Putnam Notes

Mladen Bestvina and Gordan Savin

Contents

1. Induction

Induction is an extremely versatile method for solving a variety of problems. The basic principle is:

Every nonempty set of positive integers has a smallest element.

Now suppose we have a statement that involves a positive integer n. We will denote it $S(n)$. To prove $S(n)$ for every $n = 1, 2, 3, \cdots$ it suffices to prove the following:

(1) $S(1)$ (this is called the *basis of induction*), and

(2) the truth of $S(n)$ implies the truth of $S(n+1)$ for every $n = 1, 2, 3, \cdots$ (this is called the *inductive step*).

The way to think about this is the following. Consider the set of all n such that $S(n)$ fails. We want to show that this set is empty. Well, if not, then there is a minimal element of this set, say n_0. Now $n_0 > 1$ by (1). But then the fact that $S(n_0 - 1)$ is true while $S(n_0)$ is false contradicts (2).

Sometimes it is useful to replace (2) with:

(2') the truth of $S(1), S(2), \cdots, S(n)$ implies the truth of $S(n+1)$ for every $n = 1, 2, 3, \cdots$.

Problems.

1. Prove that for every positive integer n

$$1 \cdot 2 + 2 \cdot 3 + \cdots + n(n+1) = \frac{n(n+1)(n+2)}{3}$$

Solution. [1] Let $S(n)$ be the statement that the displayed equation holds. Thus $S(1)$ is the statement

$$1 \cdot 2 = \frac{1 \cdot 2 \cdot 3}{3}$$

which is true. Next, assume that $n > 1$ and that $S(n-1)$ holds. Thus

$$1 \cdot 2 + 2 \cdot 3 + \cdots + (n-1)n = \frac{(n-1)n(n+1)}{3}$$

Adding $n(n+1)$ to both sides we obtain

$$1 \cdot 2 + 2 \cdot 3 + \cdots + n(n+1) = \frac{(n-1)n(n+1)}{3} + n(n+1)$$

[1] How would you come up with the answer if it wasn't given to you? Maybe we'll discuss this at some later date.

By a simple manipulation the RHS equals $\frac{n(n+1)(n+2)}{3}$, and thus $S(n)$ holds. By induction, $S(n)$ holds for all n.

2. Find a formula for the sum of the first n odd numbers.

Solution. [1] Let $S(n)$ denote the statement that

$$1 + 3 + 5 + \cdots + (2n-1) = n^2$$

Thus $S(1)$ says $1 = 1^2$ and it is true. Assume $S(n-1)$, so

$$1 + 3 + 5 + \cdots + (2(n-1)-1) = (n-1)^2$$

Add $2n-1$ to both sides to obtain

$$1 + 3 + 5 + \cdots + (2n-1) = (n-1)^2 + (2n-1)$$

The RHS is n^2, so we proved $S(n)$. By induction, $S(n)$ holds for all n.

3. Prove that

$$2(\sqrt{n+1}-1) < 1 + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n}} < 2\sqrt{n}$$

Solution. [2] By $S(n)$ denote the displayed inequalities. Thus $S(1)$ reads

$$2(\sqrt{2}-1) < 1 < 2\sqrt{1}$$

or equivalently $\sqrt{2} < 1.5$, which is true. Now assume $S(n-1)$, i.e.

$$2(\sqrt{n}-1) < 1 + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n-1}} < 2\sqrt{n-1}$$

Add $\frac{1}{\sqrt{n}}$ to all 3 sides:

$$2(\sqrt{n}-1) + \frac{1}{\sqrt{n}} < 1 + \frac{1}{\sqrt{2}} + \cdots + \frac{1}{\sqrt{n}} < 2\sqrt{n-1} + \frac{1}{\sqrt{n}}$$

The statement $S(n)$ will be proved if we can establish

$$2(\sqrt{n+1}-1) < 2(\sqrt{n}-1) + \frac{1}{\sqrt{n}}$$

and

$$2\sqrt{n-1} + \frac{1}{\sqrt{n}} < 2\sqrt{n}$$

The first inequality, after canceling -2 and multiplying by $\sqrt{n}$, becomes

$$2\sqrt{n(n+1)} < 2n+1 \tag{1}$$

which can be seen to hold by squaring. The second inequality, after multiplying by $\sqrt{n}$, becomes

$$2\sqrt{(n-1)n} + 1 < 2n$$

which is the same inequality as (1) except that n is replaced by $n-1$.

[2] If you know about Riemann sums you will be able to figure out where these inequalities come from.

4. Prove that $7^{2n} - 48n - 1$ is divisible by 2304 for every positive integer n.

   Solution. Let $x_n = 7^{2n} - 48n - 1$ and denote by $S(n)$ the statement that x_n is divisible by 2304. Thus $S(1)$ says that $x_1 = 7^2 - 48 - 1 = 0$ is divisible by 2304, which is evidently true.

   Now suppose $S(n-1)$, i.e. that x_{n-1} is divisible by 2304. To show $S(n)$ it suffices to prove that $x_n - x_{n-1}$ is divisible by 2304 since then x_n will also be divisible by 2304.

   Now compute:

$$x_n - x_{n-1} = 7^{2n} - 7^{2n-2} - 48n + 48(n-1) = 7^{2n-2}(7^2 - 1) - 48 = 48(7^{2n-2} - 1)$$

   Since $2304 = 48 \cdot 48$ it suffices to argue that $7^{2n-2} - 1$ is divisible by 48. But

$$7^{2n-2} - 1 = 49^{n-1} - 1 = (49 - 1)(49^{n-2} + 49^{n-3} + \cdots + 49^1 + 1)$$

   is evidently divisible by 48.

5. For every positive integer n, show that

$$u_n = \frac{(1+\sqrt{5})^n - (1-\sqrt{5})^n}{2^n\sqrt{5}}$$

   is a positive integer. In fact, u_n is the nth Fibonacci number.

   Solution. [3] We compute

$$u_1 = \frac{(1+\sqrt{5})^1 - (1-\sqrt{5})^1}{2^1\sqrt{5}} = 1$$

   and

$$u_2 = \frac{(1+\sqrt{5})^2 - (1-\sqrt{5})^2}{2^2\sqrt{5}} = 1$$

   We will now show that $u_{n+2} = u_{n+1} + u_n$ for $n \geq 1$.

$$u_{n+1} + u_n = \frac{(1+\sqrt{5})^{n+1} - (1-\sqrt{5})^{n+1}}{2^{n+1}\sqrt{5}} + \frac{(1+\sqrt{5})^n - (1-\sqrt{5})^n}{2^n\sqrt{5}} =$$

$$\frac{2(1+\sqrt{5})^{n+1} - 2(1-\sqrt{5})^{n+1} + 4(1+\sqrt{5})^n - 4(1-\sqrt{5})^n}{2^{n+2}\sqrt{5}} =$$

$$\frac{(2(1+\sqrt{5})+4)(1+\sqrt{5})^n - (2(1-\sqrt{5})+4)(1-\sqrt{5})^n}{2^{n+2}\sqrt{5}} =$$

$$\frac{(1+\sqrt{5})^2(1+\sqrt{5})^n - (1-\sqrt{5})^2(1-\sqrt{5})^n}{2^{n+2}\sqrt{5}} = u_{n+2}$$

6. Let $f(n)$ be the number of regions which are formed by n lines in the plane, where no two lines are parallel and no three meet in a point (e.g. $f(4) = 11$). Find a formula for $f(n)$.

---

[3] How on Earth did they come up with this? Remind me to talk about recursively defined sequences sometime.

SOLUTION. Let's try to compute $f(n+1)$ in terms of $f(n)$. Consider a collection of n lines as above, so they form $f(n)$ regions. Add one more line ℓ. This line intersects each of the n lines in one point, and all these points are distinct. So there are n intersection points along ℓ, dividing ℓ into $n+1$ segments (two of these segments are infinite and the rest are finite). Each segment divides an existing region in two; in other words there are $n+1$ new regions. We conclude that

$$f(n+1) = f(n) + n + 1$$

Combined with the fact that $f(1) = 2$ we see that

$$f(n) = 2 + 2 + 3 + 4 + \cdots + n$$

Now, everybody knows that

$$1 + 2 + \cdots + n = \frac{n(n+1)}{2}$$

and $f(n)$ is 1 more than this, thus

$$f(n) = \frac{n(n+1)}{2} + 1$$

You can also guess this formula and then prove it by induction from $f(n+1) = f(n) + n + 1$.

7. Prove the arithmetic mean - geometric mean inequality (AM-GM): Suppose $a_1, \cdots a_n$ are n positive real numbers. Then

$$\frac{a_1 + a_2 + \cdots + a_n}{n} \geq (a_1 a_2 \cdots a_n)^{\frac{1}{n}}$$

Call this statement $AMGM(n)$. Prove $AMGM(n)$ for all n as follows.

(a) Prove it for $n = 1$ and $n = 2$.

SOLUTION. [4] $AMGM(1)$ says $a_1 \geq a_1$ and $AMGM(2)$ says $\frac{a_1+a_2}{2} \geq (a_1 a_2)^{\frac{1}{2}}$. The first statement is clear and the second, after multiplying by 2 and squaring, becomes

$$(a_1 + a_2)^2 \geq 4a_1 a_2$$

and this is equivalent to $(a_1 - a_2)^2 \geq 0$, which is evidently true (with equality iff $a_1 = a_2$).

(b) If it is true for $n = k$, prove that it is true for $n = k - 1$. (Hint: substitute $a_n = \frac{a_1+\cdots+a_{n-1}}{n-1}$ in $AMGM(n)$ and see what happens.)

SOLUTION. Denote by S the sum $a_1 + \cdots + a_{n-1}$. Following the hint, we see that

$$\frac{S + S/(n-1)}{n} \geq (a_1 a_2 \cdots a_{n-1} S/(n-1))^{\frac{1}{n}}$$

[4] This inequality has something to do with the concavity of the function $x \mapsto \log x$, which boils down to saying that the second derivative is negative. Remind me to talk about this sometime.

The LHS simplifies to $\frac{S}{n-1}$ so after raising to power n we have

$$\frac{S^n}{(n-1)^n} \geq a_1 \cdots a_{n-1} S/(n-1)$$

which simplifies to

$$\frac{S^{n-1}}{(n-1)^{(n-1)}} \geq a_1 \cdots a_{n-1}$$

After raising to power $1/(n-1)$ we obtain $AMGM(n-1)$.

(c) If it is true for $n = k$, prove that it is true for $n = 2k$.

SOLUTION. Let $a_1, a_2, \cdots, a_{2k-1}, a_{2k}$ be given. Define

$$b_1 = a_1 + a_2, b_2 = a_3 + a_4, \cdots, b_k = a_{2k-1} + a_{2k}$$

Now $AMGM(k)$ tells us that

$$\frac{b_1 + \cdots + b_k}{k} \geq (b_1 \cdots b_k)^{\frac{1}{k}}$$

Substitute back the a's, taking into account that $b_1/2 \geq (a_1 a_2)^{\frac{1}{2}}$ etc. to get

$$\frac{a_1 + a_2 + \cdots + a_{2k}}{k} \geq ((2(a_1 a_2)^{\frac{1}{2}}) \cdots (2(a_{2k-1} a_{2k})^{\frac{1}{2}}))^{\frac{1}{k}}$$

i.e.

$$\frac{a_1 + a_2 + \cdots + a_{2k}}{k} \geq 2(a_1 a_2 \cdots a_{2k})^{\frac{1}{2k}}$$

which is $AMGM(2k)$ after dividing by 2.

(d) Conclude!

SOLUTION. Suppose that $AMGM$ is false and let n_0 be the smallest integer such that $AMGM(n_0)$ is false. Then $n_0 > 2$ by (a). Also, n_0 cannot be even since otherwise $AMGM(n_0/2)$ would be true and $AMGM(n_0)$ would be false, contradicting (c). Thus $n_0 \geq 3$ is odd. Now $\frac{n_0+1}{2}$ is an integer smaller than n_0, so $AMGM(\frac{n_0+1}{2})$ holds, which implies $AMGM(n_0+1)$ by (c), and this implies $AMGM(n_0)$ by (b). Contradiction.

8. Suppose we have $2n$ points in space and certain n^2+1 pairs are joined by segments. Show that at least one triangle is formed. Also show that it is possible to have $2n$ points and n^2 segments without any triangles.

SOLUTION. To answer the last sentence, break up $2n$ points into two groups with n points in each group, and then draw a segment connecting any point in one group to any point in the other group. There are n^2 segments and no triangles.

Now by $S(n)$ denote the statement that any configuration of $2n$ points and $\geq n^2+1$ segments must contain a triangle. The basis of induction is $S(2)$ (actually, $S(1)$ is trivially true since we can't have 2 segments joining one pair of points, but it is good, in order to give yourself some feeling for the problem, to start with $n = 2$). If we have 4 points and ≥ 5 segments there must be a triangle. This is because there are $\binom{4}{2} = 6$ possible segments, so at most one segment is missing.

Now assume $S(n-1)$. We will prove $S(n)$. Let $2n$ points and $\geq n^2+1$ segments be given. Pick two points, say A and B, that are joined by a segment. There are $2(n-1)$ remaining points, call them $C_1, \cdots, C_{2n-2}$. We consider two cases.

Case 1. There are at least $(n-1)^2+1$ segments connecting two points among $C_1, \cdots, C_{2n-2}$. In this case we apply $S(n-1)$ to the collection $C_1, \cdots, C_{2n-2}$ and deduce that 3 of these points form a triangle, so the same is true of the original configuration.

Case 2. There are at most $(n-1)^2$ segments joining two points among $C_1, \cdots, C_{2n-2}$. This means that all the remaining segments, and there are at least $n^2 + 1 - (n-1)^2 = 2n$ of them, involve either A or B or both. One of these segments joins A to B and the remaining $\geq 2n-1$ join either A or B to some C_i. Since there are $2n-2$ C-points and $\geq 2n-1$ segments, there is some C-point, say C_i, which is joined to both A and B.[5] But then A, B, C_i form a triangle.

The two cases exhaust all possibilities, and $S(n)$ is proved.

9. Consider an $m \times n$ chess board whose squares are colored black and white as usual. We will always assume that $m, n \geq 2$. Note that if a region of the board is tiled by 2×1 dominoes then this region contains an equal number of black and white squares. Show the following:
   (a) If mn is odd and a square of the same color as the corners is removed, then the remaining board can be tiled.

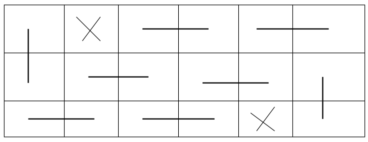
   Solution. Our convention will be that an $m \times n$ board has m columns and n rows. The idea is to induct on the total number of squares. The basis of induction is the smallest possible board, namely the 3×3 board. Taking into account the symmetries, there are two possibilities for the missing square: a corner square or the central square. In either case, it is easy to directly construct a tiling. Now on to the inductive step. We may assume $m \geq n$ for otherwise we can just rotate the board by $\pi/2$. Therefore $m \geq 5$ for otherwise $m = n = 3$ and we are in the minimal case. The missing square is either not in the first two columns (of m columns), or it is not in the last two columns. By symmetry, let's say it is not in the first two columns. Then tile the first two columns by "horizontal" 2×1 dominoes and then tile the rest of the board, which is $(m-2) \times n$, using the inductive hypothesis.

[5]This is called the pigeon-hole principle. If you have $(n+1)$ pigeons and n holes, you'll have to put (at least) two pigeons in the same hole.

(b) If mn is even and two squares are removed, one black one white, then the remaining board can be tiled.

SOLUTION. We start with the warm-up case when the board is $m \times 2$. This case is simpler and yet it illustrates the flavor of the general argument. For this case, we induct on m. The basis of induction is the case $m = 2$ when necessarily the two squares removed are adjacent and the remaining two squares form a domino.
Now consider an $m \times 2$ board with $m \geq 3$. If the first column does not contain a missing square, cover it with a domino and apply induction to the remaining $(m-1) \times 2$ board. Similarly if the last column does not contain a missing square. So we are down to the case when one missing square is in the first column and one is in the last column. If m is odd, this means that the removed squares are at the opposite corners and then the board can be tiled by horizontal dominoes. If m is even then the missing squares are corner squares in the same row, and again the board can be tiled with horizontal dominoes. This finishes the warm-up. Now we may assume $m, n \geq 3$.
Say m is even and n is either even or odd.
Case 1: Either the top row or the bottom row contain no missing squares. By symmetry, let's say the top row contains no missing squares. Then tile the top row by "horizontal" 2×1 dominoes (using that m is even) and tile the rest of the board, which is $m \times (n-1)$, using the inductive hypothesis.
Case 2: $n \geq 4$, one missing square is in the top row, and one missing square is in the bottom row. Put dominoes vertically along the top two rows, except that at the missing square a domino sticks out to the third row from the top. Now apply induction to the $m \times (n-2)$-board obtained by deleting the top two rows, and removing the square covered by the exceptional domino, as well as the missing square in the bottom row.
Case 3: $m \geq 4$ and the first two or the last two columns do not contain any missing squares. Then tile those two columns with horizontal tiles, and apply induction to the remaining $(m-2) \times n$ board.
Case 4: $m \geq 4$, $n = 3$, one missing square is in the top row, and one missing square is in the bottom row, and both the first two columns and the last two columns contain a missing square. Then there are only two possibilities: either the missing squares are in the opposite corners, or they are adjacent to the opposite corners. In the former case, tile the first and last row with a vertical domino, and tile the remaining $(m-2) \times 3$-board without missing squares in any way you like. The latter case is pictured below, with $m = 6$ (but any even m works similarly, there are two vertical dominoes containing the corners adjacent to the missing squares, and

the other dominoes are horizontal). Now check that these 4 cases



cover all possibilities.

(c) If mn is odd and three squares are removed so that equal number of black and white squres remains, then the remaining board can be tiled.

Solution. As usual, we induct on the size of the board starting with 3×3. I leave this case to you; there aren't too many possibilities.

Now assume $m \geq n$ so that $m \geq 5$ if we are not in the 3×3 case. If the first two columns or the last two columns contain no missing squares then we can tile these two columns with horizontal tiles and use induction as before. So now assume that both the first two columns and the last two columns contain at least one missing square.

Let's also agree that all corner squares are black.

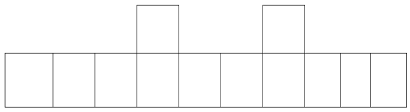
Now it couldn't be that both the first two and the last two columns have ≥ 2 missing squares, so let's say that the first two columns have exactly one missing square, call it A, and say squares B and C are the other two missing squares. Notice that column 3 can have at most one of B, C.

There are now two cases depending on the color of A.

Case 1: A **is black.** Choose a white square X in column 2 that is not adjacent to a missing square in column 3. Call that adjacent square Y. This is possible since there are at least two white squares in column two and they cannot both be adjacent to a missing square in column 3. Now use part (b) to tile the first two columns with squares A and X missing. Next, place a horizontal domino covering squares X and Y. Now apply induction to the board $(m-2) \times n$ obtained by removing the first two columns and with missing squares Y, B, C to tile the rest.

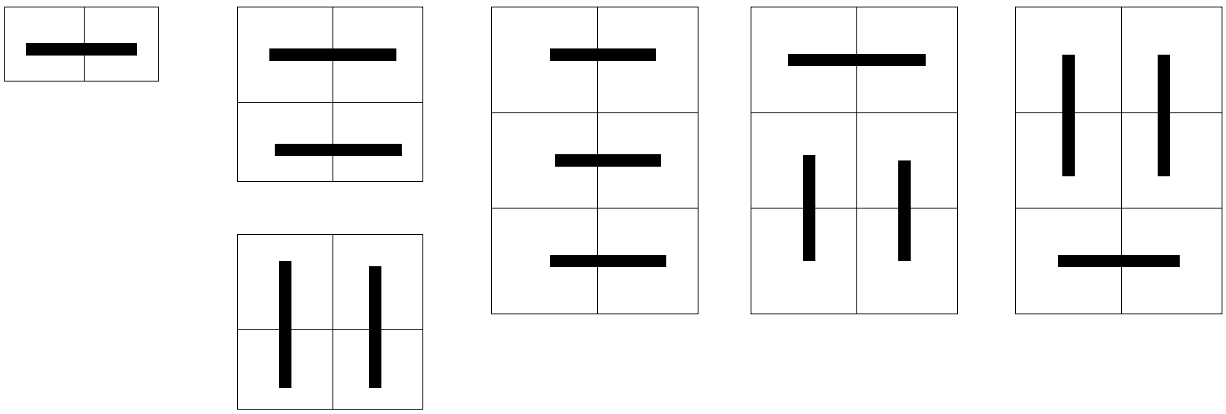
Case 2: A **is white.** Let X be a black square in column 2. Note that the square Y adjacent to X in column 3 is not one of B, C since B and C are black and Y is white. Now proceed exactly as in Case 1.

Research Project. This proof is definitely much more complicated than the others in this handout. For one thing, there are many cases to consider. It also does not seem entirely natural. For example, what if we remove 4 squares? It is easy to see that under the assumption $m, n \geq 2$ the analogous statement fails, but what if $m, n \geq 3$? What if....? When can you tile a region of a chessboard by dominoes? One necessary condition is that there must be the same number of black and white squares. Another is that each "connected component" must have the same number of black and white squares. Yet another is that after placing "forced" dominoes, the remaning connected components must have the same number of black and white squares. What I mean is illustarted in the figure below. After placing the two vertical dominoes (there is nothing else to do to cover the squares that are "sticking out") the region breaks up into 3 pieces, and two of the pieces have odd number of squares.



Can every region that satisfies the above necessary condition be tiled?

10. Prove that
$$1\cdot 1! + 2\cdot 2! + 3\cdot 3! + \cdots + n\cdot n! = (n+1)! - 1$$
11. Prove that for every $n = 1, 2, 3, \cdots$ the number $a_n = 11^{n+1} + 12^{2n-1}$ is divisible by 133.
12. Denote by D_n the number of ways in which a $2\times n$ chess board can be covered by dominoes. For example, $D_1 = 1$, $D_2 = 2$, $D_3 = 3$. These cases are illustrated in the figure.



Try to guess the formula for D_n and then prove it by induction. You will have to find a recursive formula first.

2. The Pigeon-hole principle

The pigeon-hole principle is also, along with induction, an extremely versatile method for solving a variety of problems. The basic principle is:

If you have $n+1$ pigeons and n holes, you have to put at least two pigeons in the same hole. More generally, if you have $mn+1$ pigeons and n holes, you have to put at least $m+1$ pigeons in the same hole.

Problems.

Number Theory.

1. Let A be any set of 20 distinct integers chosen from the arithmetic progression $1, 4, 7, \cdots, 100$. Prove that there must be two distinct integers in A whose sum is 104.

   SOLUTION. Consider the sets $\{1\}, \{4, 100\}, \{7, 97\}, \cdots, \{49, 55\}, \{52\}$ as "holes". Note that we have formed these sets by grouping integers from the progression so that they add up to 104, or have left them as singletons $\{1\}$ and $\{52\}$ since these numbers cannot be paired with any other number in the progression so that their sum is 104. Since $52 = 3 \cdot 17 + 1$ there are 18 holes in all. Put the numbers from A into these holes, where they belong, i.e. 4 goes into $\{4, 100\}$ etc. Since A has 20 elements, there is a hole containing two integers.

2. A *lattice point* in the plane is a point (x, y) such that both x and y are integers. Find the smallest number n such that given n lattice points in the plane, there exist two whose midpoint is also a lattice point. Hint: Consider as "holes" coordinates $\mod 2$.
3. Show that there exist two different powers of 3 whose difference is divisible by 2005.
4. Show that some multiple of 2005 is a number all of whose digits are 0's and 1's. Hint: Consider the sequence $1, 11, 111, \cdots$.
5. Show that there exists a power of 3 that ends with 001.
6. Given any sequence of n integers, some consecutive subsequence has the property that the sum is a multiple of n.
7. Given any 1000 integers, some two differ by, or sum to, a multiple of 1997. Hint: "Holes" are $\{0\}, \{1, 1996\}, \{2, 1995\}, \cdots \pmod{1997}$.
8. If $n+1$ of the integers from $\{1, 2, \cdots, 2n\}$ are selected, then some two of the selected integers have the property that one divides the other. Hint: Multiply by the largest power of 2 you can and still stay $\leq 2n$.

9. Out of the set of integers $1, 2, \cdots, 100$ you are given 10 different integers. From this set show that you can always find two disjoint nonempty subsets S and T with equal sums. Hint: How many subsets can you form?
10. Let α be an irrational number and let S be the set of all real numbers of the form $a + b\alpha$ where a, b are integers. Show that S is *dense* in the set of real numbers, i.e. any interval (u, v) with $u < v$ contains elements of S. Hint: Fix an integer $Q > 0$ and consider the holes $[0, 1/Q), [1/Q, 2/Q), \cdots, [(Q-1)/Q, 1)$. Send an integer b to a hole according to the value of $\{b\alpha\}$ (the fractional part of $b\alpha$).
11. Prove that there is some integral power of 2 that begins $2005\cdots$. Hint: Show first that $\log 2$ is irrational.
12. **(Erdös-Szekeres theorem)** Every sequence of $mn+1$ distinct real numbers has either an increasing subsequence of length $m+1$ or a decreasing subsequence of length $n+1$. Hint: Put a member a of the sequence into the hole labeled r if the longest increasing subsequence starting at a is r.
13. **(Dirichlet's theorem)**[6] Let α be an irrational number. Then there are infinitely many integer pairs (h, k) with $k > 0$ such that
$$\left|\alpha - \frac{h}{k}\right| < \frac{1}{k^2}$$
Hint: Just like #10.
14. (B2 2006) Prove that, for every set $X = \{x_1, x_2, \ldots, x_n\}$ of n real numbers, there exists a non-empty subset S of X and an integer m such that
$$\left|m + \sum_{s \in S} s\right| \leq \frac{1}{n+1}.$$
Hint: For every $i = 1, \ldots, n$ define $y_i = x_1 + x_2 + \cdots + x_i$ and $z_i = y_i - [y_i]$. Note that z_i is contained in $[0, 1)$. Use $[0, \frac{1}{n+1}), \ldots, [\frac{n}{n+1}, 1)$ as "holes".
15. **(Proizvolov's Identity)** In any partition of $1, 2, \cdots, 2n$ into decreasing and increasing sequences of n numbers each, the sum of the absolute values of the differences of the corresponding terms is always n^2. Hint: If a_i, b_i are corresponding terms, show that one of the numbers is $\leq n$ and the other is $\geq n+1$.
16. (IMO XXVI) Let S be a set of 1985 natural numbers such that all prime divisors of any number in the set S are less than 26. Show that there are four numbers in S such that their product is a 4-th power.

Geometry.

17. Prove that among any 5 points selected inside an equilateral triangle with sidelength 1, there always exists a pair at distance no more than 1/2. Hint: Subdivide into 4 copies of a scaled down triangle.

[6]The pigeon-hole principle is sometimes also called the Dirichlet principle, presumably because of this theorem.

18. Given any 6 points inside a circle of radius 1, some two of the points are within 1 of each other.
19. Mark the centers of all squares of an 8×8 chess board. Is it possible to cut the board with 13 straight lines (none passing through a marked point) so that every piece has at most one marked point. Hint: Focus on the squares along the edge of the board.
20. Given a planar set of 25 points such that among any 3 of them there exists a pair at distance < 1, prove that there exists a circle of radius 1 centered at one of the points that contains at least 13 of the points. Hint: Focus on two points at distance ≥ 1.
21. Suppose each point in the plane is colored red or blue. Show that some rectangle has its vertices all the same color. Hint: Fix 3 horizontal lines and look for a rectangle with a pair of sides on two of the lines.
22. Given any $mn + 1$ intervals, there exist $n + 1$ pairwise disjoint intervals or $m + 1$ intervals with a nonempty intersection.
23. A polygon in the plane has area > 1. Show that it contains two distinct points (x_1, y_1) and (x_2, y_2) that differ by (a, b) where a and b are integers.
24. (IMO XXI) Consider a pentagonal prism whose vertices of the top and the bottom pentagons are denoted by A_1, A_2, A_3, A_4, A_5 and B_1, B_2, B_3, B_4, B_5, respectively. Edges of these two pentagons, as well as all edges $\overline{A_iB_j}$ $(i, j = 1, \ldots, 5)$ are painted blue or red. If any triangle formed with these painted edges contains an edge of each color, show that all ten edges of two pentagons are painted in the same color.

Combinatorics.

25. Given any 10 4-element subsets of $\{1, 2, \cdots, 11\}$, some two of the subsets intersect in at least 2 elements.
26. Show that if more than half of the subsets of $\{1, 2, \cdots, n\}$ are selected, then some two of the selected subsets have the property that one is contained in the other. Hint: A typical hole is $\{A, A \cup \{n\}\}$.
27. Show that if more than half of the subsets of $\{1, 2, \cdots, n\}$ are selected, then some two of the selected subsets are disjoint.
28. Show that in any group of 6 people there are either 3 mutual friends or 3 mutual strangers.
29. In a follow-up to the previous question, show that there is some n so that in any group of n people there are either 4 mutual friends or 4 mutual strangers. Hint: Define a function $R(m, n)$ of two integers $m, n \geq 2$ recursively: $R(m, 2) = R(2, m) = m$ for $m \geq 2$ and $R(m, n) = R(m - 1, n) + R(m, n - 1)$ for $m, n > 2$. E.g. $R(3, 3) = 6$ and $R(4, 4) = 20$. By induction prove that if the edges of a complete graph on $R(m, n)$ vertices are colored red or blue, there are either m vertices so that all

edges between them are red, or there are n vertices so that all edges between them are blue.[7]

30. At a round table with n seats there are more than $(k-1)n/k$ people seated. Show that there exist k consecutive chairs that are occupied. Hint: If $k|n$ it should be easy. In general arrange this by passing to a multiple of n and "unwrapping".
31. Let M be a 14×14 matrix with all entries 0 or 1. If M has 58 entries equal to 1, then there are two rows and two columns so that all 4 entries in their intersection are 1's. Hint: This is similar to #19.
32. The squares of an $n \times n$ chess board are labeled arbitrarily with numbers 1 through n^2. Prove that there are two adjacent squares whose labels differ by at least n. Hint: Put the labels one at a time starting with $1, 2, \cdots$. Stop when a row or a column gets filled up. Now argue that there are n pairwise disjoint 2×1 subrectangles with one square filled and one empty.

[7] This is a special case of the so called Ramsey Theory. In general k colors are allowed. What is the recursion in that case?

3. Inequalities

There are several standard methods for proving inequalities, and there are also some classical inequalities you should know about.

Method 1: Good old calculus. If $y = f(x)$ is defined and differentiable on some interval I and has $f'(x) > 0$ [$f'(x) < 0$] except possibly at the endpoints of I, then f is increasing [decreasing] and so $a < b$ implies $f(a) < f(b)$ [$f(a) > f(b)$]. To see how this works we prove:

THEOREM 1 (Bernoulli's inequality). *Let $x > -1$.*

- *If $r > 1$ or $-1 < r < 0$ then*
$$(1+x)^r \geq 1 + rx$$
- *If $0 < r < 1$ then*
$$(1+x)^r \leq 1 + rx$$

As a warm-up, first prove this (by induction) in the case that $r = n$ is a positive integer.

PROOF. Consider the function
$$f(x) = (1+x)^r - rx - 1$$
defined for $x \geq -1$. Note that $f(0) = 0$, so our task is to show that f has its global minimum at 0 when $r > 1$ or $-1 < r < 0$ and that it has its global maximum when $0 < r < 1$. This will be accomplished if we argue that f is decreasing on $(-1, 0]$ and increasing on $[0, \infty)$ in the first case, and the opposite in the second case. We have
$$f'(x) = r(1+x)^{r-1} - r = r\Big((1+x)^{r-1} - 1\Big)$$
and there are four cases to look at:

- $r > 1$ or $r < 0$ and $x < 0$. Then $f'(x) < 0$.
- $r > 1$ or $r < 0$ and $x > 0$. Then $f'(x) > 0$.
- $0 < r < 1$ and $x < 0$. Then $f'(x) > 0$.
- $0 < r < 1$ and $x > 0$. Then $f'(x) < 0$.

The details of these cases are left as an exercise. □

Method 2: Jensen's inequality. Let $y = f(x)$ be a convex[8] function defined on some interval in $\mathbb{R}$. By this we mean that f is at least twice differentiable and that $f''(x) > 0$ for all x. For example, $y = x^p$ for $p > 1$ and $y = -\log x$ are convex functions. The main thing to notice about convex functions is that if you take two points on the graph and draw the chord joining these two points, then the entire chord will be above the graph

[8]Calculus books call this property "convex up".

of the function (except at the endpoints). For example, the statement that the midpoint of the chord is above the graph is:

$$f\Big(\frac{x_1+x_2}{2}\Big) \le \frac{f(x_1)+f(x_2)}{2} \tag{2}$$

(with equality only if $x_1 = x_2$). More generally, take n values

$$x_1, \cdots, x_n$$

and consider the convex polygon with vertices at

$$((x_1, y_1), \cdots, (x_n, y_n))$$

where $y_i = f(x_i)$. A point P inside this convex polygon is an average of the vertices, i.e. there are weights $w_1, \cdots, w_n \in [0, 1]$ with $w_1 + \cdots + w_n = 1$ so that

$$P = w_1(x_1, y_1) + \cdots + w_n(x_n, y_n)$$

Now P is above the graph of f, in other words

$$f(w_1x_1 + \cdots + w_nx_n) \le w_1f(x_1) + \cdots + w_nf(x_n) \tag{3}$$

with equality only if $w_iw_j(x_i - x_j) = 0$ for all i, j. Inequality (3) generalizes (2) and both are called *Jensen's inequality.* An important special case is when all weights w_i are equal to $1/n$ and then

$$f\Big(\frac{x_1+\cdots+x_n}{n}\Big) \le \frac{f(x_1)+\cdots+f(x_n)}{n}$$

Similarly, a function is *concave*[9] if $f''(x) < 0$. If f is convex then $-f$ is concave. For concave functions the reverse of the above inequalities hold.

To illustrate this, let's show

THEOREM (AM-GM). *Let $x_1, \ldots, x_n$ be positive real numbers. Then*

$$\frac{x_1+\cdots+x_n}{n} \ge \sqrt[n]{x_1\cdots x_n},$$

with equality if and only if $x_1 = \cdots = x_n$.

PROOF. The function $f(x) = \log x$ is concave on $(0, \infty)$ and so

$$f\Big(\frac{x_1+\cdots+x_n}{n}\Big) \ge \frac{f(x_1)+\cdots+f(x_n)}{n}$$

i.e.

$$\log\frac{x_1+\cdots+x_n}{n} \ge \frac{\log x_1+\cdots+\log x_n}{n}$$

After exponentiating we have

$$\frac{x_1+\cdots+x_n}{n} \ge (x_1\cdots x_n)^{1/n}$$

□

The art of applying this method is figuring out what function to use.

[9] "Convex down" in calculus.

Method 3: Convex function on a polytope. If f is a convex function defined on a closed interval $[a, b]$ then f achieves its maximum at either a or b. More generally, if f is a (multi-variable continuous) function defined on a polytope, and the restriction of f to any straight line is convex, then f achieves its maximum at one of the vertices.

One usually does not have to check convexity on every line. For example, if f is defined on the square $[0, 1] \times [0, 1]$ then it suffices to check convexity on horizontal and vertical lines, i.e. convexity in each variable separately.

PROBLEM. *When* $0 \leq a, b, c \leq 1$ *then*

$$\frac{a}{b+c+1} + \frac{b}{c+a+1} + \frac{c}{a+b+1} + (a-1)(b-1)(c-1) \leq 1$$

SOLUTION. Consider the function

$$F(a, b, c) = \frac{a}{b+c+1} + \frac{b}{c+a+1} + \frac{c}{a+b+1} + (a-1)(b-1)(c-1)$$

defined on the cube $0 \leq a, b, c \leq 1$. If we fix two of the variables, say b, c, and let a run over $[0, 1]$ we get a convex function. So if there is some (a, b, c) where $F(a, b, c) > 1$ then also either $F(0, b, c) > 1$ or $F(1, b, c) > 1$. We can continue this until all 3 variables are either 0 or 1. In other words, we only need to check the inequality on the 8 vertices of the cube where each variable is 0 or 1. This is easy to do.

Method 4: Smoothing. This method consists of repeatedly replacing pairs of variables ultimately reducing the inequality to checking one special case. To illustrate it, I give a proof of the AM-GM inequality (so by now you have 3 proofs of this really important inequality). This proof is due to Kiran Kedlaya.

THEOREM (AM-GM). *Let* $x_1, \ldots, x_n$ *be positive real numbers. Then*

$$\frac{x_1 + \cdots + x_n}{n} \geq \sqrt[n]{x_1 \cdots x_n},$$

with equality if and only if $x_1 = \cdots = x_n$.

PROOF (KEDLAYA). We will make a series of substitutions that preserve the left-hand side while strictly increasing the right-hand side. At the end, the x_i will all be equal and the left-hand side will equal the right-hand side; the desired inequality will follow at once. (Make sure that you understand this reasoning before proceeding!)

If the x_i are not already all equal to their arithmetic mean, which we call a for convenience, then there must exist two indices, say i and j, such that $x_i < a < x_j$. (If the x_i were all bigger than a, then so would be their arithmetic mean, which is impossible; similarly if they were all smaller than a.) We will replace the pair x_i and x_j by

$$x_i' = a, x_j' = x_i + x_j - a;$$

by design, x'_i and x'_j have the same sum as x_i and x_j, but since they are closer together, their product is larger. To be precise,

$$a(x_i + x_j - a) = x_i x_j + (x_j - a)(a - x_i) > x_i x_j$$

because $x_j - a$ and $a - x_i$ are positive numbers.[10]

By this replacement, we increase the number of the x_i which are equal to a, preserving the left-hand side of the desired inequality and increasing the right-hand side. As noted initially, eventually this process ends when all of the x_i are equal to a, and the inequality becomes equality in that case. It follows that in all other cases, the inequality holds strictly. □

Note that we made sure that the replacement procedure terminates in a finite number of steps. If we had proceeded more naively, replacing a pair of x_i by *their* arithmetic mean, we would get an infinite procedure, and then would have to show that the x_i were "converging" in a suitable sense. (They do converge, but making this precise requires some additional effort which our alternate procedure avoids.)

Here is another example in the same vein. This one is more subtle because Jensen doesn't apply.

PROBLEM. *Let* $a_0, \dots, a_n$ *be numbers in the interval* $(0, \pi/2)$ *such that*

$$\tan(a_0 - \pi/4) + \tan(a_1 - \pi/4) + \cdots + \tan(a_n - \pi/4) \geq n - 1.$$

Prove that $\tan a_0 \tan a_1 \cdots \tan a_n \geq n^{n+1}$.

SOLUTION (KEDLAYA). Let $x_i = \tan(a_i - \pi/4)$ and $y_i = \tan a_i = (1 + x_i)/(1 - x_i)$, so that $x_i \in (-1, 1)$. The claim would follow immediately[11] from Jensen's inequality if only the function $f(x) = \log(1 + x)/(1 - x)$ were convex on the interval $(-1, 1)$, but alas, it isn't. It's concave on $(-1, 0]$ and convex on $[0, 1)$. So we have to fall back on the smoothing principle.

What happens if we try to replace x_i and x_j by two numbers that have the same sum but are closer together? The contribution of x_i and x_j to the left side of the desired inequality is

$$\frac{1 + x_i}{1 - x_i} \cdot \frac{1 + x_j}{1 - x_j} = 1 + \frac{2}{\frac{x_i x_j + 1}{x_i + x_j} - 1}.$$

The replacement in question will increase $x_i x_j$, and so will decrease the above quantity provided that $x_i + x_j > 0$. So all we need to show is that we can carry out the smoothing process so that every pair we smooth satisfies this restriction.

Obviously there is no problem if all of the x_i are positive, so we concentrate on the possibility of having $x_i < 0$. Fortunately, we can't have more

[10] There is a "calculus way" of doing this. Consider the function $f(x) = (x_i + x)(x_j - x)$. The derivative is $f'(x) = x_j - x_i - 2x$ so f is increasing on $[0, \frac{x_j - x_i}{2}]$. Say $a \leq \frac{x_i + x_j}{2}$, i.e. $a - x_i \leq \frac{x_j - x_i}{2}$. But then $f(a - x_i) > f(0)$ means exactly that $a(x_i + x_j - a) > x_i x_j$. If $a \geq \frac{x_i + x_j}{2}$, i.e. $x_j - a \leq \frac{x_j - x_i}{2}$ use $f(x_j - a) > f(0)$.

[11] Well, also using that f is monotonically increasing.

than one negative x_i, since $x_0 + \cdots + x_n \geq n - 1$ and each x_i is less than 1. (So if two were negative, the sum would be at most the sum of the remaining $n - 1$ terms, which is less than $n - 1$.) Let's say $x_0 < 0$. Then $x_0 + x_i \geq 0$ for all $i \geq 1$ for a similar reason, and we can't have $x_0 + x_i = 0$ for all i (otherwise adding all these up we would conclude $(n-1)x_0 + (x_0 + \cdots + x_n) = 0$ which is impossible). So choose i so that $x_0 + x_i > 0$ and we can replace these two by their arithmetic mean. Now all of the x_j are nonnegative and smoothing (or Jensen) may continue without further restrictions, yielding the desired inequality. □

Rearrangement inequality. Let $x_1 \geq x_2 \geq \ldots \geq x_n$ and $y_1 \geq y_2 \geq \ldots \geq y_n$ be two sequences of positive numbers. If $z_1, z_2, \ldots, z_n$ is any permutation of $y_1, y_2, \ldots, y_n$ then

$$x_1 z_1 + x_2 z_2 + \ldots + x_n z_n \leq x_1 y_1 + x_2 y_2 + \ldots + x_n y_n.$$

You can think about this as follows (for $n = 2$). You are selling apples at \$1 a piece and hot dogs at \$2 a piece. Do you receive more money if you sell 10 apples and 15 hot dogs, or if you sell 15 apples and 10 hot dogs?[12] You can prove the rearrangement inequality in the spirit of smoothing. If $z_i < z_j$ for some $i < j$ exchange z_i and z_j and watch the sum grow.

Likewise, $\sum x_i z_i$ is minimized over permutations of the z_i's when $z_1 \leq z_2 \leq \cdots \leq z_n$.

Problems.[13]

1. Let $x_1, \ldots, x_n$ be positive real numbers. Prove the AM-HM (arithmetic mean - harmonic mean) inequality
$$\frac{n}{\frac{1}{x_1} + \cdots + \frac{1}{x_n}} \leq \frac{x_1 + \cdots + x_n}{n}.$$
2. (Putnam 2005; B2) Find all positive integers n, $k_1, \ldots, k_n$ such that $k_1 + \cdots + k_n = 5n - 4$ and
$$\frac{1}{k_1} + \cdots + \frac{1}{k_n} = 1.$$
3. Let
$$H_n = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$$
Show that $n(n+1)^{1/n} \leq n + H_n$ for all n.
4. Let $s_n = (1 + \frac{1}{n})^n$ and $S_n = 1/(1 - \frac{1}{n})^n$. Show:
(a) $s_n < s_{n+1}$.

[12] Sorry for being crass.

[13] The hard part is figuring out to what sequence to apply AM-GM or to what function to apply Jensen. You are not expected to solve these in few minutes, but think about one or two over a period of time and experiment with different choices. You can also peek at the Hints.

(b) $S_n > S_{n+1}$.
(c) $s_n < S_n$ and sequences s_n and S_n are convergent, say to $e_1 \leq e_2$.
(d) $S_n/s_n \to 1$ so that $e_1 = e_2$.

5. Let $a_1, \cdots, a_n \in (0, \pi)$ with arithmetic mean μ. Prove that
$$\prod_i \frac{\sin a_i}{a_i} \leq \Big(\frac{\sin \mu}{\mu}\Big)^n$$
6. Let $p, q > 1$ with $\frac{1}{p} + \frac{1}{q} = 1$. If $a, b \geq 0$ show that
$$ab \leq \frac{a^p}{p} + \frac{b^q}{q}$$
with equality only if $a^p = b^q$.
7. Suppose
$$\frac{\sin^{2n+2} A}{\sin^{2n} B} + \frac{\cos^{2n+2} A}{\cos^{2n} B} = 1$$
for some $n \neq 0, -1$. Show that then equality holds for all n.
8. The *quadratic mean* of $a_1, \cdots, a_n$ is
$$QM(a_1, \cdots, a_n) = \sqrt{\frac{a_1^2 + \cdots + a_n^2}{n}}$$
Show that $AM(a_1, \cdots, a_n) \leq QM(a_1, \cdots, a_n)$ with equality only if $a_1 = \cdots = a_n$.
9. More generally, let
$$M_\alpha(a_1, \cdots, a_n) = \Big(\frac{a_1^\alpha + \cdots + a_n^\alpha}{n}\Big)^{1/\alpha}$$
for $\alpha > 0$. So $M_1 = AM$ and $M_2 = QM$. Show that
$$\alpha_1 < \alpha_2 \Rightarrow M_{\alpha_1}(a_1, \cdots, a_n) \leq M_{\alpha_2}(a_1, \cdots, a_n)$$
10. Given real numbers $x_1, \ldots, x_n$, what is the minimum value of
$$|x - x_1| + \cdots + |x - x_n|?$$
11. For $a, b, c > 0$, prove that $a^a b^b c^c \geq (abc)^{(a+b+c)/3}$.
12. Let $x_1, \ldots, x_n$ be n positive numbers whose sum is 1. Prove that
$$\frac{x_1}{\sqrt{1 - x_1}} + \cdots + \frac{x_n}{\sqrt{1 - x_n}} \geq \sqrt{\frac{n}{n-1}}.$$
13. Let A, B, C be the angles of a triangle. Prove that
(1) $\sin A + \sin B + \sin C \leq 3\sqrt{3}/2$;
(2) $\cos A + \cos B + \cos C \leq 3/2$;
(3) $\sin A/2 \sin B/2 \sin C/2 \leq 1/8$;
(Beware: not all of the requisite functions are convex everywhere!)
14. (A2 2003) If $a_1, \cdots, a_n, b_1, \cdots, b_n > 0$ then
$$(a_1 \cdots a_n)^{1/n} + (b_1 \cdots b_n)^{1/n} \leq \Big[(a_1 + b_1) \cdots (a_n + b_n)\Big]^{1/n}$$

15. **(Cauchy's inequality)**
 If $u_i, v_i > 0$ for $i = 1, 2, \cdots, n$ then
$$u_1v_1 + u_2v_2 + \cdots + u_nv_n \leq \sqrt{u_1^2 + u_2^2 + \cdots + u_n^2}\sqrt{v_1^2 + v_2^2 + \cdots + v_n^2}$$
The significance of this inequality is that $u \cdot v \leq |u||v|$ for any two vectors $u, v \in \mathbb{R}^n$.
16. **(Hölder's inequality)**
 If $u_i, v_i > 0$ for $i = 1, 2, \cdots, n$ and $p, q > 1$ with $\frac{1}{p} + \frac{1}{q} = 1$ then
$$u_1v_1 + u_2v_2 + \cdots + u_nv_n \leq (u_1^p + u_2^p + \cdots + u_n^p)^{1/p}(v_1^q + v_2^q + \cdots + v_n^q)^{1/q}$$
This generalizes Cauchy's inequality for $p = q = 2$. In terms of norms Hölder's inequality says $u \cdot v \leq |u|_p|v|_q$, where $|\cdot|_p$ has the obvious meaning. That this is really a norm follows from
17. **(Minkowski's triangle inequality)**
 If $u_i, v_i > 0$ for $i = 1, 2, \cdots, n$ and $p > 1$ then
$$\Big((u_1+v_1)^p+(u_2+v_2)^p+\cdots+(u_n+v_n)^p\Big)^{1/p} \leq (u_1^p+u_2^p+\cdots+u_n^p)^{1/p}+(v_1^p+v_2^p+\cdots+v_n^p)^{1/p}$$
In other words $|u + v|_p \leq |u|_p + |v|_p$.
18. Let $x_1, \ldots, x_n$ $(n \geq 2)$ be positive numbers satisfying
$$\frac{1}{x_1 + 1998} + \frac{1}{x_2 + 1998} + \cdots + \frac{1}{x_n + 1998} = \frac{1}{1998}.$$
Prove that
$$\frac{\sqrt[n]{x_1x_2\cdots x_n}}{n-1} \geq 1998.$$
(Again, beware of nonconvexity.)
19. (XVII IMO) Let $x_1 \geq x_2 \geq \ldots \geq x_n$ and $y_1 \geq y_2 \geq \ldots \geq y_n$ be two sequences of positive numbers. If $z_1, z_2, \ldots, z_n$ is any permutation of $y_1, y_2, \ldots, y_n$ then
$$\sum_{i=1}^{n}(x_i - y_i)^2 \leq \sum_{i=1}^{n}(x_i - z_i)^2.$$
20. (XX IMO) Suppose that $a_1, \ldots, a_n$ be a sequence of n distinct positive integers. Prove that
$$\sum_{k=1}^{n}\frac{a_k}{k^2} \geq \sum_{k=1}^{n}\frac{1}{k}.$$
21. Show that
$$x^x \geq \Big(\frac{x+1}{2}\Big)^{x+1}.$$
22. For a positive integer x and an integer n prove that
$$\sum_{k=1}^{n}\frac{[kx]}{k} \leq [nx].$$

23. Let n be a positive integer such that
$$\sin^{2n+2}(A) + \cos^{2n+2}(A) = \frac{1}{2^n}.$$
Show that $\sin^2(A) = \cos^2(A) = 1/2$.
24. Let $a, b, c > 0$. Show that
$$\frac{a}{b+c} + \frac{b}{a+c} + \frac{c}{a+b} \geq \frac{3}{2}.$$
25. (XXV IMO) Let x, y and z be non-negative real numbers such that $x + y + z = 1$. Show that
$$xy + xz + yz - 2xyz \leq \frac{7}{27}.$$
26. (B5 2006) For each continuous function $f : [0, 1] \to \mathbb{R}$, let $I(f) = \int_0^1 x^2 f(x)\,dx$ and $J(x) = \int_0^1 x\,(f(x))^2\,dx$. Find the maximum value of $I(f) - J(f)$ over all such functions f.
27. Prove that $n! < \left(\frac{n+1}{2}\right)^n$ for $n = 2, 3, \cdots$.
28. Prove that $(a+b)(b+c)(c+a) \geq 8abc$ when $a, b, c \geq 0$.
29. (A3 2003) What is the minimum of
$$|\sin x + \cos x + \tan x + \cot x + \sec x + \csc x|$$
as $x \in \mathbb{R}$?
30. (A4 2003) Let $a, b, c, A, B, C \in \mathbb{R}$ and $a \neq 0$, $A \neq 0$. Suppose also that $|ax^2 + bx + c| \leq |Ax^2 + Bx + C|$ for every $x \in \mathbb{R}$. Show that
$$|b^2 - 4ac| \leq |B^2 - 4AC|$$
31. (B2 2003) Let n be a positive integer. Starting with the sequence
$$1, \frac{1}{2}, \frac{1}{3}, \cdots, \frac{1}{n}$$
form a new sequence with $n - 1$ terms
$$\frac{3}{4}, \frac{5}{12}, \cdots, \frac{2n-1}{2n(n-1)}$$
by averaging consecutive terms of the original sequence. Repeat the process of averaging until you get a single number x_n. Prove that $x_n < \frac{2}{n}$.
32. (B6 2003) Let $f : [0, 1] \to \mathbb{R}$ be continuous. Prove that
$$\int_0^1 \int_0^1 |f(x) + f(y)|dxdy \geq \int_0^1 |f(x)|dx$$
33. (B3 2002) Show that for all integers $n > 1$
$$\frac{1}{2ne} < \frac{1}{e} - \left(1 - \frac{1}{n}\right)^n < \frac{1}{ne}$$
34. (B4 1999) Let f be a real fnction with continuous third derivative such that $f(x), f'(x), f''(x), f'''(x)$ are positive for all x. Suppose that $f'''(x) \leq f(x)$ for all x. Show that $f'(x) < 2f(x)$ for all x.

35. (B1 1998) Find the minimum value of
$$\frac{(x+1/x)^6-(x^6+1/x^6)-2}{(x+1/x)^3+(x^3+1/x^3)}$$
for $x>0$.
36. (B2 1998) Given a point (a,b) with $0<b<a$ determine the minimum perimeter of a triangle with one vertex at (a,b), one vertex on the x-axis, and one on the line $y=x$. You may assume that a triangle of minimum perimeter exists.
37. (B2 1996) Show that for every positive integer n
$$\left(\frac{2n-1}{e}\right)^{\frac{2n-1}{2}}<1\cdot 3\cdot 5\cdots(2n-1)<\left(\frac{2n+1}{e}\right)^{\frac{2n+1}{2}}$$
38. (B3 1996) Given that $\{x_1,x_2,\cdots,x_n\}=\{1,2,\cdots,n\}$ find the largest possible value of
$$x_1x_2+x_2x_3+\cdots+x_{n-1}x_n+x_nx_1$$
39. (B2 1988) Prove or disprove: if x and y are real numbers with $y\geq 0$ and $y(y+1)\leq(x+1)^2$ then $y(y-1)\leq x^2$.

Hints.

1. Apply the AM-GM inequality to the right hand side and to the inverse of the left hand side.
2. AM-HM inequality.
3. AM-GM inequality for $2, \frac{3}{2}, \frac{4}{3}, \cdots, \frac{n+1}{n}$.
4. (a) AM-GM for $n+1$ numbers $1+1/n, 1+1/n, \cdots, 1+1/n, 1$.
   (b) AM-GM for $n+1$ numbers $1-1/n, 1-1/n, \cdots, 1-1/n, 1$.
   (d) Use Bernoulli. Of course, the common limit is $e = 2.71828\cdots$.
5. $f(x) = \log\left(\frac{\sin x}{x}\right)$ is concave on $(0,\pi)$.
6. Jensen for $f(x) = \log x$ with weights $1/p$ and $1/q$ applied to a^p and b^q.
7. Inequality from the previous problem. Figure out what p, q should be from $\sin^2 B + \cos^2 B = 1$.
8. Jensen for $x \mapsto x^2$.
9. When $\alpha_1 = 1$ consider $x \mapsto x^{\alpha_2}$. In general, by substitutions show that $M_{\alpha_1} \le M_{\alpha_2}$ follows from $M_1 \le M_{\frac{\alpha_2}{\alpha_1}}$.
10. The function is piecewise linear. What are the slopes on each piece?
11. For $x > 0$ $x \mapsto x\log x$ is convex and $x \mapsto \log x$ is concave. Put the two inequalities together.
12. $x \mapsto x/\sqrt{1-x}$ is convex for $0 < x < 1$.
13. (1) $x \mapsto \sin x$ is concave for $0 \le x \le \pi$.
    (2) $x \mapsto \cos x$ is concave on $[0, \pi/2]$ but that's not quite enough. If say $C > \pi/2$ you should decrease C and simultaneously increase say A by the same amount. Thus show that $x \mapsto \cos(A+x) + \cos(C-x)$ is increasing on $[0, C - \pi/2]$.
    (3) $x \mapsto \log\sin x$ is concave for $0 < x \le \pi/2$.
14. Apply AM-GM to $\frac{a_1}{a_1+b_1}, \cdots, \frac{a_n}{a_n+b_n}$ and also to $\frac{b_1}{a_1+b_1}, \cdots, \frac{b_n}{a_n+b_n}$ and add up.
15. Special case of Hölder.
16. This generalizes Cauchy's inequality for $p = q = 2$. To derive it from Jensen's inequality with weights, let $f(t) = t^q$, the weights are $w_i = u_i^p / \sum_j u_j^p$ and the arguments are $x_i = u_i v_i / w_i$.

    Another solution: Start with $n = 2$. Put $\alpha = u_2/u_1$ and $\beta = v_2/v_1$. The inequality simplifies to $1 + \alpha\beta \le (1+\alpha^p)^{1/p}(1+\beta^q)^{1/q}$. Let $f(\alpha, \beta) = RHS - LHS$. Then $f = 0$ on the curve $\alpha^p = \beta^q$. This curve is the graph of $\alpha \mapsto \alpha^{p/q}$ and separates the first quadrant of the α–β plane into regions $\alpha^p > \beta^q$ and $\alpha^p < \beta^q$. In the first region $\frac{\partial f}{\partial \alpha} > 0$ and in the second $\frac{\partial f}{\partial \beta} > 0$. The inequality now follows by connecting a point in the first region to the curve by a horizontal segment, and a point in the second region to the curve by a vertical segment. Equality holds only if the vector (u_1^p, u_2^p) is proportional to the vector (v_1^q, v_2^q). For $n > 2$ maximize LHS while keeping $u_1^p + \cdots + u_n^p$ and $v_1^q + \cdots + v_n^q$ constant (maximum exists by the Heine-Borel theorem). By the case $n = 2$ the vectors $(u_1^p, \cdots, u_n^p)$ and $(v_1^q, \cdots, v_n^q)$ are proportional (otherwise they wouldn't be proportional when restricted to two coordinates and we could increase LHS). But when they are proportional equality holds. Excercise: Generalize directly the $n = 2$ argument to $n > 2$ thus avoiding Heine-Borel.

17. This can be proved using Jensen's inequality with weights with $f(x) = -(1 + x^{1/p})^p$, $w_i = v_i^p / \sum_j v_j^p$ and $x_i = (u_i/v_i)^p$.
18. It is convenient to make the substitution $y = \frac{1}{x+1998}$ so that $x = \frac{1}{y} - 1998$. It would be cool if the function $y \mapsto \log(\frac{1}{y} - 1998)$ were convex on $(0, \frac{1}{1998})$ but unfortunately it is convex only on the first half of this interval. Apply the smoothing technique.
19. Rearrangement inequality.
20. Rearrangement inequality.
21. Use the convexity of $x \log x$.
22. Rearrangement inequality.
23. Similar to #7.
24. Convexity of $x \mapsto x/(1-x)$. Alternatively, use the rearangement inequality twice. This is due to Masaki Iino. Assume that $a \geq b \geq c$ then $a + b \geq a + c \geq b + c$...
25. Smoothing principle. Assume that $x \geq y \geq z$ and then replace x and z by their arithmetic mean. Alternatively, use Lagrange multipliers. Show that when number 2 is replaced by 2.25 the maximum is still attained at the center of the triangle.
26. Consider an inner product on the space of continuous functions on $[0, 1]$ given by
$$(f, g) = \int_0^1 x f(x) g(x) dx.$$
Then $f(x)$ can be written as $f(x) = cx + g(x)$ where $g(x)$ is perpendicular to x. Then
$$I(f) - J(f) = (x, f) - (f, f) = c(x, x) - c^2(x, x) - (g, g) \leq (c - c^2)(x, x).$$
Since $(x, x) = 1/4$ and $c - c^2$ has a maximum $1/4$ for $c = 1/2$ it follows that
$$I(f) - J(f) \leq \frac{1}{16}$$
and the equality is achieved for $f(x) = x/2$.

4. Analysis

Integration problems are often solved by simplifying and/or re-interpretation of integral. The following are used:

Mean value theorem If f is continuous on the closed interval $[a, b]$ and differentiable on the open interval (a, b) then there exists c between a and b such that

$$f(a) - f(b) = f'(c)(a - b).$$

Integration by parts

$$\int_a^b f(x)g'(x)\ dx = f(x)g(x)|_a^b - \int_a^b f'(x)g(x)\ dx.$$

Fundamental theorem of calculus

$$f(b) - f(a) = \int_a^b f'(x)\ dx.$$

Differential equations Consider the linear differential equation

$$y^{(n)} + a_{n-1}y^{(n-1)} + \cdots + a_1 y' + a_0 y = e^{rx}.$$

In order to solve this equation, we try $y = e^{rx}$. Then the left hand side is equal to

$$P(r)e^{rx}$$

where $P(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0$. In particular, if r is not a root of $P(z)$, then $e^{rx}/P(r)$ is a solution of the original equation. If $P(r) = 0$ then e^{rx} is a solution of the corresponding homogenous equation (where we replace e^{rx} by 0 on the right). If $P(r) = 0$, then we can try substituting $y = xe^{rx}$. Then the left hand side is equal to

$$P(r)xe^{rx} + P'(r)e^{rx}.$$

Thus, if $P(r) = 0$ but $P'(r) \neq 0$ then $xe^{rx}/P'(r)$ is a solution. If $P'(r) = 0$ then xe^{rx} is another solution of the homogeneous equation. If so, we can try $y = x^2e^{rx}$, and in this case the left hand side becomes

$$P(r)x^2e^{rx} + 2P'(r)xe^{rx} + P''(r)e^{rx}.$$

Thus, if $P''(r) \neq 0$ then $x^2e^{rx}/P''(r)$ is a solution. I guess this explains how to find solutions of the original differential equation. If y_1 and y_2 are any tow solutions of the equation, then their difference is a solution of the corresponding homogeneous equation. Any solution of the homogeneous equation is a linear combination of x^ie^r where r is a root of $P(z)$ and i is any integer less then the multiplicity of the root r.

Exercises:

1. (A3 1987) For all real x, the real-valued function $y = f(x)$ satisifies
$$y'' - 2y' + y = 2e^x.$$
(1) If $f(x) > 0$ for all real x, must $f'(x) > 0$ for all real x? Explain.
(2) If $f'(x) > 0$ for all real x, must $f(x) > 0$ for all real x? Explain.
2. (B1 1987) Evaluate:
$$I = \int_2^4 \frac{\sqrt{\ln(9-x)}\,dx}{\sqrt{\ln(9-x)} + \sqrt{\ln(x+3)}}.$$
3. (A2 1995) For what pairs (a, b) of positive real numbers does the improper integral
$$\int_b^\infty \left(\sqrt{\sqrt{x+a} - \sqrt{x}} - \sqrt{\sqrt{x} - \sqrt{x-b}}\right)\,dx$$
converge?
4. (B2 1991) Suppose f and g are non-constant, differentiable, real-valued functions on $\mathbb{R}$ such that
$$f(x+y) = f(x)f(y) - g(x)g(y)$$
$$g(x+y) = f(x)g(y) + g(x)f(x)$$
for all x and y. If $f'(0) = 0$, prove that $(f(x))^2 + (g(x))^2 = 1$ for all x.
5. (B2 1997) Let f be a twice-differentiable real-valued function satisfying
$$f(x) + f''(x) = -xg(x)f'(x),$$
where $g(x) \geq 0$ for all real x. Prove that $|f(x)|$ is bounded.
6. (A3 1998) Let f be a real function on the real line with continuous third derivative. Prove that there exists a point a such that
$$f(a) \cdot f'(a) \cdot f''(a) \cdot f'''(a) \geq 0.$$
7. (A5 1993) Find the maximum value of
$$\int_0^y \sqrt{x^4 + (y - y^2)^2}\,dx$$
for $0 \leq y \leq 1$.
8. (A5 1993) Show that
$$\int_{-100}^{-10} \left(\frac{x^2 - x}{x^3 - 3x + 1}\right)^2 dx + \int_{\frac{1}{101}}^{\frac{1}{11}} \left(\frac{x^2 - x}{x^3 - 3x + 1}\right)^2 dx + \int_{\frac{101}{100}}^{\frac{11}{10}} \left(\frac{x^2 - x}{x^3 - 3x + 1}\right)^2 dx$$
is rational number.
9. (B3 1994) Find the set of all real numbers k with the following property. For any positive differentiable function $f : \mathbb{R} \to \mathbb{R}$ that satisfies $f'(x) > f(x)$ for all x, there is some number N such that $f(x) > e^{kx}$ for all $x > N$.

10. (A3 1997) Evaluate

$$\int_0^\infty \left(x - \frac{x^3}{2} + \frac{x^5}{2\cdot 4} - \frac{x^7}{2\cdot 4\cdot 6} + \cdots\right)\left(1 + \frac{x^2}{2^2} + \frac{x^4}{2^2\cdot 4^2} + \frac{x^6}{2^2\cdot 4^2\cdot 6^2} + \cdots\right) dx.$$

11. (B2 1994) For which real numbers c is there a straight line that intersects the curve

$$x^4 + 9x^3 + cx^2 + 9x + 4$$

in four distinct points?

12. (An interesting question of Troy Goodsell.) Find a real function $f(x)$ such that $f'(x) = f^{-1}(x)$, that is, the derivative of $f(x)$ is equal to the inverse of $f(x)$.

13. (A1 2006) Find the volume of the region of points (x, y, z) such that

$$(x^2 + y^2 + z^2 + 8)^2 \le 36(x^2 + y^2).$$

14. (B1 1990) Find all real-valued continuously differentiable functions f on the real line such that for all x,

$$(f(x))^2 = \int_0^x [(f(t))^2 + (f'(t))^2]\, dt + 1990.$$

15. (A2 1988) A not uncommon calculus mistake is to believe that the product rule for derivatives says that $(fg)' = f'g'$. If $f(x) = e^{x^2}$, determine, with proof, whether there exists an open interval (a, b) and a nonzero function g defined on (a, b) such that this wrong product rule is true for x in (a, b).

16. (A4 2000) Show that the improper integral

$$\lim_{B\to\infty} \int_0^B \sin(x)\sin(x^2)\, dx$$

converges.

Hints and solutions

1. The differential equation can be solved using the method in the introduction. With explicit solutions in hand it is easy to analyze the conditions $f(x) > 0$ and $f'(x) > 0$.
2. The answer is 1. Notice that, if $2 \le x \le 4$ then both, $x+3$ and $9-x$ have the same range, from 5 to 7. Thus, with the substitution $x-9 = u+3$ the integral becomes
$$I = \int_2^4 \frac{\sqrt{\ln(u+3)}\ du}{\sqrt{\ln(u+3)} + \sqrt{\ln(9-u)}}.$$
Substituting x for u and adding to the original integral, we get
$$2I = \int_2^4 1\ dx = 2.$$
3. The answer is $a = b$. Use
$$(\sqrt{x+a} - \sqrt{x})(\sqrt{x+a} + \sqrt{x}) = a$$
to rewrite the integral as
$$\int_b^\infty \frac{\sqrt{a}}{\sqrt{\sqrt{x+a} + \sqrt{x}}} - \frac{\sqrt{b}}{\sqrt{\sqrt{x} + \sqrt{x-b}}}\ dx$$
If we can show that convergence is not affected by removing a and b in the two denominators, then the integral becomes
$$\frac{\sqrt{a} - \sqrt{b}}{\sqrt{2}} \int_b^\infty x^{-\frac{1}{4}}\ dx$$
which converges unless $a = b$. To check that removing a is OK, notice that $\sqrt{x+a} + \sqrt{x}$ is sandwiched between $2\sqrt{x}$ and $2\sqrt{x+a}$. Thus it suffices to check that
$$\int_b^\infty x^{-\frac{1}{4}} - (x+a)^{-\frac{1}{4}}\ dx$$
diverges. But the mean value theorem applied to the function $f(x) = x^{-\frac{1}{4}}$ implies that the integrand is sandwiched between $x^{-\frac{5}{4}}$ and $(x+a)^{-\frac{5}{4}}$, both of which are integrable on $[b, \infty)$. This shows that a could be ignored, as assumed. A similar argument works for b.
4. We shall use the functional equation and the condition $f'(0) = 0$ to derive differential equations satisfied by f and g. Differentiate first equation with respect to x
$$f'(x+y) = f'(x)f(y) - g'(x)g(y),$$
and then put $x = 0$, which gives $f'(y) = -g'(0)g(y)$. (This also proves that f is twice differentiable.) A similar treatment of the

second equation gives $g'(y) = g'(0)f(y)$. Combining the two equations gives
$$f'' + (g'(0))^2 f = 0.$$
Combining with the initial condition, we get $f(x) = A\cos(g'(0)x)$...

5. Note if $g(x) = 0$ then $f(x) = \cos x$ is a solution. So the idea is to look at
$$h(x) = f(x)^2 + f'(x)^2,$$
which is equal to 1 if $f(x) = \cos x$. Take the derivative of $h(x)$ to show that $h(x)$ is increasing for $x < 0$ and decreasing for $x > 0$. In particular, it is bounded by $h(0)$.
6. If one of the four factors vanishes at a point, we are done. Otherwise, by continuity, each of the four factors has the same sign along the whole real line. Assume $f(x) > 0$ for all x. I claim that $f''(x) > 0$ for all x. Indeed, if $f''(x) < 0$ for all x then the function is positive and concave down. This is not possible. (For example, the concavity implies that the graph of f is below any tangent line. This is impossible since $f(x) > 0$.) On the other hand, if $f(x) < 0$ for all x, then $f''(x) < 0$ by the same argument. In ether case
$$f \cdot f'' > 0.$$
Of course, the same argument shows that $f' \cdot f''' > 0$.
7. The answer is $1/3$, the value for $y = 1$. Notice that
$$x^4 + (y - y^2)^2 \leq (x^2 + (y - y^2))^2$$
and with this replacement the integral is bounded by
$$\int_0^y x^2 + y - y^2 \, dx = y^2 - \frac{2}{3}y^3$$
which, along $0 \leq y \leq 1$, has the maximum $1/3$ at $y = 1$.
8. After staring at the end points of integration, I realized that the fractional transformation
$$f(x) = \frac{x-1}{x}$$
(which has order three : $f(f(f(x))) = x$) permutes the end points of the three integrals. This allows one to transfer all three integrals to the same interval. E.g. substituting $u = 1/(1-x)$ in the third integral leads to
$$\int_{-100}^{-10} \left(\frac{u-1}{u^3 - 3u + 1}\right)^2 \, du$$
and substituting $x = 1/(1-u)$ in the second integral leads to
$$\int_{-100}^{-10} \left(\frac{u}{u^3 - 3u + 1}\right)^2 \, du$$

Summing the three functions, we have to evaluate

$$\int_{-100}^{-10} \left(\frac{x^2 - x + 1}{x^3 - 3x + 1} \right)^2$$

It turns out that one can easily find an anti-derivative, of the form

$$\left(\frac{ax^2 + bx}{x^3 - 3x + 1} \right)' = \left(\frac{x^2 - x + 1}{x^3 - 3x + 1} \right)^2 .$$

9. (Easy part) If $k \geq 1$ then $f(x) = e^x - 1$ satisfies that $f'(x) > f(x)$ yet $f(x)$ is not strictly bigger then e^{kx}.

   (Hard part) Assume $k < 1$. Consider the function $g(x) = \ln(f(x)) - x$. Then $g'(x) = \frac{f'(x)}{f(x)} - 1 > 0$ so g is increasing and must cross the line $y = (k-1)x$ of negative slope. So for large x we have $g(x) > (k-1)x$ i.e. $f(x) > e^{kx}$.

   Here is an alternative argument. If we can show that the condition $f'(x) > f(x)$ implies that

$$f(x) > f(0)e^x$$

   then any $k < 1$ works.

   By the Fundamental Theorem of Calculus,

$$f(x) - f(0) = \int_0^x f'(t)\ dt > \int_0^x f(t)\ dt.$$

   We can estimate the integral using lower sums. Let m be an integer, and divide the segment $[0, x]$ into m subsegments of equal length x/m. Since f is increasing, the lower sum gives us

$$f(x) - f(0) > \frac{x}{m}[f(0) + f(x/m) + \ldots + f(x - x/m)]$$

   (and similar inequalities for $f(kx/m) - f(0)$ for $k < m$) which implies that

$$f(x) > f(0) \left(1 + \frac{x}{m}\right)^m .$$

   e.g. if $m = 2$ the lower sums give $f(x) - f(0) > x/2(f(0) + f(x/2))$ and $f(x/2) - f(0) > x/2f(0)$ and combining the two we get

$$f(x) > f(0)(1 + x/2)^2.$$

   Passing to $m \to \infty$ we get the estimate on f.

10. Notice that the first factor is

$$xe^{-\frac{x^2}{2}}.$$

    Use a change of variable $u = x^2/2$ and integration by parts. (You will get a series of integrals.)

11. Hint: Notice that if a line intersects the graph of a function $f(x)$ n-times then the function $f(x)$ changes convexity at least $n-2$ times. Now the question can be answered easily by considering the line through the inflection points of the quartic polynomial.

12. Try $f(x) = Cx^p$.
13. The answer is $6\pi^2$. If $x^2 + y^2 = r^2$ then z satisfies $(r^2 + z^2 + 8)^2 \leq 36r^2$ i.e. $r^2 + z^2 + 8 \leq 6r$. The roots of $r^2 - 6r + 8 = 0$ are 2 and 4. So the region is a solid torus; the area above the circle $x^2 + y^2 = r^2$ is $2\pi r(2\sqrt{-r^2 + 6r - 8})$, and the volume is
$$\int_2^4 4\pi r\sqrt{-r^2 + 6r - 8}\ dr$$
which can be calculated by translating to remove the linear term $6r$ and then the substitution $u = r^2$. Alternatively, the torus is the solid of revolution obtained by rotating a disk of radius 1 about the z-axis, and the center is at distance 3 from the axis. Thus the volume is (area of the disk)$\times$(length of the circle traversed by the center)$= \pi \times 6\pi = 6\pi^2$.

5. Polynomials

We recall some basic definitions and properties.

Fundamental Theorem of Algebra. Every nonzero polynomial of degree n with complex coefficients has precisely n complex roots $a_1, a_2, \dots, a_n$ and can be factored as

$$p(x) = c(x - a_1)(x - a_2)\cdots(x - a_n).$$

For example, the complex roots of $x^n - 1 = 0$ (n-th roots of 1) form a regular n-gon in complex plane, and can be written as

$$e^{2\pi ik/n} = \cos(\frac{2\pi k}{n}) + i\sin(\frac{2\pi k}{n}), \qquad k = 1, \dots, n.$$

Polynomial Interpolation. For any sequence $a_1, a_2, \dots, a_n$ of n complex numbers and n distinct points $x_1, x_2, \dots, x_n$ in $\mathbb{C}$ there exists a unique polynomial of degree at most $n-1$ such that

$$p(x_j) = a_j, \qquad j = 0, 1, \dots, n.$$

This polynomial is easily constructed using Lagrange's interpolation:

$$P(x) = \sum_{j=0}^{n} a_j \frac{\prod_{i\neq j}(x - x_i)}{\prod_{i\neq j}(x_j - x_i)}.$$

Difference operator and factorial polynomials. The difference operator Δ is defined by

$$\Delta p(x) = p(x+1) - p(x).$$

It is similar to the derivative. For example, it decreases the degree of the polynomial by one and, given a polynomial $q(x)$, the equation $\Delta p(x) = q(x)$ has a solution $p(x)$ and any two solutions differ by a constant. The action of Δ on x^k is complicated as the difference $(x+1)^k - x^k$ involves k terms. Instead of x^k we can look at the factorial polynomial

$$x^{(k)} = x(x-1)(x-2)\cdots(x-k+1).$$

Then $\Delta x^{(k)} = kx^{(k-1)}$. (Just as the derivative of x^k is kx^{k-1}.) Even better, one can consider a divided factorial polynomial $\frac{x^{(k)}}{k!}$. Then

$$\Delta \frac{x^{(k)}}{k!} = \frac{x^{(k-1)}}{(k-1)!}.$$

Note that the value of the divided factorial polynomial at a positive integer $n \geq k$ is equal to the binomial coefficient $\binom{n}{k}$, and it is 0 in the range $0 \leq n < k$.

Division Algorithm. If f and $g \neq 0$ are two polynomials with coefficients in a field F, then there exist unique polynomials q and r such that

$$f = qg + r.$$

here either $r = 0$ or $\deg(r) < \deg(g)$. The situation with polynomials with coefficients in a ring is more delicate. However, if f and g have integer coefficients, and g is monic (the first non-zero coefficient is 1), then q and r also have integer coefficients.

One can use the division algorithm to show that $F[x]$ is a unique factorization domain. That is, every polynomial $p(x)$ can be factored into irreducible polynomials $p(x) = q_1(x) \cdot \ldots \cdot q_m(x)$ where $q_i(x)$ are uniquely determined up to a permutation and multiplication of each $q_i(x)$ by a non-zero scalar c_i such that $c_1 \cdot \ldots \cdot c_m = 1$. Once we know that $F[x]$ is a unique factorization domain, it can be shown that $F[x_1, \ldots, x_n]$, the ring of polynomials in n variables is also a unique factorization domain.

Invariant Polynomials. Here we discuss polynomials in n variables $x_1, \ldots, x_n$. A polynomial p is said to be invariant if it does not change under any permutation of n variables. Every invariant polynomial in $x_1, \ldots, x_n$ is a polynomial in elementary symmetric polynomials $c_1, c_2, \ldots, c_n$ which are defined by

$$(x - x_1)(x - x_2) \cdots (x - x_n) = x^n + c_1 x^n + c_2 x^{n-2} + \ldots + c_n.$$

For example, if $n = 3$ then there are three elementary symmetric functions and they are

$$\begin{cases} c_1 = -(x_1 + x_2 + x_3) \\ c_2 = x_1x_2 + x_1x_3 + x_2x_3 \\ c_3 = -x_1x_2x_3. \end{cases}$$

The polynomial $S_2 = x_1^2 + x_2^2 + x_3^2$ is symmetric and in terms of c_i's it can be written as

$$S_2 = c_1^2 - 2c_2.$$

This formula is a special case of **Newton's formulas for power sums.** More precisely, let m be a positive integer. The m-th power sum in $x_1, \ldots, x_n$ is

$$S_m = x_1^m + x_2^m + \cdots + x_n^m.$$

Then

$$\begin{aligned} S_1 + c_1 &= 0 \\ S_2 + c_1S_1 + 2c_2 &= 0 \\ S_3 + c_1S_2 + c_2S_1 + 3c_3 &= 0 \\ &\cdots \\ S_n + c_1S_{n-1} + \cdots + c_{n-1}S_1 + nc_n &= 0 \\ S_m + c_1S_{m-1} + \cdots + c_nS_{m-n} &= 0 \end{aligned}$$

where the last equality holds for $m > n$. Notice that the formulas imply not only that S_k can be expressed in terms of c_k but, conversely, that c_k can be expressed in terms of S_k for $k \leq n$. In particular, it follows that any symmetric polynomial in variables $x_1, \ldots, x_n$ can be expresses as a polynomial in S_k for $k \leq n$, as well.

Palindromic polynomials. The equation $a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$ is called palindromic if $a_j = a_{n-j}$ for all j. If n is even, then by substitution $z := x + 1/x$ reduces to an equation of degree $n/2$. After finding solutions z_j, $j = 1, \ldots z_{n/2}$, the solutions of the original equation are found by solving $x + \frac{1}{x} = z_j$ for all j.

The following is an important observation. If a is a real number then solutions of

$$x + \frac{1}{x} = a$$

are real if $|a| \geq 2$ and complex numbers on the unit circle ($|x| = 1$) if $|a| \leq 2$.

For example, consider the palindromic polynomial $x^4 + bx^3 + bx + 1$. Dividing by x^2 we get

$$x^2 + bx + \frac{b}{x} + \frac{1}{x^2} = \left(x + \frac{1}{x}\right)^2 + b\left(x + \frac{1}{x}\right) - 2 = z^2 + bz - 2.$$

Assume that b is a real number. Let us determine the values of b such that the roots of the polynomial $x^4 + bx^3 + bx + 1$ are complex numbers of absolute value 1. For that the roots of $p(z) = z^2 + bz - 2$ have to be in the segment $[-2, 2]$. Since $p(0) = -2 < 0$, the roots are contained in the segment $[-2, 2]$ if and only if $p(-2) \geq 0$ and $p(2) \geq 0$. These two give $4 - 2b - 2 \geq 0$ and $4 + 2b - 2 \geq 0$ which is equivalent to $1 \geq b \geq -1$. For example, if $b = 0$ then the original polynomial is $x^4 + 1$ on its roots are (primitive) eight roots of 1.

Cubic equation. The equation $x^3 + px + q = 0$ has three solutions which are described as follows: Put

$$R = (q/2)^2 + (p/3)^3$$

and

$$A = \sqrt[3]{-\frac{q}{2} + \sqrt{R}}, \qquad B = \sqrt[3]{-\frac{q}{2} - \sqrt{R}}$$

Then the three solutions are

$$\{A + B, A\rho + B\rho^2, A\rho^2 + B\rho\}$$

where $\rho = e^{2\pi i/3}$ is a cubic root of 1. The number R is essentially the discriminant of the cubic. More precisely,

$$108R = -(x_1 - x_2)^2(x_2 - x_3)^2(x_1 - x_3)^2$$

where x_1, x_2 and x_3 are three roots of the cubic polynomial. Assume that p and q are real. If all three roots are real then $R < 0$. If one root is real and the other two are complex conjugates of each other, then $R > 0$. Thus calculating the discriminant is a quick way to see whether a cubic has one or three real roots.

Exercises:

1. Find the reminder when $x^{81}+x^{49}+x^{25}+x^9+x$ is divided by a) x^3-x, b) x^2+1, c) x^2+x+1.
2. Let p be a non-constant polynomial with integral coefficients. If $p(k)=0$ for four distinct integers k, prove that $p(k)$ is composite for every integer k.
3. Factor $(a+b+c)^3-(a^3+b^3+c^3)$.
4. Find a if a and b are integers such that x^2-x-1 is a factor of $ax^{17}+bx^{16}+1$.
5. Find the unique polynomial of degree n such that
$$p(j)=2^j$$
for $j=0,1,\dots,n$.
6. Find the unique polynomial $p(x)$ of degree n such that
$$p(j)=\frac{1}{1+j}$$
for $j=0,1,\dots,n$.
7. A polynomial p_n of degree n satisfies $p_n(k)=F_k$ for $k=n+2,n+3,\dots,2n+2$, where F_k are Fibonacci numbers. Show that $p_n(2n+3)=F_{2n+3}-1$.
8. If
$$\begin{array}{ccccccc} x & + & y & + & z & = & 1 \\ x^2 & + & y^2 & + & z^2 & = & 2 \\ x^3 & + & y^3 & + & z^3 & = & 3 \end{array}$$
find $x^4+y^4+z^4$.
9. Complex solutions of $x^n-1=0$ are ζ^k, $k=1,\dots n$ where $\zeta=e^{2\pi i/n}$. Show that
$$\sum_{k=1}^{n}\zeta^{dk}=\begin{cases} n \text{ if } d \text{ is a multiple of } n \\ 0 \text{ otherwise}\end{cases}$$
10. Find a cubic equation whose roots are cubes of the roots of $x^3+ax^2+bx+c=0$.
11. Let $x_1,x_2,\dots,x_n$ be the roots of a polynomial $P(x)=x^n+ax^{n-1}+bx^{n-2}+cx^{n-3}+\cdots$ of degree n. The number
$$\prod_{i\neq j}(x_i-x_j)$$
is called the discriminant of P. It is symmetric in variables x_i, so it can be expressed as a polynomial in the coefficients of P. Do this for $n=2$ and $n=3$. If $n=3$, assume that the polynomial is x^3+px+q.
12. Find all values of the parameter a such that all roots of the equation
$$x^6+3x^5+(6-a)x^4+(7-2a)x^3+(6-a)x^2+3x+1=0$$

are real.

13. The roots of the fifth degree equation
$$x^5 - 5x^4 - 35x^3 + \dots$$
form an arithmetic sequence. Find the roots.
14. Let $G_n = x^n \sin nA + y^n \sin nB + z^n \sin nC$ where x, y, z, A, B, C are real numbers such that $A+B+C$ is a multiple of π. Show that if $G_1 = G_2 = 0$ then $G_n = 0$ for all positive n.
15. If
$$\begin{array}{ccccccc} x & + & y & + & z & = & 3 \\ x^2 & + & y^2 & + & z^2 & = & 25 \\ x^4 & + & y^4 & + & z^4 & = & 209 \end{array}$$
find $x^{100} + y^{100} + z^{100}$.
16. (B1 2005) Find a non-zero polynomial $P(x, y)$ such that $P([a], [2a]) = 0$ for all real numbers a. (Note: $[a]$ is the greatest integer less then or equal to a.)
17. (A3 2001) Find values for the integer m such that
$$P_m = x^4 - (2m+4)x^2 + (m-2)^2$$
is a product of two non-constant polynomials with integer coefficients?
18. (B1 1985) Let k be the smallest positive integer for which there exist distinct integers m_1, m_2, m_3, m_4, m_5 such that the polynomial
$$p(x) = (x - m_1)(x - m_2)(x - m_3)(x - m_4)(x - m_5)$$
has exactly k nonzero coefficients. Find, with proof, a set of integers m_1, m_2, m_3, m_4, m_5 for which this minimum k is achieved.
19. (A2 1999) Let $p(x)$ be a polynomial that is nonnegative for all real x. Prove that for some k, there are polynomials $f_1(x), \dots, f_k(x)$ such that
$$p(x) = \sum_{j=1}^{k} (f_j(x))^2.$$
20. (B2 1999) Let $P(x)$ be a polynomial of degree n such that $P(x) = Q(x)P''(x)$, where $Q(x)$ is a quadratic polynomial and $P''(x)$ is the second derivative of $P(x)$. Show that if $P(x)$ has at least two distinct roots then it must have n distinct roots.
21. (XVII IMO) Find all homogeneous polynomials $P(x, y)$ of degree n such that
$$P(a+b, c) + P(b+c, a) + P(c+a, b) = 0$$
for all real numbers a, b and c, and $P(1, 0) = 1$.

Hints and solutions

1. (part c)). The roots of x^2+x+1 are ρ and $\bar{\rho}=\rho^2$, two cubic roots of 1:
$$\rho=-\frac{1}{2}+\frac{\sqrt{-3}}{2}$$
Thus
$$x^{81}+x^{49}+x^{25}+x^9+x=q(x)(x^2+x+1)=ax+b$$
gives
$$1+\rho+\rho+1=a\rho+b$$
which implies that $a=2$ and $b=2$.
2. Hint: Let a,b,c,d be the four integral roots. Then
$$p(x)=(x-a)(x-b)(x-c)(x-d)q(x)$$
where $q(x)$ has integral coefficients. If x is an integer, then $(x-a)(x-b)(x-c)(x-d)$ is composite.
3. Hint: Use formulas for a difference and a sum of two cubes. Then
$$(a+b+c)^3-a^3=(b+c)(\cdots) \text{ and } b^3+c^3=(b+c)(\cdots).$$
It follows that $(b+c)$ divides our polynomial. By symmetry, $a+c$ and $a+b$ also divide our polynomial, as well. Thus
$$(a+b+c)^3-(a^3+b^3+c^3)=k(a+b)(a+c)(b+c)$$
for a constant k. Now put $a=b=c=1$ to find that $k=1$.
4. Solution: The solutions of $x^2-x-1=0$ are
$$\alpha=\frac{1+\sqrt{5}}{2} \text{ and } \bar{\alpha}=\frac{1-\sqrt{5}}{2}.$$
Thus $ax^{17}+bx^{16}+1=q(x)(x^2-x-1)$ gives
$$\begin{aligned} a\alpha^{17}+b\alpha^{16}+1=0\\ a\bar{\alpha}^{17}+b\bar{\alpha}^{16}+1=0\end{aligned}$$
which is a 2×2 system with a and b as unknowns. Since $\alpha\bar{\alpha}=-1$, the determinant of this system is equal to $\alpha-\bar{\alpha}=\sqrt{5}$. Thus, using the Cramer's rule, the solution is
$$a=\frac{(1+\sqrt{5})^{16}-(1-\sqrt{5})^{16}}{2^{16}\sqrt{5}}$$
which we recognize as the 16-th Fibonacci number.
5. First solution. Let $p_n(x)$ be the solution to this problem for $n=0,1,\ldots$. Recall the difference operator Δ. Note that the requirement that $p_n(j)=2^j$ for $0\le j\le n$ implies that
$$\Delta p_n(j)=p_n(j+1)-p_n(j)=2^{j+1}-2^j=2^j$$

for $0 \leq j \leq n-1$. In other words, $\Delta p_n(x) = p_{n-1}(x)$. Now note that this recursion together with the condition $p_n(0) = 1$ uniquely determines all polynomials $p_n(x)$. Since

$$q_n(x) = \sum_{k=1}^{n} \frac{x^{(k)}}{k!}$$

satisfy these conditions, it follows that e$p_n(x) = q_n(x)$.

Second solution. Recall that $2^n = \sum_{k=1}^{n} \binom{n}{k}$. Now if we replace the binomial coefficient $\binom{n}{k}$ by the divided factorial polynomial $\frac{x^{(k)}}{k!}$ we get the polynomials $p_n(x)$.

6. Hint: Consider $q(x) = (1+x)p(x) - 1$. Then

$$q(x) = cx(x-1)\dots(x-j)$$

Now pick c so that $q(x)+1$ is divisible by $1+x$.

7. Hint: Notice that for $k = n+1, n+2, \dots, 2n$

$$p_n(k+2) - p_n(k+1) = F_{k+2} - F_{k+1} = F_k$$

so $p_{n-1}(x) = p_n(x+2) - p_n(x+1)$. Use this to do induction.

1) Base of induction: Let $n = 1$. Since $p_1(3) = 2$ and $p_1(4) = 3$ then $p_1(x) = x+1$. Thus

$$p_1(5) = 4 = F_5 - 1.$$

2) Step of induction: Assume that p_{n-1} satisfies $p_{n-1}(2n+1) = F_{2n+1} - 1$. Thus

$$p_n(2n+3) = p_n(2n+2) + p_{n-1}(2n+1) = F_{2n+2} + F_{2n+1} - 1 = F_{2n+3} - 1.$$

8. Elementary exercise in symmetric polynomials.
9. You are asked to compute the power sums for the roots of the polynomial $x^n - 1 = 0$. Note that all $c_i = 0$ except $c_n = 1$.
10. Hint: the coefficients of the desired cubic are also symmetric functions in roots of the original cubic.
11. If $n = 2$, write the polynomial in a more familiar $x^2 + px + q = 0$.

$$(x_1 - x_2)(x_2 - x_1) = 2x_1x_2 - (x_1^2 + x_2^2) = 4x_1x_2 - (x_1 + x_2)^2 = 4q - p^2.$$

Note that this expression appears in the quadratic formula! If $n = 3$, it takes a bit more to do the problem.

12. Hint: The polynomial is palindromic so it can be reduced to the degree 3. Next, the solutions of

$$x + \frac{1}{x} = b$$

are real iff $|b| \geq 2$.

13. Hint: The 5 roots are a, $a+d$, $a+2d$, $a+3d$ and $a+4d$ for two numbers a and b. The first two symmetric polynomials are known. This gives
$$5a + 10d = 5 \text{ and } 10a^2 + 40ad + 35d^2 = -35.$$
14. Solution: Put $X = xe^{iA}$, $Y = ye^{iB}$ and $Z = ze^{iC}$. Then G_n is the imaginary part of the n-th power sum
$$S_n = X^n + Y^n + Z^n.$$
Since $G_1 = G_2 = 0$ the first two elementary symmetric polynomials in X, Y, Z are real. Since
$$XYZ = xyze^{i(A+B+C)} = \pm xyz,$$
(here we are using that $A + B + C$ is a multiple of π) the third elementary symmetric polynomial is also real. Since all S_n can be expressed as polynomials with integer coefficients of the three elementary symmetric polynomials, they have to be real.
15. Hint: (I am not so sure, though.) Note that any symmetric polynomial is a polynomial in S_1, S_2 and S_3. By degree considerations, S_4 must be linear in S_3, so we can certainly figure out S_3, and therefore x, y and z as solutions of a cubic?
16. Hint: This problem is very easy. What is the possible difference $[2a] - 2[a]$?
17. Hint: Find the roots.

6. Complex numbers

Any complex number $z = a + bi$ can be written in the so-called polar form
$$z = re^{i\varphi}$$
where $r = \sqrt{a^2 + b^2}$ and φ is the angle between the x-axis and z, considered in the counter clockwise direction. The two forms combined with the Euler's formula
$$e^{i\varphi} = \cos\varphi + i\sin\varphi$$
give rise to numerous useful identities. For example, the cube of $e^{i\varphi}$ can be calculated in two ways:
$$(e^{i\varphi})^3 = e^{3i\varphi} = \cos 3\varphi + i\sin 3\varphi$$
and
$$(\cos\varphi + i\sin\varphi)^3 = \cos^3\varphi + 3i\cos^2\varphi\sin\varphi - 3\cos\varphi\sin^2\varphi - i\sin^3\varphi.$$
This gives a trigonometric identity
$$\cos 3\varphi = 4\cos^3\varphi - 3\cos\varphi.$$

Roots of 1: The complex solutions of $z^n - 1 = 0$ are called n-th roots of 1. They can be written as powers ξ_n^k, $k = 0, \ldots, n-1$ where
$$\xi_n = e^{\frac{2\pi i}{n}}.$$
Cubic roots are 1 and
$$-\frac{1}{2} \pm \frac{\sqrt{-3}}{2}.$$
All n-th roots of 1 from a regular n-gon. In particular, the sum of all n-th roots of 1 is 0. More generally,
$$\sum_{k=0}^{n-1} (\xi_n^k)^d = \begin{cases} n \text{ if } d \mid n \\ 0 \text{ otherwise.} \end{cases}$$
For example, if $n = 6$ all sixth roots of 1 form a regular hexagon, while their second powers form two equilateral triangles (third roots of 1). Again, the sum of these is 0.

Here is an application. Assume $f(x) = a_0 + a_1x + a_2x^2 + \ldots$. The 4-th roots of 1 are $1, -1, i$ and $-i$. Then
$$\frac{1}{4}[f(1) + f(i) + f(-1) + f(-i)] = a_0 + a_4 + a_8 + \ldots$$
Other sums of coefficients of type $a_k + a_{k+d} + a_{k+2d} + \ldots$ can be obtained in a similar fashion, using d-th roots of 1.

Exercises:

1. Show that $\arctan(1)+\arctan(2)+\arctan(3)=\pi$. Hint: use $e^{i\pi}=-1$.
2. Suppose $\cos(\theta)=1/\pi$. Evaluate
$$\sum_{n=0}^{\infty}\frac{\cos(n\theta)}{2^n}.$$
Hint: this is a real part of a geometric series.
3. For a positive integer n define
$$S_n=\left(\begin{array}{c}3n\\0\end{array}\right)+\left(\begin{array}{c}3n\\3\end{array}\right)+\ldots+\left(\begin{array}{c}3n\\3n\end{array}\right).$$
a) Find a closed expression for S_n. Hint: use $f(x)=(1+x)^{3n}$.
b) Show that
$$\lim_{n\to\infty}S_n^{\frac{1}{3n}}=2.$$
4. Evaluate:
$$\left(\begin{array}{c}2001\\0\end{array}\right)-\left(\begin{array}{c}2001\\2\end{array}\right)+\left(\begin{array}{c}2001\\4\end{array}\right)-\cdots\left(\begin{array}{c}2001\\2000\end{array}\right).$$
Hint: consider $f(x)=(1+x)^n$.
5. a) Express $\cos 5\varphi$ as a polynomial in $\cos\varphi$.
b) $\cos n\varphi$ can be expressed as a polynomial of degree n in $\cos\varphi$. Find the coefficient of the leading term $\cos^n\varphi$.
6. Let α be a real number such that $\cos(\alpha\pi)=\frac{1}{3}$. Show that α is irrational. Hint: if $\alpha=\frac{m}{n}$, then $\cos(n\alpha\pi)=\pm1$. Now use exercise 5.
7. Evaluate:
$$1+\frac{1}{4!}+\frac{1}{7!}+\frac{1}{10!}+\ldots$$
Hint: consider $f(x)=(e^x-1)/x$.
8. Find the minimum and the maximum of $f(z)=|z^{1000}-z^5+1|$ along the circle $|z|=1$. Hint: evaluate at roots of 1.
9. (A3 1989) Prove that if z satisfies $11z^{10}+10iz^9+10iz-11=0$ then $|z|=1$. Hint replace z by iz.
10. Let $G_n=x^n\sin nA+y^n\sin nB+z^n\sin nC$ where x,y,z,A,B,C are real numbers such that $A+B+C$ is a multiple of π. Show that if $G_1=G_2=0$ then $G_n=0$ for all positive n.
11. (A4 1975) Let $n=2m$ such that m is odd. Let $\theta=e^{2\pi i/n}$. Find a finite set of integers $a_0,\ldots,a_k$ such that
$$\frac{1}{1-\theta}=a_k\theta^k+a_{k-1}\theta^{k-1}+\cdots+a_0.$$
12. (A5 1985) Let $I_m=\int_0^{2\pi}\cos(x)\cos(2x)\cdots\cos(mx)\,dx$. For which integers m, $1\le m\le 10$ is $I_m\neq 0$?
13. (B6 1983) Let k be a positive integer, let $m=2^k+1$, and let $r\neq 1$ be a complex root of $z^m-1=0$. Prove that there exist polynomials $P(z)$ and $Q(z)$ with integer coefficients such that $P(r)^2+Q(r)^2=-1$.

14. (A2 1955) Let O be the center of a regular n-gon $P_1P_2\cdots P_n$ and let X be a point outside the n-gon on the line OP_1. Show that

$$XP_1 \cdot XP_2 \cdot \cdots \cdot XP_n + OP_1^n = OX^n$$

15. (A2 1959) Let $\omega^3 = 1$, $\omega \neq 1$. Show that $z_1, z_2, -\omega z_1 - \omega^2 z_2$ are the vertices of an equilateral triangle.

Hints and Solutions:

1. $\arctan(n)$ is the argument of the complex number $1+ni$. Thus, in order to check the statement, it suffices to show that
$$(1+i)(2+i)(3+i)$$
is a negative real number.
2. The answer is the real part of the geometric series
$$\sum_{i=0}^{\infty} \frac{e^{ni\theta}}{2^n} = \frac{1}{1-e^{i\theta}/2}$$
...
3. $$S_n = \frac{1}{3}[(1+1)^{3n} + (1+\rho)^{3n} + (1+\rho^2)^{3n}]$$
Note now that $1+\rho$ and $1+\rho^2$ are primitive sixth roots of 1. Thus
$$S_n = \frac{1}{3}[2^{3n} + (-1)^n \cdot 2].$$
4. The expression is equal to the real part of $(1+i)^{2001}$. Since $1+i = \sqrt{2}e^{\pi i/4}$ it follows that
$$(1+i)^{2001} = 2^{1000}\sqrt{2}e^{\pi i/4} = 2^{1000} + 2^{1000}i.$$
Thus, the answer is 2^{1000}.
5. $\cos(nx)$ is the real part of $(\cos x + i \sin x)^n$ which is equal to
$$\cos^n x - \left(\begin{array}{c} n \\ 2 \end{array} \right) \cos^{n-2} x \cdot \sin^2 x + \cdots$$
Using $\sin^2 x = 1 - \cos^2 x$ one easily sees that $\cos(nx) = T_n(\cos x)$ where T_n is a polynomial of degree n with integer coefficients and the leading coefficient 2^{n-1}.
6. This will be discussed in a future lecture.
7. Use the function
$$f(x) = \frac{e^x - 1}{x} = 1 + \frac{x^3}{4!} + \frac{x^6}{7!} + \cdots$$
The sum is equal to
$$\frac{1}{3}[f(1) + f(\rho) + f(\rho^2)].$$
8. The triangle inequality implies that $0 \leq f(z) \leq 3$. Substitute $z := -z$, so $f(z) = |z^{1000} + z^5 + 1|$. If z is a cube root of 1, then $z^{1000} = z$ and $z^5 = z^2$, and $f(z) = |z^2 + z + 1|$. Now $f(1) = 3$ and $f(\rho) = 0$ (ρ is a non-trivial cube root of 1).
9. After substitution, the equation becomes palindromic:
$$11z^{10} + 10z^9 + 10z + 11 = 0 \leftrightarrow 11z^5 + 10z^4 + 10\frac{1}{z^4} + 11\frac{1}{z^5} = 0$$

Next, using the substitution $x = z + 1/z$ we have a degree 5 polynomial

$$p(x) = 11x^5 + 10x^4 - 55x^3 - 40x^2 + 55x + 20 = 0$$

Next, one needs to check that this polynomial has 5 real roots x_j in the interval $[-2, 2]$, which assures that solutions of

$$z + \frac{1}{z} = x_j$$

sit on the unit circle. This is easily done by looking at the sign changes on the interval $[-2, 2]$: $p(-2) = -2$, $p(-1) = -21$, $p(0) = 20$, $p(1) = 1$, $p(2) = 42$. (This needs a bit of refining, but it appears that p has 3 negative and 2 positive real roots.)

10. See the lecture on invariant polynomials.
11. Factor $x^{2m} - 1 = (x^m - 1)(x^m + 1)$. Then θ is a root of the second factor. Further factorization gives

$$(x^m + 1) = (x + 1)(x^{m-1} - x^{m-2} + \cdots - x + 1).$$

Again, θ is a root of the second factor. But

$$0 = \theta^{m-1} - \theta^{m-2} + \cdots - \theta + 1 = (\theta - 1)(\theta^{m-2} + \theta^{m-4} + \cdots + \theta) + 1.$$

Elementary rearrangement gives

$$\frac{1}{1 - \theta} = \theta^{m-2} + \theta^{m-4} + \cdots + \theta.$$

7. Number Theory

Euler's function. Let n be a positive integer. The Euler function $\varphi(n)$ is equal to the number of positive integers $k = 1, 2, \ldots, n$ relatively prime to n. The Euler function can be easily calculated using

(1) If p is a prime number, then $\varphi(p^k) = p^k - p^{k-1}$.
(2) If m and n are relatively prime then $\varphi(mn) = \varphi(m)\varphi(n)$.

If a is relatively prime to n then

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

Chinese reminder theorem. Let m and n be two relatively prime integers. then the system

$$x \equiv a \pmod{m}$$
$$x \equiv b \pmod{n}$$

has a unique solution x modulo mn.

Rational roots. Let p and q be two relatively prime integers. If p/q is a root of a polynomial

$$P(x) = a_n x^n + \ldots + a_0 = 0$$

with integer coefficients then p divides a_0 and q divides a_n. In particular, if $a_n = 1$ (i.e. $P(x)$ is monic) then any rational root is an integer. This is a special case of Gauss's lemma which says that if $P(x)$ is monic and $P(x) = Q(x)R(x)$ is a factorization such that $Q(x)$ and $R(x)$ are monic polynomials with rational coefficients, then $Q(x)$ and $R(x)$ have in fact integer coefficients.

Eisenstein irreducibility criterion. Let p be a prime. Let

$$P(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0$$

be a polynomial with integer coefficients such that p divides all coefficients $a_0, \ldots, a_{n-1}$, but p^2 does not divide a_0. Then $P(x)$ cannot be factored as a product of two polynomials with integer coefficients. Proof goes as follows. If $P(x) = Q(x)R(x)$ with $Q(x) = x^q + b_{q-1}x^{q-1} + \ldots + b_0$ and $R(x) = x^r + c_{r-1}x^{r-1} + \ldots + c_0$, then

$$a_0 = b_0 c_0$$
$$a_1 = b_0 c_1 + b_1 c_1$$
$$a_2 = b_0 c_2 + b_1 c_1 + b_2 c_0$$

and so on... Since p divides a_0 but p^2 does not, either b_0 or c_0 is divisible by p, but not both. Assume that p divides b_0. Since p divides a_1 the second equation implies that p divides b_1 and so on, concluding that p divides all coefficients of $Q(x)$. This is a contradiction.

Phytagorean equation. Primitive integer solutions (no common factor) of

$$x^2 + y^2 = z^2$$

are given by $x = a^2 - b^2$, $y = 2ab$ and $z = a^2 + b^2$ for two integers a and b of different parity.

Pell's equation. If d is a positive non-square integer, then solutions of

$$x^2 - dy^2 = 1$$

with positive x and y are (x_k, y_k), $k = 1, 2, \ldots$ where (x_1, y_1) is the solution with the smallest x and y and

$$x_k + y_k\sqrt{d} = (x_1 + y_1\sqrt{d})^k.$$

The first solution is obtained by computing the period of the continued fraction expansion for to $\alpha = \sqrt{d} + [\sqrt{d}]$. (Or twice the period if it is odd.) For example, if $d = 3$ then the continued fraction of $\alpha = \sqrt{3} + 1$ has the period of length 2:

$$\alpha = 2 + \cfrac{1}{1 + \frac{1}{\alpha}}$$

which can be rewritten as

$$\sqrt{3} = \frac{3 + 2\sqrt{3}}{2 + \sqrt{3}}$$

and the denominator gives the first solution $2 + \sqrt{3}$ of $x^2 - 3y^2 = 1$. If the period is odd, then the algorithm gives the first solution of the equation $x^2 - dy^2 = -1$.

Last but not least, if $d \equiv 1 \pmod 4$, then solutions such that x and y are half integers are also considered "integral" solution. This can be justified as follows. If we write $d = 4k + 1$, $x = (2a + 1)/2$ and $y = (2b + 1)/2$ then the equation $x^2 - dy^2 = 1$ is equivalent to

$$a^2 + a - b^2 - b - k(2b + 1)^2 = 1.$$

Congruence Problems

1. Determine the last digit of
$$17^{17^{17}}.$$
2. (Essentially B5 1997) Show that for every n the sequence
$$2, 2^2, 2^{2^2}, 2^{2^{2^2}}, \ldots \pmod{n}$$
is eventually constant.
3. Find the last three digits of 7^{9999}.
4. (A3 1970) Why is the last digit, in decimal notation, of a square 0, 1, 4, 5, 6, or 9? How long is the longest sequence of equal non-zero digits at the end of a squared integer?
5. (A5 2001) Prove that there exist unique positive integers a and n such that
$$a^{n+1} - (a+1)^n = 2001.$$
6. (A4 1985) Define a sequence $a_1 = 3$, $a_{i+1} = 3^{a_i}$. Which integers between 00 and 99 inclusive occur as the last two digits in the sequence a_i?
7. (A1 2005) Show that every positive integer is a sum of one or more numbers of the form $2^r 3^s$, where r and s are nonnegative integers and no summand divides another. (For example, $23 = 9 + 8 + 6$.)
8. (A3 1983) Let p be in the set $\{3, 5, 7, 11, \ldots\}$ of odd primes and let
$$F(n) = 1 + 2n + 3n^2 + \cdots + (p-1)n^{p-2}.$$
Prove that if a and b are distinct integers in the set $\{0, 1, 2, \ldots, p-1\}$ then $F(a)$ and $F(b)$ are not congruent modulo p.

Problems on Factoring and Polynomials

9. Let α be a real number such that $\cos(\alpha\pi) = 1/3$. Show that α is irrational.
10. Let $n > 4$ be an integer. Show that $4^n + n^4$ is composite.
11. Show that $P(x) = x^n + 5x^{n-1} + 3$ can not be factored into two polynomials with integer coefficients.
12. (B1 2004) Let $P(x) = c_n x^n + c_{n-1}x^{n-1} + \cdots + c_0$ be a polynomial with integer coefficients. Suppose that r is a rational number such that $P(r) = 0$. Show that the n numbers
$$c_n r,\ c_n r^2 + c_{n-1} r,\ c_n r^3 + c_{n-1} r^2 + c_{n-2} r,$$
$$\ldots,\ c_n r^n + c_{n-1} r^{n-1} + \cdots + c_1 r$$
are integers.

Integral Solutions Problems

13. Show that there are no odd positive integer numbers x, y and z which satisfy:
$$(x+y)^2 + (x+z)^2 = (y+z)^2$$

14. Show that there are infinitely many integers such that $n^2 + (n+1)^2$ is a perfect square.
15. Find the smallest positive integer n such that $61n^2 + 1$ is a square.
16. (XXII IMO) Let m and n be two integers ($1 \leq m \leq 1981$, $1 \leq n \leq 1981$) that satisfy the equation
$$(n^2 - nm - m^2)^2 = 1.$$
Find the maximal value for $n^2 + m^2$.
17. (B4 1995) Evaluate
$$\sqrt[8]{2207 - \frac{1}{2207 - \frac{1}{2207 - \dots}}}.$$
Express your answer in the form $\frac{a+b\sqrt{c}}{d}$, where a, b, c, d are integers. Hint: relate to a Pell equation.
18. (A3 1992) For a given positive integer m, find all triples (n, x, y) of positive integers, with n relatively prime to m, which satisfy
$$(x^2 + y^2)^m = (xy)^n.$$

Hints and Solutions:

1. $\varphi(10) = 4$ so $17^{17} \equiv 1 \pmod 4$ and
$$17^{17^{17}} \equiv 7 \pmod{10}.$$
2. Idea: notice that the sequence appears in the exponents, as well. So, if the sequence stabilizes modulo $\varphi(n)$, it will stabilize modulo n, as well. Write $n = 2^k m$ with m odd. Use the Chinese reminder theorem and induction on m.
3. Use $\varphi(1000) = 100 \cdot 4 = 400$. So
$$7^{9999} \equiv 7^{-1} \pmod{1000}.$$
$1000 = 142 \cdot 7 + 6$ which is equivalent to $1000 = 143 \cdot 7 - 1$. So the answer is 143.
4. 0, 1, 4, 5, 6 and 9 are quadratic residues modulo 10. Thus, 11, 44, 55, 66 and 99 are possible two digits repeats. But any square is congruent to 1 or 0 modulo 4. This leaves 44 and 55. 55 implies that the last digit is 5, but then the square ends with 05. So we are left with 44 which appears for 12^2 and for $38^2 = 1444$. So 444 is also a possible ending. Finally, 4444 reduced modulo 16 (note that 16 is a divisor of 10000) gives 12, which is not a square modulo 16. So 4444 cannot appear.
5. Moving 2001 to the left hand side we see that a is a zero of a polynomial with the constant term -2002. Thus a divides $2002 = 2 \cdot 7 \cdot 11 \cdot 13$. Since 3 divides 2001, argue that $a \equiv 1 \pmod 3$. Next, argue that $a \equiv 1 \pmod 4$ and this should give you $a = 13$...
6. We need to figure out what is a_i modulo 100. Note that $\varphi(100) = 40$. In fact, it is useful to note that 3 has order 20 modulo 100. (Otherwise we would need to reduce modulo 200 which is the LCM of 40 and 100.)
$$a_2 \equiv 27 \pmod{100}$$
$$a_2 \equiv 3^7 \equiv 87 \pmod{100}$$
$$a_3 \equiv 3^7 \equiv 87 \pmod{100}$$
... keeps repeating!
7. There are two similar proofs. I will present one, the other is obtained by reversing the roles of 2 and 3.

   By induction. $n = 1$ is OK. If 3 divides n then, by the induction assumption,
$$\frac{n}{3} = \sum_i m_i$$
where m_i is of the form $2^s 3^t$ and m_i does not divide m_j if $i \neq j$. Then
$$n = \sum_i 3m_i$$
is a desired decomposition of n. Next, notice that the powers of 2: $2, 2^2, 2^3$ are congruent to 2 and 1 modulo 3 in alternating fashion. If 3 does not

divide n, let 2^r be the biggest power of 2 such that $n - 2^r$ is divisible by 3. Notice that $2^r > n/4$. By the induction assumption,

$$\frac{n - 2^r}{3} = \sum_i m_i$$

and

$$n = 2^r + \sum_i 3m_i.$$

It remans to show that 2^r does not divide any m_i. Otherwise, there exists j such that 2^r divides m_j. Then

$$n \geq 2^r + 3m_j \geq 4 \cdot 2^r$$

which contradicts $2^r > n/4$.

8. Hint: write $F(n)$ in a closed formula.
9. If $\alpha = m/n$ then $\cos(n\alpha\pi) = \pm 1$. Next, $\cos(nx)$ is the real part of $(\cos x + i \sin x)^n$ which is equal to

$$\cos^n x - \begin{pmatrix} n \\ 2 \end{pmatrix} \cos^{n-2} x \cdot \sin^2 x + \cdots$$

Using $\sin^2 x = 1 - \cos^2 x$ one easily sees that $\cos(nx) = T_n(\cos x)$ where T_n is a polynomial of degree n with integer coefficients and the leading coefficient 2^{n-1}. Thus $T_n(1/3) \pm 1 = 0$. This implies that 3 divides 2^{n-1}. A contradiction.
10. If $n^4 + 4^n$ is an odd prime, then $n = 2k + 1$.

$$4^n + n^4 = (2^n + n^2)^2 - (2^{k+1}n)^2 = (2^n + n^2 + 2^{k+1}n)(2^n + n^2 - 2^{k+1}n).$$

The smaller factor is $2^n + n^2 - 2^{k+1}n$ which is at least 5.
11. Notice that the polynomial almost satisfies Eisenstein's criterion. In fact, the same argument, as in the proof of Eisenstein's criterion, will give you that $P(x)$ cannot be factored as a product of two polynomials of degree greater or equal to 2. Thus it suffices to check that $P(x)$ does not have degree one factors. But this is equivalent to checking that there are no integer zeroes. The only possible integer zeros are ± 1 and ± 3 and these are easily eliminated.
12. I will show that $c_n r$ is an integer. Other cases are similar. Write $r = p/q$ where p and q are relatively prime. Then the equation $P(r) = 0$ can be rewritten as

$$c_n r^n = -c_{n-1} r^{n-1} - c_{n-2} r^{n-2} - \cdots .$$

Substitute $r = p/q$ and clear the denominators to get

$$c_n p^n = -q(c_{n-1} p^{n-1} + c_{n-2} p^{n-2} q + \cdots).$$

Since p and q are relatively prime, the factor p^{n-1} on the left hand side must divide $c_{n-1}p^{n-1} + c_{n-2}p^{n-2}q + \ldots$. Thus $c_n p = qD$ for some integer D, which means that $c_n r = D$.
13. Use solutions to Pythagorean triples.

14. We shall rewrite $n^2+(n+1)^2=y^2$ as a Pell equation. To do so, we shall complete the left hand side to a square:
$$n^2+(n+1)^2=2n^2+2n+1=2(n^2+n+\frac{1}{4}-\frac{1}{4})+1=2(n+\frac{1}{2})^2+\frac{1}{2}.$$
Multiplying both sides by 2, the equation $n^2+(n+1)^2=y^2$ can be rewritten as
$$(2n+1)^2-2y^2=-1.$$
The first solution of the Pell equation $x^2-2y^2=-1$ is $(1,1)$ so every solution is $x+y\sqrt{2}=(1+\sqrt{2})^{2m+1}$ (an odd power). For example,
$$(1+\sqrt{2})^3=7+5\sqrt{2} \text{ and } (1+\sqrt{2})^5=41+29\sqrt{2}$$
which give solutions (of the starting problem) $3^2+4^2=5^2$ and $20^2+21^2=29^2$.
15. Apply continued fractions to $\sqrt{61}+7$.
16. Notice that the equation is equivalent to $n^2-nm-m^2=1$ or $n^2-nm-m^2=-1$. In ether case $n>m$ or, if $n=m$, then $(n,m)=(1,1)$. Furthermore, if a pair (n,m) satisfies $n^2-nm+m^2=1$ or $=-1$ then the pair $(m,n-m)$ satisfies $m^2-m(n-m)-(n-m)^2=-1$ or $=1$, respectively. (Conversly, if (n,m) is a solution, then so is $(n+m,n)$.) So, as long as $n>m$, we can find a smaller solution by this process. The process terminates with the pair $(1,1)$. It follows that any solution is obtained from $(1,1)$:
$$(1,1),(2,1),(3,2),(5,3),\dots,(F_n,F_{n-1}),$$
where F_n is the n-th Fibonacci number. The largest two consecutive Fibonacci numbers less then or equal to 1981 are 987 and 1597, so the answer to our question is 987^2+1597^2.

Of course, the trick used to solve the problem is not easy to figure out. However, completing n^2-nm to a square gives
$$n^2-nm=n^2-nm+\frac{m^2}{4}-\frac{m^2}{4}=(n-m)^2-\frac{m^2}{4}.$$
It follows that our equation is equivalent to the Pell equation
$$x^2-5y^2=\pm 1$$
which has $1/2+\sqrt{5}/2$ as a fundamental solution. The $k+1$-st solution of the equation is obtained from k-th by
$$(x_{k+1}+y_k\sqrt{5})=(\frac{1}{2}+\frac{\sqrt{5}}{2})(x_k+y_k\sqrt{5})$$
which translates into replacing (n,m) by $(n+m,n)$.
17. Hint: relate to a Pell equation.
18.

8. Binomial coefficients

In this handout we will discuss the Binomial Theorem, binomial coefficients, and some combinatorics that goes along.

The binomial coefficients are defined as

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

For example $\binom{n}{0} = 1$, $\binom{n}{1} = n$, $\binom{n}{k} = \binom{n}{n-k}$. The fundamental relation is

$$\binom{n+1}{k} = \binom{n}{k} + \binom{n}{k-1}$$

which can be used to define the binomial coefficients recursively. This also shows that binomial coefficients are integers, a fact which is not completely obvious from the definition. The binomial coefficients are usually arranged in the *Pascal triangle*.

Combinatorially, $\binom{n}{k}$ is the number of k-element subsets of an n-element set. Equivalently, $\binom{n}{k}$ is the number of sequences consisting of k 0's and $n-k$ 1's.

The Binomial Theorem. The Binomial Theorem says that

$$(1+x)^n = \sum_{k=0}^{n} \binom{n}{k} x^k \tag{4}$$

This can be used to derive identities among the binomial coefficients. E.g. plugging in $x = 1$ and $x = -1$ gives:

$$\binom{n}{0} + \binom{n}{1} + \binom{n}{2} + \cdots = 2^n$$
$$\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \cdots = 2^{n-1}$$
$$\binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \cdots = 2^{n-1}$$

Other useful identities can be obtained by plugging in other roots of unity. For example, try $x = \pm i$. See Problems 4 and 5.

More generally, one can differentiate (4) and then substitute specific values for x to obtain interesting identities among the binomial coefficients. For example, for $x = 1$ one obtains

$$\sum_{i=0}^{n} k \binom{n}{k} = n2^{n-1}$$

One can also differentiate twice and then substitute etc. See Problem 1.

Counting paths. Let $m, n \geq 0$ be integers. Consider the grid consisting of $m \times n$ city blocks, from 0^{th} North to n^{th} North and from 0^{th} East to m^{th} East. Consider all paths from the origin to (m, n) of length $m + n$. The number of such paths is $\binom{m+n}{m}$. We can break the set of these paths into disjoint collections and obtain new identities.

Example. Fix a North-South Street, e.g. r^{th} East ($r = 1, \cdots, m$). Break up the set of all paths from $(0, 0)$ to (m, n) according to the first place where the path arrives at this street. For $k = 0, 1, \cdots, n$ the number of paths from $(0, 0)$ to (r, k) that pass through $(r - 1, k)$ is $\binom{r+k-1}{k}$, and the number of paths from (r, k) to (m, n) is $\binom{m+n-r-k}{n-k}$ so we get

$$\binom{m+n}{n} = \sum_{k=1}^{n} \binom{r+k-1}{k}\binom{m+n-r-k}{n-k}$$

Example. Now use the place where the path crosses the diagonal $k+l = r$ to break up the set of paths ($r = 1, 2, \cdots, m + n - 1$). The number of paths from $(0, 0)$ to $(k, r - k)$ is $\binom{r}{k}$ and the number of paths from $(k, r - k)$ to (m, n) is $\binom{m+n-r}{m-k}$. So we obtain the identity

$$\binom{m+n}{n} = \sum_{k=0}^{r} \binom{r}{k}\binom{m+n-r}{m-k}$$

Divisibility. What is the highest power of a prime p that divides $n!$? Every multiple of p which is $\leq n$ (i.e. $p, 2p, 3p, \cdots, [\frac{n}{p}]p$) will contribute a factor p. Moreover, multiples of p^2 will contribute an additional factor, multiples of p^3 yet one more, etc. We conclude that the answer is

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots$$

where $[q]$ stands for the largest integer which is $\leq q$.

Example. In how many 0's does $\binom{100}{49}$ end? We need to compute the largest powers of 2 and 5 that divide $\binom{100}{49}$. The answer is lower for 5, and this is the number of 0's we are looking for. The power of 5 that divides 100! is

$$\left[\frac{100}{5}\right] + \left[\frac{100}{25}\right] = 20 + 4 = 24$$

The power that divides 49! is

$$\left[\frac{49}{5}\right] + \left[\frac{49}{25}\right] = 9 + 1 = 10$$

and the power that divides 51! is

$$\left[\frac{51}{5}\right] + \left[\frac{51}{25}\right] = 10 + 2 = 12$$

So the answer is $24 - 10 - 12 = 2$, i.e. $\binom{100}{49} = \frac{100!}{49!51!}$ ends with 2 zeros.

Lucas's Theorem.

THEOREM (Lucas (1887)). *Let $m \geq n \geq 0$, and let p be a prime. Represent m and n in base p as $m = m_k m_{k-1} \cdots m_0$ and $n = n_k n_{k-1} \cdots n_0$, i.e.*

$$m = m_0 + m_1 p + m_2 p^2 + \cdots + m_k p^k$$

and

$$n = n_0 + n_1 p + n_2 p^2 + \cdots + n_k p^k$$

where $0 \leq m_i, n_i \leq p - 1$. Then

$$\binom{m}{n} \equiv \binom{m_0}{n_0}\binom{m_1}{n_1}\binom{m_2}{n_2} \cdots \binom{m_k}{n_k} \pmod{p}$$

where we take $\binom{m_r}{n_r} = 0$ if $m_r < n_r$.

The following proof is due to N.J. Fine from *American Mathematical Monthly, Vol. 54, No. 10, Part 1 (Dec 1947), 589-592.* If you have never read a math paper, this one might be a good start. It's also available online through JSTOR. Make sure all the steps make sense in this proof.

PROOF.

$$\begin{aligned}
\sum_{n=0}^{m} \binom{m}{n} x^n =& (1+x)^m = \prod_{r=0}^{k} \left((1+x)^{p^r} \right)^{m_r} \\
\equiv& \prod_{r=0}^{k} (1 + x^{p^r})^{m_r} \pmod{p} \\
=& \prod_{r=0}^{k} \Big(\sum_{s_r=0}^{m_r} \binom{m_r}{s_r} x^{s_r p^r} \Big)
\end{aligned}$$

For the second line above one needs to note that $[\frac{p^r}{i}] \geq [\frac{k}{i}] + [\frac{p^r - k}{i}]$ with strict inequality when $i = p^r$ and $0 < k < p^r$. Now consider the coefficient of x^n. On the one hand, it is $\binom{m}{n}$ from the leftmost expression we started with. On the other hand, from the last expression, it is the sum of

$$\prod_{r=0}^{k} \binom{m_r}{s_r}$$

where $(s_0, \cdots, s_k)$ range over all possible tuples such that $0 \leq s_r \leq m_r (< p)$ and $s_0 + s_1 p + s_2 p^2 + \cdots + s_k p^k = n$. There is only one such tuple, namely $s_r = n_r$. $\square$

Problems 7-10 are related to Lucas's theorem. For more about Fine's paper see Problem 9.

Problems.

The problems are arranged roughly in order of increasing difficulty.

1. (A5, 1962) Find $\binom{n}{1}1^2 + \binom{n}{2}2^2 + \binom{n}{3}3^2 + \cdots + \binom{n}{n}n^2$.
2. (A4, 1974) Find $\frac{1}{2^{n-1}} \sum_{i=1}^{[n/2]} (n-2i)\binom{n}{i}$.
3. (A2, 1965) Let $k = [(n-1)/2]$. Prove that $\sum_{r=0}^{k} \left(\frac{n-2r}{n}\right)^2 \binom{n}{r}^2 = \frac{1}{n}\binom{2n-2}{n-1}$.
4. Evaluate
$$\binom{n}{0} + \binom{n}{4} + \binom{n}{8} + \cdots$$
5. Evaluate
$$\binom{n}{0} + \binom{n}{3} + \binom{n}{6} + \cdots$$
6. Evaluate
$$\binom{n}{0}^2 + \binom{n}{1}^2 + \binom{n}{2}^2 + \cdots + \binom{n}{n}^2$$
7. (A5, 1977) p is a prime and $m \geq n$ are non-negative integers. Show that $\binom{pm}{pn} \equiv \binom{m}{n} \pmod{p}$.
8. Show that $\binom{2p}{p} \equiv 2 \pmod{p^2}$ for any prime p.
9. Let $m > 0$ and p a prime. Suppose m is represented in base p as $m_k m_{k-1} \cdots m_0$ as in the discussion of Lucas's theorem.
   (a) Show that the number of integers n with $0 \leq n \leq m$ such that $\binom{m}{n} \not\equiv 0 \pmod{p}$ is $\prod_{r=0}^{k}(m_r + 1)$.
   (b) All binomial coefficients $\binom{m}{n}$ with $0 < n < m$ are divisible by p if and only if m is a power of p.
   (c) None of the binomial coefficients $\binom{m}{n}$ with $0 \leq n \leq m$ are divisible by p if and only if all $m_r = p-1$, $r = 0, 1, \cdots, k-1$.
10. (B4, 1991) p is an odd prime. Prove that
$$\sum_{n=0}^{p} \binom{p}{n}\binom{p+n}{n} \equiv 2^p + 1 \pmod{p^2}$$
11. (B2, 2000) m and n are positive integers with $m \leq n$. d is their greatest common divisor. Show that $\frac{d}{n}\binom{n}{m}$ is integral.
12. (B4, 1965) Define $f_n : \mathbb{R} \to \mathbb{R}$ by
$$f_n(x) = \frac{\binom{n}{0} + \binom{n}{2}x + \binom{n}{4}x^2 + \cdots}{\binom{n}{1} + \binom{n}{3}x + \binom{n}{5}x^2 + \cdots}$$
Find a formula for $f_{n+1}(x)$ in terms of $f_n(x)$ and x, and determine $\lim_{n\to\infty} f_n(x)$ for all real x.
13. (A1, 1972) Show that we cannot have 4 binomial coefficients $\binom{n}{m}$, $\binom{n}{m+1}$, $\binom{n}{m+2}$, $\binom{n}{m+3}$ with $n, m > 0$ and $m + 3 \leq n$ in arithmetic progression.
14. (B5, 1976) Find $\sum_{i=0}^{n}(-1)^i\binom{n}{i}(x-i)^n$.
15. (B2, 1987) Let n, r, s be non-negative integers with $n \geq r + s$. Prove that
$$\sum_{i=0}^{s} \frac{\binom{s}{i}}{\binom{n}{r+i}} = \frac{n+1}{(n+1-s)\binom{n-s}{r}}$$

16. Show that $\binom{n}{0} + \binom{n+1}{1} + \cdots + \binom{n+k}{k} = \binom{n+k+1}{k}$.
17. (A1, 2003) Find the number of ways of writing a positive integer n as a sum of positive integers. Sums with differently ordered terms are considered different. For example, if $n = 3$ then there are 4 possible sums:

$$3, 1+1+1, 1+2, 2+1$$

18. Define a *selfish* set to be a set which has its own cardinality (number of elements) as an element. Find, with proof, the number of subsets of $\{1, 2, 3, \cdots, n\}$ which are minimal selfish sets, that is, selfish sets none of whose proper subsets is selfish. Hint: Fibonacci numbers.
19. Find $F_1\binom{n}{0} + F_2\binom{n}{1} + F_3\binom{n}{2} + \cdots + F_{n+1}\binom{n}{n}$ where $F_1, F_2, \cdots$ are the Fibonacci numbers $1, 1, 2, 3, 5, 8, 13, \cdots$.

Hints and Solutions.

1. Differentiate the binomial formula twice and put $x = 1$.
2. $i\binom{n}{i} = n\binom{n-1}{i-1}$.
3. Similar, but goes one step further. Use $r(r-1)\binom{n}{r} = n(n-1)\binom{n-2}{r-2}$.
4. In the binomial theorem put $x = 1, -1, i, -i$ and then take a suitable linear combination of the resulting expressions.
5. Similar, but plug in the 3^{rd} roots of 1.
6. Special case $m = n = r$ of the second example. Alternatively, consider the coefficient of x^n in $(\binom{n}{0} + \binom{n}{1}x + \binom{n}{2}x^2 + \cdots + \binom{n}{n}x^n)(\binom{n}{n} + \binom{n}{n-1}x + \binom{n}{n-2}x^2 + \cdots + \binom{n}{0}x^n) = (1+x)^{2n}$.
7. Lucas's theorem.
8. Note that the weaker claim that $\binom{2p}{p} \equiv 2 \pmod p$ follows from Lucas's theorem. We have $\binom{2p}{p} = \frac{2p\cdot(2p-1)\cdots(p+1)}{p!} = 2\frac{(2p-1)\cdots(p+1)}{(p-1)!}$. The numbers in the numerator are $p+(p-1), p+(p-2), \cdots, p+1$. After multiplying out we have one term with no p-factors, namely $(p-1)!$ and this contributes 1 after dividing with $(p-1)!$. There are also $(p-1)$ terms with a single p-factor, namely $p(p-1)!k^{-1}$ for $k = 1, 2, \cdots, p-1$. After dividing by $(p-1)!$ and noticing that $\pmod p$ the numbers $1^{-1}, 2^{-1}, \cdots, (p-1)^{-1}$ form a permutation of $1, 2, \cdots, p-1$ we see that the sum $\pmod{p^2}$ is $p\frac{p(p-1)}{2}$ which is divisible by p^2.
9. Follows with some work from Lucas's theorem. If you get stuck look at Fine's paper referenced in the text. Fine goes on to show that the probability that a randomly chosen binomial coefficient is divisible by p is 1.
10. Recall that $2^p = \sum_{n=0}^{p}\binom{p}{n}$. So the congruence can be rewritten as

$$\sum_{n=0}^{p}\binom{p}{n}\left(\binom{p+n}{n} - 1\right) \equiv 1 \pmod{p^2}$$

Now argue that each term on the left is divisible by p^2 except when $n = p$ when it is 1 (mod p^2) (see Problem 8). You will need Lucas's theorem for the second factor.

11. It suffices to show that $\frac{n}{n}\binom{n}{m}$ and $\frac{m}{n}\binom{n}{m}$ are integral. The first number is $\binom{n}{m}$ and the second is $\binom{n-1}{m-1}$.
12. $f_{n+1}(x) = \frac{f_n(x)+x}{f_n(x)+1}$. From the binomial theorem we see

$$f_n(x) = \sqrt{x}\frac{(1+\sqrt{x})^n + (1-\sqrt{x})^n}{(1+\sqrt{x})^n - (1-\sqrt{x})^n}$$

for $x \neq \pm 1$. When $x > 0$ then $\left|\frac{1-\sqrt{x}}{1+\sqrt{x}}\right| < 1$ and we see that $\lim_n f_n(x) = \sqrt{x}$. When $x = 1$ then $f_n(1) = 1$ so $\lim_n f_n(1) = 1$, and when $x = 0$ then $f_n(0) = \frac{1}{n}$ so that $\lim_n f_n(0) = 0$. For $x < 0$ the limit does not exist. This can be seen by taking $\sqrt{x}$ to be a purely imaginary number and considering $\frac{(1+\sqrt{x})^n+(1-\sqrt{x})^n}{(1+\sqrt{x})^n-(1-\sqrt{x})^n}$ in the complex plane.

13. If $\binom{n}{m}, \binom{n}{m+1}, \binom{n}{m+2}$ form an arithmetic progression then $\binom{n}{m} + \binom{n}{m+2} = 2\binom{n}{m+1}$ and this simplifies to a quadratic equation in m (if we view n as being fixed). The equation is

$$4m^2 + (8-4n)m + (n^2 - 5n + 2) = 0$$

Now if we had an arithmetic progression as above consisting of 4 terms, then this equation would have two roots, say m_1 and m_2, that differ by 1. The difference of the two roots of a quadratic equation $ax^2 + bx + c = 0$ is 1 when $\frac{\sqrt{b^2-4ac}}{2a} = \frac{1}{2}$ so we get the condition that $b^2 - 4ac = a^2$. In our case this means

$$(8-4n)^2 - 16(n^2 - 5n + 2) = 16$$

which gives $n = -1$, and this is absurd.

14. Answer: $n!$.

First Solution. The coefficient of x^{n-m} is $(-1)^m\binom{n}{m}\sum_{i=0}^{n}(-1)^i\binom{n}{i}i^m$. The sum can be thought of as $(x\frac{d}{dx})^m(1-x)^n$ evaluated at $x = 1$. When $m < n$ this gives 0 since $(x\frac{d}{dx})^m(1-x)^n$ will consist of summands each term of which has $1-x$ as a factor. When $m = n$ there is one term that does not have $(1-x)$ as a factor, and it is $(-1)^n x^n n!$ and it evaluates to $(-1)^n n!$.

Second Solution. Define the operator Δ on polynomials by $\Delta(p(x)) = p(x) - p(x-1)$. If p is a polynomial of degree n and leading term ax^n then $\Delta(p(x))$ has degree $n-1$ and leading term nax^{n-1}. The expression in the problem is just $\Delta^n(x^n)$ so this is $n!$.

15. **First Solution.** Put $F(r,s,n) = \sum_{i=0}^{s}\frac{\binom{s}{i}}{\binom{n}{r+i}}$ and show that $F(r,s,n) = F(r,s-1,n) + F(r+1,s-1,n)$. Then argue by induction on s.

Second Solution. We have the combinatorial identity from the text

$$\sum_{i=0}^{s} \binom{r+i}{r}\binom{n-r-i}{n-s-r} = \binom{n+1}{s}$$

corresponding to the first place where a path from $(0,0)$ to $(n+1-s, s)$ hits column $r+1$. Now check the identity

$$\frac{\binom{s}{i}\binom{n-s}{r}}{\binom{n}{r+i}} = \frac{\binom{r+i}{r}\binom{n-r-i}{n-s-r}}{\binom{n}{s}}$$

by writing out in terms of factorials and canceling.

9. Probability

Probability is done in a *probability space*.[14] On the Putnam exam there are two kinds of probability spaces that come up: finite sets and geometric figures. The measure assigns a number to certain kinds of subsets of a measure space. In the case of finite sets one usually takes the proportion of elements, i.e. a subset with k elements of an n element set has measure (or *probability*) k/n. With geometric figures one takes the proportion of length, or area, or volume etc.

These subsets are also referred to as *events* and the probability of an event A is denoted by $P(A)$. If two events A and B are disjoint, then $P(A \cup B) = P(A) + P(B)$. Two events A and B are *independent* if $P(A \cap B) = P(A)P(B)$. This means that if we restrict to the probability space A (after rescaling the measure) the probability of $A \cap B$ is the same as the probability of B in the original space.

If F is a function on the measure space, the *expected value* of F is the average value of F. The meaning is clear on finite sets; on geometric figures one takes the integral of F and divides by the length (area, volume) of the figure.

I am not featuring any techniques in this introduction, but in return the solutions are somewhat more detailed than usual (with the exception of #8, which we did in class earlier).

Geometry Problems.

1. (1961, B2) Two points are selected independently and at random from a segment of length b. What is the probability that they are at least a distance $a < b$ apart?
2. (1985, B4) Let C be the circle of radius 1, centered at the origin. A point P is chosen at random on the circumference of C, and another point Q is chosen at random in the interior of C. What is the probability that the rectangle with diagonal PQ, and sides parallel to the x-axis and y-axis, lies entirely inside (or on) C?
3. (1992, A6) Four points are chosen independently and at random on the surface of a sphere (using the uniform distribution). What is the probability that the center of the sphere lies inside the resulting tetrahedron?
4. (1993, B3) x and y are chosen at random (with uniform density) from the interval $(0, 1)$. What is the probability that the closest integer to x/y is even?

[14] a measure space with total measure 1

5. (2006, A6) Four points are chosen uniformly and independently at random in the interior of a given circle. Find the probability that they are the vertices of a convex quadrilateral.

Combinatorial Problems.

6. (1993, B2) A deck of $2n$ cards numbered from 1 to $2n$ is shuffled and n cards are dealt to A and B. A and B alternately discard a card face up, starting with A. The game ends when the sum of the discards is first divisible by $2n+1$, and the last person to discard wins. What is the probability that A wins if neither player makes a mistake?
7. (1989, A4) A player plays the following game. At each turn a fair coin is tossed (probability 1/2 of heads, and all tosses are independent), and, depending on the results of the tosses to date, (1) the game ends and the player wins, (2) the game ends and the player loses, or (3) the coin is tossed again. Given an irrational p in the interval $(0,1)$, can we find a rule such that (A) the player wins with probability p, and (B) the game ends after a finite number of tosses with probability 1?
8. (1960, A6) A player throws a fair die (prob 1/6 for each of $1,2,3,4,5,6$ and each throw independent) repeatedly until his total score is $\geq n$. Let $p(n)$ be the probability that his final score is n. Find $p = \lim_{n\to\infty} p(n)$.
9. (2004, A5) An $m \times n$ checkerboard is colored randomly: each square is independently assigned red or black with probability 1/2. We say that two squares, p and q, are in the same connected monochromatic component if there is a sequence of squares, all of the same color, starting at p and ending at q, in which successive squares in the sequence share a common side. Show that the expected number of connected monochromatic regions is greater than $mn/8$.
10. (1995, A6) Each of the n triples (r_i, s_i, t_i) is a randomly chosen permutation of $(1,2,3)$ and each triple is chosen independently. Let p be the probability that each of the three sums $\sum r_i$, $\sum s_i$, $\sum t_i$ equals $2n$, and let q be the probability that they are $2n-1$, $2n$, $2n+1$ in some order. Show that for some $n \geq 1995$, $4p \leq q$.

Abstract Probability Problems.

11. (2002, B1) An event is a hit or a miss. The first event is a hit, the second is a miss. Thereafter the probability of a hit equals the proportion of hits in the previous trials (so, for example, the probability of a hit in the third trial is 1/2). What is the probability of exactly 50 hits in the first 100 trials?
12. (2001, A2) You have a set of n biased coins. The m^{th} coin has probability $1/(2m+1)$ of landing heads $(m = 1,2,...,n)$ and the results for each coin are independent. What is the probability that if each coin is tossed once, you get an odd number of heads?
13. (1976, B3) Let $0 < a < 1/4$. Define the sequence p_n by $p_0 = 1$, $p_1 = 1-a$, $p_{n+1} = p_n - ap_{n-1}$. Show that if each of the events $A_1, A_2, ..., A_n$ has probability at least $1-a$, and for all i A_i is independent from $A_1 \cap A_2 \cap$

$\cdots \cap A_{i-2}$, then the probability of $A_1 \cap A_2 \cap \cdots \cap A_n$ is at least p_n. You may assume that all p_i are positive.

Problems without solutions.

14. (2005, A6) Let n be given, $n \geq 4$, and suppose that $P_1, P_2, \cdots, P_n$ are n randomly, independently and uniformly, chosen points on a circle. Consider the convex n-gon whose vertices are the P_i. What is the probability that at one of the vertex angles of this polygon is acute?
15. (2002, B4) An integer n, unknown to you, has been randomly chosen in the interval $[1, 2002]$ with uniform probability. Your objective is to select n in an odd number of guesses. After each incorrect guess, you are informed whether n is higher or lower, and you must guess an integer on your next turn among the numbers that are still feasibly correct. Show that you have a strategy so that your chance of winning is greater than $2/3$.

Hints and Solutions.

1. The two numbers (x, y) represent a point in the square $[0, b] \times [0, b]$. The region $|x - y| \geq a$ consists of two triangles bounded by $x - y = a$ and $x - y = -a$ of total area $(b - a)^2$. So the probability is $(b - a)^2/a^2$.
2. This calculation takes place inside $\mathbb{R}^4$ (in C times the disk). It will be simpler to let P be a randomly chosen point of C *in the first quadrant*. It's clear by symmetry that this doesn't change the answer. The key observation is that once P is chosen, then the rectangle with diagonal PQ is inside the circle iff Q belongs to the rectangle R inscribed in C with sides parallel to the axes and with one vertex at P. If $P = (\cos t, \sin t)$ then the area of R is $4 \cos t \sin t$, so the probability of choosing Q that works is
$$\frac{4 \cos t \sin t}{\pi}$$
The desired probability is then obtain by averaging over all choices of P, i.e. it is
$$\frac{2}{\pi} \int_0^{\pi/2} \frac{4 \cos t \sin t}{\pi} dt = \frac{2}{\pi^2} \int_0^{\pi/2} \sin 2t d(2t) =$$
$$= \frac{2}{\pi^2} \int_0^{\pi} \sin u du = \frac{2}{\pi^2} [-\cos u]|_0^{\pi} = \frac{4}{\pi^2}.$$
3. Place the first 3 points A, B, C. These points determine a spherical triangle. Extend the sides of this triangle to get 3 great circles. The 3 circles divide the sphere into 8 triangles, one of which is ABC. The center is in the tetrahedron $ABCD$ iff the fourth point D belongs to the opposite triangle $A'B'C'$ from ABC. Since all 8 triangles are equally likely to arise, the expected fraction of the area of the sphere for a random spherical triangle is $1/8$.
4. The set of (x, y) with x/y closer to $2n$ ($n > 0$) than to any other integer is the triangle bounded by lines $x/y = 2n - 1/2$ and $x/y = 2n + 1/2$. The

area of this triangle is $\frac{1}{4n-1} - \frac{1}{4n+1}$. For $n = 0$ the area is $1/4$. So the probability is

$$\frac{1}{4} + \frac{1}{3} - \frac{1}{5} + \frac{1}{7} - \frac{1}{9} + \cdots$$

Recalling that $\pi/4 = 1-1/3+1/5-1/7+\cdots$, the probability is $(5-\pi)/4$.

5.

6. The probability is 0, i.e. B always wins. Note that each player knows where all the cards are. For every card B can play, A has at most one card that can win at the next move, and different cards from B require different winning cards from A. But since at every move B has more cards than A, by the pigeon-hole principle he must have a card for which A does not have a winning card. Since the sum of all cards is divisible by $2n+1$ the game must end, at the latest when all the cards are played.

7. Write p in the binary system, as a number like 0.110010...; call it $p = 0.p_1p_2p_3\cdots$. The game consists of tossing a fair coin and stopping the first time heads turn up, say at toss n. Then the player wins if the n^{th} digit is 1, and loses if it is 0. The game ends with probability 1, since the probability that it does not end after n tosses is $1/2^n \to 0$. The probability that the player wins is

$$(1/2)p_1 + (1/2)^2p_2 + (1/2)^3p_3 + \cdots = p$$

8. Let $p_i(n)$ be the probability that the player stops at $n+i$ $(i = 0, 1, \cdots, 5)$. So $p(n) = p_0(n)$. Note that

$$\begin{aligned}
p_5(n) =& \frac{1}{6}p(n-1)\\
p_4(n) =& \frac{1}{6}p(n-1) + \frac{1}{6}p(n-2)\\
p_3(n) =& \frac{1}{6}p(n-1) + \frac{1}{6}p(n-2) + \frac{1}{6}p(n-3)\\
p_2(n) =& \frac{1}{6}p(n-1) + \frac{1}{6}p(n-2) + \frac{1}{6}p(n-3) + \frac{1}{6}p(n-4)\\
p_1(n) =& \frac{1}{6}p(n-1) + \frac{1}{6}p(n-2) + \frac{1}{6}p(n-3) + \frac{1}{6}p(n-4) + \frac{1}{6}p(n-5)
\end{aligned}$$

By adding and taking into account that $p_0(n)+p_1(n)+\cdots+p_5(n) = 1$ we have

$$1 = p(n) + \frac{5}{6}p(n-1) + \frac{4}{6}p(n-2) + \frac{3}{6}p(n-3) + \frac{2}{6}p(n-4) + \frac{1}{6}p(n-5)$$

Letting $n \to \infty$ we get $1 = (1 + \frac{5}{6} + \frac{4}{6} + \frac{3}{6} + \frac{2}{6} + \frac{1}{6})p$ so $p = 2/7$.

This argument assumes that the limit exists. This fact can be proved separately from the recursion

$$p(n) = \frac{1}{6}\Big(p(n-1) + p(n-2) + p(n-3) + p(n-4) + p(n-5) + p(n-6)\Big)$$

One argument is to consider $m(n) = \min(p(n-1), p(n-2), p(n-3), p(n-4), p(n-5), p(n-6))$ and $M(n) = \max(p(n-1), p(n-2), p(n-3), p(n-$

4), $p(n-5), p(n-6))$. Then the recursion, which is kind of an averaging process, implies that $m(n)$ is monotonically increasing, while $M(n)$ is monotonically decreasing. Each sequence is clearly bounded, so the limits m, M exist. It remains to show $m = M$. Think about what $p(n)$ would look like if $m < M$.

9. Add squares one by one, starting at the top left and filling rows from the top to the bottom one at a time. Argue that the expected number of components on the first k squares is at least $k/8$. When adding a square in the top row or the left column the expected number of components increases by $1/2$, and otherwise by $\geq 1/8$.
10. It is convenient to subtract 2 from the numbers $1, 2, 3$ so we are adding a permutation of $(-1, 0, 1)$ at every step. This is then a random walk in the hexagonal lattice $x + y + z = 0$. Let a_n be the probability of returning to the origin after n steps, and b_n the probability of returning to a node adjacent to the origin after n steps. We have $a_{n+1} = b_n/6$ and $b_{n+1} \geq a_n + b_n/3$. If for some n we have $a_n > b_n/4$ then $b_{n+1} > b_n/4 + b_n/3 = 7b_n/12 = 3.5a_{n+1}$ and this is not quite enough since we want $4a_{n+1}$ at the end. So we look at the probability c_n of returning to one of the 6 vertices adjacent to precisely 2 neighbors of the origin. Then the (in)equalities are:

$$\begin{aligned} a_{n+1} &= \frac{b_n}{6} \\ b_{n+1} &\geq a_n + \frac{b_n}{3} + \frac{c_n}{3} \\ c_{n+1} &\geq \frac{b_n}{3} \end{aligned}$$

and we have, assuming $a_n > b_n/4$:

$$b_{n+1} > \frac{b_n}{4} + \frac{b_n}{3} + \frac{b_{n-1}}{9} = \frac{7b_n}{12} + \frac{2a_n}{3} > \frac{7a_{n+1}}{2} + \frac{b_n}{6} = \frac{7a_{n+1}}{2} + a_{n+1} = 4.5a_{n+1}$$

Thus we have $a_n \leq b_n/4$ for at least one of any two consecutive values of n.
11. Start by computing for small n. For $n = 3$ we have $P(HMH) = 1/2$ and $P(HMM) = 1/2$ so $P(1\text{hit}) = P(2\text{hits}) = 1/2$. For $n = 4$ it's $P(HMHH) = (1/2)(2/3) = 1/3$, $P(HMHM) = (1/2)(1/3) = 1/6$, $P(HMMH) = (1/2)(1/3) = 1/6$, $P(HMMM) = (1/2)(2/3) = 1/3$, so $P(1\text{hit}) = 1/3$, $P(2\text{hits}) = 1/6 + 1/6 = 1/3$, $P(3\text{hits}) = 1/3$. Work it out for $n = 5$ – you'll find that $P(k \text{ hits}) = 1/4$ for $k = 1, 2, 3, 4$. So now we conjecture that for any n and any $1 \leq k \leq n-1$ the probability of k hits after n events is $1/(n-1)$. Prove this by induction. The calculation is

$$\frac{1}{n-1}\frac{n-k}{n} + \frac{1}{n-1}\frac{k-1}{n} = \frac{1}{n}$$

12. The trick is to consider the expansion of

$$\Big(\frac{2}{3}-\frac{1}{3}\Big)\Big(\frac{4}{5}-\frac{1}{5}\Big)\cdots\Big(\frac{2n}{2n+1}-\frac{1}{2n+1}\Big)$$

and note that the positive terms correspond to an even number of heads and the negative terms to an odd number of heads. So this expression is just $P(\text{even}) - P(\text{odd})$. But this is a telescoping product and equals $\frac{1}{2n+1}$. Since $P(\text{even}) + P(\text{odd}) = 1$ we see that $P(\text{odd}) = \frac{n}{2n+1}$.

13. Let $q_n = P(A_1 \cap \cdots \cap A_n)$. Since

$$A_1 \cap \cdots \cap A_n = A_1 \cap \cdots \cap A_n \cap A_{n+1} \bigsqcup A_1 \cap \cdots \cap A_n \cap A_{n+1}^c$$

and the latter set is contained in

$$A_1 \cap \cdots \cap A_{n-1} \cap A_{n+1}^c$$

we have

$$q_n \le P(A_1 \cap \cdots \cap A_n \cap A_{n+1}) + P(A_1 \cap \cdots \cap A_{n-1} \cap A_{n+1}^c) = q_{n+1} + aq_{n-1}$$

by the independence assumption. Say $q_{n+1} = q_n - aq_{n-1} + b_{n+1}$ for $b_{n+1} \ge 0$. Now prove by induction on n that

$$q_n = p_n + p_{n-2}b_1 + p_{n-3}b_2 + ... + p_0 b_{n-1} + b_n$$

so that $q_n \ge p_n$.

10. Recursive Sequences

In this handout we will discuss sequences defined recursively and their convergence.

Linear recursions. Let u, v be fixed numbers and the sequence $a_0, a_1, a_2, \cdots$ satisfies

$$a_{n+2} = ua_{n+1} + va_n$$

for $n \geq 0$. How do we find a closed formula for a_n? The recipe is this. Consider the *characteristic equation*

$$t^2 = ut + v$$

and assume its solutions are $t_1 \neq t_2$. Then the sequence has the form

$$a_n = At_1^n + Bt_2^n$$

with A, B computed from a_0 and a_1. This can be easily proved by induction on n (do it!). However, a better question is, how did we come up with that expression? The answer is, with the help of linear algebra! Consider the sequence of vectors in $\mathbb{R}^2$ given by

$$w_n = \begin{pmatrix} a_n \\ a_{n+1} \end{pmatrix}$$

The recursion relation becomes

$$\begin{pmatrix} 0 & 1 \\ v & u \end{pmatrix} \begin{pmatrix} a_n \\ a_{n+1} \end{pmatrix} = \begin{pmatrix} a_{n+1} \\ a_{n+2} \end{pmatrix}$$

and the "closed form" is

$$w_n = M^n w_0$$

where

$$M = \begin{pmatrix} 0 & 1 \\ v & u \end{pmatrix}$$

Note what happened here. We traded the dependence on the previous two elements in the sequence for the dependence on only one previous element, but at the expense of considering sequences in the plane. We are really iterating an initial vector

$$w_0 = \begin{pmatrix} a_0 \\ a_1 \end{pmatrix}$$

by the linear map given by the matrix M.

Iteration by diagonal matrices is easy, and we recall that most matrices can be diagonalized, including those whose eigenvalues are all distinct. The eigenvalues of M are the roots of the characteristic polynomial, which is $t^2 - ut - v$, so the roots are t_1 and t_2. To diagonalize M means to write it as

$$M = Q \begin{pmatrix} t_1 & 0 \\ 0 & t_2 \end{pmatrix} Q^{-1}$$

for a suitable matrix Q. Now

$$M^n = Q \begin{pmatrix} t_1^n & 0 \\ 0 & t_2^n \end{pmatrix} Q^{-1}$$

Now comparing entries in $w_n = M^n w_0$ gives the claim that $a_n = At_1^n + Bt_2^n$.

PROBLEM. *Find the closed formula for the elements of the Fibonacci sequence* $a_0 = 0$, $a_1 = 1$, $a_{n+2} = a_{n+1} + a_n$.

SOLUTION. Here $u = v = 1$ and the characteristic equation is $t^2 = t + 1$ whose roots are $t_{1,2} = \frac{1 \pm \sqrt{5}}{2}$ so the closed formula is

$$a_n = A\Big(\frac{1 - \sqrt{5}}{2}\Big)^n + B\Big(\frac{1 + \sqrt{5}}{2}\Big)^n$$

where $a_0 = 0$, $a_1 = 1$ implies $A = -\frac{1}{\sqrt{5}}$, $B = \frac{1}{\sqrt{5}}$. Thus

$$a_n = \frac{(1 + \sqrt{5})^n - (1 - \sqrt{5})^n}{2^n \sqrt{5}}$$

Convergence of iteration. Suppose we have a sequence given by $a_{n+1} = F(a_n)$ starting at some initial value a_0 and we would like to determine if the sequence (a_n) converges. If F is continuous then the limit a_∞ (if it exists) will have to satisfy

$$a_\infty = F(a_\infty)$$

i.e. the limit is a fixed point of F. We allow here functions defined on the plane, or on higher dimensional Euclidean spaces, or even on closed subsets of Euclidean spaces.[15]

THEOREM (Contraction Principle). *Let X be the domain of definition of F, and suppose $F(X) \subset X$. Also suppose that for some $C < 1$ we have*

$$||F(x_1) - F(x_2)|| \leq C||x_1 - x_2||$$

for any $x_1, x_2 \in X$. Then F has a unique fixed point $x_0 \in X$ and any iteration sequence a_n that starts with $a_0 \in X$ converges to x_0.

The proof is to show that the sequence (a_n) is Cauchy.

Functions that satisfy the inequality above are called *contractions*. Often, the inequality can be deduced from the Mean Value Theorem by computing the derivative.

There are many variations of the Contraction Principle allowing for the function to have derivative ± 1 at some points. Here is an example. Suppose $F : [a, b] \to [a, b]$ is differentiable and has a fixed point c. Further, suppose $|F'(x)| \leq 1$ for all $x \in [a, b]$ and $|F'(x)| < 1$ when $x \neq c$. Then any iteration sequence converges to c. One way to see this is to use the fact that a monotone bounded sequence converges.

[15]The right assumption is that the domain of definition is a complete metric space.

For other examples where a variation of the Contraction Principle is needed see Problems 3, 6, 7.

The problems include many from old Putnam exams. The first 11 use the methods of the handout (although additional wrinkles appear). Problems 12 and 13 are about solving the recursion, even though it is not linear. The others are unrelated to convergence questions, but involve recursion.

Problems.

1. Let $a_1 \geq 0$ and $a_{n+1} = \sqrt{2 + a_n}$. Prove that the sequence (a_n) converges and find the limit.
2. Let $a_1 = 0$, $a_{2n} = \frac{1}{2}a_{2n-1}$ and $a_{2n+1} = \frac{1}{2} + a_{2n}$. Determine the general term a_n and study the convergence.
3. Let $a_1 \geq 0$ and $a_{n+1} = 1 + \frac{1}{1+a_n}$. Prove that (a_n) converges and find the limit.
4. Let $x_1 = 1$, $y_1 = 2$ and $x_{n+1} = 22y_n - 15x_n$, $y_{n+1} = 17y_n - 12x_n$. Prove that $x_n, y_n \neq 0$ for any n. Prove that there are infinitely many positive and infinitely many negative terms in each sequence (x_n), (y_n). For $n = 2005^{2005}$ determine whether x_n is divisible by 7.
5. Suppose that in the linear recursion $a_{n+2} = ua_{n+1} + va_n$ the two characteristic roots are equal: $t_1 = t_2$. Show that the general term is given by
$$a_n = At_1^n + Bnt_1^n$$
6. (B5, 1960) Define a_n by $a_0 = 0$, $a_{n+1} = 1+\sin(a_n-1)$. Find $\lim(\sum_{i=0}^n a_i)/n$.
7. (A1, 1947) The sequence (a_n) of real numbers satisfies $a_{n+1} = 1/(2-a_n)$. Show that $\lim_{n\to\infty} a_n = 1$.
8. (A6, 1957) Let $\alpha > 1$. Define a_n by $a_1 = \ln\alpha$, $a_2 = \ln(\alpha - a_1)$, $a_{n+1} = a_n + \ln(\alpha - a_n)$. Show that $\lim_{n\to\infty} a_n = \alpha - 1$.
9. (A6, 1953) Show that $\sqrt{7}, \sqrt{7-\sqrt{7}}, \sqrt{7-\sqrt{7+\sqrt{7}}}, \sqrt{7-\sqrt{7+\sqrt{7-\sqrt{7}}}}, \cdots$ converges and find its limit.
10. (A3, 1966) Define the sequence (a_n) by $a_1 \in (0,1)$, and $a_{n+1} = a_n(1-a_n)$. Show that $\lim_{n\to\infty} na_n = 1$.
11. (B4, 1995) Express
$$(2207 - 1/(2207 - 1/(2207 - 1/(2207 - ...))))^{1/8}$$
in the form $(a + b\sqrt{c})/d$, where a, b, c, d are integers.
12. (B3, 1980) Define a_n by $a_0 = \alpha$, $a_{n+1} = 2a_n - n^2$. For which α are all a_n positive?
13. (A3, 1979) a_n are defined by $a_1 = \alpha$, $a_2 = \beta$, $a_{n+2} = a_n a_{n+1}/(2a_n - a_{n+1})$. α, β are chosen so that $a_{n+1} \neq 2a_n$. For what α, β are infinitely many a_n integral?
14. (A1, 1994) (a_n) is a sequence of positive reals satisfying $a_n \leq a_{2n} + a_{2n+1}$ for all n. Prove that $\sum a_n$ diverges.

15. (A2, 1993) The sequence (a_n) of non-zero reals satisfies $a_n^2 - a_{n-1}a_{n+1} = 1$ for $n \geq 1$. Prove that there exists a real number a such that $a_{n+1} = aa_n - a_{n-1}$ for $n \geq 1$.
16. (A4, 1964) The sequence of integers u_n is bounded and satisfies $u_n = (u_{n-1} + u_{n-2} + u_{n-3}u_{n-4})/(u_{n-1}u_{n-2} + u_{n-3} + u_{n-4})$. Show that it is periodic for sufficiently large n.
17. (B1, 1984) Define $f(n) = 1! + 2! + ... + n!$. Find a recursive relation $f(n+2) = a(n)f(n+1) + b(n)f(n)$, where $a(x)$ and $b(x)$ are polynomials.
18. (A5, 2002) The sequence u_n is defined by $u_0 = 1$, $u_{2n} = u_n + u_{n-1}$, $u_{2n+1} = u_n$. Show that for any positive rational k we can find n such that $\frac{u_n}{u_{n+1}} = k$.
19. (A1, 1990) Let

$$T_0 = 2, T_1 = 3, T_2 = 6,$$

and for $n \geq 3$,

$$T_n = (n+4)T_{n-1} - 4nT_{n-2} + (4n-8)T_{n-3}.$$

The first few terms are

$$2, 3, 6, 14, 40, 152, 784, 5168, 40576.$$

Find, with proof, a formula for T_n of the form $T_n = A_n + B_n$, where $\{A_n\}$ and $\{B_n\}$ are well-known sequences.
20. (A2, 1993) Let $(x_n)_{n\geq 0}$ be a sequence of nonzero real numbers such that $x_n^2 - x_{n-1}x_{n+1} = 1$ for $n = 1, 2, 3, \ldots$. Prove there exists a real number a such that $x_{n+1} = ax_n - x_{n-1}$ for all $n \geq 1$.

Hints.

1. $F : [0, \infty) \to [0, \infty)$, $F(x) = \sqrt{x+2}$ is a contraction.
2. Look at odd and even terms separately.
3. $F : [0, \infty) \to [0, \infty)$, $F(x) = 1 + 1/(1+x)$. But F is not a contraction since $F'(0) = -1$. Show that $F \circ F$ is a contraction.
4. This is about iteration of 2×2 matrices with complex eigenvalues. The second part takes place in the 2-dimensional vector space over the field $\mathbb{F}_7$ with 7 elements.
5. Induction, or linear algebra as in the text. The "diagonal form" is now $t_1\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$.
6. It is convenient to replace a_n by $b_n = a_n - 1$, so the sequence b_n is obtained by repeatedly hitting the sin button on your calculators. The fixed point is $x = 0$ and the derivative there is 1. If you experiment on the computer, note how slowly the sequence converges.
7. If some $a_n \leq 1$ the Contraction Principle applies. Show that if $a_1 > 1$ then the sequence increases until some $a_n \geq 2$ and then the next term is negative.

8. Consider the interval $[0, \alpha - 1]$. The main step is to show that the function maps this interval into itself.
9. Break up the sequence into even and odd terms. The function is $F(x) = \sqrt{7 - \sqrt{7 + x}}$ but we need to find the right interval. The fixed point is $x = 2$ and some (not too big) interval around it works.
10. First show using contraction methods that $\lim a_n = 0$. The problem is about the speed of convergence. For example, if $F(1/n) < 1/(n+1)$ for all n then this will show that $a_{n+k} < 1/n$ for a suitable k. For a reverse inequality look at $1/(n + \sqrt{n})$.
11. This one is a strange mixture of analysis and number theory. Compute the limit without the exponent with contraction methods. Express it in the form $\frac{a+b\sqrt{5}}{2}$. Then take square root 3 times, looking for a number of the same form. Answer: $\frac{3+\sqrt{5}}{2}$.
12. Solve the recursion. Look for the expression $a_n = k2^n + an^2 + bn + c$.
13. Solve the recursion. It is of the form $a_n = 1/(an + b)$.
14. Find disjoint groups each of which is $> \epsilon > 0$.
15. Define $b_n = (a_n + a_{n-2})/a_{n-1}$ and show that recursion implies $b_{n+1} = b_n$.
16. Pigeon-hole.
17. $f(n+2) = (n+3)f(n+1) - (n+2)f(n)$.
18. Use induction on $\max(p, q)$ to show that p/q is realized as u_n/u_{n+1} for some n.