A–1 The only such \( \alpha \) are \( 2/3, 3/2, (13 \pm \sqrt{601})/12. \)

**First solution:** Let \( C_1 \) and \( C_2 \) be the curves \( y = \alpha x^2 + \alpha x + 1/3 \) and \( x = \alpha y^2 + \alpha y + 1/3 \), respectively, and let \( L \) be the line \( y = x \). We consider three cases.

If \( C_1 \) is tangent to \( L \), then the point of tangency \((x, x)\) satisfies

\[
2\alpha x + \alpha = 1, \quad x = \alpha x^2 + \alpha x + 1/24;
\]

by symmetry, \( C_2 \) is tangent to \( L \) there, so \( C_1 \) and \( C_2 \) are tangent. Writing \( \alpha = 1/(2x + 1) \) in the first equation and substituting into the second, we must have

\[
x = \frac{x^2 + x + 1}{2x + 1} + \frac{1}{24},
\]

which simplifies to \( 0 = 24x^2 - 2x - 1 = (6x + 1)(4x - 1) \), or \( x \in \{1/4, -1/6\} \). This yields \( \alpha = 1/(2x + 1) \in \{2/3, 3/2\} \).

If \( C_1 \) does not intersect \( L \), then \( C_1 \) and \( C_2 \) are separated by \( L \) and so cannot be tangent.

If \( C_1 \) intersects \( L \) in two distinct points \( P_1, P_2 \), then it is not tangent to \( L \) at either point. Suppose at one of these points, say \( P_1 \), the tangent to \( C_1 \) is perpendicular to \( L \); then by symmetry, the same will be true of \( C_2 \), so \( C_1 \) and \( C_2 \) will be tangent at \( P_1 \). In this case, the point \( P_1 = (x, x) \) satisfies

\[
2\alpha x + \alpha = -1, \quad x = \alpha x^2 + \alpha x + 1/24;
\]

writing \( \alpha = -1/(2x + 1) \) in the first equation and substituting into the second, we have

\[
x = \frac{x^2 + x + 1}{2x + 1} + \frac{1}{24},
\]

or \( x = (-23 \pm \sqrt{601})/72 \). This yields \( \alpha = -1/(2x + 1) = (13 \pm \sqrt{601})/12. \)

If instead the tangents to \( C_1 \) at \( P_1, P_2 \) are not perpendicular to \( L \), then we claim there cannot be any point where \( C_1 \) and \( C_2 \) are tangent. Indeed, if we count intersections of \( C_1 \) and \( C_2 \) (by using \( C_1 \) to substitute for \( y \) in \( C_2 \), then solving for \( y \)), we get at most four solutions counting multiplicity. Two of these are \( P_1 \) and \( P_2 \), and any point of tangency counts for two more. However, off of \( L \), any point of tangency would have a mirror image which is also a point of tangency, and there cannot be six solutions. Hence we have now found all possible \( \alpha \).

**Second solution:** For any nonzero value of \( \alpha \), the two conics will intersect in four points in the complex projective plane \( \mathbb{P}^2(\mathbb{C}) \). To determine the \( y \)-coordinates of these intersection points, subtract the two equations to obtain

\[
(y - x) = \alpha(x + y)(x + y) + (x - y).
\]

Therefore, at a point of intersection we have either \( x = y \), or \( x = -1/\alpha - (y + 1) \). Substituting these two possible linear conditions into the second equation shows that the \( y \)-coordinate of a point of intersection is a root of either \( Q_1(y) = \alpha y^2 + (\alpha - 1)y + 1/24 \) or \( Q_2(y) = \alpha y^2 + (\alpha + 1)y + 25/24 + 1/\alpha \).

If two curves are tangent, then the \( y \)-coordinates of at least two of the intersection points will coincide; the converse is also true because one of the curves is the graph of a function in \( x \). The coincidence occurs precisely when either the discriminant of at least one of \( Q_1 \) or \( Q_2 \) is zero, or there is a common root of \( Q_1 \) and \( Q_2 \). Computing the discriminants of \( Q_1 \) and \( Q_2 \) yields (up to constant factors) \( f_1(\alpha) = 6\alpha^2 - 13\alpha + 6 \) and \( f_2(\alpha) = 6\alpha^2 - 13\alpha - 18 \), respectively. If on the other hand \( Q_1 \) and \( Q_2 \) have a common root, it must be also a root of \( Q_2(y) - Q_1(y) = 2y + 1 + 1/\alpha \), yielding \( y = -1/\alpha \). Thus the values of \( \alpha \) for which the two curves are tangent must be contained in the set of zeros of \( f_1 \) and \( f_2 \), namely \( 2/3, 3/2, \) and \( (13 \pm \sqrt{601})/12 \).

**Remark:** The fact that the two conics in \( \mathbb{P}^2(\mathbb{C}) \) meet in four points, counted with multiplicities, is a special case of Bézout’s theorem: two curves in \( \mathbb{P}^2(\mathbb{C}) \) of degrees \( m,n \) and not sharing any common component meet in exactly \( mn \) points when counted with multiplicity.

Many solvers were surprised that the proposers chose the parameter \( 1/24 \) to give two rational roots and two nonrational roots. In fact, they had no choice in the matter: attempting to make all four roots rational by replacing \( 1/24 \) by \( \beta \) amounts to asking for \( \beta^2 + \beta + 1 \) to be perfect squares. This cannot happen outside of trivial cases (\( \beta = 0, -1 \)) ultimately because the elliptic curve 24A1 (in Cremona’s notation) over \( \mathbb{Q} \) has rank 0. (Thanks to Noam Elkies for providing this computation.)

However, there are choices that make the radical milder, e.g., \( \beta = 1/3 \) gives \( \beta^2 + \beta = 4/9 \) and \( \beta^2 + \beta + 1 = 13/9 \), while \( \beta = 3/5 \) gives \( \beta^2 + \beta = 24/25 \) and \( \beta^2 + \beta + 1 = 49/25. \)

A–2 The minimum is 4, achieved by the square with vertices \((\pm 1, \pm 1)\).
First solution: To prove that 4 is a lower bound, let $S$ be a convex set of the desired form. Choose $A, B, C, D \in S$ lying on the branches of the two hyperbolas, with $A$ in the upper right quadrant, $B$ in the upper left, $C$ in the lower left, $D$ in the lower right. Then the area of the quadrilateral $ABCD$ is a lower bound for the area of $S$.

Write $A = (a, 1/a)$, $B = (-b, 1/b)$, $C = (-c, -1/c)$, $D = (d, -1/d)$ with $a, b, c, d > 0$. Then the area of the quadrilateral $ABCD$ is

$$\frac{1}{2} (a/b + b/c + c/d + d/a) = \frac{1}{2} (a + b + c + d / a + b / c + c / d + d / a),$$

which by the arithmetic-geometric mean inequality is at least 4.

Second solution: Choose $A, B, C, D$ as in the first solution. Note that both the hyperbolas and the area of the convex hull of $ABCD$ are invariant under the transformation $(x, y) \mapsto (xm, y/m)$ for any $m > 0$. For $m$ small, the counterclockwise angle from the line $AC$ to the line $BD$ approaches 0; for $m$ large, this angle approaches $\pi/2$. By continuity, for some $m$ this angle becomes $\pi/2$, that is, $AC$ and $BD$ become perpendicular. The area of $ABCD$ is then $AC \cdot BD$.

It thus suffices to note that $AC \geq 2\sqrt{2}$ (and similarly for $BD$). This holds because if we draw the tangent lines to the hyperbola $xy = 1$ at the points $(1, 1)$ and $(-1, -1)$, then $A$ and $C$ lie outside the region between these lines. If we project the segment $AC$ orthogonally onto the line $x = y = 1$, the resulting projection has length at least $2\sqrt{2}$, so $AC$ must as well.

Third solution: (by Richard Stanley) Choose $A, B, C, D$ as in the first solution. Now fixing $A$ and $C$, move $B$ and $D$ to the points at which the tangents to the curve are parallel to the line $AC$. This does not increase the area of the quadrilateral $ABCD$ (even if this quadrilateral is not convex).

Note that $B$ and $D$ are now diametrically opposite; write $B = (-x, 1/x)$ and $D = (x, -1/x)$. If we thus repeat the procedure, fixing $B$ and $D$ and moving $A$ and $C$ to the points where the tangents are parallel to $BD$, then $A$ and $C$ must move to $(x, 1/x)$ and $(-x, -1/x)$, respectively, forming a rectangle of area 4.

Remark: Many geometric solutions are possible. An example suggested by David Savitt (due to Chris Brewer): note that $AD$ and $BC$ cross the positive and negative $x$-axes, respectively, so the convex hull of $ABCD$ contains $O$. Then check that the area of triangle $OAB$ is at least 1, et cetera.

A–3 Assume that we have an ordering of $1, 2, \ldots, 3k + 1$ such that no initial subsequence sums to 0 mod 3. If we omit the multiples of 3 from this ordering, then the remaining sequence mod 3 must look like $1, 1, -1, 1, -1, \ldots$ or $-1, -1, 1, -1, \ldots$. Since there is one more integer in the ordering congruent to 1 mod 3 than to $-1$, the sequence mod 3 must look like $1, 1, -1, 1, -1, \ldots$.

It follows that the ordering satisfies the given condition if and only if the following two conditions hold: the first element in the ordering is not divisible by 3, and the sequence mod 3 (ignoring zeroes) is of the form $1, 1, -1, 1, \ldots$. The two conditions are independent, and the probability of the first is $(2k + 1)/(3k + 1)$ while the probability of the second is $1/(2k + 1)$, since there are $(2k + 1)$ ways to order $(k + 1)$’s and $k$’s. Hence the desired probability is the product of these two, or $\frac{k!(k+1)!}{(3k+1)!(2k)!}$.

A–4 Note that $n$ is a repunit if and only if $9n + 1 = 10^m$ for some power greater than 1. Consequently, if we put

$$g(n) = 9f\left(\frac{n-1}{9}\right) + 1,$$

then $f$ takes repunits to repunits if and only if $g$ takes powers of 10 greater than 1 to powers of 10 greater than 1. We will show that the only such functions $g$ are those of the form $g(n) = 10^k n^d$ for $d \geq 0$, $c \geq 1 - d$ (all of which clearly work), which will mean that the desired polynomials $f$ are those of the form

$$f(n) = \frac{1}{9} (10^d (9n + 1)^d - 1)$$

for the same $c, d$.

It is convenient to allow “powers of 10” to be of the form $10^k$ for any integer $k$. With this convention, it suffices to check that the polynomials $g$ taking powers of 10 greater than 1 to powers of 10 are of the form $10^k n^d$ for any integers $c, d$ with $d \geq 0$.

First solution: Suppose that the leading term of $g(x)$ is $a x^d$, and note that $a > 0$. As $x \to \infty$, we have $g(x)/x^d \to a$; however, for $x$ a power of 10 greater than 1, $g(x)/x^d$ is a power of 10. The set of powers of 10 has no positive limit point, so $g(x)/x^d$ must be equal to $a$ for $x = 10^k$ with $k$ sufficiently large, and we must have $a = 10^c$ for some $c$. The polynomial $g(x) - 10^c x^d$ has infinitely many roots, so must be identically zero.

Second solution: We proceed by induction on $d = \deg(g)$. If $d = 0$, we have $g(n) = 10^c$ for some $c$. Otherwise, $g$ has rational coefficients by Lagrange’s interpolation formula (this applies to any polynomial of degree $d$ taking at least $d + 1$ different rational numbers to rational numbers), so $g(0) = t$ is rational. Moreover, $g$ takes each value only finitely many times, so the sequence $g(10^0), g(10^1), \ldots$ includes arbitrarily large powers of 10. Suppose that $t \neq 0$; then we can choose a positive integer $h$ such that the numerator of $t$ is not divisible by $10^h$. But for $c$ large enough, $g(10^c) - t$ has numerator divisible by $10^b$ for some $b > h$, contradiction.

Consequently, $t = 0$, and we may apply the induction hypothesis to $g(n)/n$ to deduce the claim.
Remark: The second solution amounts to the fact that $g$, being a polynomial with rational coefficients, is continuous for the 2-adic and 5-adic topologies on $\mathbb{Q}$. By contrast, the first solution uses the “$\infty$-adic” topology, i.e., the usual real topology.

A–5 In all solutions, let $G$ be a finite group of order $m$.

First solution: By Lagrange’s theorem, if $m$ is not divisible by $p$, then $n = 0$. Otherwise, let $S$ be the set of $p$-tuples $(a_0, \ldots, a_{p-1}) \in \mathbb{G}^p$ such that $a_0 \cdots a_{p-1} = e$; then $S$ has cardinality $m^{p-1}$, which is divisible by $p$. Note that this set is invariant under cyclic permutation, that is, if $(a_0, \ldots, a_{p-1}) \in S$, then $(a_1, \ldots, a_{p-1}, a_0) \in S$ also. The fixed points under this operation are the tuples $(a, \ldots, a)$ with $a^p = e$; all other tuples can be grouped into orbits under cyclic permutation, each of which has size $p$. Consequently, the number of $a \in G$ with $a^p = e$ is divisible by $p$; since that number is $n + 1$ (only $e$ has order 1), this proves the claim.

Second solution: (by Anand Deopurkar) Assume that $n > 0$, and let $H$ be any subgroup of $G$ of order $p$. Let $S$ be the set of all elements of $G \setminus H$ of order dividing $p$, and let $H$ act on $G$ by conjugation. Each orbit has size $p$ except for those which consist of individual elements $g$ which commute with $H$. For each such $g$, $g$ and $H$ generate an elementary abelian subgroup of $G$ of order $p^2$. However, we can group these $g$ into sets of size $p^2 - p$ based on which subgroup they generate together with $H$. Hence the cardinality of $S$ is divisible by $p$; adding the $p - 1$ nontrivial elements of $H$ gives $n = -1 \mod p$ as desired.

Third solution: Let $S$ be the set of elements of $G$ having order dividing $p$, and let $H$ be an elementary abelian $p$-group of maximal order in $G$. If $|H| = 1$, then we are done. So assume $|H| = p^k$ for some $k \geq 1$, and let $H$ act on $S$ by conjugation. Let $T \subseteq S$ denote the set of fixed points of this action. Then the size of every $H$-orbit on $S$ divides $p^k$, and so $|T| \equiv |T| \mod p$. On the other hand, $H \subseteq T$, and if $T$ contained an element not in $H$, then that would contradict the maximality of $H$. It follows that $H = T$, and so $|S| \equiv |T| = |H| = p^k \equiv 0 \mod p$, i.e., $|S| = n + 1$ is a multiple of $p$.

Remark: This result is a theorem of Cauchy; the first solution above is due to McKay. A more general (and more difficult) result was proved by Frobenius: for any positive integer $m$, if $G$ is a finite group of order divisible by $m$, then the number of elements of $G$ of order dividing $m$ is a multiple of $m$.

A–6 For an admissible triangulation $\mathcal{T}$, number the vertices of $P$ consecutively $v_1, \ldots, v_n$, and let $a_i$ be the number of edges in $\mathcal{T}$ emanating from $v_i$; note that $a_i \geq 2$ for all $i$.

We first claim that $a_1 + \cdots + a_n \leq 4n - 6$. Let $V, E, F$ denote the number of vertices, edges, and faces in $\mathcal{T}$. By Euler’s Formula, $(F + 1) - E + V = 2$ (one must add 1 to the face count for the region exterior to $P$). Each face has three edges, and each edge but the $n$ outside edges belongs to two faces; hence $F = 2E - n$. On the other hand, each edge has two endpoints, and each of the $V - n$ internal vertices is an endpoint of at least 6 edges; hence $a_1 + \cdots + a_n + 6(V - n) \leq 2E$. Combining this inequality with the previous two equations gives

$$a_1 + \cdots + a_n \leq 2E + 6n - 6(1 - F + E) = 4n - 6,$$

as claimed.

Now set $A_3 = 1$ and $A_n = A_{n-1} + 2n - 3$ for $n \geq 4$; we will prove by induction on $n$ that $\mathcal{T}$ has at most $A_n$ triangles. For $n = 3$, since $a_1 + a_2 + a_3 = 6$, $a_1 = a_2 = a_3 = 2$ and hence $\mathcal{T}$ consists of just one triangle.

Next assume that an admissible triangulation of an $(n - 1)$-gon has at most $A_{n-1}$ triangles, and let $\mathcal{T}$ be an admissible triangulation of an $n$-gon. If any $a_i = 2$, then we can remove the triangle of $\mathcal{T}$ containing vertex $v_i$ to obtain an admissible triangulation of an $(n - 1)$-gon; then the number of triangles in $\mathcal{T}$ is at most $A_{n-1} + 1 < A_n$ by induction. Otherwise, all $a_i \geq 3$. Now the average of $a_1, \ldots, a_k$ is less than 4, and thus there are more $a_i = 3$ than $a_i \geq 5$. It follows that there is a sequence of $k$ consecutive vertices in $P$ whose degrees are $3, 4, 4, \ldots, 3$ in order, for some $k$ with $2 \leq k \leq n - 1$ (possibly $k = 2$, in which case there are no degree 4 vertices separating the degree 3 vertices). If we remove from $\mathcal{T}$ the $2k - 1$ triangles which contain at least one of these vertices, then we are left with an admissible triangulation of an $(n - 1)$-gon. It follows that there are at most $A_{n-1} + 2k - 1 \leq A_{n-1} + 2n - 3 = A_n$ triangles in $\mathcal{T}$. This completes the induction step and the proof.

Remark: We can refine the bound $A_n$ somewhat. Supposing that $a_i \geq 3$ for all $i$, the fact that $a_1 + \cdots + a_n \leq 4n - 4$ implies that there are at least six more indices $i$ with $a_i = 3$ than with $a_i \geq 5$. Thus there exist six sequences with degrees $3, 4, 4, \ldots, 3$, of total length at most $n + 6$. We may thus choose a sequence of length $k \leq \lceil \frac{n}{4} \rceil + 1$, so we may improve the upper bound to $A_n = A_{n-1} + 2 \lceil \frac{n}{6} \rceil + 1$, or asymptotically $\frac{1}{6} n^2$.

However (as noted by Noam Elkies), a hexagonal swatch of a triangular lattice, with the boundary as close to regular as possible, achieves asymptotically $\frac{1}{6} n^2$ triangles.

B–1 The problem fails if $f$ is allowed to be constant, e.g., take $f(n) = 1$. We thus assume that $f$ is nonconstant. Write $f(n) = \sum_{i=0}^d a_i n^i$ with $a_i > 0$. Then

$$f(f(n) + 1) = \sum_{i=0}^d a_i (f(n) + 1)^i \equiv f(1) \mod f(n).$$

If $n = 1$, then this implies that $f(f(n) + 1)$ is divisible by $f(n)$. Otherwise, $0 < f(1) < f(n)$ since $f$ is nonconstant and has positive coefficients, so $f(f(n) + 1)$ cannot be divisible by $f(n)$. 
Remark: 4

\[ x = \frac{2}{\sqrt{5}} \]

<table>
<thead>
<tr>
<th>n</th>
<th>a_n</th>
<th>b_n</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>0.6180339887</td>
<td>0.3819660113</td>
</tr>
<tr>
<td>1</td>
<td>0.9545588235</td>
<td>0.0454411765</td>
</tr>
<tr>
<td>2</td>
<td>1.6180339887</td>
<td>0.3819660113</td>
</tr>
<tr>
<td>3</td>
<td>2.5574570851</td>
<td>0.4423562571</td>
</tr>
<tr>
<td>4</td>
<td>4.0624792398</td>
<td>0.9375207602</td>
</tr>
<tr>
<td>5</td>
<td>6.6209363249</td>
<td>1.6180339887</td>
</tr>
<tr>
<td>6</td>
<td>11.6209363249</td>
<td>2.5574570851</td>
</tr>
<tr>
<td>7</td>
<td>20.2418726498</td>
<td>4.1264944138</td>
</tr>
<tr>
<td>8</td>
<td>35.3687099748</td>
<td>6.6171522289</td>
</tr>
<tr>
<td>9</td>
<td>65.5865426247</td>
<td>13.2242522077</td>
</tr>
<tr>
<td>10</td>
<td>130.9550525595</td>
<td>26.4585044154</td>
</tr>
</tbody>
</table>

The sequence is described as the case \( S(1,5) \) of the sequence \( S(a_0, a_1) \) in which \( a_{n+2} \) is the least integer for which \( a_{n+2}/a_{n+1} > a_{n+1}/a_n \). Sloane cites D. W. Boyd, Linear recurrence relations for some generalized Pisot sequences, Advances in Number Theory (Kingston, ON, 1991), Oxford Univ. Press, New York, 1993, p. 333–340.

B–4 The number of pairs is \( 2^{n+1} \). The degree condition forces \( P \) to have degree \( n \) and leading coefficient \( \pm 1 \); we may count pairs in which \( P \) has leading coefficient \( 1 \) as long as we multiply by 2 afterward.

Factor both sides:

\[
\frac{(P(X) + Q(X)i)(P(X) - Q(X)i)}{n-1} = \prod_{j=0}^{n-1} \left( \frac{X + \exp(2\pi i(2j+1)/(4n))}{X + \exp(2\pi i(2j+1)/(4n))} \right). 
\]

Then each choice of \( P, Q \) corresponds to equating \( P(X) + Q(X)i \) with the product of some \( n \) factors on the right, in which we choose exactly the two factors for each \( j = 0, \ldots, n-1 \). (We must take exactly \( n \) factors because as a polynomial in \( X \) with complex coefficients, \( P(X) + Q(X)i \) has degree exactly \( n \). We must choose one for each \( j \) to ensure that \( P(X) + Q(X)i \) and \( P(X) - Q(X)i \) are complex conjugates, so that \( P, Q \) have real coefficients.) Thus there are \( 2^n \) such pairs; multiplying by 2 to allow \( P \) to have leading coefficient \(-1\) yields the desired result.

Remark: If we allow \( P \) and \( Q \) to have complex coefficients but still require \( \deg(P) > \deg(Q) \), then the number of pairs increases to \( 2^{2n} \), as we may choose any \( n \) of the \( 2n \) factors of \( X^{2n}+1 \) to use to form \( P(X) + Q(X)i \).

B–5 For \( n \) an integer, we have \( \left\lfloor \frac{n}{2} \right\rfloor = \frac{n-j}{k} \) for \( j \) the unique integer in \( \{0, \ldots, k-1\} \) congruent to \( n \) modulo \( k \); hence

\[
\prod_{j=0}^{k-1} \left\lfloor \frac{n}{k} - \frac{n-j}{k} \right\rfloor = 0.
\]

By expanding this out, we obtain the desired polynomials \( P_0(n), \ldots, P_{k-1}(n) \).

Remark: Variants of this solution are possible that construct the \( P_i \) less explicitly, using Lagrange interpolation or Vandermonde determinants.

B–6 (Suggested by Oleg Golberg) Assume \( n \geq 2 \), or else the problem is trivially false. Throughout this proof, any \( C_i \) will be a positive constant whose exact value is immaterial. As in the proof of Stirling’s approximation, we estimate for any fixed \( c \in \mathbb{R} \),

\[
\sum_{i=1}^{n} (i + c) \log i = \frac{1}{2} n^2 \log n - \frac{1}{4} n^2 + O(n \log n)
\]
by comparing the sum to an integral. This gives
\[
\frac{n^2}{2} - C_1 n e^{-n^2/4} \leq 1 + e \left( \frac{n^2}{2} + \cdots + n^{n-c} \right)
\leq n^2/2 + C_2 n e^{-n^2/4}.
\]

We now interpret \( f(n) \) as counting the number of \( n \)-tuples \((a_1, \ldots, a_n)\) of nonnegative integers such that
\[
a_1! + \cdots + a_n n! = n!.
\]

For an upper bound on \( f(n) \), we use the inequalities \( 0 \leq a_i \leq n!/i! \) to deduce that there are at most \( n!/i! + 1 \leq 2(n!/i!) \) choices for \( a_i \). Hence
\[
f(n) \leq 2 \frac{n!}{1!} \cdots \frac{n!}{n!} = 2^n \frac{n!}{1!} \frac{n!}{2!} \cdots \frac{n!}{n!} \leq n^2/2 + C_3 n e^{-n^2/4}.
\]

For a lower bound on \( f(n) \), we note that if \( 0 \leq a_i < (n-1)!/i! \) for \( i = 2, \ldots, n-1 \) and \( a_n = 0 \), then \( 0 \leq a_2! + \cdots + a_n n! \leq n! \), so there is a unique choice of \( a_1 \) to complete this to a solution of \( a_1! + \cdots + a_n n! = n! \). Hence
\[
f(n) \geq \frac{(n-1)!}{2!} \cdots \frac{(n-1)!}{(n-1)!} = 3 \frac{4^2 \cdots (n-1)^{n-3}}{2! \cdots (n-1)!} \geq n^2/2 + C_4 n e^{-n^2/4}.
\]