1. [20] Consider a regular $n$-gon with $n > 3$, and call a line acceptable if it passes through the interior of this $n$-gon. Draw $m$ different acceptable lines, so that the $n$-gon is divided into several smaller polygons.

(a) Prove that there exists an $m$, depending only on $n$, such that any collection of $m$ acceptable lines results in one of the smaller polygons having 3 or 4 sides.

(b) Find the smallest possible $m$ which guarantees that at least one of the smaller polygons will have 3 or 4 sides.

Answer: [N/A] We will prove that if $m \geq n - 4$, then there is guaranteed to be a smaller polygon with 3 or 4 sides, and if $m \leq n - 5$, there might not be a polygon with 3 or 4 sides. This will solve both parts of the problem.

Given a configuration of lines, let $P_1, \ldots, P_k$ be all of the resulting smaller polygons. Let $E(P_i)$ be the number of edges in polygon $P_i$, and let $E = E(P_1) + \cdots + E(P_k)$. First, note that whenever a new polygon is formed, it must have been because a larger polygon was split into two smaller polygons by a line passing through it. When this happens, $k$ increases by 1 and $E$ increases by at most 4 (it might be less than 4 if the line passes through vertices of the larger polygon). Therefore, if adding an acceptable line increases the number of polygons by $a$, then $E$ increases by at most $4a$.

Now, assume $m \geq n - 4$. At the beginning, we have $k = 1$ and $E = n$. If the number of polygons at the end is $p + 1$, then $E \leq n + 4p$, so the average number of edges per polygon is less than or equal to $\frac{n + 4p}{1+p}$. Now, note that each acceptable line introduces at least one new polygon, so $p \geq m \geq n - 4$. Also, note that as $p$ increases, $\frac{n + 4p}{1+p}$ strictly decreases, so it is maximized at $p = n - 4$, where $\frac{n + 4p}{1+p} = \frac{5n - 16}{n - 3} = \frac{5}{n - 3} < 5$. Therefore, the average number of edges per polygon is less than 5, so there must exist a polygon with either 3 or 4 edges, as desired.

We will now show that if $m \leq n - 5$, then we can draw $m$ acceptable lines in a regular $n$-gon $A_1A_2\ldots A_n$ such that there are no polygons with 3 or 4 sides. Let $M_1$ be the midpoint of $A_3A_4$, $M_2$ be the midpoint of $A_4A_5$, ..., $M_{n-5}$ be the midpoint of $A_{n-3}A_{n-4}$. Let the $m$ acceptable lines be $A_1M_1, A_1M_2, \ldots, A_1M_m$. We can see that all resulting polygons have 5 sides or more, so we are done.

2. [25] 2014 triangles have non-overlapping interiors contained in a circle of radius 1. What is the largest possible value of the sum of their areas?

Answer: [N/A] This problem turned out to be much trickier than we expected. We have yet to see a complete solution, but let us know if you find one!

Comment. We apologize for the oversight on our part. Our test-solvers essentially all misread the problem to contain the additional assumption that all triangle vertices lie on the circumference (which is not the case).

3. [30] Fix positive integers $m$ and $n$. Suppose that $a_1, a_2, \ldots, a_m$ are reals, and that pairwise distinct vectors $v_1, \ldots, v_m \in \mathbb{R}^n$ satisfy

$$\sum_{j \neq i} a_j \frac{v_j - v_i}{\|v_j - v_i\|^3} = 0$$

for $i = 1, 2, \ldots, m$.

Prove that

$$\sum_{1 \leq i < j \leq m} \frac{a_i a_j}{\|v_j - v_i\|} = 0.$$ 

Answer: N/A Since $v_i \cdot (v_j - v_i) + v_j \cdot (v_i - v_j) = -\|v_j - v_i\|^2$ for any $1 \leq i < j \leq m$, we have

$$0 = \sum_{i=1}^{m} a_i v_i \cdot 0 = \sum_{i=1}^{m} a_i v_i \sum_{j \neq i} a_j \frac{v_j - v_i}{\|v_j - v_i\|^2} = -\sum_{1 \leq i < j \leq m} \frac{a_i a_j}{\|v_j - v_i\|},$$

as desired.

Alternative Solution. Fix $a_1, \ldots, a_m$, and define $f : (\mathbb{R}^n)^m \rightarrow \mathbb{R}$ by

$$f(x_1, \ldots, x_m) = \sum_{1 \leq i < j \leq m} \frac{a_i a_j}{\|x_j - x_i\|}.$$

Now if we view $f(x_1, \ldots, x_m)$ individually as a function in $x_k$ ($k$ fixed), then the problem condition for $i = k$ says precisely that the gradient of $f$ with respect to $x_k$ (but of course, multiplied by $a_k$) evaluated at $(v_1, \ldots, v_m)$ is 0.

Finally, the multivariate chain rule shows that $F(t) := f(tv_1, \ldots, tv_m) = \frac{1}{t} f(v_1, \ldots, v_m)$ must satisfy $F'(1) = 0$. Yet $F'(1) = -\frac{1}{t^2} f(v_1, \ldots, v_m)$, so we have $f(v_1, \ldots, v_m) = 0$, as desired.

Comment. This is (sort of) an energy minimization problem from physics (more precisely, minimizing electrostatic or gravitational potential).

Comment. It would be interesting to determine all differentiable $A : \mathbb{R}^+ \rightarrow \mathbb{R}$ such that the problem still holds when the terms are replaced by $\frac{v_i \cdot v_j}{\|v_j - v_i\|^2} A'(\|v_j - v_i\|)$ and $A(\|v_j - v_i\|)$. (Here $A(t) = 1/t$, which has a nice physical interpretation, but that’s not important.) The obvious examples are $A(t) = ct^s$ for constant $c$ and real $s$ (where both solutions easily carry through). But there may be others where instead of defining $F(t)$ through the scaling transformation $(v_1, \ldots, v_m) \rightarrow (tv_1, \ldots, tv_m)$, there’s a subtler translation.

4. [35] Let $\omega$ be a root of unity and $f$ be a polynomial with integer coefficients. Show that if $|f(\omega)| = 1$, then $f(\omega)$ is also a root of unity.

Answer: N/A Suppose $\omega$ is a primitive $n$th root, so that $\Phi_n(x)$ is the minimal polynomial of $\omega$ (over $\mathbb{Q}$). Thus $f(\omega)f(\omega^{-1}) = 1$ implies $\Phi_n(x) | f(x)f(x^{-1}) - 1$ (divisibility as Laurent polynomials). Hence $|f(\omega^k)| = 1$ whenever $\gcd(k, n) = 1$, and $\prod_{\gcd(k, n) = 1} (t - f(\omega^k))$ is a monic integer-coefficient polynomial with all roots within the unit disk, so its roots must all be roots of unity (since 0 is clearly not a root), and we’re done.

Comment. The result used at the end (a monic integer-coefficient polynomial with all roots within the unit disk has every root either 0 or a root of unity) is classical. See for instance the discussion here or here. This result is sometimes called Kronecker’s theorem, and appears, for instance, in Problems from the Book.

Comment. Note that the proof works as long as $f \in \mathbb{Q}[x]$ and $f(\omega)$ is an algebraic integer. Once it is known that $f(\omega)$ is a root of unity, more can be said about the order $m$ of $f(\omega)$. If $\omega$ is a primitive $n$th root of unity, then the conjugates of $f(\omega)$ lie among the $\leq \phi(n)$ numbers in $\{f(\omega^k) : \gcd(k, n) = 1\}$. In particular, $\phi(m) \leq \phi(n)$, which (e.g. through a naive estimate using $p - 1 \geq \sqrt{p}$ for $p \geq 3$ to get $\phi(m) \geq \sqrt{m/2}$) shows that $m \leq 2\phi(n)^2$ (for instance), so there exists $g \in \mathbb{Q}[x]$ with $g(\omega)$ a root of unity of maximal order $N$, which then must generate the unit group of $\mathbb{Q}(\omega)$ (or else we could find a larger order). In particular, since $\omega$ lies in this group, $n \mid N$. But $\phi(N) \leq \phi(n)$ by our earlier argument, so either $N = n$ or $N = 2n$ if $n$ is odd. Either way, it’s clear that $g(\omega) = \pm \omega^k$ for some $k$, so our original $f(\omega)$ must also be $\pm \omega^j$ for some $j$.

Alternative Solution. We follow the paper here but fill in some of the details to make the ideas as accessible as possible. We will use the fact that if $A$ is a finitely generated abelian group, then any subgroup $B$ is also finitely generated, and furthermore, $\text{rank}(B) \leq \text{rank}(A)$. (For instance, see Theorem 14.6.5 in Artin’s Algebra, 3rd ed. for a proof of finite generation, which for our particular case of modules over a PID (namely, $\mathbb{Z}$) can be done in parallel to the rank$(B) \leq \text{rank}(A)$ proof—the proof is very similar to Gaussian elimination.)
Let $K = \mathbb{Q}(\omega)$, $V$ the set of algebraic integers in $K$ of modulus 1 (which must be units of $K$), $U \supseteq V$ the set of units in $K$, $R = U \cap \mathbb{R}$ the set of real units in $K$ (which, importantly, is also the set of units in $K \cap \mathbb{R}$), and $L = K \cap \mathbb{R}$ denote the maximal real subfield of $K$.

The key is that $\text{rank}(V) = \text{rank}(U) - \text{rank}(R)$. To prove this, we note that for $u \in U$, $\pi \in U$ as well (since $K = K$), so that $u\pi = |u|^2 \in R$ and $u/\pi \in V$, which gives $u^2 = (u\pi)(u/\pi) \in RV$. Thus $S := \{u^2 : u \in U\} \subseteq RV \subseteq U$. But $U$ is a finitely generated abelian group by Dirichlet’s unit theorem so $S, RV$ are as well, and furthermore $\text{rank}(S) \leq \text{rank}(RV) \leq \text{rank}(U)$. Now take multiplicatively independent $u_1, \ldots, u_{\text{rank}(U)} \in U$; then clearly $u_1^2, \ldots, u_{\text{rank}(U)}^2 \in S$ are multiplicatively independent as well, so $\text{rank}(U) \leq \text{rank}(S)$, whence $\text{rank}(RV) = \text{rank}(U)$. Of course, $R \cap V = \{\pm 1\}$, so $\text{rank}(RV) = \text{rank}(R) + \text{rank}(V) - \text{rank}(R \cap V) = \text{rank}(R) + \text{rank}(V)$ (the proof here for $\mathbb{Z}$-modules is essentially the same as that for $\mathbb{Q}$-vector spaces), finishing the proof.

$V$ contains only roots of unity if and only if $\text{rank}(V) = 0$ (no free elements), so we must prove $\text{rank}(U) = \text{rank}(R)$. Let $r, s$ denote the number of real and complex embeddings of a number field, so $[K: \mathbb{Q}] = r(K) + 2s(K)$, $[L: \mathbb{Q}] = r(L) + 2s(L)$, and thus $r(K) + 2s(K) = [K: L]r(L) + 2s(L))$. By Dirichlet’s unit theorem, $\text{rank}(U) = r(K) + s(K) - 1$ and $\text{rank}(R) = r(L) + s(L) - 1$.

If $K = L$ (equivalently, $K$ is totally real), we’re trivially done. Otherwise, if $[K: L] > 1$, it’s easy to check that we have $\text{rank}(U) = \text{rank}(R)$ if and only if $[K: L] = 2$ and $r(K) = s(L) = 0$ ($K$ is totally imaginary and $L$ is totally real)—then $r(L) = s(K)$ automatically holds. This is precisely the condition that $K$ is a CM-field (CM-field $K$ just means $K$ is totally imaginary (no real embeddings), and $K$ is a quadratic extension of $K \cap \mathbb{R}$.)

In particular, the cyclotomic field $K = \mathbb{Q}(\omega) = \mathbb{Q}[\omega]$ is a totally imaginary quadratic extension of the totally real field $\mathbb{Q}(\omega + \omega^{-1}) = \mathbb{Q}[\omega + \omega^{-1}]$. Indeed, it is easy to check that the latter is simply $K \cap \mathbb{R}$, and $K = \mathbb{Q}(\omega + \omega^{-1}, \omega - \omega^{-1}) = \pm \sqrt{(\omega + \omega^{-1})^2 - 4}$. So we’re done.

5. [40] Let $n$ be a positive integer, and let $A$ and $B$ be $n \times n$ matrices with complex entries such that $A^2 = B^2$. Show that there exists an $n \times n$ invertible matrix $S$ with complex entries that satisfies $S(AB - BA) = (BA - AB)S$.

**Answer:** $\begin{bmatrix} \text{N/A} \end{bmatrix}$ Let $X = A + B$ and $Y = A - B$, so $XY = BA - AB$ and $YX = AB - BA$. Note that $XY = -YX$.

It suffices (actually is equivalent) to show that $AB - BA$ and $BA - AB$ have the same Jordan forms. In other words, we need to show that for any complex number $\lambda$, the Jordan $\lambda$-block decompositions of $AB - BA$ and $BA - AB$ are the same.

However, the $\lambda$-decomposition of a matrix $M$ is uniquely determined by the infinite (eventually constant) sequence $(\dim \ker(M - \lambda I))^1, \dim \ker(M - \lambda I)^2, \ldots$, so we only have to show that $\dim \ker(XY - \lambda I)^k = \dim \ker(YX - \lambda I)^k$ for the positive integers $k$ and complex numbers $\lambda$.

For $\lambda = 0$, this follows trivially from $XY = -YX$: we have $(XY)^k v = 0$ if and only if $(YX)^k v = 0$.

Now suppose $\lambda \neq 0$, and define the (matrix) polynomial $p(T) = (T - \lambda I)^k$. Let $V_1 = \{v \in \mathbb{C}^n : p(XY)v = 0\}$, and $V_2 = \{v \in \mathbb{C}^n : p(YX)v = 0\}$. Note that if $v \in V_1$, then $0 = |Yp(XY)|v = [p(YX)]v = p(YX)[Yv]$, so $Yv \in V_2$. Furthermore, if $v \neq 0$, then $Yv \neq 0$, or else $p(XY)v = p(0)v = (-\lambda I)^k v \neq 0$ (since $(XY)^j v = 0$ for all $j \geq 1$), contradiction. Viewing $Y$ (more precisely, $v \rightarrow Yv$) as a linear map from $V_1$ to $V_2$, we have $\dim V_1 = \dim YV_1 + \dim \ker Y = \dim YV_1 \leq \dim V_2$ (alternatively, if $v_1, \ldots, v_r$ is a basis of $V_1$, then $Yv_1, \ldots, Yv_r$ are linearly independent in $V_2$). By symmetry, $\dim V_1 = \dim V_2$, and we’re done.

**Comment.** If $A, B$ are additionally real, then we can also choose $S$ to be real (not just complex). Indeed, note that if $S = P + Qi$ for real $P, Q$, then since $A, B$ are real, it suffices to find $c \in \mathbb{R}$ such that $\det(P + cQ) \neq 0$. However, $\det(P + xQ)$ is a polynomial in $x$ that is not identically zero (it is nonzero for $x = i$), so it has finitely many (complex, and thus real) roots. Thus the desired $c$ clearly exists.
Comment. Note that $A(AB - BA) = (BA - AB)A$, since $A^2B = B^3 = BA^2$. (The same holds for $A \to B$.) Thus the problem is easy unless all linear combinations of $A, B$ are noninvertible. However, it seems difficult to finish without analyzing generalized eigenvectors as above.

Comment. See this paper by Ross Lippert and Gilbert Strang for a general analysis of the Jordan forms of $MN$ and $NM$. 