REU 2012 - Problems

Puzzle Problems Sheet

Instructor: László Babai e-mail: laci@cs.uchicago.edu

Sun, June 24

1. ♡ **(Balancing numbers)** Suppose we have 13 real numbers with the following property: if we remove any one of the numbers, the remaining 12 can be split into two sets of 6 numbers each with equal sum. Prove: all the 13 numbers are equal. (Hint: first assume all the numbers are integers.)

2. ♡ **(Dividing a rectangle)** A large rectangle is cut up into a finite number of smaller rectangles. (All edges are either horizontal or vertical.) Suppose each of the smaller rectangles has at least one side of integer length. Prove that the same holds for the large rectangle.

3. ♡ **(Spreading Infection)** Some of the 64 cells of a chessboard are initially infected. Subsequently the infection spreads according to the following rule: if two neighbors of a cell are infected then the cell gets infected. (Neighbors share and edge, so each cell has at most four neighbors.) No cell is ever cured. What is the minimum number of cells that need to be initially infected to guarantee that the infection spreads all over the chessboard? It is easy to see that 8 are sufficient in many ways. Prove that 7 are not enough. (This is an AH-HA problem. The main idea of a clear and convincing solution can be summarized in a single 9-letter word.)

4. ♡ **(Polynomials with prime exponents)** Prove: every polynomial $f(x) \neq 0$ has a multiple $g(x) = f(x)h(x) \neq 0$ in which every exponent is prime. (So $g(x)$ has the form $\sum_p a_p x^p$ where the summation is over primes.)

5. ♡ **(Dominoes)** Prove: if we remove two opposite corners from the chessboard, the board cannot be covered by dominoes. (Each domino covers two neighboring cells of the chessboard.) Look for an "AH-HA" proof: brief, convincing, no cases to distinguish.

6. ♡ **(Triominoes)** Remove a corner from a $n \times n$ chessboard. We attempt to tile the board by *triominoes*. (A triomino is like a domino except it consists of three squares in a row; each cell can cover one cell on a chessboard. Each triomino can either "stand" or "lie.") There is certainly no such tiling when $n \equiv 0 \pmod 3$, and it is easy to find such a tiling when $n \equiv 1 \pmod 3$. Prove that no tiling exists when $n \equiv -1 \pmod 3$. Find an "Ah-ha" proof.

7. ♡ **(*Band-Aids* - László Surányi)** Consider three pairwise adjacent faces of an $n \times n \times n$ cube. For what values of n is it possible to tile the three faces with 3×1 "band-aids"? A band-aid may wrap around and edge, but cannot bend (see Fig. 1).

8. ♡ **(Cleaning the corner - Tom Hayes)** We label the cells of the positive quadrant (the "game board") by pairs of integers $\{(i, j) : i, j \geq 0\}$. The neighbor to the North of cell

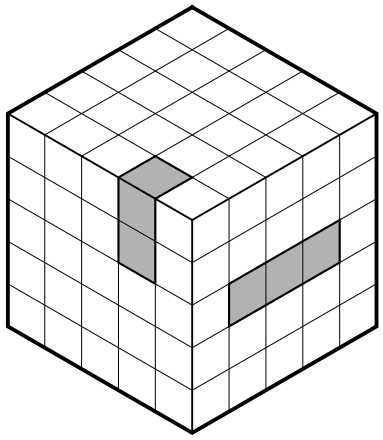

Figure 1: Two possible positions of a "band-aid" tile.

(i, j) is cell $(i + 1, j)$; the neighbor to the East is cell $(i, j + 1)$. The corner cell is $(0, 0)$. The Manhattan distance between cells (i_1, j_1) and (i_2, j_2) is $|i_1 - i_2| + |j_1 - j_2|$.

Chips are placed on some of the cells, at most one chip per cell. Cells can be "cleaned" in the following manner: suppose a chip is on cell (i, j). If both its neighbor to the North and its neighbor to the East are empty, we can remove the chip from (i, j) and place a chip on its neighbor to the North and another chip on the neighbor to the East.

Initially we put a chip on cell $(0, 0)$; otherwise the game board is empty. We wish to clean the corner, i. e., we wish to achieve, by a sequence of cell-cleaning moves, that there be no chip left within Manhattan distance d from the corner. Prove that this is impossible (a) for $d = 3$; (b) for $d = 2$.

Hint: *potential function:* assign a real number to every configuration by assigning weights to each cell; the "potential" of the configuration will be the total weight of occupied cells. Make this assignment such that the potential never increases when we clean a cell; and the initial potential (the weight of cell $(0, 0)$ be greater than the total weight of all cells outside the immediate neighborhood of the origin).

9. ♡ **(North versus South)** On an infinite square grid with horizontal Equator, the well-equipped North invades the defenseless South. However, North's troop movements come at a heavy cost, partly due to treacherous terrain (swamps, jungles, and such). Initially, North is permitted to position any number of soldiers above the Equator, at most one soldier per square. No new soldiers are added later; but soldiers can move as follows. If soldier X is adjacent to soldier Y, then X may 'jump over' to the other side of Y if that square is unoccupied, but as a consequence Y is removed from the board. Adjacency is vertical, horizontal, or diagonal (8 directions).

   (a) Show that North's troops cannot get further than 100 squares south of the Equator.

   (b) Show that North's troops cannot get further than 9 squares south of the Equator.

Hint: potential function.

10. **(Rational indepedence)** Show that $\{1, \sqrt{2}, \sqrt{3}\}$ are linearly independent over $\mathbb{Q}$.

11. **(*More rational independence*)** Show that $\{\sqrt{p} \mid p \text{ is prime}\}$ are linearly independent over $\mathbb{Q}$. Show further that $\{\sqrt{n} \mid n \text{ is squarefree}\}$ are linearly independent over $\mathbb{Q}$. Recall that n is *squarefree* if it is a product of distinct primes.

12. **(Points in general position)** Find a continuous function $f : \mathbb{R} \to \mathbb{R}^n$ so that for all $\alpha_1 < \alpha_2 < \cdots < \alpha_n$ with $\alpha_i \in \mathbb{R}$, the vectors $\{f(\alpha_1), \ldots, f(\alpha_n)\}$ are linearly independent.

13. ♡ **(Generalized Fisher Inequality)** Let k be a positive integer. Suppose $A_1, \ldots, A_m$ are distinct subsets of $[n] = \{1, 2, \ldots, n\}$ such that $|A_i \cap A_j| = k$ for all $i \neq j$. Show that $m \leq n$. (HINT. **(R. C. Bose, 1949)** The **incidence vectors** ("membership vectors") of the A_i are linearly independent.)

14. **(Erdős-de Bruijn families)**

    (a) We call a collection of sets $A_1, \ldots, A_m \subseteq [n]$ an *Erdős-de Bruijn family* if $|A_i \cap A_j| = 1$ for all $i \neq j$. Find an Erdős-de Bruijn family with $m = n = 7$ and such that $|A_i| = 3$ for all i.

    (b) **(Challenge)** For each prime p, find an Erdős-de Bruijn family with $m = n = p^2+p+1$ and $|A_i| = p + 1$.

15. ♡ **(Mod p complex numbers)** For which primes p does the set $\mathbb{F}_p[i] = \{a+bi : a, b \in \mathbb{F}_p\}$ form a field (where $i^2 = -1$)? (Experiment, notice simple pattern, conjecture, prove.)

16. **(Finite commutative ring)** Prove that a finite commutative ring R is a field if and only if $|R| \geq 2$ and for all $a, b \in R$, the equality $ab = 0$ holds if and only if $a = 0$ or $b = 0$.

17. **(Minimal subfield)** If F is a field, a *subfield* is a subset $H \subseteq F$ so that $1 \in H$ and H is closed under the four arithmetic operations. Show that every field F contains a unique minimal subfield H; and show that either $H \cong \mathbb{Q}$ or $H \cong \mathbb{F}_p$ for some prime p. In the former case we say that F has *characteristic zero*; in the latter case, *characteristic p*.

18. **(Polynomial gcd)** Suppose that $f, g \in F[x]$ are polynomials over a field F. Show that there exist $u, v \in F[x]$ so that $fu + gv = \gcd(f, g)$.

19. ♡ **(Inscribed polygons)** Suppose that a regular n-gon with vertices $A_0, A_1, \ldots, A_{n-1}$ is inscribed in the unit circle. Prove that

$$\prod_{i=1}^{n-1} \overline{A_0 A_i} = n.$$

    (Hint: Use polynomials and complex numbers.)

20. ♡ **(Random relative primes)** Show that the probability that two random positive integers are relatively prime is $6/\pi^2$. What does this question mean?

    To give a meaning to the question, consider the probability p_n that two positive integers less than n are relatively prime. Explicitly, we have

    $$p_n = \frac{|\{a, b \mid a, b \in [n] \text{ and } \gcd(a, b) = 1\}|}{n^2}.$$

    Let $p = \lim_{n\to\infty} p_n$ be the probability that "two random numbers are relatively prime." Show that $p = 6/\pi^2$. (Assume first that the limit exists.)

21. **(Real polynomial roots)** Show that every real polynomial of odd degree has a real root.

22. **(Rational irreducibility)** Show that $1 + x + \cdots + x^{p-1}$ is irreducible over $\mathbb{Q}$ for every prime p.

23. **(Gauss lemma)** (#1) Note that if $f, g \in F[x]$ are non-zero polynomials then $f \cdot g$ is also non-zero. Use this fact to prove that if $f, g \in \mathbb{Z}[x]$ are primitive, then $f \cdot g$ is also primitive. Recall that an integer polynomial $a_0+a_1x+\cdots+a_nx^n$ is *primitive* if $\gcd(a_0, a_1, \ldots, a_n) = 1$. (#2) Use (#1) to prove: if $f \in \mathbb{Z}[x]$ has a nontrivial factorization over the rationals then it has a nontrivial factorization over the integers.

24. **(Schönemann-Eisenstein irreducibility criterion)** (a) If $f(x) = a_0+a_1x+\cdots+a_nx^n \in \mathbb{Z}[x]$ and there exists a prime p so that $p \nmid a_n$, $p^2 \nmid a_0$, and $p \mid a_i$ for $i = 0, \ldots, n-1$, then f is irreducible over $\mathbb{Q}$. (b) Use this to prove that $(x^p - 1)/(x - 1)$ is irreducible.

25. ♡ **(More irreducible polynomials)** Let $a_1, \ldots, a_n$ be distinct integers. Prove that

    $$f(x) = \prod_{i=1}^{n}(x - a_i) - 1$$

    is irreducible over $\mathbb{Q}$. Hint: use Gauss Lemma #2.

26. **(Yet more irreducible polynomials)** Let $a_1, \ldots, a_n$ be distinct integers. Prove that

    $$g(x) = \left(\prod_{i=1}^{n}(x - a_i)\right)^2 + 1$$

    is irreducible over $\mathbb{Q}$.

27. **(Irreducibility over finite fields)** Let p be a prime and n a natural number.

    (a) Prove that there is an irreducible polynomial over $\mathbb{F}_p$ of degree n.

    (b) (b) Prove that if p^n is large then roughly a $1/n$ fraction of all monic polynomials of degree n over $\mathbb{F}_p$ are irreducible.

28. **(Galois fields)** (a) Construct $\mathbb{F}_4$. Hint: Consider $\mathbb{F}_2[\alpha]$, where you pretend that α is a root of $x^2 + x + 1 \in \mathbb{F}_2[x]$. (b) Let f be an irreducible polynomial of degree n over $\mathbb{F}_p$. Construct a field of order p^n by extending the method of part (a). (Cf. Prob. 15.)

29. **(2-distance sets)** We write $a_n = \Theta(b_n)$ if there exist $c_1, c_2 > 0$ so that $c_1 a_n \leq b_n \leq c_2 a_n$ for all n sufficiently large. Find $\Theta(n^2)$ points in $\mathbb{R}^n$ with just 2 distances.
Challenge: Show that $\Theta(n^2)$ is optimal for $\mathbb{R}^n$.

30. ♡ **(Maximal Eventown systems)** In Eventown, each club has an even number of members, each pair of clubs shares an even number of members, and no two clubs have identical membership. Show that there are at most $2^{\lfloor n/2 \rfloor}$ clubs in Eventown.

31. **(Another maximal Eventown)** Show that for all sufficiently large n, there exist maximum Eventown club systems that are not isomorphic to the "married couples" system. (In the "married couples" system, there are $\lfloor n/2 \rfloor$ couples; the couples join clubs together; if n is odd, the one unmarried citizen is banned from all clubs.) Hint: use the next exercise.

32. **(Maximal implies maximum in Eventown)** Show that every *maximal* Eventown club system is *maximum.* In other words, if there are fewer than $2^{\lfloor n/2 \rfloor}$ clubs in Eventown, one can add a club. (Note the contrast with Oddtown.)

33. **(Oddtown varieties)** In Oddtown, there are n citizens and m clubs satisfying the rules that each club has an odd number of members and each pair of clubs shares an even number of members. Find $c > 0$ so that there are more than 2^{cn^2} collections of n clubs in Oddtown.

34. ♡ **(Oddtown Theorem)** Prove that there are no more than n clubs in Oddtown. (Hint: prove that the incidence vectors of the clubs are linearly independent over $\mathbb{F}_2$.)

35. **(2-distances revisited)** Show that there are 2-distance sets of size $m = \binom{n+1}{2}$ in $\mathbb{R}^n$.

36. **(Counting monomials)** Find a simple closed-form expression for the number of monomials of degree k in n variables.

37. **(Multiple roots)** Given a polynomial $f(x) = \sum_{i=0}^{n} a_i x^i \in F[x]$, define the *formal derivative* to be the polynomial $f'(x) = \sum_{i=1}^{n} i a_i x^{i-1}$. (This definition works over any field; note that we have no concept of limit over fields like $\mathbb{F}_p$, so the usual definition from calculus is not applicable.) (a) Show that the usual rules of differentiation apply, including the product rule and the chain rule. (b) Show that α is a multiple root of $f \in F[x]$ if and only if $f(\alpha) = 0$ and $f'(\alpha) = 0$.

38. **(Complex polynomials)** Prove: $f \in \mathbb{C}[x]$ has a multiple root if and only if $\gcd(f, f') \neq 1$.

39. **(Zero to the zero)** (a) For each real number $r \in [0, 1]$ find a pair $\{x_n\}_{n=1}^{\infty}$ and $\{y_n\}_{n=1}^{\infty}$ of sequences converging to zero from above such that

$$\lim_{n \to \infty} x_n^{y_n} = r.$$

(b) Find a pair $\{x_n\}_{n=1}^{\infty}$ and $\{y_n\}_{n=1}^{\infty}$ of sequences converging to zero from above such that every real number $r \in [0, 1]$ is the limit of some subsequence of the sequence $x_n^{y_n}$.

40. **(Almost sure limit)** Show that
$$\lim_{x,y\to 0^+} x^y = 1$$
almost surely. Your main task is to define what this statement means.

41. **(Irreducibility over $\mathbb{F}_p$)** If p^n is large, roughly a $\frac{1}{n}$ fraction of the degree n monic polynomials over $\mathbb{F}_p$ are irreducible.

42. ♡ **(Most integral polynomials are irreducible)** Prove: almost all polynomials of degree n over $\mathbb{Z}$ are irreducible over $\mathbb{Q}$. (Hint: Consider the collection of polynomials $P_k = \{\sum_{i=0}^n a_i x^i \mid |a_i| \le k\}$. Then, take k to infinity. The value n is fixed in this problem.)

43. **(Isotropic vectors over $\mathbb{F}_p$)** Recall that for $\vec{a} = (\alpha_1, \ldots, \alpha_n) \in F^n$ and $\vec{b} = (\beta_1, \ldots, \beta_n) \in F^n$ we define the standard dot product as $\vec{a} \cdot \vec{b} = \sum_{i=1}^n \alpha_i \beta_i$. We say that $\vec{a} \perp \vec{b}$ ("$\vec{a}$ and $\vec{b}$ are perpendicular") if $\vec{a} \cdot \vec{b} = 0$. We say that $\vec{a}$ is *isotropic* if $\vec{a} \neq \vec{0}$ and $\vec{a} \perp \vec{a}$. (a) For which primes p does there exist an isotropic vector $\vec{a} \in \mathbb{F}_p^2$? (b) Prove that for all primes p there is an isotropic vector in $\mathbb{F}_p^3$.

44. **(The card game "SET")** Let us call a subset $S \subseteq \mathbb{F}_3^n$ *SET-free* if it does not contain an affine line. (Verify that affine lines correspond to "SETs" in the card-game "SET".) Denote by α_n the maximum size of a SET-free subset of $\mathbb{F}_3^n$. Prove that:

    (a) $\alpha_{n+m} \ge \alpha_n \alpha_m$;

    (b) **(Fekete's Lemma)** Infer from (a) that $\alpha_n^{1/n}$ tends to a limit as $n \to \infty$, which is $L := \sup_n \alpha_n^{1/n}$;

    (c) $2^n \le \alpha_n < 3^n$, and hence $2 \le L \le 3$;

    (d) $L > 2$, and find as good a lower bound on L as you are able. (Check the web about the card game "SET!");

    (e**) **(Meshulam's Theorem)** $\alpha_n < 2 \cdot 3^n/n$ (but still $\lim_{n\to\infty}(2 \cdot 3^n/n)^{1/n} = 3$);

    (f***) **(Open problem)** Is $L < 3$?

45. **(The degenerate projective planes)** Recall that the three axioms of a projective plane are

    1. There exists a line through every distinct pair of points.
    2. Every distinct pair of lines intersects in a unique point.
    3. There exist four points no three of which are collinear (are on a line).

    The following is a weaker condition than axiom 3.

    3'. There exist three points which are not collinear.

    A set system satisfying conditions 1, 2 and 3' but *not* 3 is called a "degenerate projective plane." Describe all degenerate projective planes; show that for every $n \ge 3$ there is exactly one degenerate projective plane with n points.

46. **(Projective plane of order n)** For every finite projective plane (P, L) there exists n such that

$$\begin{aligned} &|P| = n^2 + n + 1 \\ &|L| = n^2 + n + 1 \\ &\#\text{ of points per line} = n + 1. \\ &\#\text{ of lines per point} = n + 1 \end{aligned}$$

where $|P|$ is the number of points and $|L|$ the number of lines.

47. **(Neighbor transpositions)** (a) Show that the neighbor transpositions $(12), (23), \ldots, (n-1\ n)$ generate the symmetric group S_n. (b) Show that $O(n^2)$ neighbor transpositions suffice to generate S_n and $\Omega(n^2)$ are necessary to generate S_n. That is, there exist positive constants c_1, c_2 such that (b1) each element of S_n can be expressed as the composition of at most $c_1 n^2$ neighbor transpositions; and (b2) there exists a permutation which cannot be expressed as the composition of fewer than $c_2 n^2$ neighbor transpositions. - The "word length" of a permutation with respect to a set of generators is the smallest length of a word in the generators that expresses the given permutation. So what you were asked to show was that the maximum word length with respect to neighbor transpositions is $\Theta(n^2)$, i.e., it is between $c_2 n^2$ and $c_1 n^2$ for some positive constants c_1 and c_2.

48. **(A set of two generators for S_n)** The symmetric group is generated by the n-cycle $\rho = (12 \ldots n)$ and the transposition (12). Show that, as in the previous exercise, the maximum word length is $\Theta(n^2)$.

49. **(The identity is even)** Show that the identity permutation cannot be expressed as the product of an odd number of transpositions.

50. **(Alternating group)** The alternating group A_n is the subgroup of S_n consisting of the even permutations. Show that $|A_n| = \frac{n!}{2}$ for $n \geq 2$.

51. ♡ **(Sam Lloyd's 15 Puzzle)** Arrange the numbers $1, \ldots, 15$ on a 4×4 grid together with a blank. You may alter the board by transposing the blank with a neighboring square. Show that a random arrangement has $1/2$ chance to be feasible (have a solution).

52. **(Rubik's cube)** Suppose we pull Rubik's cube apart and reassemble it at random. This leads to $8! \cdot 3^8 \cdot 12! \cdot 2^{12}$ configurations. Show that exactly $\frac{1}{12}$ of these are feasible (solvable by legal moves).

53. Of the following statements, show that (a)$\Leftrightarrow$ (b)$\Leftrightarrow$ (c) $\Leftarrow$ (d).

    (a) $\mathbb{F}_p[\sqrt{-1}]$ is not a field.

    (b) $\exists$ an isotropic vector in $\mathbb{F}_p^2$.

    (c) $(\exists x)\,(x^2 \equiv -1 \bmod p)$.

    (d) $(\exists a, b > 0)\,(p = a^2 + b^2)$.

54. ***** Show that in fact (d) is equivalent to the rest of the statements.

55. (a) (Experiment) Observe a very simple characterization of the primes for which the statements in Problem 53 are true.

    (b) Show: there exist infinitely many primes for which all the statements in problem 53 are false. (Hint: Fermat's little Theorem)

    (c*) Show: there exist infinitely many primes for which all the statements in problem 53 are true. (Hint: use the theorem that there exists a primitive root modulo p.)

56. **(Miklós Abért)** Let $A_1, \ldots, A_m, B_1, \ldots, B_m \in M_n(F)$ be $n \times n$ matrices. Suppose that $A_i B_j = B_j A_i$ if and only if $i \neq j$. Prove: $m \leq n^2$.

    (Open: m is much less than n^2.)

57. **(Latin squares)** Prove that every Latin rectangle can be extended to a Latin square.

58. (a) Show that if n is odd then there exists a pair of orthogonal Latin squares.

    (b) Show that if $n = 4$, then there exist 3 pairwise orthogonal Latin squares.

    (c) Show that the 4×4 circulant $C(1, 2, 3, 4)$, which is a Latin square, has no orthogonal mate.

    (d) Prove that the number of pairwise orthogonal $n \times n$ Latin squares is at most $n - 1$.

    (e) There exists $n - 1$ pairwise orthogonal $n \times n$ Latin squares $\iff$ there exists a projective plane of order n.

59. **(Graphs)** A graph G has a closed Eulerian trail $\iff$ G is connected and every vertex has even degree.

60. What is the maximum number of edges in a triangle-free graph on n vertices?

61. Planar graphs are 6-colorable.

62. K_5 and $K_{3,3}$ are not planar.

63. Is the Petersen's graph isomorphic to the other graph drawn on the board?

64. Find a graph that is not 3-colorable but does not contain K_3. (Hint: find such a graph with $n = 11$ vertices; your graph should have a drawing with 5-fold symmetry. These properties determine the graph uniquely. The graph is called the **Grötzsch's graph.**)

65. Let G be a regular graph of degree r and girth ≥ 5. (The *girth* is the length of the shortest cycle in G.) Prove $n \geq r^2 + 1$.

66. **(Algebraic numbers)** We say that $\alpha \in \mathbb{C}$ is an *algebraic number* if there is a nonzero polynomial $f \in \mathbb{Z}[x]$ so that $f(\alpha) = 0$.

    (a) The algebraic numbers form a (number-)field.

    (b) The field of algebraic numbers is algebraically closed.

(c) As a hint for the previous: If $F \subset G \subset H$ are field extensions, then $\dim_F H = \dim_G H \cdot \dim_F G$.

67. **(Symmetric polynomials)** The k^{th} elementary symmetric polynomial is defined as

$$\sigma_k(x_1, \ldots, x_n) = \sum_{i_1 < \cdots < i_k} x_{i_1} \cdots x_{i_k}.$$

(a) Express $\sum_{i=1}^{n} x_i^2$ in terms of σ_1 and σ_2.

(b) Show that every symmetric polynomial of $x_1, \ldots, x_n$ is a polynomial of $\sigma_1, \ldots, \sigma_n$.

68. ♡ **(Polynomial hidden treasure)** You land on a deserted island, looking for pirate treasure. Sure enough, there is an old, weathered treasure map with fiendishly complicated instructions written by a pirate who was a mathematician before following the lure of filthy lucre at sea. You realize that the information of the treasure's location is encoded in the roots of some polynomial which starts "$x^{100} - 5x^{99} + 13x^{98} + \ldots$." Unfortunately, the rest of the polynomial is lost to the sands of time. Show that not every root of this polynomial is real.

69. ♡ Let R_n denote the set of fixed-point-free permutations of $[n]$, i. e.,
$R_n = \{\sigma \in S_n \mid (\forall i)(\sigma(i) \neq i)\}$.
(a) Decide whether there are more even permutations or more odd permutations in R_n.
(b) Prove that

$$\sum_{\sigma \in R_n} \operatorname{sgn}(\sigma) = (-1)^{n-1}(n-1).$$

70. Let F_n denote the n-th Fibonacci number ($F_0 = 0, F_1 = 1$, $F_n = F_{n-1} + F_{n-2}$). Prove:
(a) If $d \mid n$ then $F_d \mid F_n$.
(b) If $d = \gcd(k, \ell)$ then $F_d = \gcd(F_k, F_\ell$.

71. ♡ **(Secret Sharing)** There is a committee of n members, the president (which is not part of the committee) chooses a secret random number $x \in \{0, \ldots, p-1\}$, where p is some fixed prime number. The president then gives each member a number in $\{0, \ldots, p-1\}$ in such a way that if k members get together, they can compute x exactly but if only $k-1$ get together, they have no information about x. How can the president do that? Hint: Polynomials over $\mathbb{F}_p$.

72. **(Automorphisms of graphs)** Count the automorphisms of

(a) K_n: the complete graph with n vertices.

(b) C_n: the cycle with n-vertices.

(c) The cube. You should get 48; then show that the subgroup of orientation preserving congruences, which has 24 elements, is isomorphic to S_4.

(d) The dodecahedron. You should get 120; then show that the group of orientation preserving congruences is isomorphic to A_5.

(e) The other platonic solids: tetrahedron, octahedron, icosahedron.

(f) The Petersen Graph. You should get 120; show that this group is isomorphic to S_5. (Hint: (1) use the isomorphism of the two drawings of the Petersen graph shown in class to show that any directed path of length 3 can be sent to any other directed path of length 3 by an automorphism. (2) Ignore (1). Find a simple connection of the Petersen graph to K_5 that will make it obvious that their automorphism groups are isomorphic.)

73. All congruences of $\mathbb{R}^3$ that fix the origin are one of the following types: rotation about an axis, reflection with respect to a plane, rotational reflection with axis perpendicular to the plane (so the rotation and the reflection commute).

74. Find the rotational reflection that permutes the vertices of the tetrahedron in a 4-cycle.

75. **(Adjacency matrix of a graph)** Let f_G be the characteristic polynomial of the adjacency matrix of a graph G. Prove: if f_G is irreducible over $\mathbb{Q}$, then $|\operatorname{Aut}(G)| = 1$.

76. **(Primitive roots of unity)** Recall that the complex number z is a *primitive n-th root of unity* if $z^n = 1$ but $z^k \neq 1$ for any $1 \leq k < n$. Note that the number $\omega = \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})$ is a primitive n^{th} root of unity. Recall further that Euler's φ function is defined as $\varphi(n) = |\{k \mid 1 \leq k \leq n,\ \gcd(k,n) = 1\}|$. Now, prove:

(a) ω^j is a primitive n^{th} root of unity iff $\gcd(n,j) = 1$.
(b) The number of primitive n^{th} roots of unity equals $\varphi(n)$
(c) The φ function is "multiplicative," i. e., if $\gcd(a,b) = 1$ then $\varphi(ab) = \varphi(a)\varphi(b)$.
(d) If $n = {p_1}^{k_1} \dots {p_n}^{k_n}$ then $\varphi(n) = n \cdot \prod_{i=1}^{n}(1 - \frac{1}{p_i})$.
(e) Prove that $\inf_n \frac{\varphi(n)}{n} = 0$.
(f) Prove that $\sum_{d|n} \varphi(d) = n$.

77. **(Moebius function)** Define

$$\mu(n) = \begin{cases} 0 & n \text{ is not square free} \\ (-1)^k & n = p_1 \dots p_k \text{ is a product of } k \text{ distinct primes.} \end{cases}$$

Prove the following.

(a) $\sum_{d|n} \mu(d) = \begin{cases} 1 & n = 1 \\ 0 & \text{otherwise} \end{cases}$
(b) If $f : \{1, 2, \dots\} \to \mathbb{C}$ define $g(n) = \sum_{d|n} f(d)$. Show that $f(n) = \sum_{d|n} \mu(\frac{n}{d}) g(d)$.
(c) Show that f is multiplicative iff g is multiplicative.
(d) Let s_n denote the sum of all primitive n^{th} roots of unity. Show that $s_n = \mu(n)$.
(e) Define $\Phi_n(x) = \prod(x - \omega_i)$ where the product is taken over all primitive n^{th} roots of unity ω_i. Then, $\deg(\Phi_n) = \varphi(n)$. Prove: $\Phi_n \in \mathbb{Z}[x]$.
(f*) Prove that Φ_n is irreducible. The case n prime was handled in class via the Schönemann-Eisenstein criterion.

78. **(GCD matrix)** Let $D = (d_{ij})_{n\times n}$ where $d_{ij} = \gcd(i, j)$. Then,

$$\det(D) = \varphi(1)\varphi(2)\ldots\varphi(n)$$

where φ is Euler's φ function: $\varphi(m) = |\{\ k \mid 1 \leq k \leq m,\ \gcd(k, m) = 1\ \}|$.