Let $\mathbb{Z}^+$ denote the set of positive integers. If $f : \mathbb{Z}^+ \to \mathbb{Z}^+$ is a function and $m \in \mathbb{Z}^+$, let $f^{(m)}$ denote the composite function $f \circ f \circ \cdots \circ f$ (with $m$ copies of $f$). Find all functions $f : \mathbb{Z}^+ \to \mathbb{Z}^+$ with the property that $f^{(m)}(n) = f(mn)$ for all $m, n \in \mathbb{Z}^+$.

**Solution.** Observe first that there are certainly going to be infinitely many solutions, since all constant functions $f$ have this property.

Suppose $f : \mathbb{Z}^+ \to \mathbb{Z}^+$ satisfies the desired property. Setting $n = 1$, we see that $f^{(m)}(1) = f(m)$ for all $m \in \mathbb{Z}^+$. Hence for any $m, n \in \mathbb{Z}^+$ with $m \geq 2$ we have $f(m) = f(f(m - 1))$, and also

$$f(mn) = f^{(m)}(n) = f^{(m-1)}(f(n)) = f^{(m-1)}(f(n)(1)) = f^{(m+n-1)}(1) = f(m + n - 1).$$

We claim that these properties force $f(n) = f(3)$ for all $n \geq 3$. To show this it suffices to show that $f(n + 1) = f(n)$ for all $n \geq 3$, for which we use induction. The base case holds because

$$f(4) = f(2 \times 2) = f(2 + 2 - 1) = f(3),$$

and if $n \geq 4$ and we assume that $f(n) = f(n - 1)$, then $f(n + 1) = f(f(n)) = f(f(n - 1)) = f(n)$ as required.

Now write $A = f(1)$, $B = f(2)$, $C = f(n)$ for all $n \geq 3$. We must determine which choices of $A, B, C \in \mathbb{Z}^+$ satisfy the desired property. Note that we always have $B = f(A)$ and $C = f(B)$. We separate into cases.

**Case 1:** $C = 1$. Then we have $A = f(C) = f(f(3)) = f(4) = 1$ and $B = f(A) = f(1) = A = 1$ also, so $f$ is in fact the constant function with value 1.

**Case 2:** $C = 2$. Then we have $B = f(C) = f(f(3)) = f(4) = 2$ also, and $2 = f(A)$ which forces $A \neq 1$. We can in fact let $A = f(1)$ be any number bigger than 1, and set $f(n) = 2$ for $n \geq 2$; it is easy to see that the desired property is satisfied.

From now on, $C \geq 3$ so the desired property $f^{(m)}(n) = f(mn)$ is automatic when $n \geq 3$, both sides equalling $C$. Its non-automatic content when $n \leq 2$ is simply the requirements $B = f(A)$ and $C = f(B)$ that we have already observed; so it is enough to ensure that these hold.

**Case 3:** $C \geq 3$, $B = 1$. Then the requirement $C = f(B)$ says that $A = C$, and the requirement $B = f(A)$ gives a contradiction.

**Case 4:** $C \geq 3$, $B = 2$. Then the requirement $C = f(B)$ gives a contradiction.

**Case 5:** $C \geq 3$ and $B = C$. Then the requirement is just that $C = f(A)$, which holds exactly when $A > 1$.

**Case 6:** $C \geq 3$, $B \geq 3$, and $B \neq C$. Then the requirement $C = f(B)$ is automatic, and the requirement that $B = f(A)$ holds exactly when $A = 2$.

To sum up, the possible values of the triple $(A, B, C)$ are as follows:

$$(1, 1, 1), (2, 2, 2), (a, 2, 2), (a, c, c), \text{ and } (2, b, c),$$

where $a, b, c$ denote integers $\geq 3$ (not necessarily distinct).
2. Let \( n \) be a positive integer. Prove the inequality

\[
\sum_{k=1}^{n} \sqrt{n^2 - k^2} \sqrt{n^2 - (k-1)^2} < \frac{2n^3 + n}{3}.
\]

**Solution.** In fact, one can easily prove smaller upper bounds for the left-hand side, hereafter denoted LHS. Many entrants used the AM–GM inequality to do this; the Cauchy–Schwarz inequality, as used below, gives a better bound.

Note that the \( k = n \) term in LHS is zero, so we can rewrite it:

\[
\text{LHS} = \sum_{k=1}^{n-1} \sqrt{n^2 - k^2} \sqrt{n^2 - (k-1)^2}.
\]

We can now apply the Cauchy–Schwarz inequality

\[
\left( \sum_{k=1}^{n-1} a_k b_k \right)^2 \leq \left( \sum_{k=1}^{n-1} a_k^2 \right) \left( \sum_{k=1}^{n-1} b_k^2 \right)
\]

to find that

\[
\text{LHS}^2 \leq \left( \sum_{k=1}^{n-1} n^2 - k^2 \right) \left( \sum_{k=1}^{n-1} n^2 - (k-1)^2 \right).
\]

In fact, for \( n \geq 3 \) the inequality is strict, because equality holds in the Cauchy–Schwarz inequality only when \((a_1, \ldots, a_{n-1})\) and \((b_1, \ldots, b_{n-1})\) are proportional \((n-1)\)-tuples, which it is easy to see does not hold here.

Using the well-known formula \( 1^2 + 2^2 + \cdots + m^2 = \frac{m(m+1)(2m+1)}{6} \), our upper bound becomes

\[
\text{LHS}^2 \leq \left( (n-1)n^2 - \frac{(n-1)n(2n-1)}{6} \right) \left( (n-1)n^2 - \frac{(n-2)(n-1)(2n-3)}{6} \right)
= \left( (n-1)n(4n+1) \right) \left( (n-1)(4n^2 + 7n - 6) \right)
= \frac{(n-1)^2 n(4n+1)(4n^2 + 7n - 6)}{36}
= \frac{16n^6 - 65n^4 + 60n^3 - 5n^2 - 6n}{36}.
\]

It is easy to see that this upper bound for \( \text{LHS}^2 \) is less than the square of \( \frac{2n^3 + n}{3} \).

3. Let \( n \) be a positive integer. A **composition** of \( n \) is an ordered \( k \)-tuple \((n_1, n_2, \ldots, n_k)\) of positive integers satisfying \( n_1 + n_2 + \cdots + n_k = n \). Let \( C(n) \) be the set of all compositions of \( n \), where the length \( k \) of the tuple is allowed to vary (it can be anything from 1 to \( n \)). Prove that

\[
\sum_{(n_1, n_2, \ldots, n_k) \in C(n)} (-1)^{n-k} 1^{n_1} 2^{n_2} \cdots k^{n_k} = 1.
\]

**Solution.** It is convenient to prove a more general statement depending on two positive integers, \( m \) and \( n \):

\[
\sum_{(n_1, n_2, \ldots, n_k) \in C(n)} (-1)^{n-k} m^{n_1}(m+1)^{n_2} \cdots (m+k-1)^{n_k} = m.
\]
The original problem is the $m = 1$ case.

Our proof is by induction on $n$ (treating all $m$ simultaneously). The $n = 1$ base case simply says that $m = m$, so we can assume that $n \geq 2$ and that the result is known when $n$ is replaced by $n-1$. The idea of the inductive step is to write $\mathcal{C}(n)$ as the disjoint union of two subsets $\mathcal{C}(n)'$ and $\mathcal{C}(n)''$, where $\mathcal{C}(n)'$ consists of those compositions $(n_1, n_2, \cdots, n_k)$ where $n_1 \geq 2$ and $\mathcal{C}(n)''$ consists of those compositions $(n_1, n_2, \cdots, n_k)$ where $n_1 = 1$. We clearly have a bijection $\mathcal{C}(n)' \rightarrow \mathcal{C}(n-1)$ sending $(n_1, n_2, \cdots, n_k)$ to $(n_1 - 1, n_2, \cdots, n_k)$, and another bijection $\mathcal{C}(n)'' \rightarrow \mathcal{C}(n-1)$ sending $(n_1, n_2, \cdots, n_k)$ to $(n_2, n_3, \cdots, n_k)$, which is well defined because $k$ cannot equal 1 in the latter case (since $n \geq 2$). These bijections, incidentally, show that $|\mathcal{C}(n)| = 2|\mathcal{C}(n-1)|$, which with the base case $|\mathcal{C}(1)| = 1$ clearly implies that $|\mathcal{C}(n)| = 2^{n-1}$.

For the present problem, the bijections and the induction hypothesis show that

$$\sum_{(n_1, n_2, \cdots, n_k) \in \mathcal{C}(n)'} (-1)^{n-k} m^{n_1} (m + 1)^{n_2} \cdots (m + k - 1)^{n_k}$$

$$\quad = -m \sum_{(n_1 - 1, n_2, \cdots, n_k) \in \mathcal{C}(n-1)} (-1)^{(n-1)-k} m^{n_1-1} (m + 1)^{n_2} \cdots (m + k - 1)^{n_k}$$

$$\quad = -m^2$$;

$$\sum_{(n_1, n_2, \cdots, n_k) \in \mathcal{C}(n)''} (-1)^{n-k} m^{n_1} (m + 1)^{n_2} \cdots (m + k - 1)^{n_k}$$

$$\quad = m \sum_{(n_2, \cdots, n_k) \in \mathcal{C}(n-1)} (-1)^{(n-1)-(k-1)} (m + 1)^{n_2} \cdots (m + k - 1)^{n_k}$$

$$\quad = m(m + 1),$$

so the total sum is $-m^2 + m(m + 1) = m$, as required to complete the inductive step.

4. If $P$ is a convex polygon in the plane, let $M(P)$ be the convex polygon whose vertices are the midpoints of the edges of $P$. Say that $P$ is periodic if $M^k(P)$ is similar to $P$ for some positive integer $k$, where $M^k$ denotes $k$ applications of the operation $M$. For example, every triangle $T$ is periodic, because $M(T)$ is similar to $T$; every parallelogram $Q$ is periodic, because $M^2(Q)$ is similar to $Q$. Show that there is a periodic pentagon in which no two edges have the same length.

Solution. In fact, we will show that there are infinitely many similarity classes of pentagons $P$ with the property that no two edges have the same length and $M(P)$ is similar to $P$.

Identify the plane with the set of complex numbers. A convex pentagon $P$ can be specified (non-uniquely) by listing its vertices in (say) anti-clockwise order, starting from an arbitrarily chosen vertex. This gives a 5-tuple of complex numbers $(a_1, \cdots, a_5)$. Note that not every 5-tuple of complex numbers corresponds to a convex pentagon. However, any scalar multiple $(a a_1, \cdots, a a_5)$ of $(a_1, \cdots, a_5)$ with $a \neq 0$ (another complex number) does correspond to a convex pentagon, and one which is similar to $P$. To see this, write $a = r e^{i \theta}$; multiplying by $a$ has the effect of dilating by a factor of $r$ and rotating by $\theta$.

If the 5-tuple associated to $P$ as above is $(a_1, \cdots, a_5)$, the 5-tuple associated to $M(P)$ (or rather one of the 5-tuples associated to $M(P)$, namely that obtained by choosing as the first vertex the midpoint opposite the first vertex of $P$) is

$$T(a_1, \cdots, a_5) := \left( \frac{a_3 + a_4}{2}, \frac{a_4 + a_5}{2}, \frac{a_1 + a_5}{2}, \frac{a_1 + a_2}{2}, \frac{a_2 + a_3}{2} \right).$$

Hence, if $(a_1, \cdots, a_5)$ is an eigenvector of this linear transformation $T$ of $\mathbb{C}^5$ for a nonzero eigenvalue, i.e. $T(a_1, \cdots, a_5) = a(a_1, \cdots, a_5)$ with $a \neq 0$, then $M(P)$ is similar to $P$. 

A straightforward calculation shows that the characteristic polynomial of $T$ is
\[\frac{16x^5 - 20x^3 + 5x - 1}{16} = (x - 1)(4x^2 + 2x - 1)^2.\]
To find this factorization, it helps to realize that 1 is an eigenvalue of $T$ because $T(1, 1, 1, 1, 1) = (1, 1, 1, 1, 1)$. We conclude that the other eigenvalues of $T$ are $-\frac{1 \pm \sqrt{5}}{2}$, each repeated. If we let $\phi$ denote the golden ratio $\frac{1 + \sqrt{5}}{2}$ as is customary, then these other eigenvalues of $T$ can be written $-\phi/2$ and $\phi^{-1}/2$.

One can see directly that $-\phi/2$ is an eigenvalue of $T$, because if we start with a regular pentagon with centre at the origin, we find that indeed $T = (\phi/2) a_5$ (this uses the fact that $\cos(\pi/5) = \phi/2$). For example, this holds for the pentagon $P_0$ with vertices equal to the five complex $5$th roots of 1, namely $1, \zeta, \zeta^2, \zeta^3, \zeta^4$ where $\zeta = e^{2\pi i/5}$. Of course, this is not a solution to the problem, because all edges of $P_0$ have equal length. However, the fact that $(1, \zeta, \zeta^2, \zeta^3, \zeta^4)$ is an eigenvector of $T$ for the (real) eigenvalue $-\phi/2$ implies that so is the complex conjugate vector $(1, \bar{\zeta}, \zeta^2, \zeta^3, \zeta)$, and hence so is any linear combination of the form
\[\epsilon(1, \zeta, \zeta^2, \bar{\zeta}, \zeta) + (1, \zeta, \zeta^2, \zeta^3, \zeta),\]
where $\epsilon$ is a nonzero complex number. If $\epsilon$ is sufficiently small, then the resulting $5$-tuple must still correspond to a convex pentagon $P$ with vertices listed in anti-clockwise order, which is only a “small perturbation” of the regular pentagon $P_0$. It is easy to see that for generic values of $\epsilon$, $P$ will have no two edges of the same length, so it solves the problem.

Notice that this solution pentagon $P$ is obtained from the regular pentagon $P_0$ by applying the transformation $z \mapsto z + \epsilon\bar{z}$ of the complex plane, which is a linear transformation of the plane thought of as a real vector space.

5. Let $F$ be the field of integers modulo $p$, where $p$ is a prime number. Define a finite set
\[X = \{(x, y, z) \in F^3 \mid x^6 + y^3 + z^2 = 0\}.
\]
Show that $|X| = p^2$ if and only if $p \equiv 1 \pmod{6}$.

**Solution.** Assume that $p \equiv 1 \pmod{6}$. Then $p \equiv 1 \pmod{3}$, since there are clearly no primes congruent to 4 modulo 6. The $p-1$ nonzero elements of $F$ form a group $F^\times$ under multiplication (in fact, a cyclic group), with identity element $1_F$. The fact that $3 \nmid p - 1$ means that the only $y \in F$ such that $y^3 = 1_F$ is $y = 1_F$ itself. So the group homomorphism $F^\times \to F^\times : y \mapsto y^3$ has trivial kernel and therefore must be injective, hence bijective because its codomain and domain have the same finite size; this means that the map $F \to F : y \mapsto y^3$ is also bijective. So $X$ is in bijection with the set
\[X' = \{(x, y', z) \in F^3 \mid x^6 + y' + z^2 = 0\}\]
via the map $X \to X' : (x, y, z) \mapsto (x, y^3, z)$. It is clear that $X'$ is in bijection with $F^2$ via the map $X' \to F^2 : (x, y', z) \mapsto (x, z)$, so $|X| = |X'| = |F^2| = p^2$.

If $p \equiv 1 \pmod{6}$, then consider the following element of the field $F$:
\[S = \sum_{(x,y,z) \in F^3} (x^6 + y^3 + z^2)^{p-1}.
\]
On the one hand, for any nonzero $a \in F$ we have $a^{p-1} = 1_F$, so
\[S = (p^3 - |X|) \cdot 1_F \quad \text{(meaning } 1_F + 1_F + \cdots + 1_F \text{ with } p^3 - |X| \text{ terms}).\]
In other words, $S$ is the integer $-|X|$ interpreted modulo $p$.

On the other hand, we can expand the trinomial and obtain

$$S = \sum_{(x,y,z) \in F^3} \sum_{a,b,c \in \mathbb{N}} \frac{p-1}{(a,b,c)} \cdot x^6a y^3b z^{2c}.$$

$$= \sum_{a,b,c \in \mathbb{N}} \frac{p-1}{(a,b,c)} \cdot \left( \sum_{x \in F} x^6a \right) \left( \sum_{y \in F} y^3b \right) \left( \sum_{z \in F} z^{2c} \right).$$

Now $\sum_{x \in F} x^0 = p \cdot 1_F = 0$. If $1 \leq e \leq p-2$, we claim that $\sum_{x \in F} x^e = 0$ also. The simplest proof is that, since $F^\times$ is cyclic, there exists some $y \in F^\times$ such that $y^e \neq 1_F$, whereas we have

$$(y^e - 1_F) \sum_{x \in F} x^e = \sum_{x \in F} (xy)^e - \sum_{x \in F} x^e = \sum_{x \in F} (x')^e - \sum_{x \in F} x^e = 0.$$

So the product of the three sums $\sum_{x \in F} x^6a, \sum_{y \in F} y^3b, \sum_{z \in F} z^{2c}$ can only be nonzero if

$$a \geq \frac{p-1}{6}, \quad b \geq \frac{p-1}{3}, \quad \text{and} \quad c \geq \frac{p-1}{2}.$$

The constraint that $a + b + c = p - 1$ then forces $a = \frac{p-1}{6}, b = \frac{p-1}{3},$ and $c = \frac{p-1}{2}$; since $p \equiv 1 \mod 6$, these are indeed all integers. Note that $\sum_{x \in F} x^{p-1} = (p-1) \cdot 1_F = -1_F$. We conclude that

$$S = \left( \frac{p-1}{6}, \frac{p-1}{3}, \frac{p-1}{2} \right) \cdot (-1_F)^3,$$

and hence

$$|X| \equiv \left( \frac{p-1}{6}, \frac{p-1}{3}, \frac{p-1}{2} \right) \mod p.$$

The trinomial coefficient here is a divisor of $(p-1)!$, which is not divisible by $p$. Thus $|X| \neq 0 \mod p$, which obviously implies $|X| \neq p^2$ as required.

6. Define a function $f : (-\infty, 1) \to \mathbb{R}$ by

$$f(x) = \int_0^1 \frac{\sqrt{2-x}}{\sqrt{1 - s^2 \sqrt{1 - xs^2}}} ds.$$

Show that $f(x)$ has a global minimum at $x = 0$.

**Solution.** (Due to entrant Terence Harris, University of New South Wales). Fix $x \in (-\infty, 1)$. The change of variable $s = \sin \frac{\pi t}{2}$ gives

$$f(x) = \frac{\pi \sqrt{2-x}}{2} \int_0^1 (1 - x(\sin \frac{\pi t}{2})^2)^{-1/2} dt.$$

Notice that $1 - x(\sin \frac{\pi t}{2})^2 > 0$, so $(1 - x(\sin \frac{\pi t}{2})^2)^{-1/2}$ is well defined. Since the function $y \mapsto y^{-1/2}$ is convex on its domain $(0, \infty)$, we can apply the integral version of Jensen's
7. Let \( \zeta = e^{\pi i/6} = \sqrt{3}/2 + \frac{1}{2}i \), and let \( \mathbb{Z}[\zeta] \) denote the set of integer linear combinations of the powers of \( \zeta \). Suppose that \( u, v \in \mathbb{Z}[\zeta] \) satisfy \( |u|^2 = 3|v|^2 + 1 \) and \( v \neq 0 \). Show that \( |v|^2 \geq 2 + \sqrt{3} \), and find when equality occurs.

**Solution.** Since the minimal polynomial of \( \zeta \) is \( x^4 - x^2 + 1 \), any element of \( \mathbb{Z}[\zeta] \) can be written uniquely as \( a + b\zeta + c\zeta^2 + d\zeta^3 \) where \( a, b, c, d \in \mathbb{Z} \). Finding real and imaginary parts, we see that

\[
a + b\zeta + c\zeta^2 + d\zeta^3 = (a + \frac{\sqrt{3}}{2}b + \frac{1}{2}c) + (\frac{1}{2}b + \frac{\sqrt{3}}{2}c + d)i
\]

so

\[
|a + b\zeta + c\zeta^2 + d\zeta^3|^2 = (a + \frac{\sqrt{3}}{2}b + \frac{1}{2}c)^2 + \left(\frac{1}{2}b + \frac{\sqrt{3}}{2}c + d\right)^2
\]

\[
= (a^2 + ac + c^2 + b^2 + bd + d^2) + (ab + bc + cd)\sqrt{3}.
\]

Thus, if we let \( u = a + b\zeta + c\zeta^2 + d\zeta^3 \) and \( v = a' + b'\zeta + c'\zeta^2 + d'\zeta^3 \) where \( a, b, c, d, a', b', c', d' \in \mathbb{Z} \), the equation \( |u|^2 = 3|v|^2 + 1 \) becomes the following two equations:

\[
a^2 + ac + c^2 + b^2 + bd + d^2 = 1 + 3(a'b' + b'c' + c'd'), \tag{1}
\]

and

\[
ab + bc + cd = a'^2 + a'c' + c'^2 + b'^2 + b'd' + d'^2. \tag{2}
\]

Now the quadratic form \( x^2 + xy + y^2 \) is positive-definite, since

\[
4(x^2 + xy + y^2) = (x - y)^2 + 3(x + y)^2. \tag{3}
\]

Since \( a^2 + ac + c^2 \) is an integer, we have \( a^2 + ac + c^2 \geq 1 \) unless \( a = c = 0 \), and similarly \( b^2 + bd + d^2 \geq 1 \) unless \( b = d = 0 \). If either \( a = c = 0 \) or \( b = d = 0 \), then the left-hand side of (2) vanishes, forcing the right-hand side of (2) to vanish, which then by the same positive-definiteness forces \( a' = b' = c' = b' = d' = 0 \), contrary to the assumption that \( v \neq 0 \). We conclude that \( a^2 + ac + c^2 \geq 1 \) and \( b^2 + bd + d^2 \geq 1 \), meaning that the left-hand side of (1) is at least 2. Hence the right-hand side of (1) is at least 2, implying that \( a'b' + b'c' + c'd' \geq 1 \). This in turn implies that it is not true that \( a' = c' = 0 \) or that \( b' = d' = 0 \), so \( a'^2 + a'c' + c'^2 \geq 1 \) and \( b'^2 + b'd' + d'^2 \geq 1 \). Hence we have

\[
|v|^2 = (a^2 + a'c' + c'^2 + b^2 + b'd' + d'^2) + (a'b' + b'c' + c'd')\sqrt{3} \geq 2 + \sqrt{3},
\]
as claimed.

For equality to hold, i.e. to have \( \left| v \right|^2 = 2 + \sqrt{3} \), we need \( a', b', c', d' \in \mathbb{Z} \) to be such that 
\( a'^2 + a'c' + c'^2 = 1 \) and \( b'^2 + b'd' + d'^2 = 1 \), in addition to \( a'b' + b'c' + c'd' = 1 \). Using (3) we see 
that \( a'^2 + a'c' + c'^2 = 1 \) forces either \( a' = \pm 1, c' = \mp 1 \) or \( a' = \pm 1, c' = 0 \) or \( a' = 0, c' = \pm 1 \). 
The same trichotomy holds for \( b' \) and \( d' \). Applying the final condition \( a'b' + b'c' + c'd' = 1 \), we get the following twelve possibilities for \( (a', b', c', d') \) (and thus for \( v \)):

\[
(a', b', c', d') \in \{ \pm(1, 0, -1, -1), \pm(1, 1, -1, -1), \pm(1, 1, 0, 0), \\
\pm(1, 1, 0, 1), \pm(0, 1, 1, 0), \pm(0, 0, 1, 1) \}.
\]

Since \(|\zeta| = 1\), all these possible values of \( v \) can be obtained from just one (say, \( v = 1 + \zeta \)) by multiplying by the twelve distinct powers of \( \zeta \).

We also need to have \( |u|^2 = 4 + 2\sqrt{3} \), i.e. we need \( a, b, c, d \in \mathbb{Z} \) to be such that \( a^2 + ac + c^2 + b^2 + bd + d^2 = 4 \) and \( ab + bc + cd = 2 \). Considering (3) modulo 3, we see that we cannot have \( a^2 + ac + c^2 = 2 \), so the only possibilities are \( a^2 + ac + c^2 = 1 \) and \( b^2 + bd + d^2 = 3 \) or \( a^2 + ac + c^2 = 3 \) and \( b^2 + bd + d^2 = 1 \). In the first of these cases, we have the trichotomy for \( a \) and \( c \) as above, whereas \( b^2 + bd + d^2 = 3 \) forces either \( b = d = \pm 1 \) or \( b = \pm 2, d = \mp 1 \) or \( b = \pm 1, d = \mp 2 \). Applying the final condition \( ab + bc + cd = 2 \), we get the following possibilities for \( (a, b, c, d) \) (and thus for \( u \)):

\[
(a, b, c, d) \in \{ \pm(1, 1, -1, -2), \pm(1, 2, 0, -1), \pm(0, 1, 1, 1) \}.
\]

The other case gives the following possibilities for \( (a, b, c, d) \) (and thus for \( u \)):

\[
(a, b, c, d) \in \{ \pm(2, 1, -1, -1), \pm(1, 0, -2, -1), \pm(1, 1, 1, 0) \}.
\]

So there are twelve possibilities for \( u \) in all; again, they can be obtained from just one (say, \( u = 1 + 2\zeta - \zeta^3 = 1 + \sqrt{3} \)) by multiplying by the twelve distinct powers of \( \zeta \).

8. Let \( d \) be a fixed integer, at least 2. If \( P(x) \) is a polynomial in \( x \), let \( \lceil P(x) \rceil \) be the polynomial obtained by rounding up each exponent of \( x \) to the nearest multiple of \( d \), so that \( \lceil P(x) \rceil \) is a polynomial in \( x^d \). For example, if \( d = 3 \) then

\[
\lceil 2 + 5x^2 + 4x^3 + x^4 \rceil = 2 + 5x^3 + 4x^3 + x^6 = 2 + 9x^3 + x^6.
\]

Suppose that all we know about \( P(x) \) is that it has nonnegative real coefficients. Show that if we are given all of the polynomials \( \lceil P(x) \rceil, \lceil P(x)^2 \rceil, \lceil P(x)^3 \rceil, \ldots \), we can determine \( P(x) \).

**Solution.** The intention of the question, as stated by a clarification on the competition webpage, was that the integer \( d \) was also to be regarded as given.

The wording “Show that . . . we can determine \( P(x)^m \)” was also ambiguous. On one interpretation, it simply requires us to show that there cannot be two different polynomials \( P(x) \) with nonnegative real coefficients that give rise to the same sequence of polynomials \( \lceil P(x)^m \rceil \) for \( m \geq 1 \). As pointed out by entrant Terence Harris (University of New South Wales), this follows from the fact that for any fixed real number \( y \geq 1 \),

\[
P(y)^m \leq \lceil P(y)^m \rceil \leq y^{d-1} P(y)^m,
\]

and hence

\[
\lim_{m \to \infty} \lceil P(y)^m \rceil^{1/m} = P(y).
\]
However, on another interpretation, “determining $P(x)$” requires a finite algorithm (in particular, not involving limits) to determine the various coefficients of the polynomial $P(x)$ from the coefficients of the known polynomials $[P(x)]^m$. Such an algorithm follows.

A trivial but vital observation is that the operation $[\cdot]$ is linear, in the sense that $[aQ(x) + bR(x)] = a[Q(x)] + b[R(x)]$ for any polynomials $Q(x), R(x)$ and numbers $a, b$. Also note that $[x^k Q(x)] = x^k [Q(x)]$ for all nonnegative integers $k$. We will use these rules henceforth without further comment.

If $Q(x)$ is any polynomial, write $Q(x)[x^j]$ for the coefficient of $x^j$ in $Q(x)$. We first show that it suffices to prove the claim in the case when $P(x)[x^0] = 0$ (i.e. $P(x)$ has no constant term). The reason is that if we know $[P(x)^m]$ for all $m \geq 0$, then we know $P(x)[x^0] = [P(x)][x^0]$, and so we also know

$$[(P(x) - P(x)[x^0])^m] = \sum_{j=0}^{m} \binom{m}{j} (-P(x)[x^0])^{m-j}[P(x)^j] \quad \text{for all } m \geq 0.$$ 

So assuming we can solve the problem for polynomials with no constant term, we can determine $P(x) - P(x)[x^0]$ and hence the original $P(x)$.

Now it is enough to prove the following claim for all nonnegative integers $n$: for a polynomial $P(x)$ with $P(x)[x^i] \geq 0$ for all $j$ and $P(x)[x^0] = 0$, if we know $[P(x)^m]$ for all $m \geq 0$, then we can determine $P(x)[x^n]$. We prove this claim by induction on $n$, the $n = 0$ case being obvious. So we can assume that $n \geq 1$ and that the claim is true when $n$ is replaced by a smaller nonnegative integer.

The inductive hypothesis implies that from the assumed knowledge of $[P(x)^m]$ for all $m \geq 0$, we can determine the coefficients $P(x)[x^i], \ldots, P(x)[x^{n-1}]$. If these coefficients are all zero (or if $n = 1$), then $(P(x)^d)[x^j] = 0$ for all $j < nd$ and $P(x)^d)[x^{nd}] = (P(x)[x^n]^d$. So $[P(x)^d][x^{nd}] = (P(x)[x^n])^d$ also, and hence we know $(P(x)[x^n])^d$ and can determine $P(x)[x^n]$ by taking the $d$th root. Here is where it matters that we are dealing with nonnegative real numbers.

Otherwise, we have $P(x)[x^i] = \cdots = P(x)[x^{i-1}] = 0$ and $P(x)[x^i] > 0$ for some positive integer $i < n$. In particular, $x^{-i}P(x)$ is a polynomial in $x$ with constant term $P(x)[x^i]$. Define

$$Q(x) = (x^{-i}P(x))^d - (P(x)[x^i])^d \quad \text{and} \quad R(x) = x^{-i}P(x) - P(x)[x^i],$$

two other polynomials in $x$ with nonnegative real coefficients and no constant term. By assumption we know

$$[Q(x)^m] = \sum_{j=0}^{m} \binom{m}{j} (-P(x)[x^i])^{d-j} x^{-ij}[P(x)^{jd}] \quad \text{for all } m \geq 0.$$

So by the inductive hypothesis we can determine the coefficient $Q(x)[x^{n-i}]$. By definition,

$$Q(x)[x^{n-i}] = ((R(x) + P(x)[x^i])^d - (P(x)[x^i])^d)[x^{n-i}] = \sum_{k=1}^{d} \binom{d}{k} (P(x)[x^i])^{d-k} R(x)^k[x^{n-i}].$$

Now if $k \geq 2$ and we write the coefficient $R(x)^k[x^{n-i}]$ as a function of the coefficients $R(x)[x^1] = P(x)[x^{i+1}], R(x)[x^2] = P(x)[x^{i+2}], \ldots$ of $R(x)$, we see that it cannot involve any coefficient $R(x)[x^a] = P(x)[x^{a+i}]$ for $a \geq n - i$, because $k - 1 + a > n - i$. So in
the above expression for $Q(x)[x^{n-i}]$, all the terms of the sum with $k \geq 2$ involve only coefficients of $P(x)$ that have already been determined. Thus we can determine the remaining $k = 1$ term, which is $d(P(x)[x^i])^{d-1} P(x)[x^n]$. Since $P(x)[x^i] \neq 0$ by assumption, we can determine $P(x)[x^n]$ from this, completing the inductive step.