REU APPRENTICE PROBLEMS 1–193

INSTRUCTOR: LÁSZLÓ BABAI
SCRIBES: ASILATA BAPAT, MARKUS KLIEGL, DANIEL SCHÄPPI, MICHAEL SMITH, MATTHEW WRIGHT, BOWEI ZHENG

Last updated: Friday, July 22, 2011

1. Puzzle Problems

Problem 1. Give a simple condition for when a prime number p can be expressed as the sum of two squares. That is, when do there exist integers a, b such that $p = a^2 + b^2$? Experiment, discover simple pattern, formulate conjecture. Your conjecture will be an "if and only if" statement. One direction will be much easier to prove than the other.

Problem 2. Consider an 8×8 chessboard, with two opposite corners removed. Is it possible to tile this with non-overlapping dominoes?

Problem 3. We are are given thirteen weights (real numbers) with the following property: if any one weight is removed, the remaining twelve can be split into two groups of six each such that the two groups have equal total weight. Prove that all thirteen weights must be equal. [Updated 6/24/2012]

2. What is the answer? What is the question?

Problem 4. What is the probability that two positive integers are relatively prime? (What does this question mean? Use limits to define the meaning of the probability in question. Does that limit exist?) (Hint: The limit does exist, and is equal to $6/\pi^2$. The fun part is this: assume the limit exists; then prove in a few lines that it can only be $6/\pi^2$. Use the fact (Euler) that $\sum_{n=1}^{\infty} 1/n^2 = \pi^2/6$.)

Problem 5. Show that "almost always," we have:

$$\lim_{\substack{x\to 0+\\ y\to 0+}} x^y = 1.$$

What does this statement mean?

Problem 6. What is the title of the novel that describes a quest to find the "ultimate answer" (which turns out to be 42), and then the "ultimate question"?

Problem 7. Let $\pi(n)$ be the number of primes in $\{1, \ldots, n\}$. Prove, from first principles, that

$$\lim_{n\to\infty} \frac{\pi(n)}{n} = 0.$$

3. Vectors and fields

Problem 8. Let $g(x) = (x - \alpha_1) \cdots (x - \alpha_n)$, where the numbers α_i are distinct real number. Let $f_i(x) = g(x)/(x - \alpha_i)$. Show that the polynomials $f_1, \ldots, f_n$ are linearly independent.

Problem 9. Prove that $1, \cos x, \sin x, \cos 2x, \sin 2x, \cdots \in C[0, 2\pi]$ is an orthogonal system under the inner product $\langle f, g\rangle = \int_0^{2\pi} f(x)g(x)dx$. Infer that these trig. functions are linearly independent.

Problem 10. Prove that:

(1) $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ is a number field.
(2) $\mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt{2} + c\sqrt{4} \mid a, b, c \in \mathbb{Q}\}$ is a number field.

Problem 11. Show that if F is a number field, then $F \supset \mathbb{Q}$.

Problem 12. Prove that $1, \sqrt{2}, \sqrt{3}$ are linearly independent over $\mathbb{Q}$.

4. Clubtown, Eventown, Oddtown

Recall the first rule of Clubtown: no two clubs can have the same set of members. If there are n residents, then there can be at most 2^n clubs.

Problem 13. Suppose that now every club must have an even number of members. What is the maximum number of clubs possible? Prove by a simple bijection that the number of even subsets is equal to the number of odd subsets.

Problem 14. Now consider Eventown, where every club must have an even number of members, and every pair of clubs must share an even number of members. What is the maximum possible number of clubs in Eventown? (Hint: The answer is $2^{\lfloor n/2 \rfloor}$.)

Observe that one way to produce $2^{\lfloor n/2 \rfloor}$ clubs is to pair up people into couples, and treat each couple as one unit. If one member of a unit joins a club, the other also automatically joins. Let us call this the "couples solution."

Problem 15. Show that for $n \geq 8$ there exists a non-couples solution that exhibits the maximum number of Eventown clubs.

First construct some system (not necessarily a maximum one) that does not come from any set of couples.

Problem 16. Show that every *maximal* system of clubs in Eventown is a *maximum* system.

Problem 17. Now consider Oddtown: every club must have an odd number of members, and every pair of clubs must share an even number of members. What is the maximum number of clubs possible? (Hint: The answer is equal to n.)

Problem 18. Show that the membership vectors of an Oddtown club system are linearly independent. (Hint: First prove this over $\mathbb{Q}$.)

Problem 19. If $v_1, \ldots, v_k$ are vectors in $\mathbb{Z}^n$ that are linearly independent over $\mathbb{Q}$, then show that they are also linearly independent over $\mathbb{R}$.

5. More puzzle problems

Let $f(x) = \sum_{i=1}^{n} a_i x^i$. Call f a *prime-exponent polynomial* if $a_i = 0$ for all i that are not prime.

Problem 20. Prove that every non-zero polynomial has a non-zero multiple that is a prime-exponent polynomial.

Consider a regular n-gon inscribed in a circle of radius 1, with consecutive vertices $P_0, P_1, \ldots, P_{n-1}$.

Problem 21. Show that the product of all the lengths $\overline{P_0 P_i}$ is equal to n.

(Hint: polynomials, complex numbers.)

6. The Fibonacci space

Consider the vector space V consisting of sequences $(a_0, a_1, \ldots)$ of real numbers.

Say that $s \in V$ is a *Fibonacci-type* sequence if for every $n \in \mathbb{N}$, we have $s_{n+2} = s_{n+1} + s_n$. For example, the Fibonacci numbers form a Fibonacci-type sequence.

Problem 22.
(a) The set Fib, consisting of all the Fibonacci-type sequences, is a subspace of V with dimension 2. Show that the sequences s and t form a basis of Fib, where $s_0 = 1$, $s_1 = 0$, $t_0 = 0$ and $t_1 = 1$.
(b) Find a basis of Fib consisting of two geometric progressions: $(1, r, r^2, \ldots)$ and $(1, s, s^2, \ldots)$. Then if F_n is the n-th Fibonacci number, we will have $F_n = \alpha r^n + \beta s^n$. Find r, s, α, β.

7. Matrix rank

Problem 23. Elementary row and column operations do not change either the row-rank or the column-rank of the matrix. Prove this by proving that

(a) elementary column operations do not change the column space (but elementary row operations may);
(b) elementary row operations do not change linear independence of any set of columns (but elementary column operations may).

Problem 24. The rows of a matrix are linearly independent if and only if the columns span F^k. Similarly the columns are linearly independent if and only if the rows span F^n.

8. More puzzles

Problem 25. What was Problem 25?

Problem 26. What if we use triominoes (three in a row) instead of dominoes to cover a board, and we have an $n \times n$ square with one square removed? If n is divisible by 3 we clearly can't do this, but for all other n the numbers at least work out. In particular, why can't we tile when $n = 101$?

9. Roots of unity

Problem 27. Prove that the sum $z_0 + z_1 + \cdots + z_{n-1}$ of all the nth roots of unity is 0 if $n \geq 2$, and 1 if $n = 1$.

Problem 28. For what k is the sum

$$\sum_{i=0}^{n-1} z_i^k = 0?$$

Problem 29. If z is a primitive nth root of unity, then for what values of k is z^k a primitive nth root of unity? How many powers of z will be primitive nth roots of unity?

Problem 30. Study the sum

$$S_n = \sum \text{primitive } n\text{-th roots of unity.}$$

What can you say or conjecture about S_n? We can see that $S_3 = -1$, $S_4 = 0$, and $S_6 = 1$; what are the rest? Experiment, discover pattern, conjecture, prove!

Problem 31. (1) Show that $\operatorname{ord}(z_1 z_2)$ is not necessarily equal to $\operatorname{lcm}(t_1, t_2)$.
(2) Show that if t_1 and t_2 are relatively prime, then $\operatorname{ord}(z_1 z_2) = t_1 t_2$.

10. Polynomials

Problem 32. Let h be a polynomial. If $h(x) = 0$ for all values of x, is h necessarily the zero polynomial?

11. Matrices, graphs, random walks (Markov Chains)

Problem 33. Let A and B be matrices. Show that

$$\operatorname{rk}(A + B) \leq \operatorname{rk}(A) + \operatorname{rk}(B).$$

Problem 34. Find two 2×2 matrices A, B such that $AB \neq BA$.

Problem 35. Show that

$$\operatorname{tr}(AB) = \operatorname{tr}(BA),$$

even if A and B aren't necessarily square.

Problem 36. Let

$$A = \begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$$

with $|a| < 1$ and $|d| < 1$. (The entries are complex numbers.) Show that

$$\lim_{k \to \infty} A^k = 0.$$

Problem 37. Let

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

What is A^k?

Problem 38. Let A be the adjacency matrix of a directed graph. Show that the (ij)-entry of A^t counts the t-step walks from i to j. Note that a walk is allowed to repeat vertices and edges, unlike a path!

Problem 39. Let $T = (p_{ij})$ denote the transition matrix of a Markov Chain. This means that p_{ij} is the probability that at time t the particle is in state j given that at time $t-1$ it was in state i (one-step transition probability). Let p_{ij}^{ℓ} denote the probability that the particle is in state j given that at time $t-\ell$ it was in state i (ℓ-step transition probability). Verify that

$$\left(p_{ij}^{(\ell)}\right) = T^{\ell};$$

that is, taking the ℓ-th power of the one-step transition matrix gives us the ℓ-step transition matrix.

12. Parity of permutations

Problem 40. Show that, for permutations π and σ,

$$\operatorname{sgn}(\pi\sigma) = \operatorname{sgn}(\pi)\operatorname{sgn}(\sigma).$$

Problem 41. (a) Prove directly, without using the previous problem, that the product of an odd number of transpositions can never be the identity. (b) Use this to solve the problem about Sam Lloyd's 15 puzzle.

13. The Symmetric Group

Problem 42. Find permutations π, σ such that $\operatorname{supp}(\pi) \cap \operatorname{supp}(\sigma) \neq \varnothing$ and $\pi\sigma = \sigma\pi$.

Problem 43. If $|\operatorname{supp}(\pi) \cap \operatorname{supp}(\sigma)| = 1$, then the commutator $[\pi, \sigma] = \pi\sigma\pi^{-1}\sigma^{-1}$ of π and σ is a 3-cycle.

Problem 44. A (possibly infinite) intersection of subgroups is a subgroup.

Problem 45.
(a) Show that there are many non-isomorphic arrangements of $n-1$ transpositions that generate S_n. (That is, the graph with an edge between i and j for every transposition (ij) in the respective generating sets are not isomorphic.)
(b) Show that S_n cannot be generated by fewer than $n-1$ transpositions.

Problem 46. The identity cannot be written as a product of an odd number of transpositions.

Problem 47. Let $\sigma = (1, 2, \ldots, n)$ and let $\tau = (12)$. Then:
(a) $S_n = \langle \sigma, \tau \rangle$
(b) Every permutation is a product of $O(n^2)$ instances of $\{\sigma, \sigma^{-1}, \tau\}$.
(c) For some permutations we need $\Omega(n^2)$.

Recall that $O(n^2)$ means *at most* $C \cdot n^2$, $\Omega(n^2)$ means *at least* $C' \cdot n^2$ for some constants $C, C' > 0$.

14. Groups and fields

Problem 48. In the multiplication table of a group, every element appears exactly once in each row and each column.

Problem 49. Prove that $\mathbb{Z}_n$ is a field if and only if n is a prime number.

Problem 50. If $\mathbb{F}$ is a finite field, then $|\mathbb{F}|$ is a prime power. (Note: the converse is also true: for every prime power q there is a field of order q, and this field is unique up to isomorphism.)

Problem 51. Let $\mathbb{C}_p = \{a + bi \mid a, b \in \mathbb{F}_p\}$ be the "mod p complex numbers." For what values of the prime number p is $\mathbb{C}_p$ a field? (Experiment, conjecture, prove. Hint: use Problem 52.)

Problem 52. A *finite* commutative ring R is a field if and only if $|R| \geq 2$ and for all $a, b \in R$, $ab = 0$ implies $a = 0$ or $b = 0$.

Problem 53. Give an example of an infinite field that is not isomorphic to a number field.

15. Asymptotics

Problem 54. Prove that $\ln(x!) \sim x\ln(x)$, where $a_n \sim b_n$ is short for $\lim_{n\to\infty} a_n/b_n = 1$ (asymptotic equality).

Problem 55. Let

$$P(x) = \prod_{p\le x \text{ prime}} p$$

be the product of all primes up to x. Prove that the statement

$$\ln\big(P(x)\big) \sim x$$

is equivalent to the Prime Number Theorem.

Problem 56. Find the log-asymptotics of the largest order of a permutation in S_n.

16. Variations on previous themes

Problem 57. Let A_1, A_2, A_3 be $n \times n$-matrices. For which permutations $\sigma \in S_3$ is the equation

$$\operatorname{tr}(A_1A_2A_3) = \operatorname{tr}(A_{\sigma(1)}A_{\sigma(2)}A_{\sigma(3)})$$

an identity? Being an identity means the equation holds for all possible choices of the matrices A_i.

Problem 58. Let F_n be the n-th Fibonacci number, i.e., $F_0 = 0$, $F_1 = 1$ and $F_n = F_{n-2} + F_{n-1}$. Prove (or disprove) that

(a) $\gcd(F_n, F_{n+1}) = 1$
(b) $\gcd(F_k, F_\ell) = F_d$ where $d = \gcd(k, \ell)$.

Problem 59. Let $A = (a_{ij})$ be an upper triangular $n \times n$ matrix and assume $|a_{ii}| < 1$ for $i = 1, \dots, n$. Show that $\lim_{k\to\infty} A^k = 0$.

Problem 60. Out of the 16! possible configurations of "Sam Lloyd's 15 puzzle," how many are feasible, i.e., how many can be rearranged into the configuration below by repeatedly shifting numbered tiles into the blank space?

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

Problem 61. Prove or disprove: if π and σ are permutations with $\operatorname{supp}(\pi) = \operatorname{supp}(\sigma)$, and if π and σ commute ($\pi\sigma = \sigma\pi$), then there exists a permutation ψ and integers k, l such that $\pi = \psi^k$, $\sigma = \psi^l$.

Problem 62. Prove the Binomial Theorem:

$$(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$$

Problem 63. Let

$$S_3(n) = \binom{n}{0} + \binom{n}{3} + \binom{n}{6} + \dots$$

be the number of subsets of $[n]$ whose cardinality is divisible by 3. Prove that

$$\left| S_3(n) - \frac{2^n}{3} \right| < 1.$$

Problem 64. Consider the limit

$$L = \lim_{n\to\infty} \mathrm{P}\big(\{(x,y) \in [n]\times[n] \,\big|\, \gcd(x,y) = 1\}\big)$$

of the probability that two positive integers $x, y \le n$ are relatively prime. Assume this limit exists. Use this assumption to give a very simple argument that $1/L$ must be equal to

$$\sum_{n=1}^{\infty} \frac{1}{n^2}.$$

17. Arithmetic of integers and polynomials

Problem 65. Prove the **prime property** (without using the fundamental theorem of arithmetic): if p is a prime number, $a, b \in \mathbb{Z}$, then $p \mid ab$ implies $p \mid a$ or $p \mid b$. (Hint: use Problem 72.)

Problem 66. Find an infinite field of finite characteristic.

Problem 67. (a) If $\mathrm{char}(F) = 0$, then $F \supseteq \mathbb{Q}$.
(b) If $\mathrm{char}(F) = p > 0$, then $F \supseteq \mathbb{F}_p$.

Problem 68 (Lagrange's Theorem)**.** Let G be a finite group and let $H \leq G$. Then $|H|$ divides $|G|$.

Problem 69. Let G be a group. Prove that for any $a \in G$, $\mathrm{ord}(a) = |\langle a \rangle|$.

Problem 70. Prove: if F is an infinite field, then two polynomials over F are equal if and only if the corresponding polynomial functions are equal.

Problem 71. Prove from first principles (without using the fundamental theorem of arithmetic) that for all $a, b \in \mathbb{Z}$, there exists a greatest common divisor d (in the sense defined in class: a common divisor that is divisible by all common divisors), and that there exist $x, y \in \mathbb{Z}$ such that the equation

$$d = ax + by$$

holds. (Hint: it suffices to show that there is a linear combination of a and b which is a common divisor of a and b.)

Problem 72. Use Problem 71 to show that $\gcd(ac, bc) = |c| \gcd(a, b)$.

Problem 73. Show that Problem 71 also holds for polynomials over a field.

18. Field Extensions

Problem 74. The only finite extensions of $\mathbb{R}$ are $\mathbb{R}$ and $\mathbb{C}$.

Problem 75. Find a field extension F of $\mathbb{Q}$ with $[F : \mathbb{Q}] = 10$.

Problem 76. Suppose $K \subseteq L \subseteq H$ are field extensions. Prove that $[H : K] = [H : L] \cdot [L : K]$.

Problem 77. The algebraic numbers form a field.

Problem 78. If α is algebraic over F, the minimal polynomial is irreducible over F.

Problem 79. $F(\alpha)$ exists and is unique. (Lemma: Any intersection of subfields is a subfield.)

Problem 80. If α is algebraic, then $F(\alpha) = F[\alpha]$, and $[F(\alpha) : F] = \deg_F(\alpha)$.

Problem 81. Corollary: If H is a finite extension of F, then every $\alpha \in H$ is algebraic, and if $\alpha \in H$, then $\deg_F(\alpha) \mid [H : F]$.

Problem 82. $\sqrt[3]{2}$ cannot be constructed by straightedge and compass.

19. Determinants

Problem 83. $\mathrm{sgn}(\sigma) = \mathrm{sgn}(\sigma^{-1})$

Problem 84. Prove (in an arbitrary field, including characteristic 2) that if two columns of A are equal, then $\det A = 0$.

Problem 85. Theorem: Suppose A is an $n \times m$ matrix which has an $r \times r$ submatrix with nonzero determinant. Then $\mathrm{rk}(A) \geq r$. In fact, $\mathrm{rk}(A)$ is the maximum of such r.

Problem 86. Let $A \in F^{k \times n}$. Show that A has a right inverse if and only if A has full row-rank, i.e. $\mathrm{rk}(A) = k$. Similarly, show that A has a left inverse if and only if $\mathrm{rk}(A) = n$.

Problem 87. If $k \neq n$, $|F| = \infty$, and A has a right inverse, then A has infinitely many right inverses.

Problem 88. Give a simple explicit formula for

$$\det \begin{pmatrix} a & b & b & \dots & b & b & b \\ b & a & b & \dots & b & b & b \\ b & b & a & \dots & b & b & b \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ b & b & b & \dots & a & b & b \\ b & b & b & \dots & b & a & b \\ b & b & b & \dots & b & b & a \end{pmatrix}.$$

The resulting expression should be completely factored.

Problem 89. Let $x_1, \dots, x_n \in F$, and define the Vandermonde matrix

$$V(x_1, \dots, x_n) = \begin{pmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} \end{pmatrix}.$$

Show that

$$\det V(x_1, \dots, x_n) = \prod_{i<j} (x_j - x_i)$$

Problem 90. What is

$$\det \begin{pmatrix} 1 & 1 & 0 & \dots & 0 & 0 & 0 \\ -1 & 1 & 1 & \dots & 0 & 0 & 0 \\ 0 & -1 & 1 & \dots & 0 & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & 1 & 0 \\ 0 & 0 & 0 & \dots & -1 & 1 & 1 \\ 0 & 0 & 0 & \dots & 0 & -1 & 1 \end{pmatrix}?$$

20. Determinant Expansion

Problem 91. Prove the cofactor expansion formula.

Problem 92. If $A, B \in M_n(F)$, then $\det(AB) = \det(A) \cdot \det(B)$.

Problem 93. The area of a parallelogram in $\mathbb{R}^3$ defined by two integer vectors is the square root of an integer.

Problem 94. Find infinitely many positive integers that cannot be written as $a^2 + b^2 + c^2$ for integers a, b, c.

Problem 95.

- Find a matrix A whose entries are all 0 or 1 such that $\mathrm{rk}_2(A) \neq \mathrm{rk}_0(A)$.
- Prove that if A is an integer matrix, then $\mathrm{rk}_p(A) \leq \mathrm{rk}_0(A)$.

21. Dot Products

Problem 96. $\dim S^\perp = n - \mathrm{rk}(S)$.

Problem 97. $\dim U + \dim(U^\perp) = n$.

Problem 98. If $U \subseteq F^n$ is a subspace, then $(U^\perp)^\perp = U$.

Problem 99. If U is a subspace of $\mathbb{R}$, then $U \cap U^\perp = \{0\}$.

Problem 100. For all even n, and for $F = \mathbb{C}, \mathbb{F}_5$, and $\mathbb{F}_p$ for infinitely many other primes p (which ones?), find an $(n/2)$-dimensional subspace U of F^n such that $U = U^\perp$.

Problem 101. A subspace $U \leq F^n$ is *totally isotropic* if $U \perp U$, i. e., $U \leq U^\perp$. (a) Prove that any totally isotropic subspace U of F^n satisfies $\dim U \leq n/2$. (b) Use this fact to prove that in Eventown, the number of clubs is at most $2^{\lfloor n/2 \rfloor}$. (Recall that in Eventown, every club has an even number of members and every pair of clubs shares an even number of members.)

22. Euler's φ function

Problem 102. Prove that $\varphi(n)$ is equal to the number of primitive nth roots of unity.

Problem 103. Show that for the matrix

$$D_n = (\gcd(i,j))_{1 \leq i,j \leq n},$$

we have

$$\det(D_n) = \prod_{i=1}^{n} \varphi(i).$$

Hint: Find an upper-triangular $(0,1)$-matrix Z such that

$$D_n = Z^T \begin{pmatrix} \varphi(1) & & 0 \\ & \ddots & \\ 0 & & \varphi(n) \end{pmatrix} Z.$$

23. Eigenvalues, Eigenvectors, the Characteristic Polynomial

Problem 104. For all $A \in M_n(\mathbb{C})$ and for all eigenvalues $\lambda \in \mathbb{C}$, we have

$$\text{algebraic multiplicity of } \lambda \geq \text{geometric multiplicity of } \lambda.$$

Problem 105. Let $A, B \in M_n(F)$ where F is an arbitrary field. Prove: if $A \sim B$, then $f_A(t) = f_B(t)$. (Recall: $A \sim B$ (A, B are similar) means that $(\exists S, S^{-1} \in M_n(F))(B = S^{-1}AS)$.)

Problem 106. The converse to Problem 105 is false. *Hint:* Find A, B such that $\mathrm{rk}(A) \neq \mathrm{rk}(B)$ but $f_A(t) = f_B(t)$.

Problem 107. (a) Consider the matrices

$$A = \begin{pmatrix} 2 & 7 \\ 0 & 3 \end{pmatrix}, \qquad B = \begin{pmatrix} 2 & 0 \\ 0 & 3 \end{pmatrix}.$$

Are they similar?

(b) Same question for the matrices

$$A = \begin{pmatrix} 2 & 7 \\ 0 & 2 \end{pmatrix}, \qquad B = \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}.$$

Problem 108. Prove that $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ is not diagonalizable.

Problem 109. Over $\mathbb{C}$, a matrix A is diagonalizable if and only if for all eigenvalues λ of A, we have

$$\text{alg.mult.}(\lambda) = \text{geom.mult.}(\lambda).$$

24. Problem Session

Problem 110. If $a_1, ..., a_k \in \mathbb{Z}^n$, then $\text{volume}_k(\text{para.}(a_1, ..., a_k) = \sqrt{\text{integer}}$, where

$$\text{para.}(a_1, ..., a_k) = \left\{ \sum_{i=1}^{n} \alpha_i a_i \mid 0 \leq \alpha_i \leq 1 \right\}$$

is the parallelepiped spanned by $a_1, \ldots, a_k$.

Problem 111. For what primes p does there exist $\sqrt{-1}$ in $\mathbb{F}_p$?

Problem 112. If U is a totally isotropic subspace of $\mathbb{F}_2^n$ and $\dim U < \lfloor \frac{n}{2} \rfloor$, then U is not *maximal*, that is, there exists a totally isotropic subspace $U' \leq \mathbb{F}_2^n$ such that $U' \supsetneq U$.

Problem 113. If $v_1, ..., v_k$ are eigenvectors of A to **distinct** eigenvalues ($v_i \neq 0, Av_i = \lambda_i v_i$, $\lambda_i \neq \lambda_j$ for $i \neq j$), then the v_i are linearly independent.

25. Greatest Common Divisors of Polynomials

Problem 114. Prove: For all $f, g \in F[x]$, there exists $d \in F[x]$ such that

(1) $d \mid f$ and $d \mid g$,
(2) $(\forall e \in F[x])$(if $e \mid f$ and $e \mid g$ then $e \mid d$),
(3) $(\exists u, v \in F[x])(d = u \cdot f + v \cdot g)$.

Problem 115. Let $f \in \mathbb{Q}[x]$. Then f has a multiple root in $\mathbb{C}$ if and only if $\gcd(f, f') \neq 1$.

26. Euler-Fermat Congruence and Arithmetic Functions

Problem 116. Prove that

$$\mathbb{Z}_m^\times := \{1 \leq a \leq m \mid \gcd(a, m) = 1\}$$

is a group under multiplication modulo m. Observe that $|\mathbb{Z}_m^\times| = \varphi(m)$. Infer the Euler-Fermat congruence: if $\gcd(a, m) = 1$ then

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Problem 117. If $\gcd(a, b) = 1$, then $\varphi(ab) = \varphi(a)\varphi(b)$.

Problem 118. Show that $\inf_{n \in \mathbb{N}} \dfrac{\varphi(n)}{n} = 0$.

Problem 119. Let $d(n)$ be the number of positive divisors of $n \in \mathbb{N}$. If $\gcd(a, b) = 1$, then $d(ab) = d(a)d(b)$.

Problem 120. Give an explicit formula for $d(n)$ given the prime factorization of n.

Problem 121. Show the Möbius function is multiplicative: If $\gcd(a, b) = 1$, then $\mu(ab) = \mu(a)\mu(b)$.

Problem 122. (a) If $\omega \in G$ and $\operatorname{ord}(\omega) = n$, then $\operatorname{ord}(\omega^j) = n$ if and only if $\gcd(j, n) = 1$.
(b) If $\omega \in G$, then $\operatorname{ord}(\omega^j) = \frac{\operatorname{ord}(\omega)}{\gcd(j,n)}$.

Problem 123. Let S_n denote the sum of the primitive nth roots of unity. Show that $S_n = \mu(n)$.

Problem 124. Show that $\displaystyle\sum_{d|n} \varphi(d) = n$.

Problem 125. If f is multiplicative, then so is $g(n) = \displaystyle\sum_{d|n} f(d)$.

Problem 126 (Möbius inversion)**.** Show that

$$f(n) = \sum_{d|n} \mu\left(\frac{n}{d}\right) g(d)$$

for all $f : \mathbb{N} \to \mathbb{C}$ and $g(n) = \displaystyle\sum_{d|n} f(d)$.

Problem 127. (a) $\sum_{\text{primes}} 1/p = \infty$.
(b) $\sum_{p \leq n} 1/p = \ln \ln n + \theta_n^*$ with $|\theta_n^*|$ bounded.

27. Functions of Matrices

Problem 128. Prove the Cayley-Hamilton theorem ($f_A(A) = 0$) for diagonalizable matrices.

Problem 129. If λ is an eigenvalue of A and $f \in F[x]$, then $f(\lambda)$ is an eigenvalue of $f(A)$. (Is the converse true?)

Problem 130. For $a \in M_n(\mathbb{R})$, (a) define e^A, and (b) prove that if λ is an eigenvalue of A, then e^λ is an eigenvalue of e^A. (Is the converse true?)

28. Algebraically closed fields

Problem 131. Let $F \subseteq H$ be a field extension, and let $\mathrm{Alg}_F(H) = \{\alpha \in H \mid \alpha \text{ is algebraic over } F\}$. Then

- $\mathrm{Alg}_F(H)$ is a subfield of H.
- If H is algebraically closed, then $\mathrm{Alg}_F(H)$ is algebraically closed.
- In this case, $\mathrm{Alg}_F(H)$ is the smallest algebraically closed field containing F. Call this field the algebraic closure of F, and denote it by $\overline{F}$.
- Show that $\overline{F}$ is unique up to an isomorphism fixing F.

Problem 132. If F is countable, then $\overline{F}$ is countable.

Problem 133 (Liouville)**.** Show that

$$\sum_{n=0}^{\infty} \frac{1}{2^{n!}}$$

is transcendental.

29. Irreducible polynomials

Problem 134 (Gauss Lemma #1)**.** A polynomial with integer coefficients is called a *primitive polynomial* if the gcd of its coefficients is 1. Show that the product of primitive polynomials is primitive.

Problem 135 (Gauss Lemma #2)**.** Let $f \in \mathbb{Z}[x]$ and $f = g_1 \dots g_k$ be a factorization into polynomials $g_i \in \mathbb{Q}[x]$. Show there is an equivalent factorization $f = h_1 \dots h_k$ into polynomials with integer coefficients, i.e., there exist rational numbers $\alpha_1, \dots, \alpha_k$ such that $h_i = \alpha_i f_i \in \mathbb{Z}[x]$ and $\prod \alpha_i = 1$.

Problem 136. Prove the Schönemann-Eisenstein criterion for irreducibility over $\mathbb{Q}$ of polynomials in $\mathbb{Z}[x]$: Let $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ be a polynomial with integer coefficients. Suppose there exists a prime p such that $p \nmid a_n$, $p \mid a_{n-1}, \dots, a_1, a_0$, and $p^2 \nmid a_0$. Then f is irreducible over $\mathbb{Q}$.

Problem 137. Prove that $x^{10} - 8$ is irreducible over $\mathbb{Q}$.

Problem 138. Let $\Phi_n(x)$ denote the n-th cyclotomic polynomial, defined as $\Phi_n(x) = \prod(x - \omega)$ where the product is over all primitive n-th roots of unity. Observe that $\deg(\Phi_n) = \varphi(n)$.

- Calculate $\Phi_n(x)$ for $n \leq 10$.
- Prove that $\Phi_n(x)$ has integer coefficients.
- * Prove that $\Phi_n(x)$ is irreducible.

Problem 139. Let $A \in M_n(\mathbb{Q})$. If $f_A(t)$ is irreducible over $\mathbb{Q}$, then A is diagonalizable over $\mathbb{C}$.

30. The Cayley-Hamilton Theorem

Problem 140. Almost all matrices in $M_n(\mathbb{C})$ are diagonalizable. That is, the set of nondiagonalizable matrices has Lebesgue measure zero.

Problem 141. Let $A \in M_n(\mathbb{C})$. Show that there is an invertible $S \in M_n(\mathbb{C})$ such that $S^{-1}AS$ is upper-trinagular.

Problem 142. Give a simple argument to show that if the Cayley-Hamilton theorem holds over the integers, it holds over every commutative ring with an idenity element.

Problem 143.

- Show that if $A, B \in M_n(\mathbb{R})$, then $AB - BA \neq I$.
- Show the same is true over all fields of characteristic zero.
- Find a field for which this is not true.
- Find two linear transformations A and B of $\mathbb{R}[x]$ such that $AB - BA = I$.

31. Nonnegative matrices, Directed Graphs, Perron-Frobenius Theory

Problem 144. Let A be an $n \times n$ matrix over a field F. Suppose that u is a right eigenvector, that is $Au = \lambda u$, and v is a left eigenvector, that is $v^t A = \mu v$. If $\lambda \neq \mu$, then show that $u \perp v$.

Problem 145. Let A be an $n \times n$ matrix over $\mathbb{R}$. Let $A = (a_{ij})$.

(a) Suppose that for all i, j, we have $a_{ij} > 0$. Show that there exists an eigenvector with all positive coordinates.
(b) Now suppose that for all i, j, we have $a_{ij} \geq 0$. Construct a directed graph (digraph) with vertex set $\{1, \ldots, n\}$ as follows. Put an edge (arrow) $i \to j$ if $a_{ij} \neq 0$. Suppose that the associated digraph is strongly connected. That is, for all i, j there is a (directed) path from i to j. Show that there is an all-positive eigenvector.
(c) Suppose that for all i, j, we have $a_{ij} \geq 0$. Show that there exists a non-negative eigenvector.
(d) Show that parts (b) and (c) imply that every finite Markov Chain has a stationary distribution.
(e) If a digraph is strongly connected, then it follows that such a stationary distribution is unique.
(f) Construct a Markov Chain with non-unique stationary distribution.

These are elements of the Perron-Frobenius theory of nonnegative matrices, which are key to the theory of finite Markov Chains.

The *period* of a vertex v in a directed graph is the gcd of the lengths of all closed walks from the vertex v.

Problem 146. If two vertices of a digraph are in the same strong component, then they have the same period.

Problem 147. Assume that X is strongly connected. Then the period of X is the gcd of the lengths of all the cycles in X.

Problem 148. All closed walks in a graph have lengths divisible by some natural number d if and only if the vertices can be grouped in d blocks around a circle, such that edges only go from one block to the next along the circle.

Problem 149. Let A be an $n \times n$ matrix over $\mathbb{C}$. Let X_A be the associated digraph on the vertex set $\{1, \ldots, n\}$. That is, there is an edge $i \to j$ if $a_{ij} \neq 0$. Suppose that X_A is strongly connected with period h. Let ω be an h-th root of unity. Show that if λ is an eigenvalue of A, then so is $\lambda\omega$.

32. Undirected graphs, Hamiltonicity, automorphisms

An undirected graph X is called *tough* if for every $k \in \mathbb{N}$ if k vertices are removed from X, then there are at most k connected components.

Problem 150. Show that not every tough graph is Hamiltonian. (Only consider graphs with at least three vertices.)

Problem 151. Does Petersen's graph have an automorphism that interchanges the outer five and the inner five vertices?

Problem 152. In class, we drew another 3-regular graph of girth 5 with 10 vertices. Is this graph isomorphic to the Petersen graph?

Problem 153. Show that Petersen's graph is not Hamiltonian.

Problem 154. (a) Show that Petersen's graph is tough.
(b) Show that Petersen's graph is vertex-transitive.
(c) $(*)$ Show that every connected vertex-transitive graph is tough.

Problem 155. For what values of $k, \ell \in \mathbb{N}$ is the $k \times \ell$ grid Hamiltonian?

Problem 156. Consider a $3 \times 3 \times 3$ grid of cubes of cheese. Suppose that a mouse wants to eat all cheese cubes one at a time such that any two consecutive cubes share a common face. Suppose that the mouse wants to eat the centre cube last. Show that this is not possible.

Problem 157.

(a) The number of automorphisms of Petersen's graph is 120.
(b) Is the automorphism group of Petersen's graph isomorphic to S_5?
(c) Show that the order of the automorphism group of the dodecahedron is 120.
(d) Show that the automorphism group of the dodecahedron is not isomorphic to S_5. (Hint: the dodecahedron has a symmetry that commutes with all of its symmetries.)
(e) Show that half of the automorphisms of the dodecahedron form a subgroup isomorphic to a subgroup consisting of half the elements of S_5. Namely, the group of sense-preserving symmetries of the dodecahedron is isomorphic to A_5.

Problem 158. If X is a regular graph of degree r and girth at least 5, then X has at least $r^2 + 1$ vertices.

33. Complex eigenvalues of real matrices. Real eigenvalues of complex matrices.

Problem 159. Let R_θ denote the matrix of the rotation of the plane by θ. Find an eigenbasis of R_θ over $\mathbb{C}$, and observe that it is independent of θ.

Problem 160. If A is a self-adjoint complex matrix, then show that all the (complex) eigenvalues of A are real.

34. Hermitian dot product, unitary matrices

Problem 161. $(\forall A \in \mathbb{C}_{n\times n})(\exists \text{ upper triangular } T \in M_n(\mathbb{C}))(A \sim_u T)$.

35. Normal Matrices, Orthogonal Matrices

Problem 162. If a triangular matrix is normal, prove it is diagonal.

Problem 163. If A is unitary and λ is an eigenvalue of A, prove that $|\lambda| = 1$.

Problem 164. If A is normal, prove

(1) A is Hermitian iff all eigenvalues of A are real.
(2) A is unitary iff all eigenvalues of A have unit absolute value.

Problem 165. Let $A \in M_n(\mathbb{R})$. Prove that A is similar to a triangular matrix iff A is orthogonally similar to a triangular matrix iff all (complex) eigenvalues of A are real.

Problem 166 (Real Spectral Theorem)**.** Let $A \in M_n(\mathbb{R})$. Prove that A is orthogonally similar to diagonal matrix iff A is symmetric ($A = A^t$).

Problem 167. Prove A is an orthogonal matrix iff A is orthogonally similar to a block-diagonal matrix of the following form: each diagonal block is 1×1 or 2×2; the 1×1 blocks are ± 1; and the 2×2 blcoks are rotation matrices of the form $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$..

Problem 168 (Rayleigh quotient)**.** Let A be an $n \times n$ real symmetric matrix. The *Rayleigh quotient* of A is the $\mathbb{R}^n \setminus \{0\} \to \mathbb{R}$ function $R_A(x) = x^t Ax/x^t x$. Let the eigenvalues of A be $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_n$. Prove $\lambda_1 = \max_{x\in\mathbb{R}} R_A(x)$ and $\lambda_n = \min_{x\in\mathbb{R}} R_A(x)$.

36. Real Euclidean Space, Gram-Schmidt Orthogonalization, Complex Hermitian Space

Problem 169. $B = B^t$ is a positive definite matrix iff all eigenvalues of B are positive.

Problem 170. $B = B^t$ is a positive definite matrix iff all the corner determinants of B are positive, i. e., $(\forall k \leq n)(\det((b_{ij})_{i,j\leq k}) > 0$.

Problem 171. Prove that $1, \cos x, \sin x, \cos 2x, \sin 2x, \cdots \in C[0, 2\pi]$ is an orthogonal system and thus linearly independent under the inner product $\langle f, g\rangle = \int_0^{2\pi} f(x)g(x)dx$.

Problem 172. During the Gram-Schmidt orthogonalization process, we have $v_k - b_k = \sum_{j=1}^{k-1} \alpha_{kj} b_j$. Prove that

$$\alpha_{ki} = \frac{\langle b_i, v_k \rangle}{\|b_i\|^2}, \forall k = 1, 2, \ldots, i = 1, \ldots, k-1$$

.

Problem 173. State and prove the Gram-Schmidt orthogonalization theorem in complex Hermitian space case.

Problem 174. What was problem 174?

Problem 175. Show that the set $U(n) = \{A \in M_n(\mathbb{C}) \mid AA^* = I\}$ of unitary matrices forms a group.

Problem 176. Suppose that $f(x_1, \ldots, x_n)$ is a multivariate polynomial of degree at most d over a field F. Let $\alpha_0, \ldots, \alpha_d$ are distinct elements of the field. Suppose that for every substitution of values $\beta_i \in \{\alpha_0, \ldots, \alpha_n\}$ we have $f(\beta_1, \ldots, \beta_n) = 0$, then $f = 0$.

(Hint: Use induction on the number of variables.)

Problem 177. Show that in $\mathbb{R}^3$, every sense-preserving (orientation-preserving) congruence that fixes a point is a rotation.

37. Adjacency matrix, eigenvalues of undirected graphs

Problem 178. Let $A, B \in M_n(\mathbb{C})$. Assume $AB = BA$. Prove that they have a common eigenvector.

Problem 179. Let $A, B \in M_n(\mathbb{R})$, $A = A^t, B = B^t$ and $AB = BA$. Prove that they have a common orthonormal eigenbasis.

Problem 180. Suppose $f(x), g(x) \in \mathbb{Z}[x]$ and $g(x)$ has leading coefficient 1. Prove the division $f(x) = g(x)q(x) + r(x)$ has integer coefficients quotient and remainder, i. e., $q(x), r(x) \in \mathbb{Z}[x]$.

Problem 181. Prove that $\frac{1}{n}\sum_{i=1}^{n} d(i) \leq \lambda_1 \leq \max_i d(i)$, where $d(i)$ denotes the degree of vertex i.

Problem 182. Suppose A has eigenvalues $\lambda_1, \ldots, \lambda_n$. Prove that $aA + bI$ has eigenvalues $a\lambda_i + b$ with corresponding multiplicities.

Problem 183. Assume A is a nonnegative matrix with a positive eigenvector x (all coordinates of x are positive) with eigenvalue λ, i. e., $x \neq 0$ and $Ax = \lambda x$. Prove ($\forall$ eigenvalue μ)($|\mu| \leq \lambda$).

Problem 184. Suppose an undirected graph has sorted eigenvalues $\lambda_1 \geq \cdots \geq \lambda_n$. Prove

(1) $(\forall i)(|\lambda_i| \leq \lambda_1)$
(2) If the graph G is connected, then $(\forall i \geq 2)(\lambda_i < \lambda_1)$
(3) If the graph G is connected, then $|\lambda_n| = \lambda_1$ iff G is bipartite.
(4) If G is a bipartite graph, then $(\forall i)(\lambda_i = -\lambda_{n-i+1})$.

Problem 185. Let $g \in \mathbb{C}[x]$ and $A \in M_n(\mathbb{C})$. Assume A has eigenvalues $\lambda_1, \ldots, \lambda_n$ (listed with multiplicity, i. e., $f_A(t) = \prod_{i=1}^{n}(t - \lambda_i)$). Prove that the eigenvalues of $g(A)$ are $g(\lambda_1), \ldots, g(\lambda_n)$ (again, listed with multiplicity).

38. Gram matrix, volume

Definition 1. Let $v_1, \ldots, v_k$ be k vectors in a Euclidean space. The *Gram matrix* of these k vectors, denoted by $G(v_1, \ldots, v_k)$, is the $k \times k$ matrix $(\langle v_i, v_j \rangle)_{k \times k}$. The *Gram determinant* is the determinant of the Gram matrix.

Problem 186. Prove that the Gram matrix of a list of vectors is always positive semidefinite. Moreover, prove that the Gram matrix is positive definite iff the list of vectors is linearly independent.

Problem 187. Prove that $\det G(v_1, \ldots, v_k) = \mathrm{Vol}_k(v_1, \ldots, v_k)^2$ where Vol_k denotes the k-dimensional volume.

39. Counting spanning trees of a graph

Definition 2. The *Laplacian* of a graph G, denoted by L_G, is defined as $D_G - A_G$ where D_G is the diagonal matrix $\mathrm{diag}(\deg(1), \ldots, \deg(n))$ with the degrees of the nodes on the diagonal and A_G is the adjacency matrix of the graph G.

Problem 188. (1) Prove that all cofactors of L_G are equal.

(2) * (Matrix-Tree Theorem, Kirchhoff 1848) Each cofactor of L_G equals the number of spanning trees of G.

(3) Cayley's formula says that the number of spanning trees of the complete graph on n vertices is n^{n-2}. Infer Cayley's formula from the Matrix-Tree Theorem.

40. Finite Markov Chains, mixing rate, eigenvalue gap

Problem 189. Prove: for the simple random walk on a connected graph, the stationary probability of node i is proportional to its degree $\deg(i)$.

Problem 190 (Perron-Frobenius Theorem)**.** (a) Suppose $A \in M_n(\mathbb{R})$ is a positive matrix, i. e., $(\forall i, j)(a_{ij} > 0)$. Then there exists a positive eigenvector.

(b) Infer that every Markov Chain has a stationary distribution.

Problem 191 (Mixing of ergodic Markov Chains)**.** If a finite Markov chain is ergodic, then the limit $\lim_{t\to\infty} T^t = L$ exists, where T is the transition matrix. (The Markov chain is ergodic if the digraph of possible transitions is stringly connected and aperiodic, i. e., the gcd of the lengths of coled walks is 1.)

Problem 192 (Mixing of simple random walk on a regular graph)**.** Let G be a regular graph of degree r with eigenvalues $\lambda_1 = r \geq \lambda_2 \geq \cdots \geq \lambda_n$. Let $\lambda = \max\{|\lambda_2|, \ldots, |\lambda_n|\}$. For the simple random walk on a regular graph of degree r we have $|p_{ij}^{(t)} - \frac{1}{n}| \leq \left(\frac{\lambda}{r}\right)^t$. (Here, $p_{ij}^{(t)}$ denotes the t-step transition probailities, i. e., the entires of T^t where $T = \frac{1}{r}A$ is the transition matrix.) (Hint: Spectral Theorem.)

Problem 193 (Operator norm)**.** (a) If $A = A^t$, prove $\|A\| = \max\{|\lambda_1|, \ldots, |\lambda_n|\}$.

(b) Prove $(\forall A)(\|A\| = \sqrt{\lambda_{\max}(A^T A)})$.