PRIMES 2027 ENTRANCE PROBLEM SET
Student Version
SEPT. 14, 2026

Notation. Let $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ denote the sets of integers, rational numbers, real numbers, and complex numbers, respectively. In addition, let $\mathbb{P}$, $\mathbb{N}$, and $\mathbb{N}_0$ denote the sets of primes, positive integers, and nonnegative integers, respectively. We also write $[n] := \{1, 2, \ldots, n\}$ for every $n \in \mathbb{N}$.

Problem 1 (Geometry)**.** Let $\mathscr{L}_1, \mathscr{L}_2 \subset \mathbb{R}^3$ be two affine lines. A *common perpendicular* is a line that meets both $\mathscr{L}_1$ and $\mathscr{L}_2$ and whose direction is orthogonal to the directions of both lines.

(a) Write
$$\mathscr{L}_i = \{\vec{v}_i + t\vec{d}_i : t \in \mathbb{R}\}, \qquad \vec{d}_i \neq 0.$$
Find a necessary and sufficient condition on $\vec{v}_1, \vec{v}_2, \vec{d}_1, \vec{d}_2$ for the two lines not to lie in a common affine plane, and prove directly that such lines must have a unique common perpendicular.

(b) We now introduce Plücker coordinates for affine lines. Let
$$\mathscr{P} := \{(\vec{d}, \vec{m}) \in \mathbb{R}^3 \times \mathbb{R}^3 : \vec{d} \neq 0,\ \vec{d} \cdot \vec{m} = 0\}.$$
Define an equivalence relation on $\mathscr{P}$ by
$$(\vec{d}, \vec{m}) \sim (\vec{d}', \vec{m}') \quad \Longleftrightarrow \quad (\vec{d}', \vec{m}') = (\lambda\vec{d}, \lambda\vec{m})$$
for some $\lambda \in \mathbb{R} \setminus \{0\}$, and write $[\vec{d} : \vec{m}]$ for the equivalence class.

Show that the affine line $\{\vec{u} + t\vec{d} : t \in \mathbb{R}\}$, with $\vec{d} \neq 0$, determines the class
$$[\vec{d} : \vec{u} \times \vec{d}].$$
Prove that this class is independent of the chosen base point $\vec{u}$ and of the chosen nonzero direction vector for the line. Conversely, prove that every class $[\vec{d} : \vec{m}]$ in $\mathscr{P}/\!\sim$ determines a unique affine line.

(c) Let $[\vec{d}_i : \vec{m}_i]$ represent $\mathscr{L}_i$. Determine a necessary and sufficient condition, in terms of these coordinates, for the lines not to lie in a common affine plane. Under this condition, prove that exactly one class $[\vec{d} : \vec{m}]$ represents their common perpendicular.

Recommended reading for geometry:

- MIT OpenCourseWare 18.02, Part A: Vectors, Determinants and Planes, Sessions 1–8.

Problem 2 (Probability/Algorithm)**.** For an integer $n \geq 1$ and a parameter $p \in [0,1]$, consider the sites of the square grid

$$V_n = \{1, \dots, n\}^2.$$

Independently declare each site *occupied* with probability p. An occupied path is a sequence of occupied sites in which consecutive sites are horizontal or vertical nearest neighbours; a path may consist of a single site. Let $H_n(p)$ be the event that there is an occupied path from a site in the leftmost column to a site in the rightmost column, and set

$$\theta_n(p) = \Pr\left(H_n(p)\right).$$

(a) Show that θ_n is a polynomial in p. You may use without justification that it is strictly increasing. Deduce that there is a unique number $p_n \in (0,1)$ such that $\theta_n(p_n) = 1/2$.

(b) Write pseudocode for an algorithm that approximates $\theta_n(p)$ by simulating M independent random configurations and returning the proportion having a left-to-right crossing. Then implement the algorithm in a programming language of your choice. Denote the resulting estimator by $\widehat{\theta}_n(p)$. You may use

$$\Pr\left(\left|\widehat{\theta}_n(p) - \theta_n(p)\right| > \varepsilon\right) \leq 2e^{-2M\varepsilon^2}.$$

For prescribed $\varepsilon, \delta \in (0,1)$, find a sufficient integer M such that

$$\Pr\left(\left|\widehat{\theta}_n(p) - \theta_n(p)\right| \leq \varepsilon\right) \geq 1 - \delta.$$

That is to say, the error will be at most ε with confidence $1 - \delta$. Specialize to $\varepsilon = \delta = 0.05$.

Determine $\theta_1(p)$ and $\theta_2(p)$ exactly. For each $n \in \{1, 2\}$, use at least two values of p to test your implementation, using a stated value of M. For each test, report n, p, M, the estimate, the exact value, and the observed absolute error.

Recommended reading for probability:

- Robert Sedgewick and Kevin Wayne, Algorithms, Section 4.1: Undirected Graphs, especially depth-first search, breadth-first search, and connectivity.
- Princeton COS 226, Percolation Assignment.

Problem 3 (Mathematical Analysis)**.** Let $f \in C^2([0,1])$ be a strictly convex function. For $a \in [0,1]$ let

$$\mathscr{L}_a(x) := f(a) + f'(a)(x-a)$$

be the affine function whose graph is tangent to the graph of f at a. For $n \in \mathbb{N}$ and $a_1, \ldots, a_n \in [0,1]$, define the **tangent envelope** by

$$\mathscr{L}_{a_1,\ldots,a_n}(x) := \max_{1 \le i \le n} \mathscr{L}_{a_i}(x).$$

Note that by convexity, $\mathscr{L}_{a_1,\ldots,a_n}(x) \le f(x)$ for all $x \in [0,1]$. Fix a number $1 \le p < \infty$ and define the optimal error by

$$E_{n,p}(f) = \inf_{a_1,\ldots,a_n \in [0,1]} \|f - \mathscr{L}_{a_1,\ldots,a_n}\|_p,$$

where

$$\|g\|_p = \left(\int_0^1 |g(x)|^p \, \mathrm{d}x \right)^{1/p}.$$

A multiset of tangency points attaining this infimum is called optimal.

(a) For $f(x) = x^2$, determine the optimal multiset of tangency points and compute $E_{n,p}(f)$ exactly.

(b) For a general strictly convex function $f \in C^2([0,1])$, determine the sharp decay exponent α; that is, prove that there are constants $0 < c_{f,p} \le C_{f,p} < \infty$, independent of n, such that

$$c_{f,p} n^{-\alpha} \le E_{n,p}(f) \le C_{f,p} n^{-\alpha} \qquad (n \ge 1).$$

In other words, find α such that $E_{n,p}(f) = \Theta(n^{-\alpha})$.

(c)* Assume $f''(x) > 0$ on $[0,1]$ and make the following formal continuum approximation. Suppose the tangency points have a continuous positive density ρ with $\int_0^1 \rho = 1$. Write

$$h_n(x) = \frac{1}{n\rho(x)}$$

for the length of a cell near x, where a *cell* is an interval on which a single tangent line realizes the envelope. In this formal model, regard each such cell as centered at its tangency point to leading order. Assume that boundary effects, deviations from this symmetry, and Taylor-remainder terms contribute $o(n^{-2p})$ to the pth power of the approximation error.

Show, using a quadratic approximation, that one cell near x contributes formally

$$\frac{(f''(x))^p}{2^{3p}(2p+1)} h_n(x)^{2p+1}$$

to the pth power of the error. Deduce that a configuration with density ρ has the formal leading term

$$\frac{n^{-2p}}{2^{3p}(2p+1)} \int_0^1 (f''(x))^p \rho(x)^{-2p} \, \mathrm{d}x$$

for the pth power of its error. Minimize this expression over ρ and derive the formal prediction

$$E_{n,p}(f) \sim \kappa_p(f) n^{-\alpha}.$$

A rigorous proof of this asymptotic equivalence is not required.

Here $A_n \sim B_n$ means $A_n/B_n \underset{n\to\infty}{\longrightarrow} 1$. You may use Hölder's inequality: if $r, s > 1$ satisfy $1/r + 1/s = 1$, then $\|uv\|_1 \le \|u\|_r \|v\|_s$ with equality if and only if the functions $|u(x)|^r$ and $|v(x)|^s$ are proportional to each other.

Recommended reading for calculus and mathematical analysis:

- Keith Conrad, The Remainder in Taylor Series, Sections 1 and 3.
- Stephen Boyd and Lieven Vandenberghe, Convex Optimization (Chapter 3, First-order conditions).

Problem 4 (Data Analysis)**.** An edge-weighted complete graph records pairwise data on $n \geq 5$ objects. Let $\mathscr{E} = \binom{[n]}{2}$ be the set of two-element subsets of $[n]$, or equivalently, the edge set of the complete graph on n vertices. Let $x = (x_e)_{e\in\mathscr{E}} \in \mathbb{R}^{\mathscr{E}}$, and write $x_{ab} = x_{\{a,b\}}$.

Let $d \in \mathbb{N}_0$. A degree-d scoring rule is a map

$$F = (F_1, \ldots, F_n) : \mathbb{R}^{\mathscr{E}} \longrightarrow \mathbb{R}^n$$

such that each coordinate function F_i is a homogeneous polynomial of degree d. The value $F_i(x)$ is the score assigned to object i. Let S_n be the group of permutations of $[n]$. The rule is *anonymous* if

$$F_{\pi(i)}(\pi\cdot x) = F_i(x) \qquad (\pi \in S_n,\ i \in [n],\ x \in \mathbb{R}^{\mathscr{E}}),$$

where

$$(\pi\cdot x)_{\{a,b\}} = x_{\{\pi^{-1}(a),\pi^{-1}(b)\}}.$$

Let $\mathscr{A}_n^{(d)}$ be the vector space of anonymous degree-d rules. A *common-score rule* has the form $h(x)\mathbf{1}_n$, where h is an S_n-invariant homogeneous polynomial of degree d and $\mathbf{1}_n = (1, \ldots, 1) \in \mathbb{R}^n$; let $\mathscr{C}_n^{(d)}$ denote this subspace. Adding a common score changes none of the pairwise score differences, so we study rules modulo $\mathscr{C}_n^{(d)}$.

You may use the orbit-sum principle: a polynomial invariant under a finite permutation group is a linear combination of its monomial orbit sums (the sum of the distinct monomials in the orbit of a given monomial).

(a) Fix $i \in [n]$. Classify the orbits of edges under the subgroup of S_n fixing i. Deduce that

$$\dim\bigl(\mathscr{A}_n^{(1)}/\mathscr{C}_n^{(1)}\bigr) = 1,$$

and identify a rule whose class spans this quotient.

(b) Set $\mathscr{Q}_n := \mathscr{A}_n^{(2)}$ and $\mathscr{C}_n := \mathscr{C}_n^{(2)}$. A quadratic monomial $x_e x_f$ corresponds to an unordered multiset of two edges, with $e = f$ allowed. Fix $i \in [n]$. Classify these multisets under the subgroup of S_n fixing i, and deduce

$$\dim \mathscr{Q}_n = 7, \qquad \dim \mathscr{C}_n = 3, \qquad \dim(\mathscr{Q}_n/\mathscr{C}_n) = 4.$$

Show that the classes of $A = (A_1, \ldots, A_n)$, $B = (B_1, \ldots, B_n)$, $C = (C_1, \ldots, C_n)$, $D = (D_1, \ldots, D_n)$ form a basis of $\mathscr{Q}_n/\mathscr{C}_n$, where

$$A_i = \sum_{a\neq i} x_{ia}^2, \qquad B_i = \sum_{\{a,b\}\in\binom{[n]\setminus\{i\}}{2}} x_{ia}x_{ib},$$

$$C_i = \sum_{a\neq i}\ \sum_{b\notin\{i,a\}} x_{ia}x_{ab}, \qquad D_i = \sum_{a\neq i}\ \sum_{\{b,c\}\in\binom{[n]\setminus\{i,a\}}{2}} x_{ia}x_{bc}.$$

(c) Construct explicit weights x and two vertices $i \neq j$ such that every linear anonymous rule assigns the same score to i and j, but some quadratic anonymous rule assigns them different scores. Explain both assertions.

Recommended reading for Data Analysis:

- Keith Conrad, Group Actions, Sections 1–3, especially orbits and stabilizers.
- MIT OpenCourseWare 18.06SC, Independence, Basis and Dimension.

Problem 5 (Combinatorics)**.** Let ω be the primitive cube root of unity in the upper half of the complex plane and consider the subset $U := \{\pm 1, \pm\omega, \pm\omega^2\}$ of the ring

$$\mathbb{Z}[\omega] := \{a + b\omega : a, b \in \mathbb{Z}\}.$$

For $S \subseteq U$ and $n \in \mathbb{N}_0$, an S**-walk of length** n is a sequence $z_0, z_1, \ldots, z_n$ in $\mathbb{Z}[\omega]$ such that $z_0 = 0$ and $z_k - z_{k-1} \in S$ for every integer k with $1 \leq k \leq n$. For $\alpha \in \mathbb{Z}[\omega]$, let $c_n(\alpha; S)$ denote the number of S-walks of length n with endpoint $z_n = \alpha$.

(a) For $S_+ := \{1, \omega, \omega^2\}$ and $\alpha \in \mathbb{Z}[\omega]$, consider the ordinary generating function

$$G_\alpha(t) := \sum_{n=0}^{\infty} c_n(\alpha; S_+)t^n.$$

Prove that, for every fixed $\alpha \in \mathbb{Z}[\omega]$, the radius of convergence of G_α is $1/3$. More precisely, show that

$$G_\alpha(t) = -\frac{\sqrt{3}}{2\pi}\log(1 - 3t) + O_\alpha(1)$$

as $t \to (1/3)^-$ through real values. In particular, the coefficient of the leading logarithmic term is independent of the endpoint α.

(b) Let $\lambda := 1 - \omega \in \mathbb{Z}[\omega]$. A U-walk $z_0, z_1, \ldots, z_\ell$ of positive length is called λ-**primitive** if $z_\ell = 0$ and

$$z_k \notin \lambda\mathbb{Z}[\omega] := \{\lambda z : z \in \mathbb{Z}[\omega]\}$$

for every integer k with $1 \leq k \leq \ell - 1$. Let p_ℓ denote the number of λ-primitive U-walks of length ℓ. Determine

$$\lim_{n\to\infty} (p_{2n})^{1/(2n)}.$$

Recommended reading for combinatorics:

- *Enumerative Combinatorics* by R. Stanley (Vol. 1, Chapters 1–3)

Problem 6 (Abstract Algebra)**.** A subset $M \subseteq \mathbb{Q}$ is an **additive submonoid** of $\mathbb{Q}$ if $0 \in M$ and $q + r \in M$ for all $q, r \in M$. If M and N are two additive submonoids of $\mathbb{Q}$ then we say that M is a **submonoid** of N if $M \subseteq N$.

For $S \subseteq \mathbb{Q}$, let M_S be the additive submonoid generated by S, that is, the smallest additive submonoid of $\mathbb{Q}$ containing S; in particular, $M_\varnothing = \{0\}$.

For a submonoid M of $\mathbb{Q}$, let $\mathrm{Aut}(M)$ be the group, under composition, of all bijections $\varphi : M \to M$ satisfying $\varphi(q + r) = \varphi(q) + \varphi(r)$ for all $q, r \in M$.

(a) For $q \in \mathbb{Q}$ with $q > 0$, determine $\mathrm{Aut}(M_{S_q})$, where $S_q := \{q^n : n \in \mathbb{Z}\}$.

(b) Determine, up to isomorphism, which groups occur as $\mathrm{Aut}(M_S)$ as S ranges over the subsets of $\mathbb{Q}$ consisting of positive rationals.

For a field F and an additive submonoid M of $\mathbb{Q}$, let

$$F[M] := \bigoplus_{q \in M} F x^q$$

denote the F-vector space with basis $\mathscr{M} := \{x^q : q \in M\}$, where x^q is a formal symbol for each $q \in M$ (elements of $F[M]$ are finite linear combinations of the elements in $\mathscr{M}$). Define a multiplication in $F[M]$ similar to the standard multiplication of polynomials: for all $q, r \in M$, set

$$x^q x^r := x^{q+r}$$

and extend this to the whole $F[M]$ via the distributive law. Then let $\mathrm{Aut}_{\mathrm{gr}}(F[M])$ denote the set of all F-algebra automorphisms Φ of $F[M]$ such that, for every $q \in M$,

$$\Phi(x^q) = c x^{q'}$$

for some nonzero $c \in F$ and $q' \in M$ (note that c and q' may depend on q). The set $\mathrm{Aut}_{\mathrm{gr}}(F[M])$ is also a group under composition. Let $\mathrm{Hom}(M, F^\times)$ denote the group, under pointwise multiplication, consisting of all maps $\chi \colon M \to F \setminus \{0\}$ satisfying $\chi(0) = 1$ and $\chi(q + r) = \chi(q)\chi(r)$ for all $q, r \in M$.

(c) Describe $\mathrm{Aut}_{\mathrm{gr}}(F[M])$ in terms of $\mathrm{Aut}(M)$ and $\mathrm{Hom}(M, F^\times)$. For the submonoid $D_2 := \{n/2^m : m, n \in \mathbb{N}_0\}$ of $\mathbb{Q}_{\geq 0}$ consisting of all nonnegative dyadic rationals, describe the groups

$$\mathrm{Hom}(D_2, \mathbb{C}^\times) \qquad \text{and} \qquad \mathrm{Aut}_{\mathrm{gr}}(\mathbb{C}[D_2])$$

explicitly. For $\mathrm{Hom}(D_2, \mathbb{C}^\times)$, a description as the group of sequences $(z_0, z_1, \ldots)$ of nonzero complex numbers satisfying $z_{m+1}^2 = z_m$ for every $m \in \mathbb{N}_0$, with coordinatewise multiplication, is acceptable. Finally, compare $\mathrm{Hom}(D_2, \mathbb{C}^\times)$ with $\mathrm{Hom}(\mathbb{N}_0, \mathbb{C}^\times)$ by determining, in each case, the image and kernel of the evaluation homomorphism $\chi \mapsto \chi(1)$ into $\mathbb{C}^\times$.

Note: You are allowed to use the following known theorem without proving it.

- **Theorem.** Every subgroup of a free abelian group is a free abelian group.

Recommended reading for abstract algebra:

- *Algebra: Abstract and Concrete* by Frederick M. Goodman [3] (Chapters 1–6)

Problem 7 (Number Theory)**.** Fix a positive $r \in \mathbb{R}$, and let $\mathbb{N}_0[r]$ be the set of values $p(r)$, where $p(x)$ is a polynomial with nonnegative integer coefficients. Note that $\mathbb{N}_0[r]$ contains 0 and 1 and is closed under the standard addition and multiplication of real numbers. Then set

$$\mathbb{N}_0[r]^\times := \{s \in \mathbb{N}_0[r] \setminus \{0\} : 1/s \in \mathbb{N}_0[r]\}$$

and call the elements of $\mathbb{N}_0[r]^\times$ **units** of $\mathbb{N}_0[r]$. A nonzero nonunit $a \in \mathbb{N}_0[r]$ is called **irreducible** if every factorization $a = uv$ with $u, v \in \mathbb{N}_0[r]$ has a unit factor. Two nonzero elements are called **associates** if one is a unit multiple of the other; thus,

$$t\mathbb{N}_0[r]^\times = \{tu : u \in \mathbb{N}_0[r]^\times\}$$

is the associate class of a nonzero element t.

For $\ell \in \mathbb{N}$, we say that $\mathbb{N}_0[r]$ has the ℓ-**Goldbach property** if there exists a finite collection $\mathscr{F}$ of associate classes such that every nonzero element $a \in \mathbb{N}_0[r]$ that belongs to none of the classes in $\mathscr{F}$ can be written as

$$a = u_1 + \cdots + u_j$$

for some $1 \le j \le \ell$, where $u_1, \ldots, u_j$ are irreducible (repetitions among the u_i are allowed). We say that $\mathbb{N}_0[r]$ has the **Goldbach property** if it has the ℓ-Goldbach property for some $\ell \in \mathbb{N}$. If $\mathbb{N}_0[r]$ has the Goldbach property, then its **Goldbach number** is

$$\min\big\{\ell \in \mathbb{N} : \mathbb{N}_0[r] \text{ has the } \ell\text{-Goldbach property}\big\}.$$

(a) Determine all $q \in \mathbb{Q}_{>0}$ such that $\mathbb{N}_0[q]$ contains infinitely many pairwise nonassociate irreducibles.

(b) Prove that $\mathbb{N}_0[q]$ has the Goldbach property if and only if $q \in \mathbb{N} \cup \mathbb{N}^{-1}$, where

$$\mathbb{N}^{-1} := \left\{\frac{1}{d} : d \in \mathbb{N}\right\}.$$

(c) Prove that the following two statements hold:
- For $k \in \mathbb{N}$, the Goldbach number of $\mathbb{N}_0[k]$ belongs to $\{3, 4\}$;
- For $k \in \mathbb{N}$ with $k \ge 2$, the Goldbach number of $\mathbb{N}_0[1/k]$ belongs to $\{2, 3, 4\}$.

Note: You are allowed to use the following results without proving them.

- **Ternary Goldbach theorem (Helfgott)** [1]**.** Every odd integer greater than 5 is a sum of three primes.
- **Finite-avoidance corollary of the almost-equal-summands theorem (Matomäki, Maynard, and Shao)** [2]**.** For every finite set of primes P, every sufficiently large odd integer is a sum of three primes not in P.

Recommended reading for number theory:

- *Problems in Algebraic Number Theory* by M. R. Murty and J. Esmonde (Chapters 1–5)

References

[1] H. A. Helfgott, *The ternary Goldbach conjecture is true*, arXiv:1312.7748. This proves that every odd integer greater than 5 is a sum of three primes.

[2] K. Matomäki, J. Maynard, and X. Shao, *Vinogradov's theorem with almost equal summands*, Proceedings of the London Mathematical Society **115** (2017), 323–347, doi:10.1112/plms.12040. The theorem places all three primes near one third of the target and therefore implies avoidance of any fixed finite set for sufficiently large targets.

[3] F. M. Goodman, *Algebra: Abstract and Concrete*, edition 2.6. The author's online edition is available at https://homepage.divms.uiowa.edu/~goodman/algebrabook.dir/download.htm.