to two of the vertices in the cicuit, creating two circuits of length 3 with a common edge. Suppressing this edge gives a circuit of length 4. Accordingly, one can see that there must be a circuit with an even number of edges.

Suppose that the result holds for $2 \leq n \leq m-1$. We may assume that we have a graph G with $2m+1$ edges and at least $3m+1$ vertices that contains no instances where two separate edges join the same pair of vertices and no two vertices are connected by more than two chains. Since $3m+1 > 2m$, the graph is not a tree or union of disjoint trees, and therefore must contain at least one circuit. Consider one of these circuits, L. If it has evenly many edges, the result holds. Suppose that it has oddly many edges, say $2k+1$ with $k \geq 1$. Since any two vertices in the circuit are joined by at most two chains (the two chains that make up the circuit), there are exactly $2k+1$ edges joining pairs of vertices in the circuit. Apart from the circuit, there are $(2m+1)-(2k+1) = 2(m-k)$ vertices and $(3m+1)-(2k+1) = 3(m-k)+k \geq 3(m-k)+1$ edges.

We now create a new graph G', by coalescing all the vertices and edges of L into a single vertex v and retaining all the other edges and vertices of G. This graph G' contains $2(m-k)+1$ vertices and at least $3(m-k)+1$ edges, and so by the induction hypothesis, it contains a circuit M with an even number of edges. If this circuit does not contain v, then it is a circuit in the original graph G, which thus has a circuit with evenly many edges. If the circuit does contain v, it can be lifted to a chain in G joining two vertices of L by a chain of edges in G'. But these two vertices of L must coincide, for otherwise there would be three chains joining these vertices. Hence we get a circuit, *all* of whose edges lie in G'; this circuit has evenly many edges. The result now follows by induction.

Here is a counterexample with $3n$ edges. Consider $2n+1$ vertices partitioned into a singleton and n pairs. Join each pair with an edge and join the singleton to each of the other vertices with a single edge to obtain a graph with $2n+1$ vertices, $3n$ edges whose only circuits are triangles.

Solution 2. [J. Tsimerman] For any graph H, let $k(H)$ be the number or circuits minus the number of components (two vertices being in the same component if and only if they are connected by a chain of edges). Let G_0 be the graph with $2n+1$ vertices and no edges. Then $k(G_0) = -(2n+1)$. Suppose that edges are added one at a time to obtain a succession G_i of graphs culminating in the graph G with $2n+1$ vertices and at least $3n+1$ edges. Since adding an edge either reduces the number of components (when it connects two vertices of separate components) or increases the number of circuits (when it connects two vertices in the same component), $k(G_{i+1}) \geq k(G_i)+1$. Hence $k(G) \geq k(G_{3n+1}) \geq -(2n+1)+(3n+1) = n$. Thus, the number of circuits in G is at least equal to the number of components in G plus n, which is at least $n+1$. Thus, G has at least $n+1$ circuits.

If a circuit has two edges, the result is known. If all circuits have at least three edges, then the total number of edges of all circuits is at least $3(n+1)$. Since $3(n+1) > 3n+1$, there must be two circuits that share an edge. Let the circuits be A and B and the endpoints of the common edge be u and v. Follow circuit A along from u in the direction away from the adjacent vertex v, and suppose it first meets circuit B and w (which could coincide with v). Then there are three chains connecting u and w, namely the two complementary parts of B and a portion of A. The number of edges of two of these chains have the same parity, and can be used to constitute a circuit with an even number of edges.

A counterexample can be obtained by taking a graph with vertices $a_1, \cdots, a_n, b_0, b_1, \cdots, b_n$, with edges joining the vertex pairs (a_i, b_{i-1}), (a_i, b_i) and (b_{i-1}, b_i) for $1 \leq i \leq n$.

380. Factor each of the following polynomials as a product of polynomials of lower degree with integer coefficients:

(a) $(x+y+z)^4 - (y+z)^4 - (z+x)^4 - (x+y)^4 + x^4 + y^4 + z^4$;

(b) $x^2(y^3 - z^3) + y^2(z^3 - x^3) + z^2(x^3 - y^3)$;

(c) $x^4 + y^4 - z^4 - 2x^2y^2 + 4xyz^2$;

(d) $(yz + zx + xy)^3 - y^3z^3 - z^3x^3 - x^3y^3$;

(e) $x^3y^3 + y^3z^3 + z^3x^3 - x^4yz - xy^4z - xyz^4$;

(f) $2(x^4 + y^4 + z^4 + w^4) - (x^2 + y^2 + z^2 + w^2)^2 + 8xyzw$;

(g) $6(x^5 + y^5 + z^5) - 5(x^2 + y^2 + z^2)(x^3 + y^3 + z^3)$.

Solution. (a) Let $P_1(x, y, z)$ be the expression to be factored. Since $P_1(0, y, z) = P_1(x, 0, y) = P_1(x, y, 0) = 0$, three factors of $P_1(x, y, z)$ are x, y and z. Hence, $P_1(x, y, z) = xyzQ_1(x, y, z)$, where $Q_1(x, y, z)$ must be linear and symmetric. Hence $Q_1(x, y, z) = k(x + y + z)$ for some constant k. Since $3k = P_1(1, 1, 1) = 81 - 48 + 3 = 36$,

$$P_1(x, y, z) = 12xyz(x + y + z) \ .$$

Comment. The factor $x + y + z$ can be picked up from the Factor Theorem using the substitution $x + y + z = 0$ (*i.e.*, $x + y = -z$, $y + z = -x$, $z + x = -y$).

(b)

$$\begin{aligned}
&x^2(y^3 - z^3) + y^2(z^3 - x^3) + z^2(x^3 - y^3) \\
&\qquad = x^2(y^3 - z^3) + y^2(z^3 - x^3) - z^2(z^3 - x^3) - z^2(y^3 - z^3) \\
&\qquad = (x^2 - z^2)(y^3 - z^3) + (y^2 - z^2)(z^3 - x^3) \\
&\qquad = (x - z)(y - z)[(x + z)(y^2 + yz + z^2) - (y + z)(z^2 + zx + x^2)] \\
&\qquad = (x - z)(y - z)[xy(y - x) + z^2(x - y) + z(y^2 - x^2) + z^2(y - x)] \\
&\qquad = (x - z)(y - z)(y - x)[xy + z(y + x)] = (x - y)(y - z)(z - x)(xy + yz + zx) \ .
\end{aligned}$$

(c)

$$\begin{aligned}
&x^4 + y^4 - z^4 - 2x^2y^2 + 4xyz^2 = (x^4 + 2x^2y^2 + y^4) - (z^4 + 4x^2y^2 - 4xyz^2) \\
&\qquad = (x^2 + y^2)^2 - (z^2 - 2xy)^2 = (x^2 + y^2 + z^2 - 2xy)(x^2 + y^2 - z^2 + 2xy) \\
&\qquad = (x^2 + y^2 + z^2 - 2xy)[(x + y)^2 - z^2] = (x^2 + y^2 + z^2 - 2xy)(x + y + z)(x + y - z) \ .
\end{aligned}$$

(d) *Solution 1.*

$$\begin{aligned}
&(yz + zx + xy)^3 - y^3z^3 - z^3x^3 - x^3y^3 \\
&\qquad = 3(xy^2z^3 + xy^3z^2 + x^2yz^3 + x^2y^3z + x^3yz^2 + x^3y^2z + 2x^2y^2z^2) \\
&\qquad = 3xyz(yz^2 + y^2z + xz^2 + xy^2 + x^2z + x^2y + 2xyz) \\
&\qquad = 3xyz(x + y)(y + z)(z + x) \ .
\end{aligned}$$

Solution 2. Let the polynomial be $P_4(x, y, z)$. Since $P_4(0, y, z) = P_4(x, 0, z) = P_4(x, y, 0) = P_4(x, -x, 0) = P_4(0, y, -y) = P_4(-z, 0, z) = 0$, $P_4(x, y, z)$ contains the factors $x, y, z, x + y, y + z, z + x$. Hence

$$P_4(x, y, z) = kxyz(x + y)(y + z)(z + x) \ .$$

Since $8k = P_4(1, 1, 1) = 24$, $k = 3$ and we obtain the factorization.

Solution 3. [D. Rhee]

$$\begin{aligned}
P_4(x, y, z) &= [z(x + y) + xy]^3 - x^3y^3 - y^3z^3 - z^3x^3 \\
&= z^3(x + y)^3 + 3z^2(x + y)^2xy + 3z(x + y)(xy)^2 - z^3(x + y)(x^2 - xy + y^2) \\
&= (x + y)z[z^2(x + y)^2 + 3z(x + y)xy + 3(xy)^2 - z^2(x + y)^2 + 3z^2(xy)] \\
&= 3(x + y)xyz[z(x + y) + xy + z^2] = 3(x + y)xyz(x + z)(y + z) \ .
\end{aligned}$$

(e) Let $P_5(x,y,z)$ be the polynomial to be factored. Since

$$x^3y^3 - x^4yz = x^3y(y^2 - xz) = x^2(xy)(y^2 - xz) ,$$

$$y^3z^3 - xyz^4 = yz^3(y^2 - xz) ,$$

and

$$z^3x^3 - xy^4z = z^3x^3 - x^2y^2z^2 + x^2y^2z^2 - xy^4z = z^2x^2(zx - y^2) + xy^2z(zx - y^2) ,$$

it follows that

$$\begin{aligned} P_5(x,y,z) &= (y^2 - zx)[x^3y + yz^3 - z^2x^2 - xy^2z] \\ &= -(y^2 - zx)(z^2 - xy)(x^2 - yz) = (zx - y^2)(xy - z^2)(yz - x^2) , \end{aligned}$$

(f) Let $P_6(x,y,z,w)$ be the polynomial to be factored. Any factorization of $P_6(x,y,z,w)$ will reduce to a factorization of $P_6(x,y,0,0)$ when $z = w = 0$, so we begin by factoring this reduced polynomial:

$$P_6(x,y,0,0) = 2(x^4 + y^4) - (x^2 + y^2)^2 = (x^2 - y^2)^2 = (x + y)^2(x - y)^2 .$$

Similar factorizations occur upon suppressing other pairs of variables. So we look for linear factors that reduce to $x + y$ and $x - y$ when $z = w = 0$, *etc.*. Also the factors must either be symmetrical in x, y, z or come in symmetrical groups. The possibilities, up to sign, are $\{x + y + z + w\}$, $\{x + y + z - w, x + y - z + w, x - y + z + w, -x + y + z + w\}$ and $\{x + y - z - w, x - y + z - w, x - y - z + w\}$. Since $P_6(x,y,z,w)$ has degree 4, there are two possible factorizations:

$$(1) \qquad (x + y + z + w)(x + y - z - w)(x - y + z - w)(x - y - z + w)$$

$$(2) \qquad -(x + y + z - w)(x + y - z + w)(x - y + z + w)(-x + y + z + w)$$

Checking (1) yields

$$\begin{aligned} &(x + y + z + w)(x + y - z - w)(x - y + z - w)(x - y - z + w) \\ &\quad = [(x + y)^2 - (z + w)^2][(x - y)^2 - (z - w)^2] \\ &\quad = [(x^2 + y^2 - z^2 - w^2) + 2(xy - zw)][(x^2 + y^2 - z^2 - w^2) - 2(xy - zw)] \\ &\quad = (x^2 + y^2 - z^2 - w^2)^2 - 4(xy - zw)^2 \\ &\quad = x^4 + y^4 + z^4 + w^4 + 2x^2y^2 + 2z^2w^2 - 2x^2z^2 - 2x^2w^2 - 2y^2z^2 - 2y^2w^2 \\ &\qquad\quad - 4x^2y^2 - 4z^2w^2 + 8xyzw \\ &\quad = x^4 + y^4 + z^4 + w^4 - 2(x^2y^2 + x^2z^2 + x^2w^2 + y^2z^2 + y^2w^2 + z^2w^2) + 8xyzw \\ &\quad = 2(x^4 + y^2 + z^4 + w^4) - (x^2 + y^2 + z^2 + w^2)^2 + 8xyzw . \end{aligned}$$

Thus, we have found the required factorization. ((2), of course, is not correct.)

(g) Let $P_7(x,y,z)$ be the polynomial to be factored.

Solution 1. Note that

$$\begin{aligned} P_7(x,y,0) &= 6(x^5 + y^5) - 5(x^2 + y^2)(x^3 + y^3) \\ &= (x + y)[6x^4 - 6x^3y + 6x^2y^2 - 6xy^3 + 6y^4 - 5(x^2 + y^2)(x^2 - xy + y^2) \\ &= (x + y)(x^4 - x^3y - 4x^2y^2 - xy^3 + y^4) \\ &= (x + y)[x^4 - 2x^2y^2 + y^4 - xy(x^2 + 2xy + y^2)] \\ &= (x + y)[(x + y)^2(x - y)^2 - xy(x + y)^2] = (x + y)^3(x^2 - 3xy + y^2) . \end{aligned}$$

Similarly, $(y+z)^3$ divides $P_7(0,y,z)$ and $(x+z)^3$ divides $P_y(x,0,z)$. This suggests that we try the factorization

$$Q_7(x,y,z) \equiv (x+y+z)^3(z^2+y^2+z^2-3xy-3yz-3zx) \ .$$

Since $P_7(1,0,0) = 1 = Q_y(1,0,0)$ and $P_7(1,1,1) = 18-45 = -27 \neq Q_7(1,1,1) = 27(-6)$, this does not work. So we need to look at the above factorizations differently:

$$P_7(x,y,0) = (x+y)^2(x^3+y^3-2x^2y-2xy^2) \ ;$$

$$P_7(x,0,z) = (x+z)^2(x^3+z^3-2x^2z-2xz^2) \ ;$$

$$P_7(0,y,z) = (y+z)^2(y^3+z^3-2y^2z-2yz^2) \ .$$

This suggests the trial:

$$R_7(x,y,z) \equiv (x+y+z)^2(x^3+y^3+z^3-2x^2y-2xy^2-2y^2z-2yz^2-2z^2x-2zx^2+kxyz) \ .$$

Now $P_7(1,1,1) = -27$ and $R_7(1,1,1) = 9(-9+k)$, so this will not work unless $k=6$. Checking, we find that

$$P_7(x,y,z) \equiv (x+y+z)^2(x^3+y^3+z^3-2x^2y-2xy^2-2y^2z-2yz^2-2z^2x-2zx^2+6xyz) \ .$$

Solution 2. [Y. Zhao] For $k=1,2,3$, let $S_k = x^k+y^k+z^k$; let $\sigma_1 = x+y+z$, $\sigma_2 = xy+yz+zx$ and $\sigma_3 = xyx$. Then $S_1 = \sigma_1$, $S_2 = \sigma_1 S_1 - 2\sigma_2$, $S_3 = \sigma_1 S_2 - \sigma_2 S_1 + 3\sigma_3$, $S_4 = \sigma_1 S_3 - \sigma_2 S_2 + \sigma_3 S_1$ and $S_5 = \sigma_1 S_4 - \sigma_2 S_3 + \sigma_3 S_2$, so that $S_2 = \sigma_1^2 - 2\sigma_2$, $S_3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$, $S_4 = \sigma_1^4 - 4\sigma_1^2\sigma_2 + 4\sigma_1\sigma_3 + 2\sigma_2^2$ and $S_5 = \sigma_1^5 - 5\sigma_1^3\sigma_2 + 5\sigma_1^2\sigma_3 + 5\sigma_1\sigma_2^2 - 5\sigma_2\sigma_3$.

$$\begin{aligned} P_7(x,y,z) &= 6S_5 - 5S_2S_3 \\ &= 6(\sigma_1^5 - 5\sigma_1^3\sigma_2 + 5\sigma_1^2\sigma_3 + 5\sigma_1\sigma_2^2 - 5\sigma_2\sigma_3) - 5(\sigma_1^2 - 2\sigma_2)(\sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3) \\ &= \sigma_1^5 - 5\sigma_1^3\sigma_2 + 15\sigma_1^2\sigma_3 = \sigma_1^2(\sigma_1^3 - 5\sigma_1\sigma_2 + 15\sigma_3) \ . \end{aligned}$$